Secure, Efficient and Privacy-aware Framework for Unstructured Peer-to-Peer Networks

A Thesis Submitted in Partial Fulfilment of the
Requirements of
Liverpool John Moores University
for the Degree of
Doctor of Philosophy

Behnam Bazli

December 2015

Abstract

Recently, the advances in Ubiquitous Computing networks and the increased computational power of network devices have led designers to create more flexible distributed network models using decentralised network management systems. Security, resilience and privacy issues within such distributed systems become more complicated while important tasks such as routing, service access and state management become increasingly challenging. Low-level protocols over ubiquitous decentralised systems, which provide autonomy to network nodes, have replaced the traditional client-server arrangements in centralised systems.

Small World networks represent a model that addresses many existing challenges within Ubiquitous Computing networks. Therefore, it is imperative to study the properties of Small World networks to help understanding, modelling and improving the performance, usability and resiliency of Ubiquitous Computing networks. Using the network infrastructure and trusted relationships in the Small World networks, this work proposes a framework to enhance security, resilience and trust within scalable Peer-to-Peer (P2P) networks. The proposed framework consists of three major components namely network-aware topology construction, anonymous global communication using community trust, and efficient search and broadcasting based on granularity and pro-active membership management.

We utilise the clustering co-efficient and conditional preferential attachment to propose a novel topology construction scheme that organises nodes into groups of trusted users to improve scalability. Network nodes communicate locally without advertising node identity at a global scale, which ensures user anonymity. The global communication is organised and facilitated by Service Centres to maintain security, privacy and integrity of member nodes. Service Centres are allocated using a novel leader election mechanism within unstructured scalable P2P networks. This allows providing fair and equitable access for existing and new nodes without having to make complex changes to the network topology. Moreover, the scale-free and clustering co-efficient characteristics of Small World networks help organising the network layout to maintain its balance in terms of the nodes distribution.

Simulation results show that the proposed framework ensures better scalability and membership management in unstructured P2P networks, and improves the performance of the search and broadcasting in terms of the average shortest path and control overhead while maintaining user anonymity and system resiliency.

List of Publications

Journal Articles

- B. Bazli, D. Llewellyn-Jones, M. Merabti, (2014) 'Privacy Observation using Resource Allocation within Scalable P2P Systems', *International Journal of Information Security.*

- B. Bazli, D. Llewellyn-Jones, M. Anil, (2014), 'Data Encryption Using Bio-Molecular Information', *International Journal on Cryptography and Information Security.*

- B. Bazli, D. Llewellyn-Jones, M. Merabti, (2013) 'Efficient Routing within Scalable Distributed Networks', *Scientific and Practical Journal of Problems of Information Society.*

Conferences

- B. Bazli, D. Llewellyn-Jones, M. Merabti, (2014). 'Privacy Concerns within Scalable P2P Systems', *Proceeding of World Symposium on Computer and Network & Information Security*, Tunisia, 2014.

- B. Alselwi, B. Bazli, B. Askwith, M. Merabti, (2014). 'Wireless Security using DNA Inspired Networks', *15th Symposium on the Convergence of Telecommunications, Networking and Broadcasting PGNET*, Liverpool, UK.

- B. Bazli, D. Llewellyn-Jones, M. Merabti, (2014). 'Data Encryption in Communication Using DNA Sequences', *15th Symposium on the Convergence of Telecommunications, Networking and Broadcasting PGNET*, Liverpool, UK.

- B. Bazli, D. Llewellyn-Jones, M. Merabti, (2011), 'Using Network Infrastructure to enhance Security and Trust within Ubiquitous Computing Networks', *13th Symposium on the Convergence of Telecommunications, Networking and Broadcasting PGNET,* Liverpool, UK.

Table of Contents

Table of Figures

List of Tables

List of Abbreviations

ALM	Application Layer Multicast
AP	Access Point
CC	Clustering co-efficient
CI	Confidence Interval
DDoS	Distributed Denial of Service
DHT	Distributed Hash Table
GSM	Global System for Mobile communications
ID	Identification Number
IEEE	Institution of Electrical and Electronics Engineers
IETF	Internet engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
KBR	Key Based Routing
LAN	Local Area Network
Mb	Mega Byte
MSC	Mobile Switching Centre
NT	Naming Table
OBA	Online Behavioural Advertising
P2P	Peer to Peer
PDA	Personal Digital Assistant
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RF	Radio Frequency
RFID	Radio Frequency Identification
RPC	Remote Procedure Call
SC	Service Centre
TCP	Transmission Control Protocol
TTL	Time to Live
UDP	User Datagram Protocol
UML	Unified Modelling Language
UMTS	Universal Mobile Telecommunication System
URL	Universal Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VoIP	Voice over IP
WAN	Wireless Area Network
WWW	World Wide Web

List of Symbols

$\bar{x}$	Mean value
MC	Maximum capacity in a group
C	Response Message
cc	Clustering co-efficient
ci	Confidence Interval
cMessage	Challenge Message
destID	Destination ID
Enc	Encrypted Type of the Value
G	Group
k	Degree of a Node
L	proportion of the links within a group
N	number of nodes in a group
n	global number of nodes
Nk	Number of nodes with degree k
nodeID	Node Identification
PK	Public Key
S	Samples
SC1	Service Centre 1
SC2	Service Centre 2
Sk	Private Key
Y	number of hops, path length in a communication
Z	Level of Confidence Margin of Error
ε	Margin of Error
σ	Standard Deviation

1. Introduction

The interconnection of autonomous computers and isolated communication networks form distributed networks that enable new services and applications. Despite the typical centralised computer networks, a distributed network operates more efficiently and effectively over a mix of workstations, LAN servers, wireless networks, regional, Web and other servers. Indeed, this brings in new security challenges.

Secure communication and confidentiality, tolerance to failure, ensuring availability and integrity of resources, and also prevention of and response to intrusion are the main security concerns in a distributed network. Most networks are secured by firewalls, which apply packet filtering between the internal and the external network (Hampton, 1999). The security measures are complex because of the network architecture and spread of nodes, mobility and locality within the network. The security mechanism should consider cost, time and space as well as confidentiality, integrity and availability of resources.

Since the properties of a distributed network fit within other real networks, humans and communication networks, scientists and researchers and even psychologists have brought many concepts and proposals to the field. These have all been used to model the characteristics of the nodes and entities within the network to predict future behaviours. Several studies have actively examined the properties of the distributed networks, resilience to random and targeted attacks and how the whole network and individual node would be affected by the attacks (Ying Li *et al.*, 2010; Cohen, *et al.*, 2003; Hayes, 2000; Hayrynen, 2005; and Albert *et al.*, 2000).

Developments in Ubiquitous Computing and Internet of Things (IoT) are expected to introduce interactive, interconnected and configurable living spaces as an integral part of future computing environments. Such a user-oriented environment will require a secure network infrastructure to ensure integrity, interoperability, privacy, fault tolerance and simple development and execution of applications. Various solutions have been proposed for Ubiquitous Computing environments to secure the network infrastructure, enable integrity, privacy and reliability as part of the service access interfaces and the implementations provided. Such solutions have only been addressed and implemented within small networks with limited functionalities and services. Little attention has been given to the scalability and privacy in these solutions. Expanding the network

infrastructure would ordinarily require the architecture to support new entities through extensive reprogramming to accommodate the changes in the network size.

Studies have shown that Small World, Scale-free networks and ubiquitous networks share similar characteristics and behaviour. Networks that exhibit Small World behaviour achieve better security (Kak, 2011), have more effective communication schemes (Al-Muhtadi *et al*., 2004) and improved performance (Zhang & Goel, 2004). Thus, it is imperative to study the properties of Small World, ubiquitous and Scale-free networks. This will help us to model real networks, scientific networks and human-centred or computer networks. This also contributes to our understanding of these systems and helps to improve their properties including performance, security and usability. These networks have recently received more attention and research effort from academia with interesting achievements and advances.

This research aims at using Small World infrastructure to allocate network resources and organise the network layout to maintain balance by rebinding to equivalent security services at specific locations within the network as the size of the network changes. This work utilises Small World network infrastructure and properties to propose a framework that first coordinates the components in large-scale networks efficiently. Secondly, using novel allocation and state management techniques, it allocates Service Centres within a scalable distributed and ubiquitous system to provide fair and equitable access for existing and new nodes without complex changes to the network topology, policy or procedures. Thirdly, it contributes to efficient communication and addresses privacy and security concerns within the Ubiquitous Computing paradigm.

1.1. Distributed Networks

A distributed network is a type of computer network that is spread over different networks or a wide geographical space. This provides a single data communication channel within a network, as well as distributing processors, resources and assets creating autonomous, collaborative and robust computational capabilities across a range of small computing devices. This introduces new security challenges and the need for an appropriate defence system.

Distributed networks are part of distributed sensor networks with a fast evolving technology for gathering information from natural and social environments as well as for collaborating with other devices. All nodes within distributed networks communicate by passing messages between them. Most networks are secured by firewalls which apply packet filtering between the internal

and external network (Vogt, 2005). Within distributed networks the spread, mobility and locality of nodes, and the architecture of the network, make the security measures complex. The security mechanisms should consider cost, time and space as well as privacy, confidentiality, integrity and availability of resources.

The current work in the literature demonstrates that a number of researchers have actively studied the properties of distributed networks and their resilience to random and targeted failures (Hampton, 1999; Watts & Strogatz, 1998; Morens *et al.*, 2006; and Dyke *et al*., 2003). It has considered how both the whole network and individual nodes will be affected by such failures. The scale and complexity of newly introduced systems makes conventional security approaches hard to implement due to the number of nodes, dynamic membership changes and the lack of central control.

The popularity, efficiency and effectiveness of distributed networks lead to new services and revolutionary advances in technology. We are now living in a society where personal devices, computers and appliances are connected together with constant and uninterrupted interaction. Combined with the Internet and emerging technologies, we find ourselves within an environment full of devices connected to each other, processing information and transferring data constantly.

Ubiquitous Computing is a communication paradigm in which technology becomes virtually invisible in our lives. Instead of having a desktop or laptop machine, the technology we use will be embedded in our environment. There has been an emergence of cheap and widely available technologies that are embedded in everyday objects around us and which interact with one another using wireless technology. This phenomenon has come to be known as the Internet of Things (IoT).

"*We are still living in a world where information is trapped in a few of our objects. We stare into our screens, which are like goldfish bowls full of information swimming around, but unable to escape. The dream is, a world where information would be a butterfly, flitting freely all over the place, and occasionally landing on any of the objects we touch to give them life and enrich them*" (Haladjian, 2006).

Haladjian states that the ambition is not only to digitise all devices and objects around us but also to connect them together. Waves of technological changes have deeply altered our way of living and the place of technology within it. It is therefore essential to study the social and ethical

impact of ubiquitous computing as well the security and privacy of users and availability of services and consider them when developing ubiquitous systems.

As ubiquitous computing and IoT mature, the most important issues separate from simple technological problems to become social and security issues. Researchers focus on uninterrupted communication between users and devices. We will soon be able to include computer hardware into virtually every manufactured product and provide a wireless infrastructure to let those devices communicate directly or indirectly.

From a practical point of view, the world of networking is facing rapid changes with innovations and efficiency in communications, wireless connections and network evolution. However, privacy is the least concern with those technological advances, which rather focus on interoperability of systems. From technological complications to lack of rules and regulations to cover every aspect of ubiquitous systems, privacy advocates are facing tremendous challenges in this matter where many believe that privacy is fading away in the digital age. Ubiquitous computing systems and flows of information and Internet communication have now created a gold mine for marketing companies. Nonetheless, the choice between privacy and security on one hand and the efficiency and interoperability on the other hand is often a trade-off.

1.2. Small World Networks

The Small World network phenomenon was first introduced in 1967 when Milgram tried to show that the average path length between two people, even when those people have only a few acquaintances, is only six steps (Milgram, 1967). Known as the "six degrees of separation" rule, this suggests that everybody in the world is connected to everybody else either directly or using a chain of intermediary people containing at most six people.

Milgram asked random people in Omaha, Nebraska to send letters to specific individuals – called 'targets' that were not known to the senders (Kleinfeld, 1967). Senders or originators had basic information about target recipients. It was anticipated that, the senders knew a friend who could most likely forward the letter to the destination target. Milgram then examined the mail routes that successfully reached their destinations. He discovered that the average chain each letter took to reach its target recipient had a length of six hops. Although only 15% of packages made it to the destination, it created an explosion of interest by social scientists, mathematicians

and neuroscientists. The excitement still remains and confirms what people believe naturally; that “It’s a Small World” is a valid claim.

When Milgram attempted to achieve what then has been determined as the *six-degrees of separation*, he suggested that participants relied on clues to direct the package to a presumed target or acquaintance (Milgram, 1967). The one-dimensional clue was the possibility of knowing the next intermediary chain. The characteristics of Small World networks within this experiment mean that the extension of the chain of acquaintances grows exponentially. In other words, within Small World networks, the diameter is smaller than the size (Kleinberg, 2000). Given the flooding type search algorithm in Milgram’s experiment, the lookup has only one dimension in the exponentially distributed network as shown in Figure 1.1.

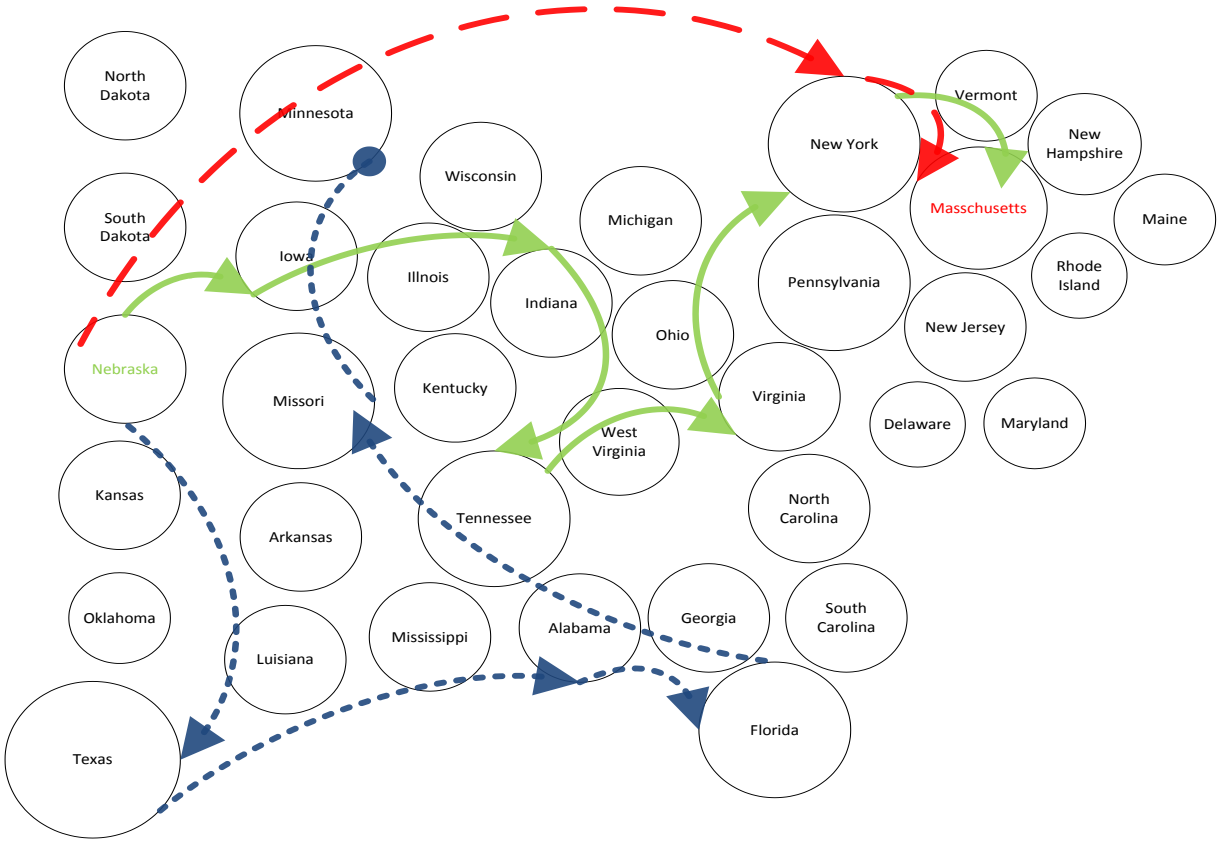

Figure 1.1 Three Possible Routes in the Milgram's Small World Experience

The possibility of the package arriving at its destination could take *log N* steps where *N* is the number of acquaintances within the chain of acquaintances. In this work, we use the terms neighbors and acquaintances interchangeably. The calculated shortest chain of acquaintances was later labelled as the degree of separation. This can be interpreted as average shortest path in computer networks. Given the underlying unstructured property of such an arrangement, the

lookup method used can in ubiquitous computer networks, particularly within community trust (Llewellyn-Jones *et al.*, 2009).

Within community trust, the communication between one node and every other node is peered and therefore much more secure than any other approach (Li *et al*., 2010 and Chung, 2012). We use such a scheme to model the Ubiquitous Computing networks. We use Power-Law distribution of nodes within unstructured P2P networks can help maintain network balance (Jacob & Orters, 2012) and model network growth (Fotouhi & Rabbat, 2013). Furthermore, the alternative path shown as dotted line in Figure 1.1 can be considered as a query in a Small World network if the network resource or initial route is not available. This will maintain the shortest path as well as minimal hops increasing network efficiency and avoiding redundancy.

In a small world network, a message is directed from one to other using acquaintances until it reaches the destination. If there is clue, an identifier in this case, the message is forwarded to the corresponding node or the one closer to it. It is important to use the clues to discover the shortest path. Using information about neighbouring nodes has already been used for state management (Rowstron & Druschel, 2001) and subsequently efficient routing (Gupta *et al*., 2003). Given the common interests within a community trust, finding the clue can be straightforward. In Milgram's experience, a package arrived at the destination with only one intermediate chain. However, many of the packages arrived using eight or more chains. Considering the initial instruction that the packages should be directed to people who are known to senders by first name, it is understandable that some packages may take a longer route than anticipated. Given the circumstances, one can conclude that, although that was a wonderful attempt, the outcome of the experiment and the plan has been determined with absolute uncertainty. In the experiment, the states are not only represented with great distance geographically, but the distribution represents social disparity as well (Barabási, 2003).

In Milgram's experiment, only 15% of the packages that are sent from the experiment base arrived at the destination in Massachusetts. Most of the packages did not arrive at the destination because of broken links. In Figure 1.1, the package starting from Nebraska got stuck in Minnesota because, most likely, the recipient in Minnesota did not know anyone to direct the package to. Although the diagram shows that, the effort stopped after five attempts – the dotted route – there have been many instances recorded of higher numbers of attempts before reaching a dead end. Based on the instructions of the experience, the last recipient did not have any desire or information to re-direct the package to a possible target recipient or acquaintance. This is

very similar to flooding-type routing with blind search, which has been used in many P2P systems, which have been proved relatively inefficient, especially as the network scales (Ritter, 2001).

There have been instances where the package arrived at the destination by only one chain of acquaintances as shown – red dashed line – in Figure 1.1. The accuracy of this case relies on the pre-existing adequate information about the next acquaintance. However, the desire to participate and the level of interaction and previous relationship of the entities have a direct influence in the successful and effective completion of the task. Such an approach has been adapted by Kleinberg (Kleinberg, 2000), as illustrated in Figure 1.2. Using local information not only maintains the integrity, but improves efficiency and successful navigation within a Small World network environment.

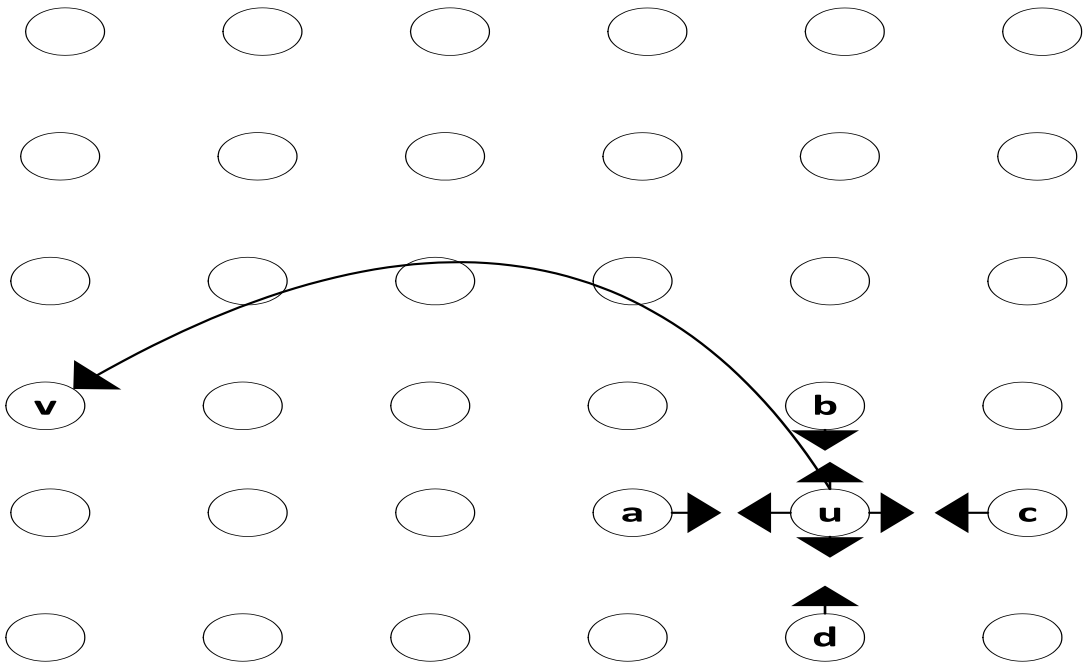

Figure 1.2 Navigation Using Local Information within Clustering Exponent

To determine a more realistic approach in dealing with navigation within a scale-free network, the third route is more appealing than other methods. It shows a reflection of the shortest path within the experiment. If the experiment was set with some conditions such as distance limitation, target direction, or provided with a different instruction to move through an alternative route, then the success rate would have been much higher, considering the 15% churn. However, such an approach opened an insight to navigation in other types of networks

and inspired later discoveries but nonetheless presents an inefficient approach to network communication and navigation.

Watts & Strogatz however, discovered that there are a few random long range connections existing within the networks that follow the 'small-world' paradigm (Watts & Strogatz, 1998). In Kleinberg's model, routing is carried out by using another dimension – delivery time T – restricting the routing to be performed within a local cluster (Kleinberg, 2000). By doing so, the probability of a connection between two nodes is determined as a function of their lattice distance. This contributes to global knowledge of connections within the network and facilitating discovery of the shortest path. Using this algorithm, it takes $(log\ N)^2$ steps to arrive at the destination point where N is the size of the network. Figure 1.2 is revised version of the Kleinberg's navigation model in Small World network using local information within clustered environment.

The communication from node u is facilitated using navigational information from the neighbouring nodes. This method eliminates the possibility of flooding search, which may lead to exhaustive or failed lookups. Calculating and finding the shortest path is an expensive process. As stated earlier, Milgram's experience relied on one dimensional probability to navigate through the chains. However, Kleinberg states that finding short chains in Small World networks is easier than others, since local information is used to navigate through the network. Therefore, within small diameter and highly clustered networks such as the Small World networks modelled by Watts and Strogatz (1998), the shortest path can be captured by connecting two vertices. This technique has been used in the Chord system (Stoica *et al.*, 2001) with some variation to facilitate scalable key allocation and managing membership changes.

1.3. Motivation

The privacy concern that is addressed within this project is based on the hypotheses that individuals should be able to manage their own privacy based on trust and level of involvement. The trust based communication model is better suited in privacy-aware P2P systems. Llewellyn-Jones *et al*. (Llewellyn-Jones *et al.*, 2009) suggest that community trust can be implemented within a group of users to improve and manage reputation. The earned reputation is then applied to other members within a data sharing architecture preventing illegitimate decisions by members. By earning the reputation, individuals gain trust and move between groups considering their own interests and privacy concerns.

While dealing with privacy in Ubiquitous Computing, different entities have different interests and there have been many heated debates to push for legal recognition and respect for the benefits of the entity (Dwyer *et al*., 2007). On the other hand, people with the intention of online file sharing, Freedom of Information and free expression push for complete privacy rights and personal data protection. As mentioned later in Section 2.4.3, almost everyone who uses the Internet faces privacy risks that come from marketers and advertisers with powerful web features and capabilities that facilitate Web browsing on smart phones and digital devices. A Californian programmer, Samy Kamkar has created a cookie called *Evercookie* that is not easily deleted, even by Web experts. In creating the *Evercookie* he was curious about how advertisers tracked him on the Internet and drew attention to violation of privacy within the Web (Vega, 2010). Samy states that, *"I think it ['] s O.K. for them to say we want to provide [a]better service, however, I should also be able to opt out because it is my computer"*.

While those additional capabilities and developments enthuse many users, there are serious privacy concerns around tracking user's activities and capturing personal information such as location, shopping cart contents, emails, Web history and even photos (Vega, 2010). Moreover, users may also suffer privacy breaches resulting from loopholes within smart phones, and social engineering attacks that may cause user accounts and devices to be compromised and personal information to leak into the hands of unauthorised users (McCallion, 2014).

Trust has been dealt with as a key element for security within Ubiquitous Computing (Wellman, 1999). However, can you build a robust security mechanism that is only based on trust? Is the 'trust' trustworthy when it comes to information security? Implementation of a trustworthy system based on trust with the minimum human role is the ideal approach for ubiquitous system security. However, research has shown that, without involvement of central authority or relying on existing nodes, it is practically impossible to present a personalised distinct identity in a distributed computing environment (Douceur, 2002). When distinct identities of remote nodes cannot be verified, the system might be vulnerable to a Sybil attack (Douceur, 2002). Most P2P systems have subscription free access for personal users and therefore they do not control memberships. Access control is normally managed by user names and passwords created by users. The lack of strong identity management may lead to system vulnerabilities and attacks such as Sybil attacks (Douceur, 2002). This can occur when, within a large-scale P2P system, an entity with a single faulty member presents multiple identities undermining redundancy. Douceur argues that without logical centralised access control, Sybil attacks are always possible. However, the author acknowledges that such attacks can be prevented under some conditions

such as resource uniformity and systematic coordination among members. Large-scale distributed ubiquitous systems are heterogeneous, therefore providing a uniform topology and node degree distribution with equal resource access to all entities is required to achieve such a condition is very difficult.

For instance, Pastry is a structured P2P system that provides locality using information about neighbouring nodes. The information includes the *node Id* and *IP address* of the nodes that are physically closest to the node. Pastry uses proximity to determine the physical location of neighbouring nodes. The naming techniques and routing method used in Pastry are similar to that of a Distributed Hash Table (DHT); it therefore shares the same limitations such as inefficiency of depth search (Kak, 2011). Therefore, the naming policy in Pastry may introduce vulnerabilities such as the potential for Sybil attacks (Douceur, 2002). The node state needs to be updated within the routing table, however Pastry has no mechanism for updating such information, especially for failed nodes. This leads to redundancy and subsequently bandwidth cost when lookups for a failed node returns without success. The author proposes direct identity validation using coordination and information about other entities to vouch for new entities.

In a decentralised and distributed system such as Gnutella, a node should know at least one existing node to join the network (Portman *et al.*, 2001). Gnutella was the first conventional overlay network to have pervasive use. Each user maintains connections to others and communication through trusted relationships. Gnutella is designed as a content sharing and file-sharing platform with no anonymity in mind, and the design structure and network topology and routing protocol were not intended to do so. The intention was to form a community of users to share files and resources over the Internet. The Gnutella network is dominated by a few users with high speed internet access, activity and content who share content and actively respond to queries but use most of the network traffic (Sen and Wang, 2004). If a node wants to join to the Gnutella network, it should know at least another node within the network. Although this was an innovative system when developed with great intentions in mind, this model of network management has significant privacy and other infrastructural issues, some still unchanged after several overhauls.

Although freedom of expression, flow and exchange of personal information on social media are often claimed to have created an open-data environment – increasing the popularity of P2P systems – these trends do introduce serious consequences, especially in terms of privacy. A comprehensive survey of P2P overlay networks compares various attributes and creates an

algorithm taxonomy of those systems to illustrate the different elements and metrics (Lua *et al.*, 2005). This provides a comprehensive list, which covers concepts from architecture, look up techniques, routing and performance to resilience and security. Apart from Freenet, none of the solutions have considered privacy and protection of user identity while preserving freedom of information and promoting the free flow of information. Most of the attention has concentrated on efficient routing algorithms, flexible naming and discovery schemes and performance. On the other hand, Freenet is a P2P system that has been designed with anonymity in mind. However, the design and infrastructure of the network has suffered serious flaws. In Freenet, the communications between nodes are encrypted and routed through other nodes to make it extremely difficult to determine its originator as well as content (Clarke *et al.*, 1999). Peers on the network participate in managing queries, data storage and retrieval of data items. The data distributed within Freenet are identified by keys. A request for a key is passed along peers using a flooding algorithm, which returns the corresponding data. These keys are location-independent.

The notion of '*the wisdom of the crowd*' suggests that large groups of people are smarter than a smart or elite few, no matter how brilliant the few are at solving problems or making wise decisions (Surowiecki, 2004). In 1906, Francis Galton observed a weight-judging contest in Surrey to guess the weight of an ox on display after being slaughtered. There were over 800 guesses from the diverse group of people who entered. He wanted to prove that the average value of the voters' guesses was very close to the actual weight. He collected all the raffle tickets and the average came to total of 1197 pounds, just one-pound difference comparing to the actual weight after the ox was slaughtered. Galton observed that this was more accurate than those of alleged cattle experts' predictions.

However, this method is ill-suited for many applications. If there are many wireless access points in a town centre, a particular access point can be overloaded through the application of '*the wisdom of the crowd*'. The implication of the notion on car GPS systems where an alternative route is offered using live traffic information on roads may lead commuters to divert their way through quiet roads to overcome traffic at peak times. Therefore, the decision made by the crowd can be influenced by many factors. Global recession, inflation and many financial and statistical flaws demonstrate that collective information should not be relied on as an accurate judgment. A study carried out by Joseph Simmons of the Yale School of Management in New Haven, Connecticut found that group predictions about American football results were

far from the real results, because of the influence of fans over-confidence in their decision (Ball, 2014).

The diverse examples above however are not intended to cement the reliability or unreliability of crowd judgment. Instead, it explores the reasons and influences that make crowd judgment biased, inaccurate and sometimes damaging. Governments' decisions on limiting freedom on the Internet or freedom of expression and flow of information are fine examples of this kind. Surowiecki stated that one requirement for a good crowd judgment is that the peoples' decisions are independent of one another (Surowiecki, 2004). Within a dictatorship, The Wisdom of Crowd is biased by the enforced views of the dictator. Therefore, the main requirement of '*the wisdom of the crowd'* is mistreated by adaptation of a biased decision, which would serve the interests of individuals rather than a group. To this extent, promotion of security may accomplish some predefined objectives within those settings, but the privacy of the users will be violated with different justifications. The revelations by whistle blowers on global surveillance have set off within online communities and activists (Access, 2014).

In this work, the heart of the privacy concerns within ubiquitous systems is based on the concept that individuals should be able to manage their own privacy settings based on trust and level of involvement. This theory is able to fit well within a dynamic, interactive environment where distribution of the services demands autonomous decisions. Therefore, it is imperative that ubiquitous system design and development should move to user-oriented design even within the service-oriented environment to distribute privacy context and maintain an individual's privacy. Such requirements are crucial in social settings such as where a user is subject to an oppressive government, where the user identity, data context and interaction history may pose a considerable risk to welfare. In particular, mobile devices operating within a cloud service require privacy policies in a cooperative manner to operate within a dynamic environment, preserving users' privacy.

By exploring the current privacy capabilities of P2P and ubiquitous systems, this work develops a user-centred privacy policy based on trusted relationship of those clustered communities.

1.4. Objectives

1.4.1. Network-aware Topology Construction

The distributed ubiquitous system has a dynamic structure where access control, resource allocation and efficient communication are all required for effective traffic, routing and control. Implementing multiple tasks within such a decentralised and highly clustered network, while preserving privacy and security, is very challenging task considering the dynamic and rapid membership change.

This work uses the power-law distribution and clustering co-efficient properties of Small World networks and other modelling capabilities such as conditional preferential attachment to introduce a novel network-aware topology construction approach for an unstructured P2P system. A high degree node called a 'Service Centre' with the highest processing power and memory is nominated to administer bootstrapping and facilitate membership management. Service Centres create groups of trusted users and administer important tasks to provide fair and equitable access for existing and new members without complex changes to the network topology, policy or procedures. Creating new Service Centres where the network is expanding to serve newly joined nodes ensures the accessibility, availability and granularity of the network without needing new sets of policies and resources. Moreover, the design presented will ensure that existing storage and memory will be sufficient and available to overcome the requirements of a scalable network.

Connecting new nodes and expansion of the network introduces new challenges to the scalable network services. The proposed framework keeps the preferential attachment characteristic under control by using a novel topology construction algorithm, so the system does not end up forming a random network. We propose an algorithm to limit the number of nodes attached to each Service Centre. This ensures a structured and orderly arrangement of nodes so the network keeps the existing balance to provide services and resources to all members. If the number of nodes linking to a Service Centre exceeds the predefined limit, then the Service Centre is split in two, increasing the capacity for linking new nodes. In this way the power-law distribution of the network and the network scalability are unaffected.

1.4.2. Secure Communication

Communication over large area networks can be complex. The shortest path and direct communication have been tested as an efficient and secure communication method and employed by Ying Li *et al.* (2010). Keeping the path length to the minimum will provide a trusted and direct relationship between every pair of nodes even where long range links are

concerned. The average short paths also improve the granularity of the network. The number of nodes connected to each hub and their geographical distance using location sensing and allocation algorithm improves efficiency.

The proposed method will simplify communication methods, by using a peered approach and encrypted messages administered by the Service Centre to maintain simple and secure communication over a long range. This is the main research element within this framework to maintain integrity and confidentiality.

1.4.3. Privacy Preservation

While the rapid growth of ubiquitous services, digital communications and file sharing systems is generally encouraging for users, it does introduce security and privacy issues as well as ethical and legal concerns. Freedom of expression, free flow of personal information in ubiquitous systems is often claimed to have created an open-data environment. However, these trends introduce serious consequences especially in terms of privacy. Anonymity can provide a level of privacy for users within a communication system. Because of the topology, dynamicity and design of ubiquitous environments and P2P systems, privacy has not generally been considered as a major concern in many existing systems.

Anonymity is the property that maintains privacy, which in turn should be addressed at the routing level since exchanging and/or transferring information is involved. Nonetheless, privacy measures must be applied carefully to minimise the impact on users and the system while at the same time maximise the efficiency and fair resource access in the network. In order to accomplish this task, we study a popular P2P overlay structure with the aim of enhancing the efficiency and effectiveness of the network, which also addresses privacy concerns. The privacy of the nodes and agents is maintained in this way because of reputation and trusted relationships (Faloutsos *et al.*, 1999; Soldatos *et al*., 2007; and Jakubowski *et al.*, 2010).

1.5. Approach

We analysed and investigated current approaches and different solutions for unstructured P2P systems, and discovered that most of the current tools and topologies do not support scalability. Those, which do support network scalability, neglect user privacy and system resiliency. This work aims to address and tackle different aspects of ubiquitous P2P overlays such as scalability, efficiency, security and privacy.

A qualitative approach (Gomm *et al*., 2000 and Schofield, 2002) has been used to reach overall aims and objectives of the project in terms of user privacy. It has been characterised to provide deeper understanding of the privacy to develop a research strategy that enabled exploring different case studies and observing use privacy within different P2P systems. In order to evaluate the privacy and security concerns within those systems, analysis of the roles, processes and entities involved is demonstrated to critically appraise the privacy implications.

Triangulation is a strategy that can be used to strengthen the confidence of research findings (Arksey and Knight) and to increase the probability of generalising the research findings from different methods (Decrop, 1990). We have used theoretical triangulation where we approached the research with varied prospective, considering different hypothesis.

We followed deductive and triangulation approach in order to achieve the design rationale and objectives defined later in Section 1.4. In the deductive approach, the researcher develops hypotheses and designs a research strategy to test the formulated theory (Saunders *et al*., 2003). In an inductive approach –also known as building a hypothesis – the researcher starts with collecting data in an attempt to develop a theory (Saunders *et al*., 2003). The reason for choosing the deductive approach over the inductive approach in this work is that, implementing the design rationale and achieving the research objectives fit well within a deductive approach. The process of achieving a Small World inspired network structure to enhance the trust and security within ubiquitous systems is divided into the following stages: literature review and study of the current developments in P2P overlay systems, design of rationale specifications of privacy-aware end-to-end communications, and implementation of the design rationale and performance evaluation. This approach makes the process simple and easy to understand. Furthermore, due to the rigidity of the model, we define the requirements and deliverables of each phase to be reviewed and completed before moving to the next stage.

The requirements specifications are focused on related works using different network structures and current advances in security and resiliency methods within scalable ubiquitous computing environments. The intention is to capture requirements for the proposed structure and framework with lessons learnt from ubiquitous P2P systems introduced rapidly over the past two decades. This includes investigation of different types of network, their properties, structures and behaviours under different circumstances to define a requirements specification for a novel solution. The requirements specification phase uses all available parameters and system constraints to address the availability and confidentiality of the services within the

ubiquitous system. These parameters are identified independent of the technology of the system and utilised for the requirements of the proposed framework. To serve this purpose well, different security, privacy and scalability parameters incorporating with current tools, technology and prototypes are identified to propose a development plan within an innovative framework.

For the implementation phase, we have developed a typical Small World network and Ubiquitous Computing network consisting of several nodes arranged in a decentralised manner using OverSim (Baumgart *et al.*, 2007), an open-source discrete-event simulator based on OMNET++ (Varga, 2001). The simulator is an open-source simulation framework used to model large-scale structured and unstructured P2P networks. The network simulator provides a platform to virtually present all nodes and effective communications to analyse the source and destination, and to implement the proposed algorithm within a scalable network environment.

The analysis phase follows an analytical appraisal, critical review and evaluation of current P2P overlay approaches to help design and transform the specifications captured during the requirements phase. This includes thorough analysis of unstructured P2P systems, arrangement of nodes, their roles and location information to establish a secure communication scheme and effective membership management.

The evaluation phase includes assessment of the simulation scenarios based on case studies to demonstrate the produced results and to evaluate the effectiveness of the proposed framework. The derived outcomes are then followed by an appraisal of outcomes in simulation environments and comparisons to alternative methods.

1.6. Scope

This thesis covers the following areas.

1. Introduction of distributed networks, Ubiquitous Computing and IoT scenarios.
2. Analysis of P2P communication systems, existing tools and technologies and current solutions with insertion of P2P overlay networks.
3. The need for efficiency, scalability, relative anonymity and confidentiality of the message content.
4. Trust relationships that exist between nodes within the groups, but do not necessarily exist across groups.

5. A framework to address the challenges in unstructured P2P applications with inspiration from trust models and the potential existing within Small World networks.
6. Design of the framework which addresses the scalability, security and privacy.
7. Design and implementation of novel algorithm for anonymous routing within P2P systems using trusted relationships.
8. Thorough analysis of network resiliency towards random and targeted attacks.
9. Thorough performance evaluation of the proposed framework under different scenarios, comparing to the existing best solutions.
10. Thorough analysis of privacy concerns within scalable P2P overlay networks with emphasis on the project contributions.
11. Conclusion of the analysis and outline of plan for future works.

1.7. Contributions

This work introduces a framework consisting of a novel privacy-aware and network-aware topology construction, and a novel leader selection algorithm. It uses the transparency, which is based on trusted relationships, and a privacy preserving routing and broadcasting algorithm to create balance between privacy and efficient communication. Furthermore, the modelling technique from Small World and real world network characteristics inspires the unstructured P2P network growth and the pro-active state management.

In order to ensure end-to-end routing efficiency, we modelled the network growth that maintains availability of members through reachable shortest paths and using a novel pro-active membership management is necessary. However, privacy and security issues have emerged while dealing with the distribution of network resources. Thus, we propose a novel privacy-aware routing and broadcasting algorithm with the help of a trusted and highly capable node, Service Centre, that facilitates routing and forwarding within the P2P overlay environment. We have performed a thorough analysis of the current tools and technologies and social concepts as well as appropriate guidelines and technology trends regarding user privacy and individuals' right to set a scene for critical analysis of the current ubiquitous solutions.

The efficient routing using proactive membership management and creating responsible points, i.e., Service Centres, which act like 'Rendezvous nodes' as explained by Goyal *et al.* (2009), is an important feature, which is incorporated into our proposed framework. It does not only facilitate the effective topology management within the network, but also administers important

tasks such as routing and forwarding to ensure privacy within trusted community and provide anonymity to users.

By enforcing the network to follow a power-law distribution and sustaining clustering co-efficient, the system maintains load balancing and manages membership change easily. By organising network members as clusters of trusted communities using clustering co-efficient, we provide privacy-preserved and secure end-to-end interaction between users. This will serve the network to achieve efficiency and easy development. Joining a group of hubs with associated nodes will form a network with a power-law distribution and maintains the balance of the network. With the policies, services, resources, protocols and repositories and responsibilities assigned to highly trusted nodes, this creates 'Services Centres' that maintain network reliability, interoperability and security.

In our proposed framework, users' privacy is considered within the local clustering of nodes while secure and trusted communication paths are established between them. This is achieved using trusted relationships within the network clusters to serve anonymity as well as the security of the member nodes. To the best of our knowledge, none of the proposed schemes and methodologies used for privacy concerns utilise the existing trusted relationships within the community of users.

1.8. Structure

Chapter 1: introduces the outline of the thesis and discusses recent advances in distributed systems. It explains the motivation behind the research and how the design rationale is inspired by Small Work phenomenon. The chapter defines the research methodology to achieve objectives outlined, detailed contributions, project scope and concludes with this summary of the thesis contents.

Chapter 2: provides background information, the advances and challenges of Ubiquitous Computing and its similarities to Small World networks. It then outlines the current advances and challenges facing Ubiquitous Computing. It then brings together the two concepts with different modelling techniques in mathematics, social science and information theory in order to highlight the research motivation by outlining the current issues within ubiquitous systems such as scalability, resiliency, security and privacy. The chapter creates a baseline and preface

to outline our research motivation by studying different aspects of the Small World phenomenon.

A thorough analysis of P2P network overlays as solutions for scalability within ubiquitous systems has been carried out to highlight the challenges, research constraints and needs for user-oriented design within those systems.

Chapter 3: presents the Secure, Efficient and Privacy-aware (SEP) design and outlines different aspects of the proposed solution such as topology construction, privacy-aware routing and broadcasting, trust-based leader selection algorithm and membership management. This chapter goes through the details of modelling the network growth using degree-proportionate probability technique to maintain scale-free and power-law property of the unstructured P2P overlays.

Chapter 4: defines the plan for the performance evaluation strategy based on the design rationale, implementation methodology, outlines system validation process to implement the proposed framework, and compares it to existing methodologies. Furthermore, it defines the performance metrics in order to evaluate the design rationale and project objectives. The experimental platform and different simulation settings, limitations, configurations and strategy for performance evaluation are included.

Chapter 5: presents the implementation results, performance metrics and evaluation methodology using different techniques. The simulation scenarios and results are presented using figures, tables and statostocs. We present simulation results to be compared and analysed against other unstructured P2P systems.

Chapter 6: This chapter concludes the thesis, highlighting the research outcomes and how the research approach is developed into the contributions of this work by summarising the findings, research contributions and supporting segments with emphasis on future of the ubiquitous computing and IoT development. The chapter closes by outlining the area of the research that is considered for future work.

2. Ubiquitous Computing & Small World Networks

The ubiquitous computing concept was introduced as a development of human-centred networks. A ubiquitous computing network comprises pervasive and hidden computer devices that interact with each other and humans. The paradigm of disappearing hardware – where personal computer and workstation will become practically obsolete as computing access becomes ubiquitous – is underway; in the walls, on our clothing and every object around us (Weiser, 1993). Mark Weiser, a researcher in the Computer Science Lab at Xerox Palo Alto Research Centre, was the first to put forward the notion of ubiquitous computing (Weiser. 1991) as information technology's next wave after the mainframe and PC. In this new world, which Weiser initially called "calm technology" (Weiser & Brown, 1996), technology will reside around us, interacting with users in natural ways to anticipate their needs.

"The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it" (Weiser, 1991).

2.1. Development of Ubiquitous Computing

In the past fifty years, there have been two major eras in computing: the *mainframe* and the *PC*. Today the Internet is carrying us through an era of widespread distributed computing towards the relationship of ubiquitous computing by deeply embedding computation in the world (Gellersen *et al.*, 1999). We are now in the midst of *third wave* – mobile computing. With introduction of mobile computing and ubiquitous systems, we are now heading to the *fourth wave* – IoT.

Data-centric applications such as Web search, recommendation system and sensor networks are responsible for data gathering, analysing, processing and storing information (Ranganathan, 2011). Ubiquitous Computing systems are also context-aware in the way that they detect and monitor the current context of users. The context may contain information on location, status, and medical conditions. As Haladjian (2006) suggests, the ambition is not only to digitalise every object around us but also to connect them together.

2.1.1. Challenges

The conventional centralised security mechanism is not sufficient as nodes are becoming sparser, spreading to different locations with no administrable control over them. As security in

real networks and computer networks has always been treated separately with different methodologies to deal with, the formation of ubiquitous computing will change the balance (Chen, 2004; Zheng *et al.*, 2008; and Kak, 2011). Therefore, new methods and techniques are required when it comes to security. Mathematical analysis and simulations have been used to study the characteristics and behaviours of real world and Small World networks, and we believe these can be used to help satisfy security requirements within a dynamic ubiquitous computing network environment.

Computers can make decisions based on the circumstances around them and on the context such as location, time, temperature and other attributes. It enables applications to understand the environment and its attributes to effectively interact with other entities and provide the best user experience (John Krumm, 1999). Context-aware computing is exploiting the changing environment with applications that react to those changes accordingly (Schilit, 1994). With development and production of low cost and tiny sensors with high processing power and battery life, many attributes of the environment and resource information is captured for computation and processing. The attributes and the information are widespread such as temperature, time, size, location, state which all interact with various systems and applications.

The influence of data explosion may offer a unique opportunity for advertisers and marketing organisations, at the same time it requires new system architecture to include key design challenges such as scalability, security, privacy and trust.

2.1.1.1. Scalability

Scalability is the characteristic of a system that enables a network, process, service or infrastructure to grow in a capable manner, accommodating new services and resources as well as users (Bondi, 2000). Scalability is a significant issue in electronic systems, databases and networking as performance can be affected by system growth. Therefore, the base concept of scalability is consistency (Laudon *et al.*, 2008). For instance, if accessing a user record in an *n* member database system takes *t* seconds, after adding additional records, the system performance should not decline, or at least decline in a manageable way (e.g. linearly).

Scalability brings new challenges such as organisation of nodes, state management, resource allocation and efficient routing and communication. Measuring system effects and relationships before scalability has been the focus of many researchers (Number, Associated, & Files, 2011; Masticola *et al.*, 2005; Duboc *et al.*, 2006; and He *et al.*, 2008). However, planning for evaluation of scalability using a sequence diagram of different experimentation of scenarios as

well as simulation of abstraction of system performance can contribute to validation before the design phase.

When a Ubiquitous Computing network becomes scalable, it turns into an unstructured and decentralised network with diverse users and dynamic topology (Baeza-yates & Cambazoglu, 2014). Application developers need to improve the scalability of algorithms to accommodate large numbers of participating entities and to allow running of multiple applications and processors with large numbers of data sets (Yalagandula & Dahlin, 2004).

Scalability heavily relies on predictions and assumptions to identify system bottlenecks and outline strategies to mitigate them in order to prevent failures. In achieving scalability, system designers face the common dilemma of having to trade-off capabilities. Availability, usability, cost and interoperability are the some of the attributes that are considered when designing for scalability.

By their nature, ubiquitous environments encompass large areas, distributed systems and applications, all to cooperate and serve users' purposes (Hightower & Borriello, 2001). This may also extend beyond the prototypes to even a larger scale to make the service management much more complicated. One thing is certain: that we need to know and record the location of each node and application within the environment. The system should locate people, nodes, equipment and applications. Many researchers have been working on automatic location sensing by addressing location determination, location-awareness, infrastructure versus mobility and resolution in time and space (Han *et al.*, 2004; Shi *et al.*, 2002; and Al Muhtadi *et al.*, 2005). Since location technologies generally introduce a trade-off between accuracy and cost, the application of the feature depends on the particular requirements of the application (Schilit *et al.*, 1999). Furthermore, they introduce privacy concerns (Varshavsky & Patel, 2010).

Researchers have attempted to capture the essence of scalability by identifying the effects and relationships that characterise scalability (Duboc *et al.*, 2006; and He *et al.*, 2008). The main approach has been defined as a conceptual development model. This includes expression of variables, gathering data and then, analysing the effect of scalability to the system. The lack of a generic and global solution for scalability and growth within ubiquitous computing is evident within all available ubiquitous environment solutions (Perkins & Huang, 2008).

2.1.1.2. Security

Pfleeger & Pfleeger (2006) have highlighted three important aspects of security, namely: availability, integrity and confidentiality. To define the availability aspect of a system, it is important to describe the goals and objectives of a network. Reliability of a network maintains system functionality, tolerates faults and fulfils the expectations. In addition, network resources should stay available in the time of maintenance or disaster recovery. This can be tested with observation of quantitative expression or qualitative failure of an operation (O'Connor, 2011). The emergence of the digital era and integration of computerised systems and microprocessors within every engineering product that provides public utility, medical emergency and safety requires a design with reliability and fault tolerance. Increased emphasis should be placed on improving quality, reliability and durability of such devices. Furthermore, the performance of such components should be tested with elements such as capability to satisfy functional requirements, efficiency to realise objectives and effectiveness to analyse requirements (Modarres *et al.*, 1999).

System validation and verification represent integrity, which include state consistency, interoperability, accuracy and usability of a system. Data integrity is maintaining consistency and ensuring accuracy of data over its life cycle (Boritz, 2005). With the context-aware aspect of ubiquitous systems in mind, data integrity will play an important role in system integrity and security. Well-defined data integrity reduces redundancy and increases performance stability, application re-usability and system administration (Zhang *et al.*, 2014).

With the emergence of data explosion and IoT, security becomes a requirement for individuals as well as businesses. The amount of reasonable protection of an asset depends on the importance and value of that asset, which in turn corresponds with the possibility of an attack (Stajano, 1992). The manifesto of ubiquitous computing however changes the traditionally considered system security where computers are becoming smaller, cheaper and embedded in everything and everywhere.

2.1.1.3. Privacy

Privacy is the term referring to a state, in which one's life or affairs can be free from intrusion or interference. In information technology privacy is the relationship between technologies and legal or ethical rights or public expectations to collect or share sensitive information. The boundary or context of privacy differs among individuals, organisations and cultures.

The human rights legislation dating back to the 1948 United Nations Universal Declaration of Human Rights: Article 12; *"No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks"* (Harris et al., 2009).

Freedom of expression and flows of personal information in social media and digital media is creating an open life style for users. However, these trends sometimes cause consequences, which then trigger government action, can feed a news column for a journalist or concern by employer or relative for undesirable impacts of the expression. An 18 years old girl was fired from her office job because she posted on Facebook that "I am totally bored" (Rosen, 2010). There have been many instances such as this one where, users have been supressed because of their uploaded private information, ideas and comments on social media and online forums. Due to the massive amount of information we share or store online, the notion of privacy is fading away in the online world. The common perception is that everybody should think twice before putting sensitive information online.

One of the oldest pieces of legislation to protect personal information against US Federal Agencies to control over collection, storage and maintenance was the Privacy Act of 1974. The Privacy Act prohibits the disclosure of personal information. The Privacy Act applies only to records that are stored in a database or system of records, from which information is retrieved by the name of an individual or document identifier (Privacy Act, 1974). The right to access records about oneself and amendment of the records, set out in the Privacy Act is also formally expressed in the Freedom of Information Act. This provides a guideline to individuals on how to access the information stored by government agencies.

One of the major concerns about privacy within a ubiquitous system is the lack of one single privacy law across the borders. The Internet and online communications know no limit and go beyond the geopolitical borders. However, legislation by a group of countries is often ignored by other countries. For example, many countries have not signed or legalised copyright or other internationally recognised regulations such as privacy.

Not all the privacy violations are for bad intentions. Online tracking might deliver advertisements or services that we might actually appreciate. Advertisers, marketing companies and sales representatives use the contact information to promote their services and advertise their products. You might benefit from a cold caller asking you to switch your energy provider

to a cheaper alternative. However, the number of unwanted mails, electronic mails, text messages and other correspondence we receive, and the amount of information held about us by various public and private organisations, require fair and lawful storage, processing and use of sensitive information. While technology introduces many tools, techniques and innovations that maintain privacy and anonymity, advertisers find new ways of collecting personal data. With the emergence of electronic and digital media, we voluntarily upload our personal information, hobbies, interests and every detail of daily life to the online world, which we have no way of controlling. This is what has been referred as "*The Collapse of Internet Privacy*" (Nikiforakis & Acar, 2014). Private information is a valuable asset for advertisers, and with the help of social media and features embedded in Web browsers, they build a detailed profile of user interests, shopping habits and browsing activities to explore and target those interests. In this game, the mainstream browsers and online services play along with the advertisers and contribute with online tracking features such as third party cookies, browsing history and other online activities. Cookies are small pieces of text, which a web site stores and uses on future visits (IETF, 2011). This allows websites to send the information and previous activity of the user back to the server. Third party tracking cookies are common ways of recording the long browsing history of users. Even though the tracking cookies cannot carry virus, malware or malicious codes, they pose potential privacy concerns, set out by the European Parliament (EU Directive, 2013) and US lawmakers (Rockefeller, 2011). However, security vulnerabilities of a Web browser or machine may allow access to credentials or login information. Therefore, users are advised to delete browser history and cookies after visiting websites to sustain sensitive information and prevent exploitation by advertisement companies or third party tracking cookies. Furthermore, mainstream web browsers such as Internet Explorer and Netscape are advised to block third party cookies by default (Jackson, 1996).

It should come as no surprise that by the use of ubiquitous systems and daily interaction with digital devices, we put a substantial amount of personal information into the public domain. Nobody is anonymous in the Internet world. In July 1993, the New Yorker published a cartoon by Peter Steiner which portrayed a Labrador retriever sitting on a chair in front of a computer, touching the keyboard with caption saying, "*On the Internet nobody knows you're a dog*" (Figure 2.1).

Figure 2.1 Internet Privacy (Nikiforakis & Acar, 2014)

Nowadays not only do they know you are a dog, but they know the colour of your fur, how often you visit the vet and what is your favourite dish which you get weekly from your local supermarket (Nikiforakis & Acar, 2014). Every online user builds up a profile with a long list of state, location, browsing history, shopping habits and other information. Every mobile phone has microphone and camera which can take video clips and store them. We have seen spy microphone and tiny recording devices on James Bond films, but there are many tinier invisible devices around us with the capability of capturing everything about us, storing in a digital media or even emailing to a remote user. This stretches the carefully protected idea of privacy to breaking point and is referred to as the death of privacy (Joseph, 2014).

Technology always moves faster than rules and regulations, leaving the right of privacy to the constitutions, especially matters involving the most intimate personal information, choices and beliefs, which are important to one's dignity and morals. Most of the solutions for the ubiquitous systems choose a trade-off between convenience versus anonymity, performance versus privacy, personal liberty versus social concepts and the list goes on. Many people would disregard the privacy concerns in a life-threatening situation, such as rescue and recovery operation in a disaster area. To speed up the process of containing the spread of an infectious disease, disclosing location information or identity of suspected infected persons by operators will be less of an issue. That is why some researchers proposed privacy design with emergency management in mind (Cakoukian, 2011). This includes inspection tools and access control, which enhances sensitivity of personal information.

Considering all of the facts mentioned in this section, one could realise the challenges a ubiquitous system faces in terms of dealing with privacy planning, data collection and information storage and access.

There exist several P2P scalable ubiquitous applications and approaches to address the challenges facing scalable ubiquitous networks, however the privacy concerns of those systems has always been overlooked except within Freenet. Privacy arises in a wide range of contexts. One such context is privacy of users within a smart environment such as distributed or P2P systems, where enormous amounts of personal data is transmitted. Anonymity is the property that provides privacy to users within a P2P system. Because of the topology, dynamicity and design of P2P overlays, privacy has not generally been considered as a major concern. However, anonymity is the property which maintains privacy, which in turn should be addressed at the routing level since exchange or transfer of information is involved. Aggregation is a natural abstraction for scalable distributed systems to allow a node to view the detailed information about neighbouring nodes (Renesse, Birman, & Vogels, 2003). Designing scalable system has its motivation such as increasing revenue by expanding network resource to be able to attract more demands. These objectives may be worth allocating extra cost, usability and operability design strategy.

However, one attribute that has been overlooked in designing scalable system is the privacy, particularly, user privacy. A design and plan for usability within scalable system required understanding of user patterns, habits and other personal information. The tools and techniques used by advertising companies to collect information about browsing activities and online habits is the typical example that a scalability designer may use to collect information. Although Online Behavioural Advertising (OBA) has set a guideline to restrain advertisers and web site operators from releasing names and personal information, collecting information, even with the intention of offering services, is considered to be violation of privacy.

P2P file-sharing networks reflects the Ubiquitous Computing paradigm with autonomous devices within distributed decentralised systems. The share of data within a community-based environment has been considered to resemble community trust (Llewellyn-Jones *et al*., 2009).

A considerable amount of attention has been given to improve performance of ubiquitous systems; however, privacy concerns have been neglected. As mentioned earlier, ubiquitous development and interconnectivity of various smart devices and wireless sensors have generated a data explosion, with a substantial amount of personal information stored in distributed digital

media. The personal information is always exposed to threats and vulnerabilities. Therefore, while governments push for online censorship and advertisers find new ways to push for open data access, ubiquitous system designers need to maintain user privacy. Recently, people and developers start to realise the privacy impact and consequences of ethical and legal implications (Brown *et al*., 2010).

2.1.1.4. Trust

The definition of trust varies from one subject area to another. In information security, the term trust is referred to as the level of risk a system can tolerate from a user (Bamberger, 2010). When dealing with users, systems make decisions based on metrics of the trust. To grant access to a trusted user with valid credentials, a system uses binary type to quantify the trust. The value of an identity depends on the trustworthiness of the owner of the identity. If the system knows the identity – the owner of the identity is trustworthy – then little will be gained by authenticating that identity. Thus, simply proving the identity of a device would be of limited value, since it provides little assurance that the device will behave in a trustworthy manner.

A trust metric is a measurement of the degree to which one person is trusted by another (McKnight, 1996). This can be implemented so as to work with information technology. The feedback ratings of eBay members were an early implementation quantifying trust. This improves the effectiveness of the feedback and can influence future eBay members when dealing with the same person, with positive or negative feedback. This approach can be applied to virtual and social networks to form friendships and expand connections. Having a positive feedback for an eBay seller provides some form of confidence and assurance of the accuracy of item description, quality of the service and speed of the delivery (Resnick, 2002). New attributes and features have been added to better rate the members on how trustworthy they are and how effective and efficient is the service they provide. Positive feedback and reputation determine trustworthiness in online business, which directly contributes to an increase in transactions and trade (Walia, 2013).

Trust has been dealt with as a key element for security options within ubiquitous systems and even economics (Gerald, 2011. McGeer, 2008). Trustworthiness is a moral value that a person can compromise (Hieronymi, 2008). A trustworthy person is who you can trust with your assets, personal belongings or personal data. That trust can be measured by assigning a responsibility and set the expectation. The expectation determines the level of trust and expected risk from it. When considering trust, we may take in to account reliability, loyalty and even dependability of

the person. If you trust a friend, does that mean you have to trust the friend of your friend? Transitive trust is where you trust a third person by relying on an intermediary trusted relationship you already have with your friend (Mu *et al.*, 2010). However, not trusting people does not mean that you mistrust them. It would be misleading to assume that negative prediction of trust would necessarily increase influence of distrust and vice versa (Xiao Juan Ou *et al*., 2009).

Social media has played an important role in capitalising on transitive trust. Taking advantage of the concept, it has created a community of users and network of acquaintances with various interests. There are a number of challenges that have been introduced by researchers in relation to trust (Zhang & Goel, 2004).

Humans normally wish to take control of their assets. Since the term 'ownership' will not exist within ubiquitous environments, this argument will be invalid (Hawley, 2008). The security of hardware devices is nevertheless a major concern when it comes to traditional distributed networks. If I see available and accessible computers anywhere and everywhere, there is no need to carry my own around and claim possession since I can find such an asset everywhere. This will be no longer the case within Ubiquitous Computing environment as hardware will be either disappearing or valueless. Instead, the main concern will be authentication within the new environment.

Providing an implementation of a trustworthy system based on trust that needs minimal human intervention is a strategic element for ubiquitous computing system security. Trust is the industry's answer to growing security problems (ICAEW, 2011). The application of trust to the security policies of systems has always been an ambitious approach for security experts. Leaving security of sensitive information and valuable assets to trust Researchers have used trust to improve both performance and security within pervasive networks (Zhang & Goel, 2004).

The theoretical and conventional access method 'all or nothing' is not sufficient to fulfil the needs of new users. The possible scenarios above question the functionality and operability of the network and emphasise the need for a more flexible and feasible approach. To answer those needs, more generous and open access should be provided to be able to satisfy the accessibility of the network. The access method should include not only trusted users within the network but to the users who are trusted within a corporate network with similar policy. The above solution entirely excludes any user without established credentials and classes them as untrusted. Because the base of the security within the network is trust between the networks and pre-defines

users with credentials, a direct approach should be taken to expand and stretch the existing security policy to fit new solution areas. This type of access control uses limited definition of trust and it is worth exploring to include other properties. In this way the proposed solution could work effectively to overcome the circumstances and minimise the cost and effort to design and implement new policies.

Experimental evidence shows that trust-based reputation can model virtual communities (Jakubowski, 2010). Access within a Local Area Network (LAN) is restricted to clusters of agents with small sets and high mutual trust. This phenomenon should emerge naturally with a trend to spread the trust based on acquaintances existing within the network with help from the models exhibited within Small World network. That means the system should maintain some level of trust in friends of users who have already got access privilege to the network.

Some literatures exist that try to motivate this approach by quantifying the trust and offering initial practical relaxations to models that preserve some of the theoretical flavour using mathematical computation (Resnick, 2002; Boukerche, 2008; and Sabater, 2002). Trying to define a matrix for trust, Nowostawski and Foukia (2007) determine that referral to local interactions can be extended to promote further co-operation and spread trusted participation. They claim that a large number of autonomous agents can be clustered to a local community of users to be able to satisfy desirable global uniformity. In other words, the approach can act as an abstract of trusted relationships and locally interacting components can be distributed in the context of information spreading and reputation referral. This then defines a minimal and maximal matrix collaborative relationship; this is a central concept in communication infrastructure and in security in general (Jinshan & Issarny, 2007). The trust evaluation can contribute to establish the trustworthiness of an agent. A maximal trust matrix is a trust matrix where every agent has trust equal to *one* in every agent. The trust between any two agents that have no common max-trust can be set to *zero*.

On auction sites such as eBay, members have to build a record of accomplishment of reputation and have their trustworthiness assured. The site supports a ranking system through feedback and service rating in which buyers and sellers evaluate each other. Members evaluate and score transactions based on item description, quality, delivery time, communication time, and overall satisfaction. This shows that ranking a member by another user forms a maximum or minimum trust system. That is not only the application of trust but also quantifying trust, derived from qualitative interactions (Jakubowski, 2010). We should distinguish trustworthiness from

reliability. If an eBay member, describes an item incorrectly, it breaches the trustworthiness and is not trustable. However, if the item delivery time took longer than anticipated, then the service or the member is unreliable. The factors leading to late delivery may include member's busy schedule or order processing, courier service or unforeseen circumstances, which do not necessarily fit in the trust category.

Quantifying the trust within the ubiquitous network would provide an answer to the authentication dilemma within the ubiquitous environment (Aberer, 2005). In other words, with a wide range of users within a ubiquitous environment, classifying access level and granting access based on level of the trust would be the answer to providing access to all as well as maintaining security of the system. The current process of access is all-or-nothing. It forms max-trust cliques, and the trust between any system and agent is a maximal trust. This is useful as a general guideline, but in practice and in different circumstances it does not emerge as a fully effective solution. With this classification, every relationship should be divided into two positions. Quantifying trust in an online auction site and merchant relationship, the trust quantification application may apply to the various scenarios such as trust between humans and a certification authority, in the iterative prisoner's dilemma game, in the inter-relations among software modules in a system, in the stock market, and in other trust oriented applications (Xiaowen Chu *et al.*, 2010).

In an attempt to scrap the binary trust relationship and provide wider access, ubiquitous networks should explore trust and include referral, transparency and tolerance (Sabater, 2003). The design can include different access rights, a system with tolerance, to accommodate every user rather than authenticate only a certain cluster of users.

Network security is so important and valuable that it cannot be measured and applied by probabilities or statistical methods (Patel *et al.*, 2005). On the other hand, lack of trust is a reason that makes ubiquitous environments vulnerable (Kegal *et al.*, 2001). Trust is a key issue to construct security in ubiquitous environments, which emerges in Small World networks with their occurrence in human-centred networks.

2.2. Small World Networks

The term *Small World* refers to the observation that we can find a short chain of acquaintances, to connect two people in the world (Marvel *et al.*, 2013). Small World networks are well represented by technological advances and the emergence of the Internet. Most social exchanges among humans traditionally took place via face-to-face interaction. Social networks have now shifted the phenomenon, where friendship and relationships have crossed borders, with a relatively short chain of acquaintances.

2.2.1. History

The concept of a Small World network was introduced by social scientists trying to measure path length in relationships. Explicit studies of the structure of social networks go back a century and are considered the earliest examples (Albert, 2005 and Watts & Strogatz, 1998). Although the argument of Small World network is observation of the direct short distances between contacts, some implications have concluded the wave-like behaviour of such characteristics to model certain behaviours within structured populations, namely spread of diseases (Braun *et al.*, 2006).

The small-world model has been used to model many applications such as physical contacts networks in the modern world, where distribution of contacts shows Small World network characteristics. The possibility of the rapid spread of epidemic diseases around the globe in distant locations simultaneously has been studied (Marvel *et al.*, 2013). The 2009 'Swine Flu' pandemic was an outbreak, first two cases confirmed in Scotland after a flight from Mexico. The cases spread from school and workplace of those who travelled from Mexico to the UK. With the closure of schools and precautions, the cases reached to 1,000 within about a month (BBC News, 2009). The number exponentially increased to 3,000 within next month and 9,000 the month after. In October the same year 27,000 new cases had been reported (Lawrance, 2009). Health care specialists have vaccinated the main origins of the virus and prevented further spread. One can make an empirical conclusion on how a computer virus can spread quickly across a highly connected network of devices. This is the typical structure and formal definition of Small World network.

Scientists, psychologists, marketing specialists and social researchers (Kleinfeld, 1967) have examined the idea in detail (Liu *et al*., 2003 & Zhu *et al*., 2004). Small-world networks are the focus of interest because of their potential as models for interaction, economical, technological and real world networks of complex systems. There exists broad research that has considered

the properties of a variety of diverse real world networks, with the intention to model them based on their characteristics and behaviours (Kochen, 1989; Kleinberg, 2002; Zhu *et al*., 2004; Xia *et al*., 2007; & Kak, 2011).

Although Milgram received most of the credit for his ambitious experiment and introduction of this phenomenon, his work was inspired by Paris University mathematicians Manfred Kochen and Ithiel de Sola Pool (Ithiel *et al*., 1979) trying to explore the mathematics of social networks. They wrote the manuscript 'Contacts and Influences' claiming that everybody in the world is connected to everybody else either directly or within a chain of intermediary persons. They have studied the properties of a variety of diverse real world networks and tried to model them based on characteristics and behaviour. The networking formed by the Internet is shaping new social relationships (Morozov, 2011). Friendship is not limited to classmate or neighbour or between those living in the same village.

This discovery has excited not only scientists but has inspired artists, journalists and marketing specialists for many decades. Imagine you have 1,000 friends and each of your friends knows 1,000 friends. You are just one hand shake away from knowing one million people. You can easily get access to their information and resources, their lives and socialise with them, with the privilege that you share with your own friends. Social networks and digital communications have changed the way we live, communicate and participate in open society and the wider community.

2.2.2. Applications

In mathematics and sociology, Small World refers to a graph to show links of edges representing people to their neighbours (Kleinberg, 2002). Research into the Small World phenomenon tries to model this kind of network and studies their characteristics and properties. The application of security to these networks is complex. A simulation done by Vogt (2005) shows that in a Small World network the end-to-end authentication of communication within the network is much riskier than that performed peer to peer between neighbouring nodes. He has called it light-weight and collaborative authentication scheme. In a distributed set of inline nodes *A*, *B*, *C*, *D* and *E* as shown in Figure 2.2, if node *A* wants to send a secure message to *E*, the chances that message will be altered after *C* is more likely because of lack of trust and distance from each other.

Figure 2.2 Linear Trusted Communication (Chen and Yeager, 2001)

The trusted relationship and degree of trust is evaluated between nodes *A* and *B* with shared interests, mutual agreement, performance, reliability or other parameters (Chen and Yeager, 2001). Two people enrolling on the same course may have close interests and share similar goals. But a trusted relationship will be established based on good practices and not common interests only. Digital-based system will benefit from trusted communication and building confidence (ICAEW, 2011). However, transitive trust will not be integrated in social interactions and system communications and may behave harmfully. The trust value is degraded between *A* and *E* on the above diagram as the peers lack confidence and reliability in each other. Vogt (2005) has demonstrated a direct exchange of messages for authentication is not only safe and efficient, but it is easy to manage as well. Therefore, he restricts the communication to nodes with direct and collaborated links. Not only does this approach provide more security to Small World networks, it is also resilient to random failures and known attacks (Albert *et al.*, 2000).

Researchers have studied the Small World network to apply security measures to networks (Vogt, 2005 & Albert *et al.*, 2000) and to improve the interoperability and performance of a network (Zhang & Goel, 2004). Many researchers have tried to associate Small World networks and ubiquitous computing systems. Notably, Vogt (2005) has emphasised the role of *hubs* within Small World networks, a node with heavily connected links. Hubs often form the basis of the network infrastructure, responsible for the existence of Small World networks. In the electricity grid network, a power station acts as the main source to provide, distribute and supply power to every household. A main entity providing services for smaller members is the same as a father-children relationship, which requires more authority and effectiveness. However, from a security point of view, such entities introduce operational challenges and vulnerabilities. This is exploited more in depth with the introduction of comprehensive properties and applications in 'graph theory' (Ruohonen, 2013 and Hayes, 2000). A graph is a finite set of dots called *vertices* (nodes) connected by links called *edges* (in our context, communication links). In Milgram's experiment of the six-degrees of separation, the number of edges connecting everyone in the world to each other, steps through six intermediary acquaintances. This was an attempt to form an acquaintanceship graph and determine the nodes and links associated within a social graph.

The World Wide Web is distributed worldwide geographically, but the diameter of the web is not the same as the globe. To estimate the diameter of World Wide Web, Barabási and his colleagues at Notre Dame University (Barabási-Albert, 2002) used robot software to carry out a search. The robot visited the Universal Resource Locators (URL), which form edges to point to web pages (vertices) to measure the connectivity of a graph. When you click on a link on a web page, the hyperlink takes some steps to direct you to the destination web site. If you randomly click on to two different links, then what is the distance between them two? Barabási and colleagues studied a small portion of the web and applied the result to rest of the graph to determine the distribution of nodes and links. Figure 2.3 demonstrates the connectivity graph, which has been captured by a router in the US.

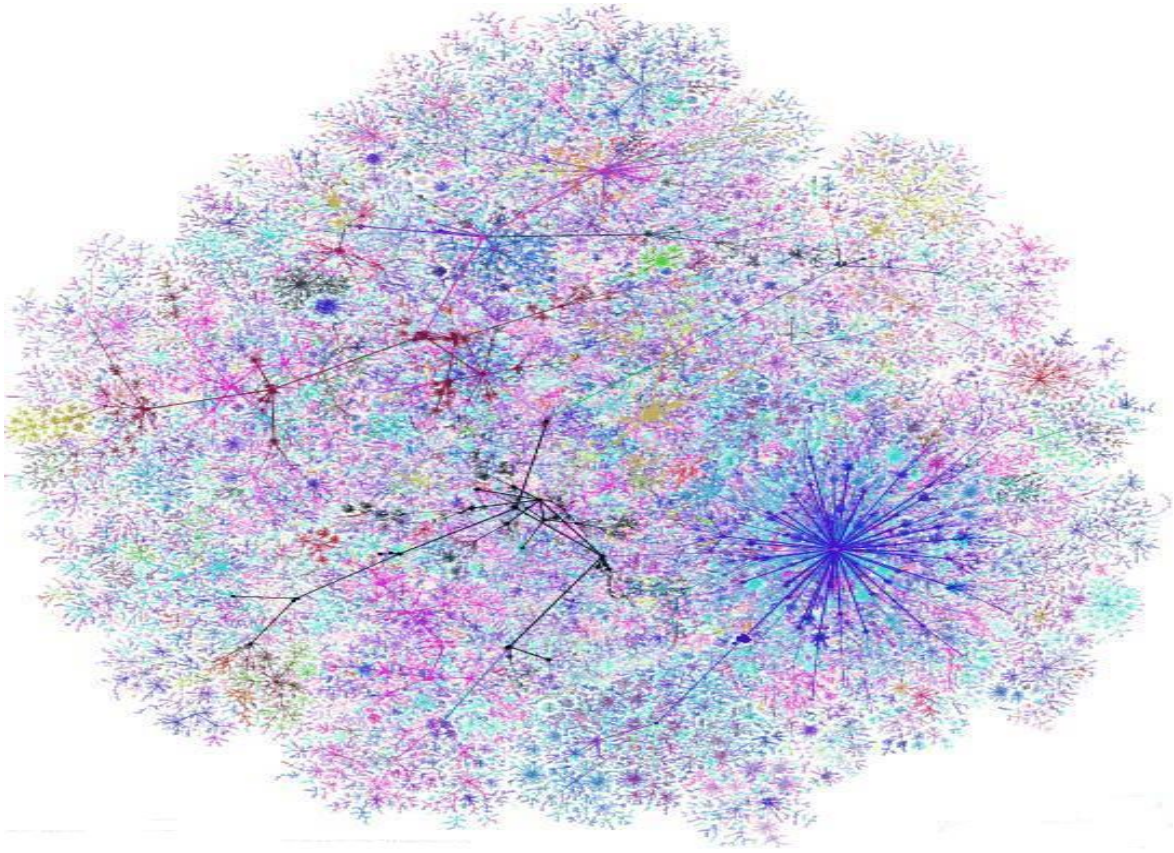

Figure 2.3 Diagram of World Wide Web, Captured by Barabási-Albert (Barabási-Albert, 2002)

Although there are only a few nodes with high-degree distribution, they have direct effect on the existence of the World Wide Web. They form several different clusters of communities with highly connected nodes as demonstrated in Figure 2.3. Those nodes (hubs) provide shortcuts between different clusters of nodes. The diameter of the graph is important when you are trying to search on the World Wide Web. The experiment conducted by Barabási *et al*. was using blind,

random and exhaustive search. Using smart techniques and clever algorithms employed by modern search engines, they reduce the number of edges to the minimum possible, improving efficiency and effectiveness.

Small World properties have been discovered in brain cells, the World Wide Web, citation websites and other collaboration networks such as social networks (Vogt, 2005). Those networks share two characteristics namely, direct collaboration and short-range communication (Hayes, 2000). Small World network properties have been implemented in many ubiquitous systems, namely within smart object collaboration environment (Siegemund, 2004). The properties have been utilised in wearable devices, sensor networks and other context-aware and self-organising computing systems.

2.2.3. Scale-free Networks

For many years, scientists who have been examining complex networks assumed them as being random (Barabási & Bonabeau, 2003). The examination included the statistical properties of those networks such as degree distribution, clustering, diameter and average path length. Erdös and Rényi then suggested that such complex systems could be effectively modelled by connecting their nodes with randomly placed links (Erdös-Rényi, 1959). It models random graphs, which sets an edge between each pair of nodes with equal probability, independent of other edges. The simplicity of their approach helped many scientists to focus on complex networks and renew graph theory with mathematical theorem (Hayes, 2000).

Scale-free networks were first investigated by Barabási-Albert (Hayrynen, 2005) after modelling the World Wide Web, scientific and social networks. Barabási and Albert have gone beyond the Small World network and opened a new research field by discovering the scale-free properties of real networks such as the Web, protein cells and social networks. They discovered that some nodes – called hubs – have many more link than others. They suggested that the highway network in America forms a random network as every road is connected to every other via a few links. The distribution of the cities has made them randomly connected to each other. However, if we study distribution of the airport network within Europe, we can realise that they form a power-law distribution with most of the small airports connected to large airports in capitals such as Heathrow, Paris, Amsterdam and Istanbul. These airports act as hubs in the Barabási model as they are connected to other small airports – nodes – with direct or short paths.

Therefore, when considering scale-free connectivity, it is important to consider the role of 'hubs' in a connectivity graph.

From the creation of the first Web page up until the emergence of the World Wide Web with billions of web pages connected to each other via links, everybody thought of the network as being random. The theory behind it was that everybody connects the newly created web page to another one based on various reasons, expectations and interests with a tremendous number of choices.

It was assumed the World Wide Web was a very random network with complete random topology up until 1998, when Barabási and his colleagues discovered the scale-free properties of it (Albert *et al.*, 2000). They discovered a few nodes with a high number of links. Although they examined only a small corner of the web, they realised that other parts of the network should follow the same principle.

In an exponential network, attaching new nodes to the network without a clear structure will follow a random distribution on a linear scale as shown in Figure 2.4. If the attachment of a newly joined node to the existing network does not follow a pattern or clear rule, the network will end up with no structure, topology or organisation. The further away the node is from the central hub the longer will be the communication time, response time and network latency therefore reducing the network efficiency.

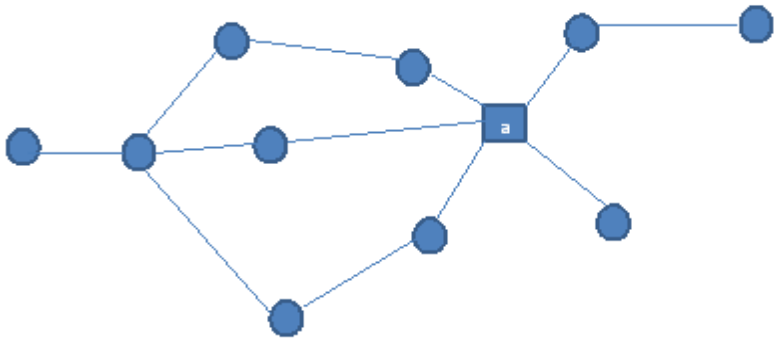

Figure 2.4 Random Network where *a* is the hub

Scale-free networks are networks whose degree of distribution follows a power-law. This shows the relationship between two quantities with preserved scale variance. In the other words, the scale feature does not change when the quantity is altered. Figure 2.5 demonstrates the distribution of nodes in a scale-free network.

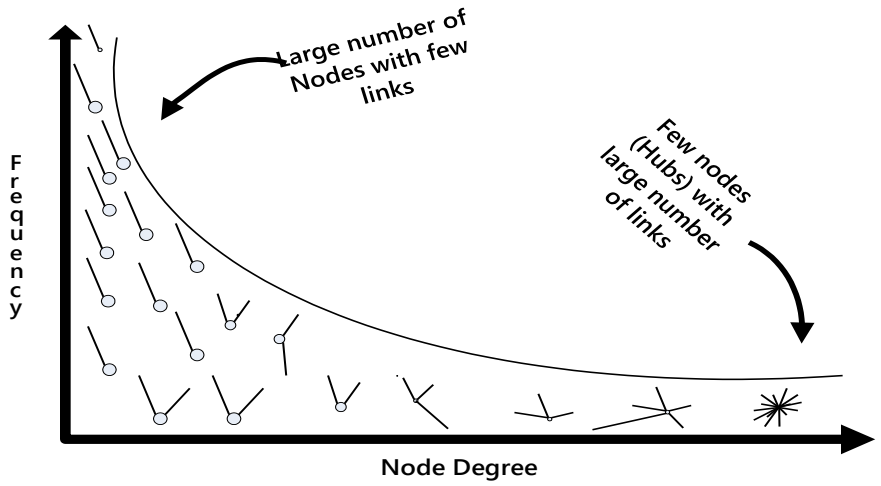

Figure 2.5 Power-law Degree Distribution of Nodes (Hayrynen, 2005)

Considering Scale-free connectivity within the typical network infrastructure represents a particular degree of distribution, this can be useful when considering security within critical systems.

For example, such scale-free connectivity will be resilient to random failures. However, considering the World Wide Web example, highly connected nodes such as search engines can have a significant impact on the operation of the system. The removal of such high degree nodes can cause failure of the network. There are hubs, where a few nodes have a high number of links to them.

The World Wide Web follows a power-law distribution as a few web sites – such as Google and Yahoo – dominate the most linked web sites. The Figure 2.6 is an indication of a scale-free networks interconnected using the dotted links.

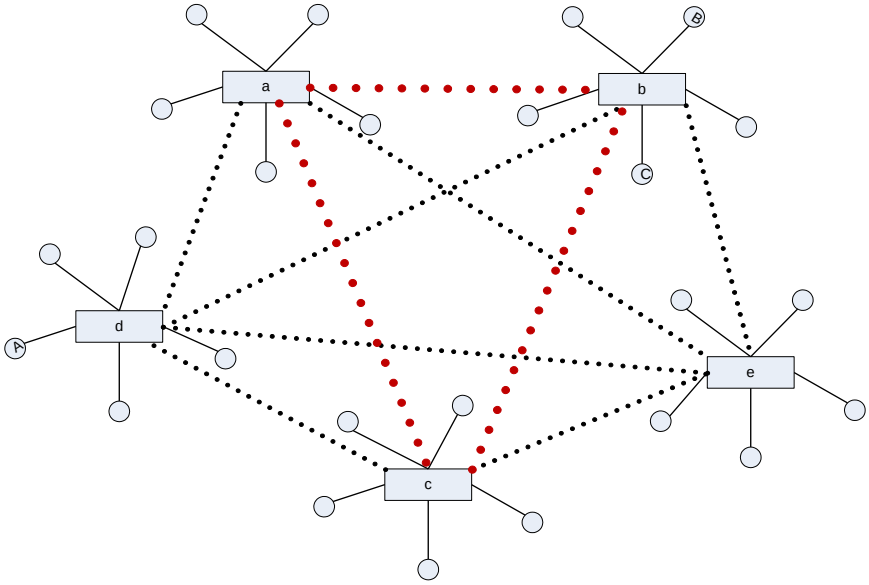

Figure 2.6 Scale-free Networks

Figure 2.7 demonstrates a random network where nodes have no organisational pattern, balance or structure.

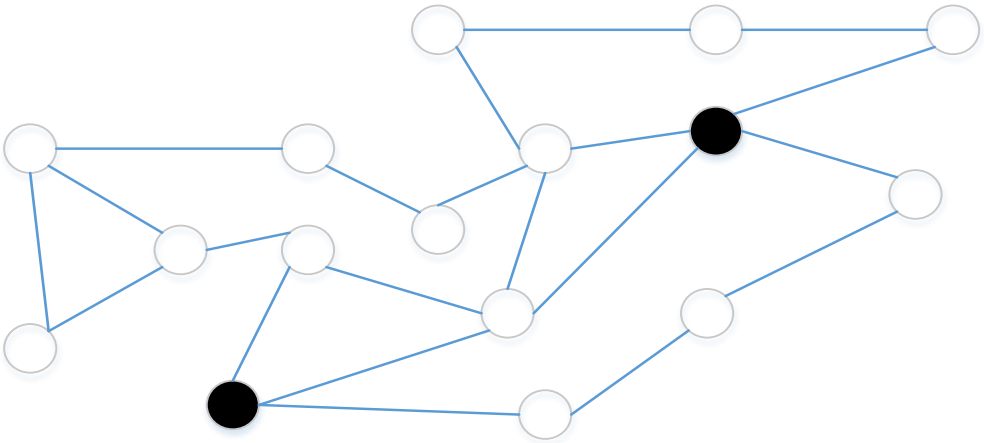

Figure 2.7 A Random Network

The node with black colour represent hubs within the random network. Figure 2.8 shows the effect of an accidental node failure with a random network.

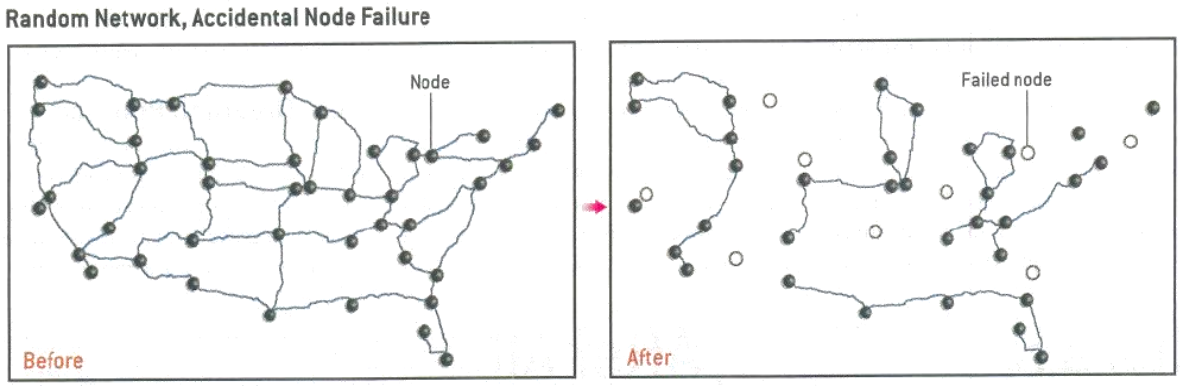

Figure 2.8 Random networks - Accidental Node Failure (Barabási & Bonabeau, 2003).

Scale-free networks have different properties from random networks, which make them attractive to the research community and security experts. Some of these properties include the following;

- Scale-free networks are more robust against random failures. If you remove a chosen node randomly from the network, the rest of the network will stay connected and functional. So removing low value nodes from the network will not have a significant impact on the operation of the network as a whole as shown in Figure 2.9.

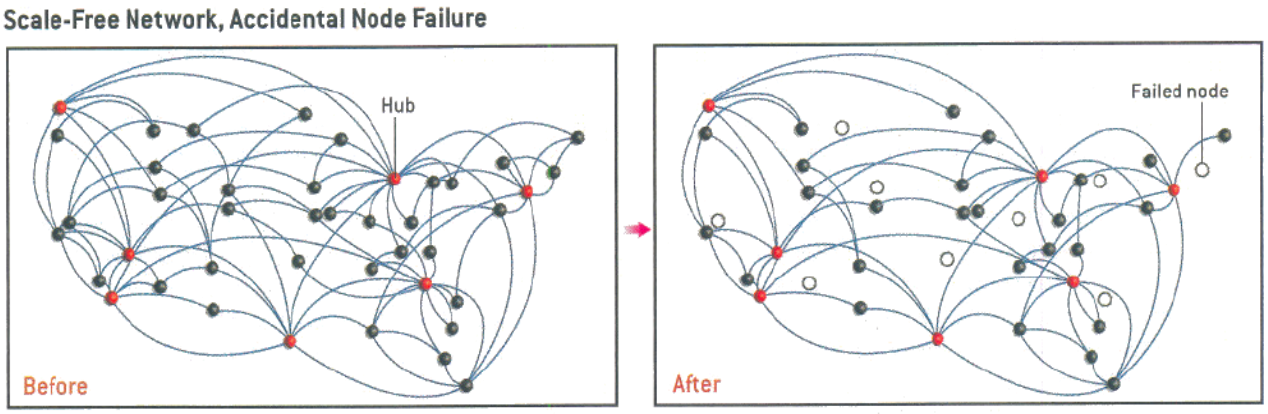

Figure 2.9 Accidental Node Failure in a Scale-free network (Barabási & Bonabeau, 2003)

- Scale-free networks are more vulnerable to deliberate attacks. This means that the network will fall apart when nodes are removed deliberately according to their degree. A targeted attack on large and high value nodes (hubs) will have a disastrous impact on the network as shown in Figure 2.10.

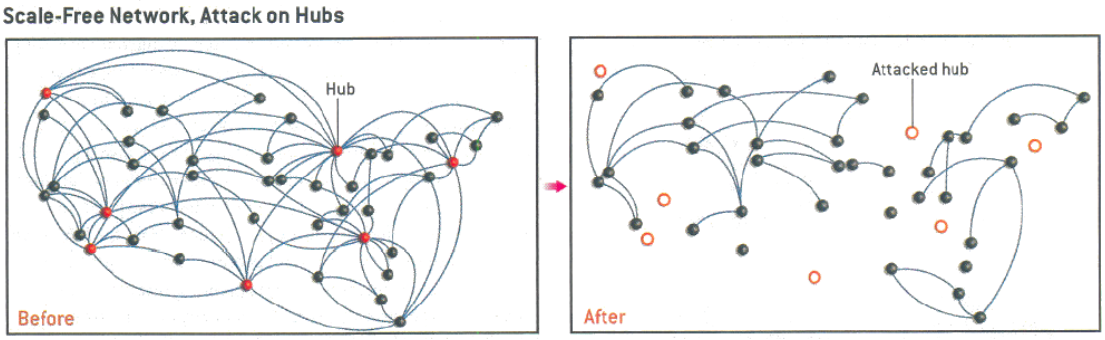

Figure 2.10 Scale-free Networks - the Effect of Targeted Attacks (Barabási & Bonabeau, 2003)

These laws have implications for many real world networks such as protein cells, brain cells, World Wide Web and so on. Eradicating viruses from the Internet is difficult if infected. Marketing companies study the spread of information on a scale-free networks model to propagate information about a new product to a community of consumers. In Medicine, identifying and vaccination of individuals with many connections can contain an infectious disease such as Swine Flu.

In a scale-free network, there are many low degree nodes, but the frequency of high degree nodes decreases relatively slowly as demonstrated in Figure 2.8. Because of the heterogeneity of scale-free networks, failure of small degree nodes will have less impact on the network operations as demonstrated in Figure 2.9. Instead, loss of high degree nodes (hubs) will cause the breakdown of the network into isolated clusters of nodes (Albert & Barabási, 2000) making most of the network difficult to operate. Such a scenario is shown in Figure 2.10.

2.2.4. Preferential Attachment

Preferential attachment involves the creation of links based on some quantity such as popularity, wealth or fame. In a computing environment, preferential attachment is a process whereby some nodes get more connections and therefore attract a higher number of nodes to connect to them. In real world, this is referred to as accumulative advantages, often informally related to the idea that '*the rich get richer'*. Barabási and Albert first introduced the preferential attachment model to explain the power-law distribution of nodes in Small World networks (Albert *et al*., 2000).

There are quite a few preferential attachment models trying to represent diverse networks with different characteristics and behaviours (Srinivasan, 2013). The links start from a few connections and form a tree-type topology with more links to the nodes with high degree like World Wide Web. Nodes with stronger ability and higher profile have more chance of attracting newly joined members. As new nodes enter the network, they are more likely to link to highly

linked nodes than nodes with just a few links, since the highly linked nodes are easier to reach and may serve their interest.

The preferential attachment paradigm introduces an explanation to the degree distributions following a power-law behaviour (Albert *et al.*, 2000 and Jacob & Orters, 2012). Networks with preferential attachment are robust under random attacks if the power-law exponent is sufficiently small, and have logarithmic diameters depending on the power-law exponent. These features, together with a reasonable degree of mathematical tractability, have all contributed to the popularity of these models (Jacob & Orters, 2012).

Preferential attachment may lead to the degree distribution of the network losing balance and forming an unbalanced, random network. However, if it is used conditionally then it can be employed to accommodate newly arrived nodes and maintain the scale-free property of the system at the same time. One approach is to distribute newly arrived nodes based on linear degree correlation by using degree-proportional probabilistic (Fotouhi & Rabbat, 2013). This approach demonstrates how different classes of network can grow by calculating degree distribution of nodes and enforcing preferential attachment to incorporate with the degree proportional value of the node of interest as shown in Figure 2.11.

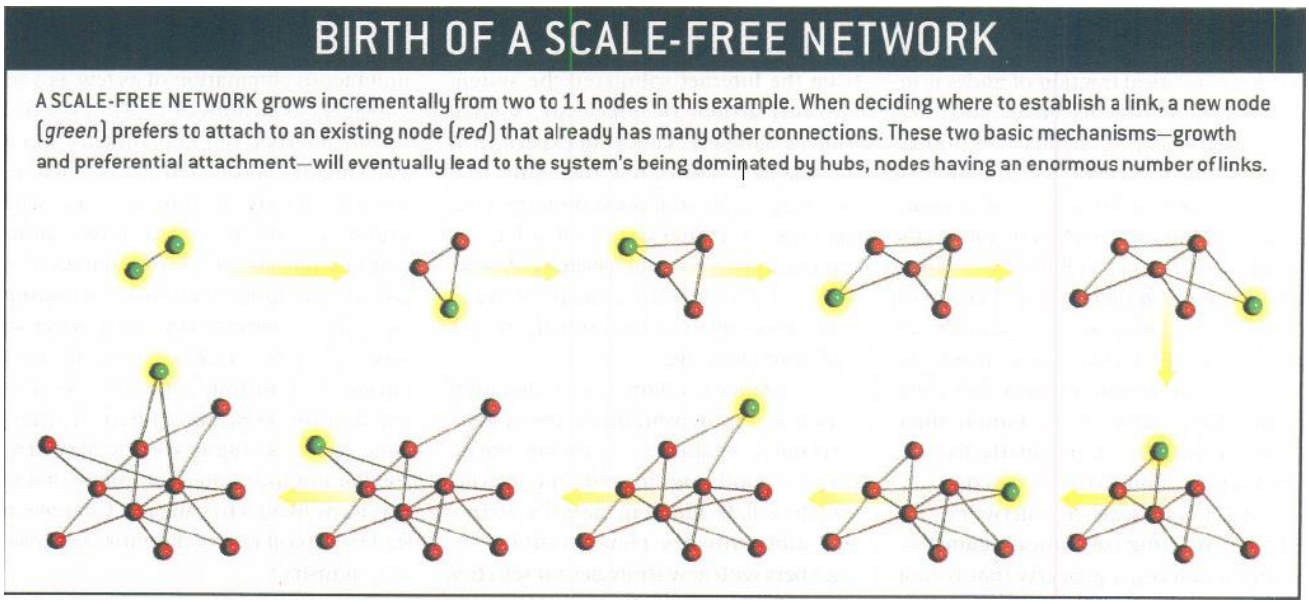

Figure 2.11 Role of Preferential Attachment in Scale-Free Growth (Barabási & Bonabeau, 2003)

Some studies suggest that although the principle is applicable in linear evolutions of fixed degree nodes, in most instances the initial "wealth" is irrelevant (Redner & Krapivsky, 2008). However, this does not contradict the primary principles of the phenomena; instead, it simplifies the mechanism and ignores correlations such as wealth, popularity, quality or importance. With

these principles in mind, we can analyse the entire dynamics of the network to model the proposed network structure. The theory demands construction of a global trust network where any node can easily contribute directly and connect by a short path. Highly linked nodes are easier to reach and generate more connections than any others. That is why by studying the structure of the World Wide Web, Barabási discovered that, unlike the theory of random distribution of the nodes, most of the pages linked to a small number of the most visited sites like Google (Barabási & Bonabeau, 2003). If a new page is created, the likelihood that particular website will be linked to Google is so much higher than to others.

2.2.5. Power-law Distribution

Scientific and communication networks are studied by observing the real geometry and topology of connections. The trend started with studying communication patterns on the Internet by Barabási and Albert (Albert *et al*., 2000). Work on human mobility has shown that the lengths of trips people take follow a power-law distribution over a wide range of scales from tens to thousands of kilometres (Kleinfeld, 1967 and Lawrance, 2009) and theoretical work by Kleinberg (Dyke, 2003) suggests that such a power-law distribution of connections implies the small-world effect. Moreover, new strains of pathogens such as Influenza are observed to travel around the globe rapidly, appearing in distant locations almost simultaneously (Hayes, 2000). One possible cause of such rapid spread is the presence of short chains of physical contacts linking individuals in distant parts of the world.

Barabási and colleagues suggested that the scale-free networks follow a power-law distribution mechanism (Albert *et al.*, 2000). Protein networks, citation networks, some social networks, the World Wide Web, and the cells in the humans brain all form Scale-free networks.

Numerous studies and experiments have examined the resilience of those networks against different attacks and vulnerabilities (Hayes, 2000; Hayrynen, 2005; and Albert *et al*., 2000). They are resilient against accidental failures. The idea can bring new prospects to information security in ubiquitous environments.

In a computer network, if an attack targets a network and destroys a small number of low degree nodes, this is not really a problem because most nodes have a low degree. Losing many low-degree nodes will not affect the network as a whole. However, an attack that targets the high-degree nodes can be disastrous. The entire network might collapse and revert to an earlier state (Albert, 2005).

2.2.6. Clustering Coefficient (CC)

Watts and Strogatz have modelled the small-world networks as a class of random graphs (Watts & Strogatz, 1998). They noticed that graphs could be classified into two independent structural features; clustering coefficient and shortest path length. The Clustering Coefficient is the measure of connections within the nodes' neighbourhood from available connections. The algorithm produced by Watts and Strogatz to measure Clustering Coefficient in a network with *N* nodes is demonstrated as below:

$$C = \frac{1}{N}\sum_{i}^{N} C_i \tag{2.1}$$

$$C_i = \frac{2\,|\{e_{jk} : v_j, v_k \in N_i, e_{jk} \in E\}|}{k_i(k_i - 1)} \tag{2.2}$$

where C_i is the local coefficient for a given node i, N_i is the set of neighbouring nodes for node i, E is the set of edges, e_{jk} is the edge connecting node j and its neighbour k, and k_i is the degree of node i – the number of its neighbours.

Watts and Strogatz (1998) have modelled the spread of a disease within a real world network. *"Infectious diseases are predicted to spread much more easily and quickly in a Small World; the alarming and less obvious point is how few short cuts are needed to make the world small"*. This statement can be related to the possibility of the spread of a malicious program within a distributed network and the resulting widespread effect can be catastrophic with critical systems, health and government and financial organisations heavily linked with computerised systems. On the other hand, considering such a model can be used to protect computer systems.

The measure is the proportion of a connection a given node can have with number of potential neighbouring nodes. The clustering coefficient of a node in a network determines how close its neighbours are with it. In a graph it is the vertex in quantifies the clique to complete the graph.

In Figure 2.12, the local clustering coefficient of node *A* is the number of triangles connected to *A* divided by number of triples around it;

$$C_A = \frac{E_A}{k_A(k_A - 1)}, \tag{2.3}$$

where E_A represents the number of edges, k is the number of A's neighbours within the corresponding cluster and C_A is the CC of A. Based on the calculation and structure shown in Figure 2.12, A has the maximum CC of 1.

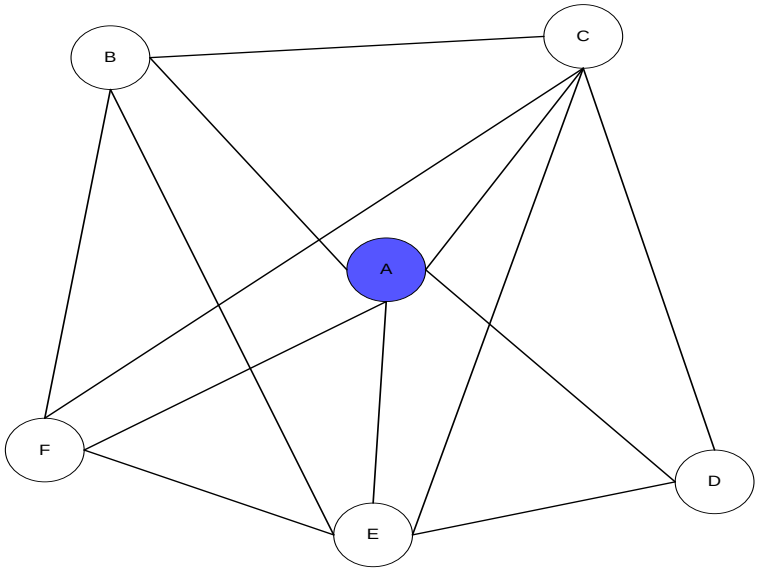

Figure 2.12 Local clustering coefficient of 1

Figure 2.13 demonstrates the possible connections of A towards four nodes in an undirected graph and their local clustering coefficient among their neighbours.

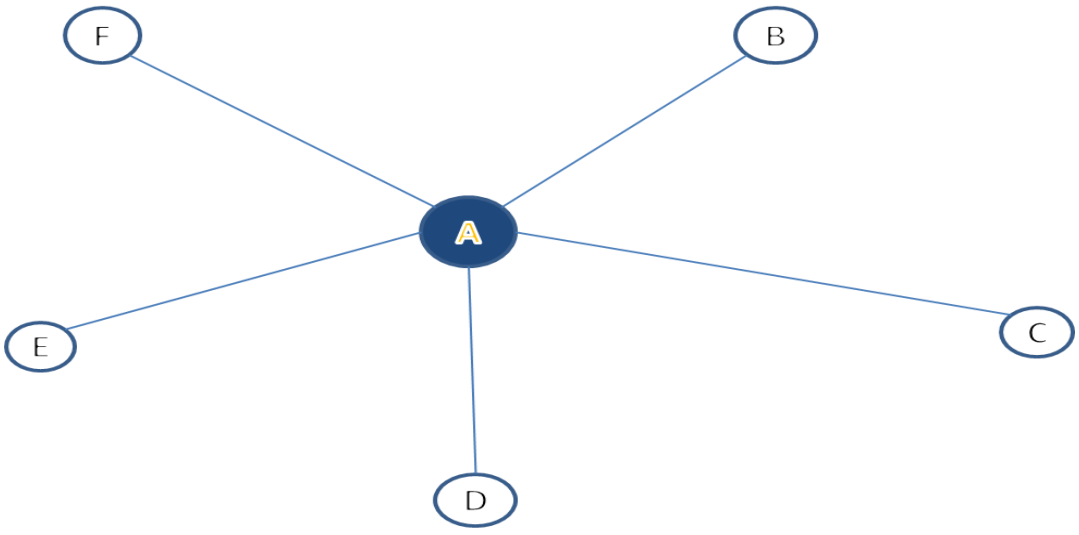

Figure 2.13 A Graph with Clustering Coefficient of 0

It is the 'local' clustering coefficient on an undirected graph. Within the demonstrated diagram the clustering coefficient is 0 therefore, it has the minimum possible clustering coefficient.

The clustering coefficient of each node is zero because there are no edges among their first neighbours. Both the maximum and average path length increase linearly with the number of

nodes and are long for pathways that have many nodes. This type of graph has been widely used as a model of an isolated signal pathway. Table 2.1 shows various complex networks, which exhibit scale-free properties. Interconnected networks with scale-free topology lead to having Small World characteristics (Mathias & Gopal, 2001).

Table 2.1 Average Shortest Path for different Scale-free Networks

Network	Vertices	Degree	Path	Cluster
WWW	2×10^8	7.5	16.0	0.10
Movie actors	150,000	28.0	11.0	0.18
Phone calls	53×10^6	3.6	Not known	n/a
Synonyms	22,311	13.0	4.5	0.70

Table 2.1 shows the degree distribution and number of vertices of some Small World networks, which exhibit a power-law property as well as values corresponding to the shortest path and clustering coefficient using the Watts and Strogatz model. In a Small World network, the average shortest path has always been the focus when determining the communication path between two nodes. A high degree node (hub) normally acts as a one of the intermediate nodes when planning routing between two chosen nodes. The concept of the shortest path and techniques that are used to determine it is explained later in Section 2.2.7.

The nodes of a graph can be characterised by the number of edges that they have (the number of other nodes to which they are adjacent). This property is called the *node degree*. In directed networks, we distinguish the in-degree, which is the number of directed edges that point toward the node, and the out-degree, which is the number of directed edges that start at the node. Whereas node degrees characterise individual nodes, one can define a *degree distribution* to quantify the diversity of the whole network (Albert, 2005).

As stated earlier, Barabási and colleagues made a breakthrough in the direction of understanding the generic features of network development (Barabási, Albert & Jeong, 1999). They discovered the degree of self-organising characteristic of large-scale complex networks such as the World Wide Web. However, Watts & Strogatz (1998) have already investigated modelling random networks. By studying the statistical aspects of random graphs using probabilistic methods, Erdős and Rényi (1959) discovered that many properties of random networks appear suddenly. In their network model, the network ends up with isolated clusters of nodes within the network.

In the Watts and Strogatz (1998) model, the topological structure of the network is formed linearly by bounding the new arrivals to the nearest neighbours. The model considers an

indefinite number of arrivals connected to one of the existing high degree nodes generating a completely random network and increasing the average path value linearly.

2.2.7. The Average Shortest Path

There are many algorithms that are used to identify scale-free connectivity and calculate properties of such systems, in particular the Average Shortest Path (Lamb, 2009). In ubiquitous, distributed and autonomous systems with so many hubs, the choice of connecting through intermediate entity is not obvious. Small World graphs are characterised by any two nodes only a few hops away from each other, with intermediary connections. Given the connectivity of the nodes and hubs in a scale-free network, overwhelming routing requests could potentially lead to system bottleneck due to potential exploitation of preferential attachment. On the other hand, choosing random routes may also lead to exhaustive hopping and cause unnecessary timing delays. When planning a route between two nodes, the average shortest path will use the most available route with efficiency and effectiveness in mind. Some suggest that, calculating the average short path between two pairs to determine the shortest available route may very well be computationally expensive (Lamb, 2009). However, with clustering and local arrangement of nodes and leaving some routing authority to hubs, this can be characterised as efficient routing methods in many ways (Schank & Wagner, 2004 and Tsang & Smith, 2008). The algorithms provided in Small World network models can simplify the complex and expensive calculations as nodes are only a few hops away from each other. High degree nodes with many connections can act as intermediary entities to not only drive the cost down, but to improve efficiency and security through direct or average short path communication using the trust element within a clustered network. Cohen and colleagues (Cohen, *et al.*, 2003) suggest 'Acquaintance Nomination', a targeted immunisation strategy aimed at identification and immunisation of such high degree nodes will improve security within such systems. This is an interesting method, which singles out the hubs in the system. It requires no previous knowledge of node density. They claim that the proposed technique improves coverage within the network topology as well as safeguarding against failures and vulnerabilities. The well-connected hubs are nominated under the acquaintance nomination. They prove that only removal of a large fraction of the network will compromise the integrity of the system. This is useful since Small World networks and Ubiquitous Computing networks share the same degree distribution pattern. Since the Shortest path and direct communication have been tested and considered to be efficient and secure (Ying *et al.,* 2010), one can justify such a mechanism in distributed and scale-free systems.

2.3. Network Overlay

A network overlay is a solution to address scalability issues within distributed systems. It is a virtual network of nodes and logical links that are built on top of the existing network (Stoica, 2004). It provides services that are not available within the existing network. A network overlay is considered to be the best option for autonomous systems (Wei *et al*., 2012). This is because within the network overlay, peers can contribute to the network or act independently. The routing and alternative communication path is facilitated by network overlays. Figure 2.14 illustrates a typical overlay network.

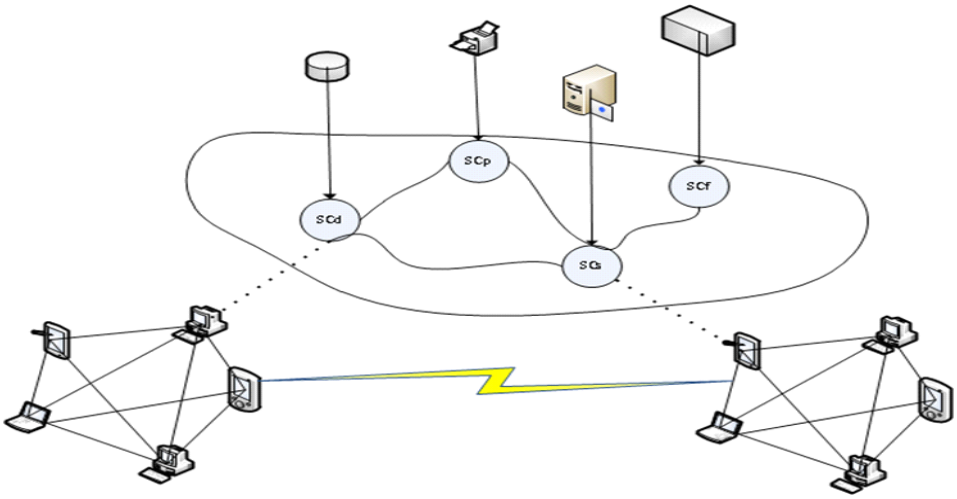

Figure 2.14 Typical Network Overlay

Distributing some network resource is not possible such as the physical peripherals or print servers on network overlays. Enterprises created cloud services for converged and shared service infrastructures; however, the Virtual Local Area Networks (VLANs) could not cope with the traffic from virtualisation in the Cloud (Brandon Hoff, 2012).

In addition to providing many answers to network scalability issues (Wei *et al*., 2012) network overlays are easy to deploy. They do not require software or protocol modification when new equipment is deployed. Network overlay also supports multicasting by sending IP datagram to a multicast address of every node joined the group (Stoica, 2004). Dynamic members such as nodes joining, leaving of failing will have a significant impact on topology, routing condition and network traffic. There are many approaches to address these issues such as state management using collective aggregate messages (*n*-dimensional graph system like CAN) or using neighbouring node aggregated messages (Gupta, 2003), Pastry (Rowstorn & Druschel, 2001) and Chord (Stoica, I. Morris, 2003).

2.3.1. P2P Overlays

P2P file-sharing networks reflect the Ubiquitous Computing paradigm with autonomous devices within distributed and decentralised systems. The popularity, success and ubiquitous use of P2P and file sharing systems and the need for efficient communication and improved management has created pressure to roll-out efficient and effective communication methods to address dynamic change of members and resources within ubiquitous P2P networks. The self-organising overlay networks that are distributed on IP networks are called peer-to-peer (P2P) networks. P2P systems are managed by protocols implemented at the application level. For example, primarily they will be implemented on top of the UDP or TCP communication protocols. Furthermore, P2P overlays provide support for scalability within dynamic and decentralised systems. The nodes within a P2P system act in a self-managing manner in contrast with the client-server model. Such overlay networks go beyond the services offered by conventional client-server systems (Lua *et al*., (2005). P2P systems are popular and pervasive, and largely used for file sharing and data communication.

A P2P overlay provides support for scalability within a dynamic and decentralised system with self-managing nodes. This means they can take advantage of the available resources, content and traffic stability independent of central servers. Nodes have dual client and server roles, meaning they can both initiate and listen for incoming connections. They can also have computational power and can run processes – called queries – at the same time.

There are many P2P networks with diverse properties that are classified based on different methods such as performance metrics, topology, protocol and structure (Jawad, 2013). Each class of system has its own advantages and disadvantages but we will focus on decentralised and heterogeneous P2P overlays that support scalability to some extent.

2.3.1.1. Chord

Chord is a lookup algorithm for Internet applications using scalable key location item (Stoica *et al.*, 2003). Keys are distributed based on item locations. The lookup protocol provides support based on item location using the key. Given a key, it maps it to the desired node, which holds the data item. If it is a file sharing application such as bit torrent, it maps to the desired file. If it

is the Internet application such as Chord, it yields IP address of the node associated with the given key. Node address is assigned based on node location. Therefore, Chord forwards messages based on numerical differences with the destination address.

Chord acts as a distributed hash function, distributes keys uniformly over different nodes providing natural degree distribution and load balancing. In Chord, routing is performed using iteration method at each hop and invoking Remote Procedure Call (RPC) at the next hop through the path. In a network with *n* member nodes and within a normal situation, each node maintains information about *O*(*log n*) other nodes and resolve all search and lookup operations using messages no more than of O(*log N*). This makes the algorithm simple and provides effective system correctness. Figure 2.15 shows how Chord uses neighbouring information and Distributed Hash Table (DHT) to deliver the packet from source (node 12) to destination (node 4);

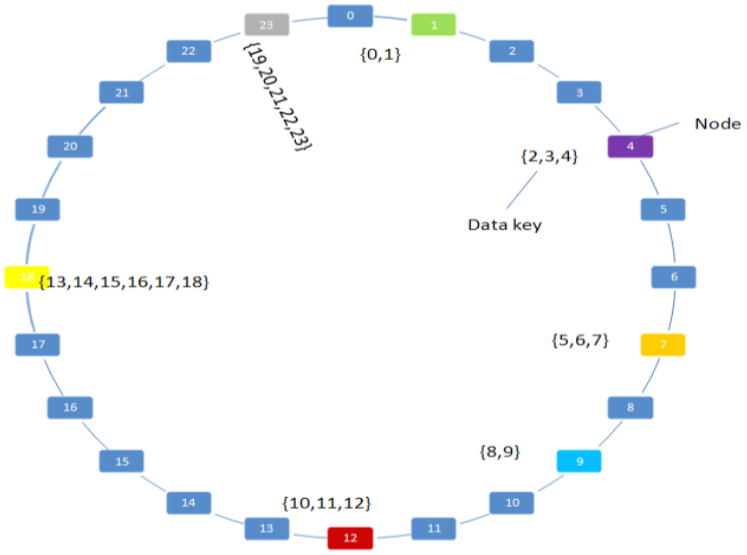

Figure 2.15 Chord DHT Routing

The coloured nodes 1, 4, 7, 9 12 18 and 23 in the circle represent finger tables. Finger tables maintain the information for the successor nodes and are referred to as hash tables. Because they are fully distributed in Chord, they are called Distributed Hash Tables. Keys represent the information held within the node. Searching for the key returns the value on the node. In the Internet communications, this value is considered the IP address. Each finger table keeps list of nodes and keys. To route from source to the destination, a key is mapped to the node, which return a resource such as file. Despite the favourable characteristics of Chord, it has some drawback such as lack of physical location consideration in look-up operations, leading to

bandwidth waste and system overhead. In addition to those advantages, Chord share some disadvantages with DHTs in terms of security such as traceability of users who share files online.

2.3.1.2. Freenet

Freenet (Clarke *et al.*, 1999) is an unstructured P2P system that has been designed to exchange information between users. It allows publishing and retrieving contents in an anonymous way that the source and destination of the information is withheld from third parties even the system servers. Freenet is decentralised, that means there is no central-server structure. There are many advantages for centralised systems such as cost effective management and efficient communication. In a community where privacy and security is the most important requirement especially for users, the client-server model is not feasible. Servers and clients can be identified and penetrated or shut down by governments or agencies. The routing process is demonstrated in Figure 2.16.

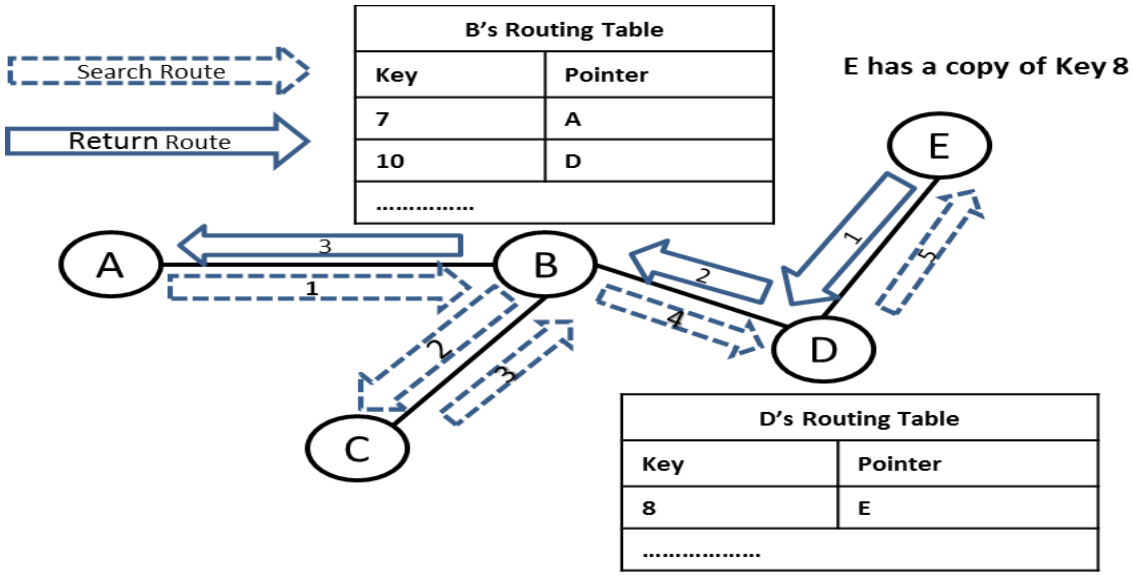

Figure 2.16 Search in Freenet – Node A Searches for Key 8, Located at E (Zhang & Goel, 2004)

Like Chord, Freenet use DHTs for key distribution. Freenet does not assign responsibility for documents to specific nodes instead; lookups are carried out by searching for cached copies. Freenet aims to provide a flat Internet topology. In other words, you can communicate with an IP address next door, the same way you would communicate with another IP on the other side of the planet, without being discovered. It was first used by a large community of online users to distribute copyrighted materials on the internet without being discovered. Clarke *et al.* (1999) claim that this was not the purpose of the project. They believe the Internet is the biggest bastion of freedom of speech, since governments try to impose censorship on the flow of information in

the press, broadcasting and printed materials. However, the design and infrastructure of the network has been suffering serious flaws such as performance (Zhang & Goel 2004) and scalability and load balancing (Portman *et al.*, 2001). The scalability issues were later resolved by changing the system architecture to support a distributed and scalable system. Communications by Freenet nodes are encrypted and routed through other nodes to make it extremely difficult to determine its originator as well as content (Clarke *et al.*, 1999). Peers in the network participate in queries, data storage and retrieval of data items. The data distributed within the Freenet are identified by 160 bits keys. A request for key is passed along peers using flooding algorithm, which returns the corresponding data. These keys are location-independent. If a node received a request and knows the location of the file, it forwards it to the destination, which holds the information. If the node does not know the destination address, it forwards it to a node, which might hold the information or is likely to know the whereabouts of the resource.

It is same as the routing mechanism, which was identified and implemented during Milgram's Small World experiment. The information is cached locally which helps subsequent routings to be effective and efficient. To make the routing more efficient and smart, Freenet uses historical information and statistics from previous routing experiences to make a decision-based estimate of the time it might take to reach the destination. Caching based on specialisation of the nodes accumulated cache of the information that it then resulted Freenet not to cope with overwhelming requests and collapsed in July 2003. It was then that the designer addressed the load balancing issues by ensuring the uniform load distribution and constrain queries to maintain the defined quota. Considering this approach has addressed the problem and works effectively, but it may lead to interoperability issues by limiting incoming requests to retrieve resources. This means that individual nodes behaving other than anticipated may affect load balancing and increase request failure rate. Therefore, the challenge in terms of scalability and performance still persists within the Freenet structure. Like any other P2P system, nodes in Freenet can have a dual role and are not distinguishable by name. This component of the system improves the anonymity. However, an adversary can easily identify the traffic load and distinguish server nodes using a packet analyser. Having said that, Freenet remains one the important systems in providing user anonymity.

2.3.1.3. Gnutella

Gnutella is one of the earliest unstructured P2P systems, developed for file sharing (Portman *et al.*, 2001). Gnutella has fully distributed architecture with no central servers. This means each

node can act as client and server. Gnutella is widely used over the Internet for file sharing with its 'simple to implement protocol' and 'search' and 'forwards' queries. Joining the Gnutella network starts with a *ping* message to one of the existing nodes and request to join. To join the network, a client should find IP address of an existing member. The system then grants access to the node with valid association to an existing group member. The system growth follows power-law connectivity to form an ad doc P2P topology.

Gnutella takes the simplest routing approach – Flooding – to support search and broadcasting. Each search, called a '*Query*', is performed by looking for the key where each key represents a data item. If successful, the data associated with the key is returned to the source via direct link. Due to lack of location information and central indexing table, the search process is unbiased without prior information. To route from first node to the last node, the message has to visit every node to arrive at the destination failing to utilise an efficient mechanism such as taking advantage of connectivity distribution (Adamic *et al.*, 2001). The network has optimised the routing with cache replacement. Each query is forwarded node by node across the network until it reaches the destination. If a file is retrieved from a destination node, it leaves the replication on every node that it visits on the response route. Gnutella has some advantages such as simplicity but its operation heavily relies on users' cooperation and consistency.

2.3.1.4. GIA

GIA has been developed in response to the design flaws and scalability issues of Gnutella and to improve heterogeneity of the network by adapting overlay topology and to replace flooding search algorithms (Chawathe *et al.*, 2003). The capacity constraints are taken into account when adapting the topology and to assign Skype-type super node role to the nodes with high degrees in terms of capacity. These high degree nodes facilitate random walks described in GIA documentation. This is also used to achieve scalability.

GIA uses random walk search rather than flooding by introducing a token-based flow control algorithm. However, the random search performs a blind search and forwards nodes based on probability that the higher degree node is likely to know the destination. The flow control ensures the heterogeneity of the system and assigns responsibility to individual nodes based on their capacity. The node capacity factors are considered processing powers, communication delay and bandwidth consumption.

As with Chord, GIA uses neighbouring information to maintain pointers to contents and provides efficient one-hop replication. GIA claims guaranteed successful results for a high number of queries using high capacity nodes. However, a constant search for high capacity nodes may exhaust system maintenance and end up flooding type search. In the absence of this issue, GIA heavily relies on client's contribution to implement flow control and topology adaptation.

GIA replaces the Chord used by Gnutella to accommodate dynamic membership change and to handle different churns. In an unstructured file sharing P2P network such as Gnutella, clients leave, join and fail, leading to unsuccessful queries and high bandwidth cost.

GIA provides dynamic topology adaptation to avoid overloading nodes with high degree and system bottlenecks. However, GIA uses random walks towards high capacity nodes as search algorithm. This is achieved by using reputation based topology adaptation. In other words, nodes with a high capacity and high capability are allowed to handle a high number of queries. However, GIA does not provide a definite success by using biased random walks. In other words, the search might well be the optimum result in random walk as the search is directed to high capacity nodes but, having high capacity does not correlate with high contribution or high success rate.

GIA allocates proportional tokens to neighbours based on their processing capabilities. This further maintains an index of content of all neighbours within the group and results in one-hop replication. GIA claim that it performs better than other algorithms such as FLOOD and RWRT (Chawathe *et al*., 2003). Furthermore, GIA system uses 'GIA Search App' using the following attributes and metrics:

- Capacity settings such as bandwidth, CPU and disk access that are configured by the user.
- Satisfaction level that is based on capacity, degree, age of neighbours and capacity of node.
- Query resilience where keep-alive messages are periodically sent and optimisations on adaptation to avoid query dropping.

GIA has never been fully implemented as a real-world application using capacity settings for supermodel configuration. It has rather, assigned random numbers to nodes to be set as node capacity, which is then used for message forwarding within a simulated environment.

2.3.1.5. NICE

Application Layer Multicast (ALM) has recently gained increasing popularity in the multicast community. In this type of multicast, group membership, multicast tree construction and data delivery are solely controlled by participating nodes with complete autonomy (Li *et al*., 2005). NICE is the early application layer multicast protocol which uses a tree topology to organise nodes into a hierarchy of users. This provides effective control of network resources, robustness of network overlay and ensures quality of data delivery path (Banerjee *et al.*, 2002). Furthermore, NICE controls the cluster size by constant topology adaptation, cluster refinement and membership updates.

NICE starts the topology by forming a cluster of users choosing a cluster leader for them. The leader is selected from where the node is located in the middle of the group. Depending on the dimension of the topology defined, the tree grows exponentially forming different clusters. The group of different clusters forms a super cluster. A rendezvous point is selected from within the cluster leaders. The cluster leader who is located closest to the middle of the super cluster is selected as the rendezvous point, which is responsible for bootstrapping, cluster refinement and other membership management tasks. It provides a central point of command and control for data path control, new member assignment to appropriate cluster and network maintenance. Cluster refinement and network maintenance is achieved using constant heartbeat messages to every member node to update and maintain members' state.

NICE provides efficient broadcasting using hierarchical layered arrangement of nodes but has no mechanism to avoid redundant queries and self-loop messages. Although NICE is the best solution in terms of multicasting and topology adaptation (Krause & Hubsch, 2010), there are serious limitations to the original design;

- **Security:** NICE's operations rely only on node state management, update and global advertisement of such parameters. All of these operations are performed at the rendezvous node, which creates a single point of failure. Furthermore, NICE has no mechanism to address the issue of misbehaving nodes.
- **Leader selection criteria:** NICE only considers the node location as a metric for cluster leader selection and subsequently the rendezvous point. There are no other considerations such as processing power, node life time or system granularity for leader selection process. This can lead to system performance compromise if the leader fails to cope with queries that require significant processing power. Frequent interchange of cluster leaders can also impose a high maintenance cost and overhead.

- **Rendezvous node vulnerability:** The location mechanism is the only parameter for choosing the rendezvous point for the NICE topology. Every node and cluster leader relies on the rendezvous point for membership management, topology adaptation and naming scheme. While replacing the rendezvous point seems a straightforward process, it creates single point of failure, which can pose serious resilience and interoperability concerns.

2.3.1.6. Scribe

Scribe is a scalable, decentralised ALM protocol built on top of Pastry, a Key Based Routing (KBR) protocol. It allows routing to random keys. Scribe supports a large number of groups of any size with high rate of membership turnover. A message is routed recursively to a node, which is closest to the given key. Scribe uses Pastry to manage the group creation, group joining and to build multicast tree, which is used to disseminate the multicast messages multicast in the group.

The group ID is the hash of the group's textual name. The collision resistant hash function ensures a uniform distribution of group IDs. Pastry nodes are uniformly distributed, ensuring an even distribution of groups across Pastry nodes.

Scribe provides reliability for the broadcasting process, which guarantees high success rate. The message delivery is ordered if there are no faults in the multicast tree. Pastry's randomisation properties and Scribe's selection of a multicast root ensures load balancing.

2.4. Summary

In this chapter, a thorough analysis of ubiquitous computing birth, growth, development and its advances such as IoT were discussed. The challenges and applications of ubiquitous systems were reviewed, considering alternatives or alteration of such elements to enhance security and interoperability of ubiquitous systems. Different aspects of system security were discussed including availability, integrity and confidentiality to safeguard computerised and digital system as well as maintaining usability, interoperability and maintainability of such systems.

This chapter provides background information about the Small World network phenomenon, its properties, advances and applications. The history and a thorough analysis of applications, properties and advances of Small World network phenomenon along with its constraints and challenges are introduced.

The chapter brought together the problems arising from development of scalable ubiquitous systems. Furthermore, we outlined the challenges and issues emerging from scalability, to draw focus to user-oriented system design and development.

It then goes through different elements of the Small World networks discovered and modelled using different approaches. This allows the reader to have a clear understanding of Small World network and its close relationship to, and great similarities with real world networks. We also looked at methods for modelling complex systems, in particular Small World networks from the networking and connectivity point of view.

The next chapter will start with an introduction of the SEP framework and describe our network-aware topology construction design policy that maintains user privacy. We then introduce a novel efficient routing protocol and provide a detailed design for our system.

3. SEP System Design

This chapter presents the design and architecture of SEP (Security, Efficiency & Privacy), a scalable P2P framework inspired by the Small World network phenomenon. It includes a novel privacy concerned topology construction, membership management, leader election and lookup algorithm. SEP constructs a network-aware topology grouping trusted users into clusters of peers. The SEP framework constructs network overlays and assigns routing and administration roles to high degree nodes with high capabilities in terms of computational power and memory. Such nodes are nominated as cluster heads and take administrative roles and responsibilities within the cluster. We refer to such nodes as 'Service Centres' where they act as 'Rendezvous' nodes to facilitate data communication, routing and forwarding.

In SEP, the network-aware topology construction manages network overlay, which consists of existing trusted users that construct friendly groups where members can communicate within the cluster using P2P communication. The topology starts by forming a membership group within trusted nodes and nominating a group leader: Service Centre. Service Centres are responsible for housekeeping and administering local membership and data transmission. In order to observe maintenance overhead and link stress, the capacity of the group is set to a predefined figure. This contributes to efficiency and security and ensures that the scale-free property of the network is maintained. After the network membership capacity exceeds the defined figure, it splits the cluster into two and nominates a new Service Centre to take admin responsibilities within the new cluster. Splitting the existing group into two groups promotes common interests and friendship and maintains community trust as the network grows. Even though the system clusters may have various sets of users with different interests and relationships, the common interest is built up to maintain reliability between them. The common interest is then passed through different groups particularly after expansion. Therefore, transparent topology management will associate the trusted relationships to new friendships, which in turn contributes to security and privacy. The topology management protocol within SEP ensures system scalability with effective and efficient membership management.

The Service Centre election process is crucial for establishing a trustworthy infrastructure, where the group leader is elected from within the nodes, which already have trusted friendships with each other. Each node has its say in electing the Service Centre promoting the trusted relationship. With such a trusted relationship and direct interaction, Service Centres have the group members' best interests in mind. We consider leader rejection to improve the integrity of

the system. This mean a member can choose to reject the leader. However, this does not mean that a member can block the election by simply rejecting the nomination. Instead, the node can leave the group in the presence of a conflict. Confirmation messages maintain the integrity of the system to include every node in the election process. If a node does not vote for the nominated Service Centre, it will be reminded again and removed from the group if it hesitates in acknowledging. Service Centres form a hierarchical level of clusters on top of the existing groups of nodes with direct communication between each other.

The membership management defines the rules and procedures to maintain node joins and how to deal with untrusted nodes that try to join the system. To maintain system security, two-stage verification is exercised to prevent unauthorised access. Every join request is controlled and evaluated by the Service Centre based on current associations and previous actions. The membership management provides autonomy to the system by leaving the membership decisions to the Service Centres. Full details and conditions are explained later on in this chapter.

The current unstructured P2P systems such as GIA, NICE and Gnutella use global identity advertisement for search and broadcasting. We maintain user anonymity by keeping the advertisements local. We introduce a discrete lookup algorithm that is facilitated by the Service Centre to preserve user anonymity; even when the routing is carried out within different clusters of users. Furthermore, this topology management and the Scale-free properties of the cluster contribute to a secure and efficient routing and lookup process. This algorithm can be used on both multicast and unicast applications.

3.1. Topology Construction Algorithm

This section explains the proposed topology architecture in SEP based on clustering co-efficient and arrangement of the nodes within a clustered overlay. The topology construction is proposed considering the scalability issues in unstructured P2P systems. This maintains the overlay structure as a logical network whose dimension represents potential ‘one hop’ or ‘minimal hop’ lookup routing. In other words, the average shortest path is guaranteed in this model with a focus on maintaining a trusted membership and a forwarding function. This determines the resource distribution policy and data distribution topology. We explain the lookup algorithm later in this chapter.

Although there are incentives for centralised approaches such as cost effective management and efficient communications just to name a few, large-scale distributed systems are a better fit with

ubiquitous and IoT applications. Gnutella (Adar *et al.*, 2000) is a good example for a resource distributed and unstructured system used for file sharing, but it suffers from many design flaws and does not scale efficiently and effectively (Ripeanu, 2001). Moreover, its successful operation depends on users' contribution, affecting availability and interoperability of the system.

Many solutions such as GIA (Chawathe *et al.*, 2003) and NICE (Banerjee. 2002) have been introduced to address the scalability issues, but security and privacy is overlooked within those systems. GIA type systems address scalability and propose super-node-based overlays with pre-defined clusters. However, GIA uses a global naming scheme and key based routing to implement its search application. GIA uses a blind search by implementing a 'random walk' broadcast and search algorithm. Furthermore, it does not consider user privacy and system security by directing search queries to random nodes with a higher degree of capacity. This approach is very similar to the Skype search and routing mechanism explained by Baset & Schulzrinne (2006).

Our topology construction algorithm considers clustering based on user reputation and association as well as nodes' technical attributes such as processing power, computational capability and memory capacity. A node with the highest value attributes is selected as a potential Service Centre and forms a cluster with nodes with common interests associated with each other. When new members join the system with no limit in numbers, it introduces scalability issues. It is important to address these issues at an early stage of the system design. To mitigate the scalability issues, we use the degree-proportional probability method of system expansion explained by Fotouhi and Rabbat (2013). If a cluster exceeds its defined capacity, a new cluster is established with the same configuration. Service Centres, which act as cluster leaders, support direct and trusted communication between each other. We allow numerous clusters to be formed using this algorithm to scale the system to an Internet-scale level. This ensures topology scalability.

A major Challenge in designing a scalable P2P network is maintaining the network balance (Henricsson & Abbas 2008). Service Centres take responsibility to ensure that the network topology stays symmetric. This means a uniform distribution of the nodes, which ensures load balancing within a network. Using the node degree proportional-probability method, new nodes are attached to the desired Service Centre until the overlay capacity is reached. We believe this method is the right candidate to support network expansion, by maintaining the relevant scale-

free properties of the system. Node join requests are directed to the closest Service Centre where a node receives a signed invitation from an existing member.

Furthermore, we exploit the heterogeneity of nodes to facilitate overlay formation and topology management. This includes how the network deals with topology initiation, join, leave and update of member nodes along with a detailed description of the naming scheme and housekeeping. The proposed topology management ensures network granularity and better state management.

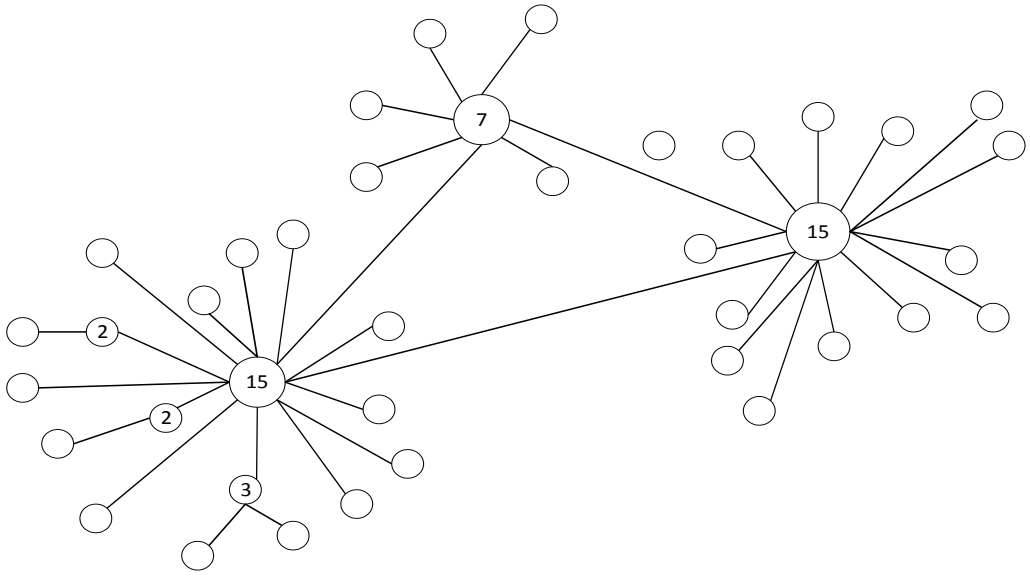

Figure 3.1 Illustration of Node Degree Distribution (Fotouhi and Rabbat, 2013)

The topology construction uses Service Centres to enforce a degree distribution of nodes within the overlay and to maintain power-law connectivity. Joining a group of nodes with an associated hub to an existing overlay will form a network with a power-law distribution and maintain the balance of the network. This is achieved by using a *merge* function, which ensures efficiency of network maintenance. To avoid network overload and achieve load balancing, the *split* function is also used to ensure the effectiveness of the approach. This has already been evaluated by (Barabási, Albert & Jeong, 1999), where they have modelled the allocation of new resources once a network has already been established, allowing the network to continue to grow without altering the Small World characteristics. Figure 3.1 demonstrates the network growth based on Fotouhi and Rabbat (2013). In our work, network growth is time independent and the expansion represents a steady-state growth with the predicted dimension of the expanded network.

The Fotouhi and Rabbat (2013) approach has been considered in merging two small groups into one overlay if the number of nodes falls below a certain limit. It is worth re-iterating that,

although SEP uses the pre-evaluated elements of Small World networks, it does not follow those characteristics step-by-step. In other words, some characteristics of the Small World have been discarded such as those techniques used in greedy routing algorithms (Jahanbakhsh *et al.*, 2010) and some have been customised for use within the proposed framework such as the use of unbiased preferential attachment.

In SEP, the model chosen for network formation and topology expansion – degree proportionate preferential attachment – is considered with special focus on node characteristics such as trustworthiness and processing power. Service Centres incorporate the degree correlation to construct and maintain a scale-free graph model topology. The formal expression of the algorithm is shown in (3.1), extracted from (Fotouhi and Rabbat, 2013). The network growth process starts off from an initial graph, whose number of links is denoted by $L(0)$ where N is the number of nodes in the network, and N_k is the number of nodes with degree k.

$$L(0) = \frac{1}{2}\sum_{k} kN_k(0) \tag{3.1}$$

Each node that is connected to other node and to the Service Centre with degree k has the following conditional probability.

$$p(l \mid k) = \frac{L_{k,l}}{kN_k} \tag{3.2}$$

where k is the number of neighbouring nodes within of the Service Centre – the degree - and l is the proportion of links. This is dictated by a trade-off between delayed communication and maintenance-cost, as the periodic sign-in would use network bandwidth to communicate with peers as shown by Adamic *et al.* (Adamic *et al.*, 2001). This would ensure effectiveness of the system and prevent unnecessary calls from adjacent Service Centres. Furthermore, if the number of nodes is about to exceed the capacity defined for a Service Centre, the *split* function is initiated by the system to divide the group into two and appoint a Service Centre for the new group. The *split* and *merge* functions are explained in detail in Sections 3.1.4 and 3.1.5.

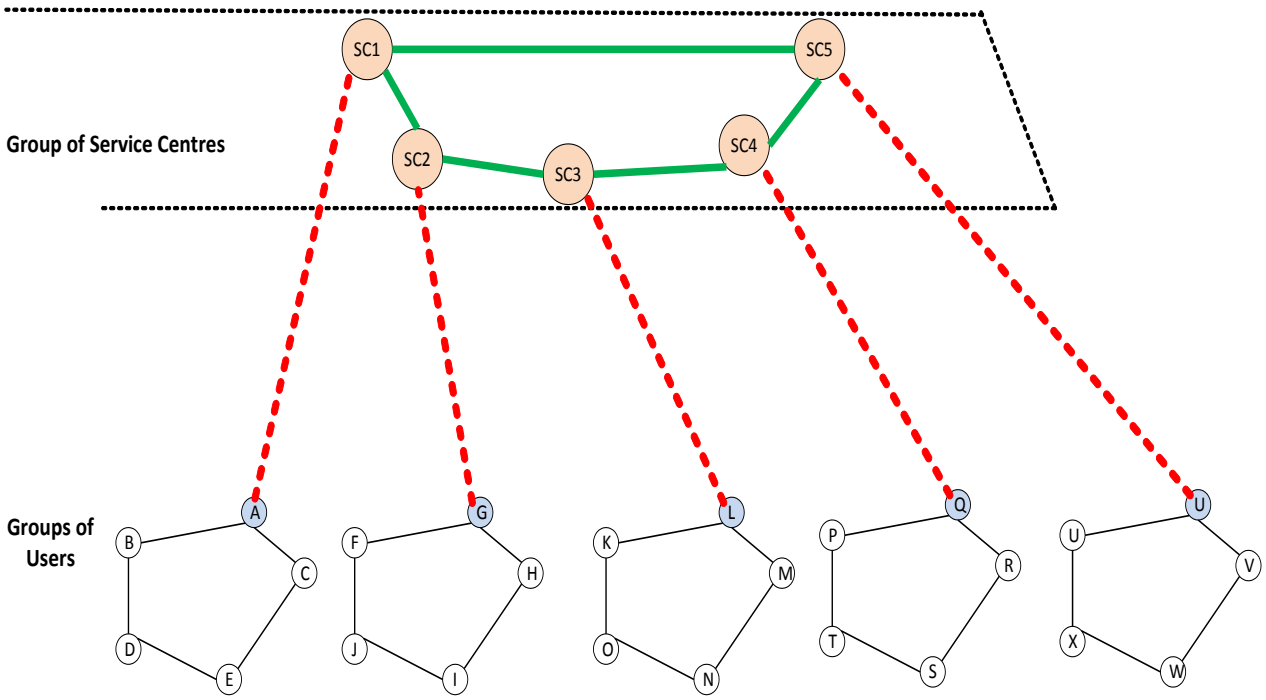

Figure 3.2 SEP Topology Construction

Figure 3.2 shows how the high degree nodes with super node responsibilities form clusters of their own to construct and maintain a trusted community. The two-tier network topology is constructed with observation of nodes' capabilities and peers' reputations.

3.1.1. Leader Election

In this section, the process of choosing a node to serve as a Service Centre is presented. This can be generally considered as 'leader election'. There are many leader election algorithms based on different objectives and criteria in the literature (Garg, 2004). For example, within 'Asynchronous Ring', a node with highest ID is simply selected as a leader, without considering other attributes. However, the naming mechanism cannot be the base of leader selection within an unstructured and dynamic P2P system, unless the naming mechanism represents many attributes of the individual node or user. This may lead to inconsistencies and naming discrepancies. Therefore, the *nodeID* may reflect its capabilities such as memory, CPU power and topological location but not all information and attributes can realistically be contained within a *nodeID*.

Skype chooses super nodes based on the Internet connection speed and maintains a list of super nodes to facilitate routing (Baset & Schulzrinne, 2006). However, there is no evidence whether they have been assigned different attributes after being selected as super nodes. GIA attempts

to choose a node with higher capacity and directs queries to nodes with higher capacity. The node capacity is measured using a random number, assigned to the node on arrival. However, the full scale of this protocol has not been implemented as a real world application due to the capacity calculation algorithm. There are also various negotiation protocols to select a leader for a group (Patterson & Bamieh, 2010) such as the following.

1. **Query-reply** protocol that involves no negotiations. This means interested parties agree on the selection without making any decision.
2. **Request** protocol where parties either agree or refuse the request with no negotiation, but the request service is guaranteed to be provided.
3. **Negotiate-commitment** protocol in which the system negotiates with all entities, acknowledges the agreement, and shares the agreement between all parties. The criteria for leader selection also includes power-based (Shah & Flikkema, 1999), heuristics-based (Dionne & Dionne, 2008) and convergence-rate-based (Johnson et al., 2008).

None of the above-mentioned leader selection algorithms is decision-based nor they are accomplished through an election process. Rather an assignment is given to a particular user to act as a leader or super node. The nominated node has no jurisdiction over the appointment. However, they can make a binary decision on selection or rejection of the nomination. Our focus is to nominate a node with higher capabilities but with the inclusion of reputation and trustworthiness. To the best of our knowledge, all of the leader selection mechanisms perform a binary decision-making process regarding leader or super node selection within unstructured P2P systems. Their system either approves or rejects the super node appointment. GIA is the only exception that uses node capacity to select super nodes. This has been implemented in Skype, which is a structured VoIP protocol. Most of the current literature introduces binary-type leader selection, considering only one attribute as criteria for being selected as a leader. However, SEP introduces a multi-dimensional approach in selecting super nodes and takes into account node capacity, location and node reputation based on trusted relationship in the selection process. The detailed description of selection criteria is explained in this section.

A node is nominated from within the group of users by the system and elected by community members after a negotiation process. The negotiation process is vote based. This is achieved by confirmation from all or a majority of the members. To nominate a member as leader, different attributes are considered such as memory capacity, processing power and location. We define an algorithm that determines the node with highest processing power and geographically closest

to the member nodes for nomination as a Service Centre. After the nomination, a voting process acknowledges and appoints the node as leader. The pseudocode for the leader election as outlined in the table below.

Table 3.1 Pseudo Code for Leader Election Process

```
/* A is the sender, SC1 is the Service Centre, CL is the Cluster */
1.  if SC1 ∉ CL then
2.        return ERROR; /*nominated leader must be within the group*/
3   if SC1 is unconfirmed then
4.    start confirmation process;
5.  else
6.    set attributes();
7.    update leaders' list();
8.    inform peers();
9.  if A∈ SC1 &A has more computing and network resources than other nodes then
10.   compute distance();
11. get Repuation value();
12. send VoteMessage(members);
13. if VoteMessage is unconfirmed then
14.    send ReminderMessage();    /*node be reminded to confirm the nomination */
15. if !VoteReminderResponse then
16.     eraseMember();              /* remove node from group */
17. if VoteMessage is confirmed && Stats = 50% + 1  then  /* if majority of nodes confirm the nomination*/
18.   if reputation rate ≥ 3 then
19.      LeaderConfirmed();
20.     setAttributes();
21.     sendLeaderAcknowledgment();
22.     setLeaderHeartBeatInterval();
```

We define the heartbeat process to sign in within the defined interval as a confirmation messages. If a Service Centre fails to acknowledge the '*HeartBeat'* message, it is assumed to have failed and a role transfer operation should take place to nominate and assign a new Service Centre.

It is possible for nodes to reject the Service Centre confirmation. We define the probability of rejection using three different situations. First, the majority of members approve the leadership and confirm it by sending an acknowledgment message. This state is denoted with state *1* where the majority is calculated as anything greater than or equal to $\frac{\text{Number of Nodes}}{2}+1$. The second situation is represented by state 2, where the majority of the nodes reject the leader selection. This occurs if the number of positive votes is less than or equal to $\frac{\text{Number of Nodes}}{2}-1$. We also consider a third situation where we can discard all other probabilities and enforce the Service Centre on the member nodes. After node selection is

complete some functions and attributes are added to the Service Centre such as Overlay Key, capacity, neighbour list and timestamp. These attributes are used to consider a nodes' suitability for leadership nomination or as a backup Service Centre in case the existing group leader leaves or fails.

3.1.2. Node Join

Like Gnutella, a node should know at least one member within the community to join. Therefore, existing friendship is necessary to complete the '*NodeJoin*' function, which further contributes to the security and privacy of the system.

Join: The join request is initiated by a node that intends to join the group accompanied by an *invitation ID* in the form of a digital *signature* of the node that invites it. To ensure that the new node is in fact a friend of an existing node, a challenge message is exchanged between two nodes to authenticate. The signed invitation is then presented to the Service Centre to be verified for security. Figure 3.3 demonstrates the sequence diagram from join request until the completion of the task.

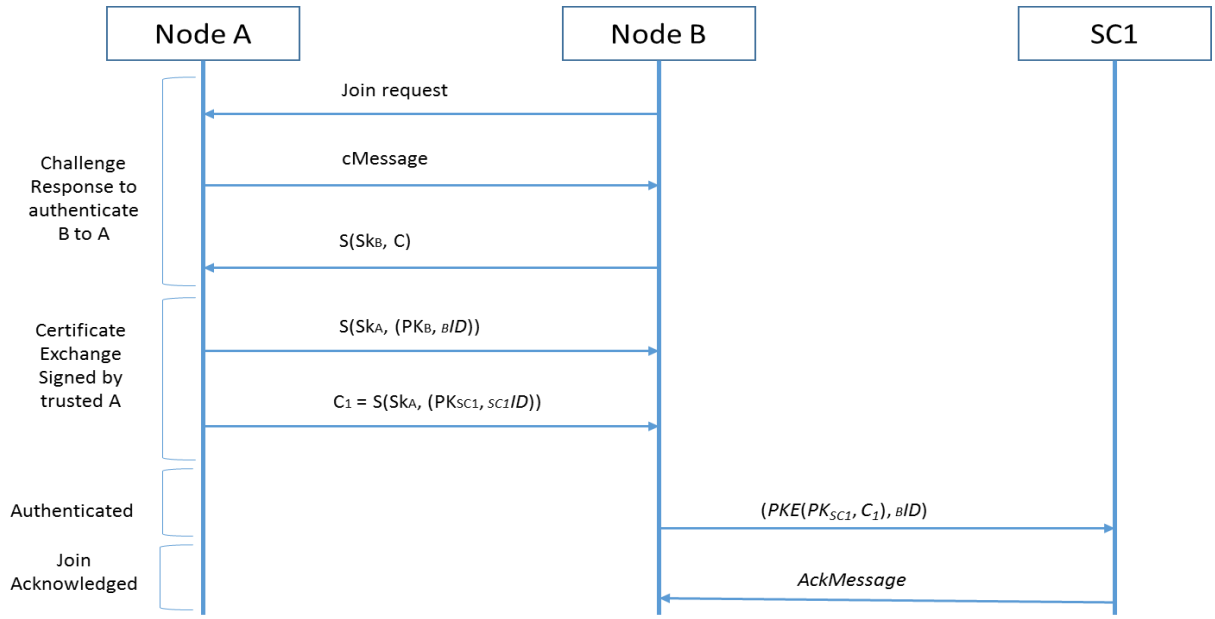

Figure 3.3 Sequence Diagram for the Node Join Process

Where cMessage is the challenging message, *C* is the response of node B to cMessage, *S*(*key*, *message*) is the signed *message* with private key *key*, PK_A is the public key of node *A*, PK_B is the public key of node *B*, PK_{SC1} is the public key of SC_1, Sk_A is the private key of node *A*, Sk_B is

the private key of node *B*, and *PKE* (*key*, *message*) is the public key encryption of the *message*. The table 3.2 demonstrates the pseudo code for the 'node join' process.

Table 3.2 Pseudo Code for Node Join Process

```
/* A is the node and G is the group */
1.   Size = getSize(G);
2.   if Size > (10k – 1) then
3.     sendMessage to Service Centre;
4.     initiate Split(G);
5.   if A ∉ G then
7.     if !SignatureMatch then
7.       remove(A); addToBlacklist(A);
8.    if AddressMatch && SignatureMatch then
9.      AddMember(A); Assign(A, Transportaddress, NodeID);
10.   else
11.      GetAddressofInvitedMember();
12.      GetPosition();
13.      GetCapability();
14.  sendAcknowledgmentMessage(); /* to neighbours */
15.  SetHeartBeatMessageIntervals();
16.  AddNodeCapability(A);
17.  AddtoNamingTable(A);
```

Several messages such as request, acknowledge and warning messages are exchanged between new member, inverter and the Service Centre to complete the node addition to the network. Node join is an important process as it may lead to a group split if the group capacity reaches the maximum. Figure 3.4 is a flow chart containing all of the entities and data transmission to accomplish the task.

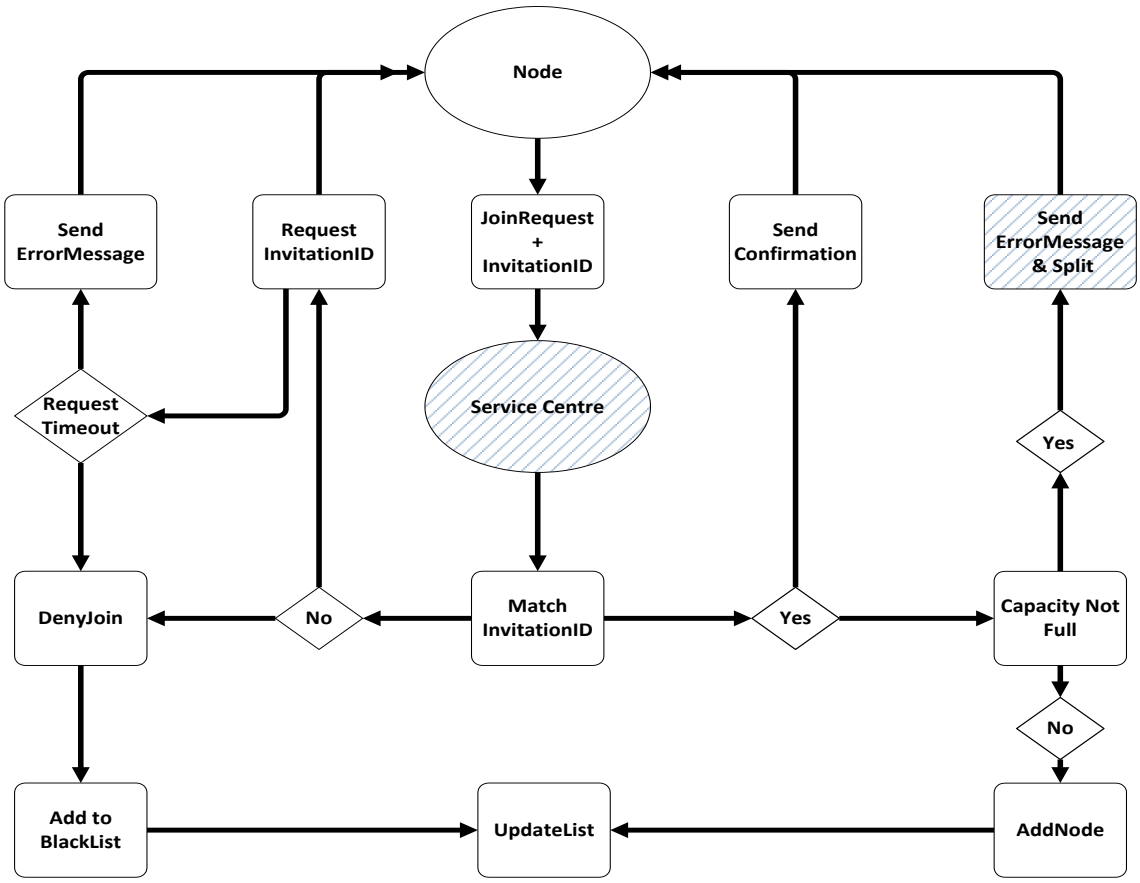

Figure 3.4 Flow chart - Add Node Function

Discovery: The discovery mechanism is acknowledgment of presence of a new node. It takes place before the node is added. As soon as a node joins a group, the Service Centre is alerted by either neighbouring nodes or response message by the new node.

Join confirm: The Service Centre matches the signature and verifies the request before the node is added to the cluster and the node list is updated with a timestamp. This is achieved by the discovery mechanism and '*AddNode*' function within the system. Considering the clustered topology of the network, this is administered by Service Centres.

Join response: The Service Centre responds to the join request by matching the signature attached to the request with the signature of an existing member of the group. Two different scenarios are considered in the join response.

- First, if the signature attached with the invitation is a match, then the node is added to the group and an acknowledgment message is sent to the node and the inviter of the node informing him of the decision.

- Secondly, if the signature is not matched or the request to send the *invitationID* times out, the join request is denied and details of the node are stored in a blacklist, with the time stamp stored for future decisions in case the node requests to join again. If the Service Centre is about to exceed its capacity upon the join operation, the *split* is initiated by the Service Centre to divide the group in two and send a message to the node informing it of this. After the split, the node is added to the group and assigned appropriate attributes in the same way as when a new node joins. The topological location the nodes determines which of groups they will be added to.

3.1.3. Node Leave

When a node leaves the network, it follows the departure protocol to maintain the network balance and the integrity of the network topology. The constant update of the node list ensures a minimal effect on lookup and multicast algorithms. If a node leaves the group, an acknowledgment message is sent to the Service Centre and its neighbouring nodes so they can update the list. After that, the *Update* function removes the node attributes and adds one to its stored *maximum capacity* value. If a node leaves the group without informing the Service Centre, it is classed as an 'ungraceful leave'. Ungraceful leaves are detected during the heartbeat message exchange when there is no response from a node.

3.1.4. Group Split

Each Service Centre maintains number of nodes and state information by exchanging constant *sign-in* messages at defined time intervals within the local group. This mechanism maintains the Service Centre membership and refines the group by asking members to register using *sign-in* intervals. If a member of the group is idle, this will trigger a wake-up call to move to the '*ready*' state. Also, this allows members of the group to dissociate from the members who left the group or have been evicted.

The Group size and state are checked periodically by the Service Centre to observe the capacity and status and to perform appropriate actions to maintain balance. Every group within the SEP system maintains a number between the minimum defined value and maximum capacity. If we define the membership ratio as 10:1, this will ensure that a minimum of 10 nodes per Service Centre exists within the topology. If the number of group members exceeds the maximum capacity, then the *split* function is initiated to split the cluster into two halves. This ensures load balancing within the system and to maintain availability of services. If the number of member

nodes exceeds the defined capacity, a split function is initiated and a message sent to member nodes. The back-up Service Centre takes responsibility and forms a new cluster. Any node wanting to join the newly created cluster exchanges request messages and acknowledgments with the Service Centre.

3.1.5. Group Merge

A cluster size is evaluated by the Service Centre regularly to compare the maximum and minimum value defined. If the number of existing group members falls below the defined minimum value, the Service Centre initiates a *merge* function to join the existing group with another group share similar interests. Since neighbouring groups have closest common interests with the group, the merge function directs the members to the closest neighbours. It is normally the closest group in terms of topological location. In merging a small group which falls below the minimum number defined, the leader of the larger group will maintain the position as a Service Centre and the sole leader of the group. The *merge* function may introduce malicious or misbehaving nodes who may oppose joining a new group or try to reject the new leader. A node exhibiting such behaviour will be forced either to join the group by confirming the new leader or to move to another group.

3.1.6. Naming Table

The naming strategy and identity management is an essential element of the networked communications. Therefore, within a ubiquitous system, each smart device is an expression of the owner and may represent some or part of their attributes (Keerthi *et al*., 2013). The group of nodes which form the overlay has an indexing table similar to DHT, which stores nodes' IDs, IP addresses, node states, neighbours' information and associated attributes. The node state and all other information are stored in the *naming table* within the Service Centre. This is only true for the nodes within the same group. Each node is assigned an identifier by hashing the associated IP address. The choice of the identifier and the length of the identifier is based on the one implemented in Chord (Stoica *et al.*, 2001). The key length is *n* bits therefore giving a choice of 2^n identifiers to assign. Consistent hashing ensures the integrity of the identifiers and eliminates the possibility of duplication.

The *naming table* within the Service Centre keeps details of nodes and node sets such as IP address, *nodeID*, node role, type, state as well as information about neighbouring Service Centres and topological network location. A prefix identifies that the node is assigned to a

specific Service Centre. Therefore, the whereabouts of the node is also kept within the naming table. Since the node information is maintained and advertised locally, it does not impact anonymity. This prefix supports the globally visible and reachable unique identification by associated Service Centres, which integrates with the IP addresses assigned to them. Also the state of the neighbouring overlay and *nodeID* is kept within the naming tables. There are different states considered in dealing with membership change. These are *Active*, *Idle* and *Failed.*

Active nodes are those that can be communicated with by peers, therefore reachable in case of any request. Routing requests are forwarded to nodes with *Active* status. Failed nodes are those that fail to communicate with other peers. This can happen when they leave the network and the network list has not been refreshed to renew memberships within the naming tables. *Idle* nodes are nodes that have been inactive for a long period of time, but they are peers that can potentially still be reached.

Each node connected to the network will join the naming table list and will be assigned a *nodeID* and associated attributes. The naming table will shift the list when a node leaves or a group is dismantled and will create new space for newly joined nodes and groups. A minimum of one link exists between adjacent overlays and an aggregate message is sent to the Service Centre to ensure consistency as well as integrity within the network. In case of failure a wakeup call message is sent to the neighbouring nodes or Service Centre. In response the state and information about the nodes is aggregated within a time interval using short messages, which will subsequently be passed to the neighbouring overlays. The Service Centre maintains these records and update the record periodically. Each node will have active, idle, or unavailable state stored within the naming tables.

The *nodeID* has a numerical prefix identifier that relates to the group the identified node belongs to. This will establish a topological location for the nodes, mapping them to the overlay set with links to neighbouring nodes along with other sets within the network. Upon arrival of a new node, the *nodeID* is assigned based on the locality of the set and the information is registered in the naming table of the Service Centre which the node is joining, along with relevant attributes.

3.2. Network-Aware Message-Forwarding

The SEP topology design supports lookup, message-forwarding, multicasting and broadcasting of services in a discrete manner. The Service Centre acts as a cluster leader and administers the 'forwarding' operation. The 'Node Handler' function is responsible for delivering a message from its source to its desired destination. If it is a search and broadcast operation within the local group, P2P communication is considered. If the communication with a node that is outside of the group, the Service Centre forwards the message to the corresponding Service Centre of the destination node, allowing it to be delivered to the destination node. The full identity of the source node is only known to its Service Centre and the destination node maintains anonymity within the process as far as possible. To ensure user security and privacy, the forwarding hops throughout are kept as short as possible. This is accomplished using network-aware Service Centres which are linked directly to each other.

With a membership management policy in place, the next part of the design considers how the lookup and communication process is performed. In defining a lookup algorithm, many designs have been considered and many trade-offs have been taken into account. To define a lookup mechanism, we have user anonymity in mind over content security.

In order to achieve privacy in a P2P system, every developer faces two choices: self-censorship by limiting the private communication to a minimum, or to contain the user communication and improve anonymity. SEP achieves the latter by proposing a novel lookup and broadcast algorithm and by clustering users into a community of trusted acquaintances. The node list is not globally advertised in contrast to GIA or NICE. Instead, SEP uses local information for P2P communication and intermediators to facilitate communication within a group of users. Figure 3.5 shows the communication model with NICE and highlights how data is transmitted at the end host level.

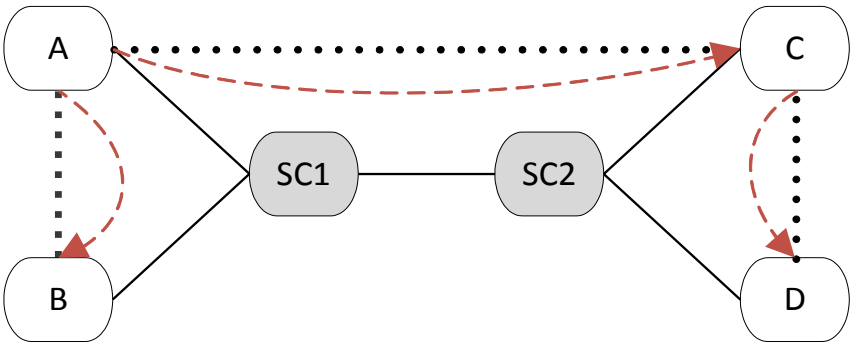

Figure 3.5 Data Transmission at the Host Level in NICE

Figure 3.6 on the other hand shows multicast data transmission within SEP administered by a Service Centre. It is an overlay consisting of two Service Centres which, administer routing and forwarding of messages between peers without significant change to the network infrastructure.

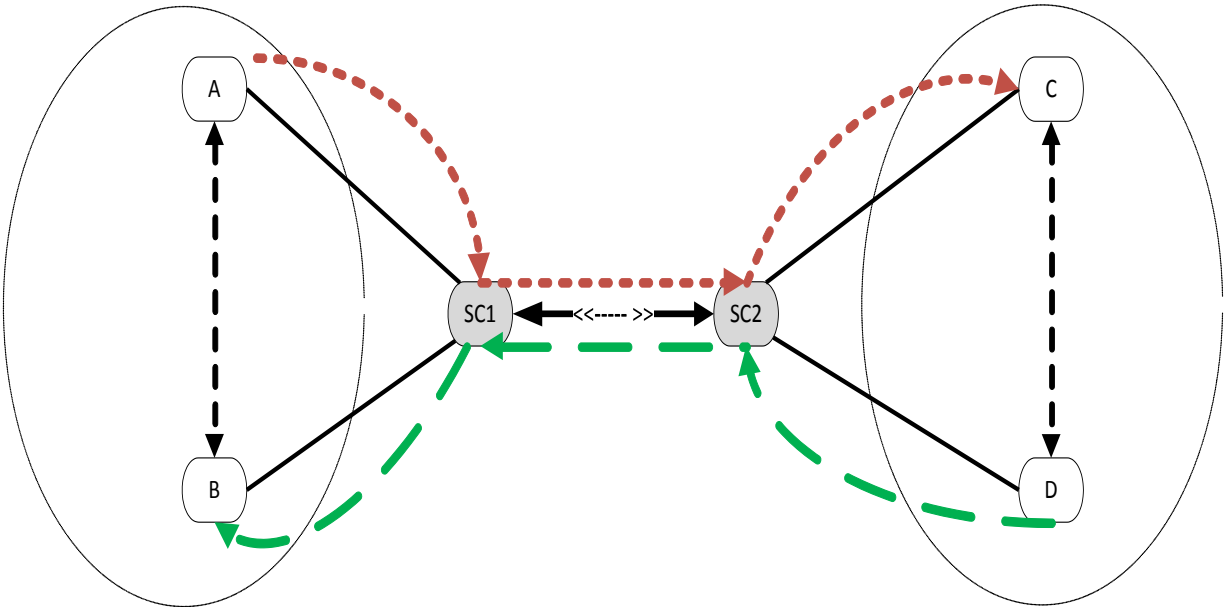

Figure 3.6 Data Transmission in SEP

The Service Centre *SC*1 coordinates the communication between local nodes *A* and *B* as *SC*2 is responsible for nodes *D* and *C*. Suppose overlay nodes *A* and *B* want to communicate with each other. A direct P2P communication is established between the two nodes as they are located within the same group. The dotted line shows the P2P channel between the two peers. As shown in Figure 3.6, the multicast message is forwarded using associated Service Centres from source to destination.

For unicast applications, the data transmission process is similar to above however, after forwarding the message from the source to destination node, a P2P channel is created for direct communications as shown in Figure 3.7.

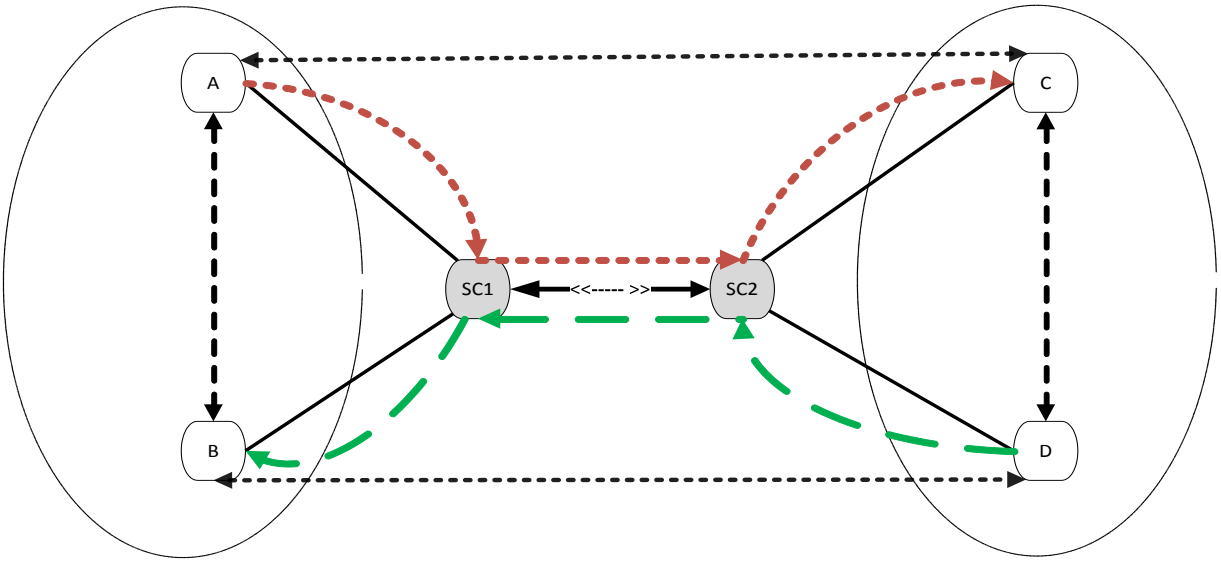

Figure 3.7 Data transmission within different overlays

In Fig 3.7, the dotted lines show the secure and direct P2P communication channel between the nodes which are located within different overlays. To communicate within the same overlay, nodes can participate in a P2P way with complete autonomy. However, if the whereabouts of a node is not known to its group members for any reason, a Service Centre initiates the communication and establishes a direct communication between the peers. An example of this can occur if a newly joined node does not know where the destination node is located due to delay or absence of an update of the naming table. Figure 3.8 demonstrates a simple communication process between two nodes – *a* and *b* - within the same overlay through Service Centre *SC*.

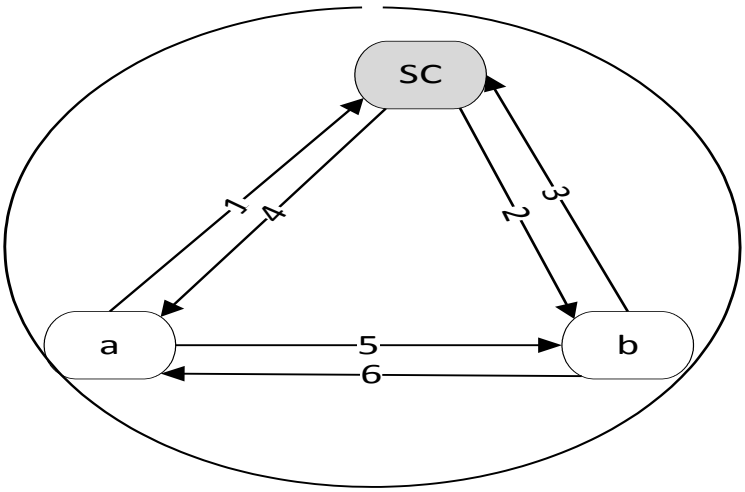

Figure 3.8 Look up within the Same Overlay

To establish a direct link between two nodes, six steps are required as shown in Figure 3.8. A query –for instance searching for a file – is initiated by node *a*, and is handled by the Service Centre *SC*, which forwards the message to node *b*.

In order to establish a connection between two nodes *A* and *B* that are located within different groups, the following protocol is followed. Node *A* encrypts the message and sends it to its corresponding Service Centre, which is *SC*1. *SC*1 decrypts the *messageID* using its private key to find out which Service Centre the destination node belongs to. It then encrypts the *messageID* with the public key of the destination Service Centre – *SC2* in this example – and forwards the message to the destination Service Centre. *SC*2 receives the message and decrypts it using its private key to determine the destination node B. Subsequently, B decrypts the *messageID* using its private key to identify the sender – node *A*. The payload is then decrypted using the private key of node *B*. Figure 3.9 also illustrates how the process preserves user identity.

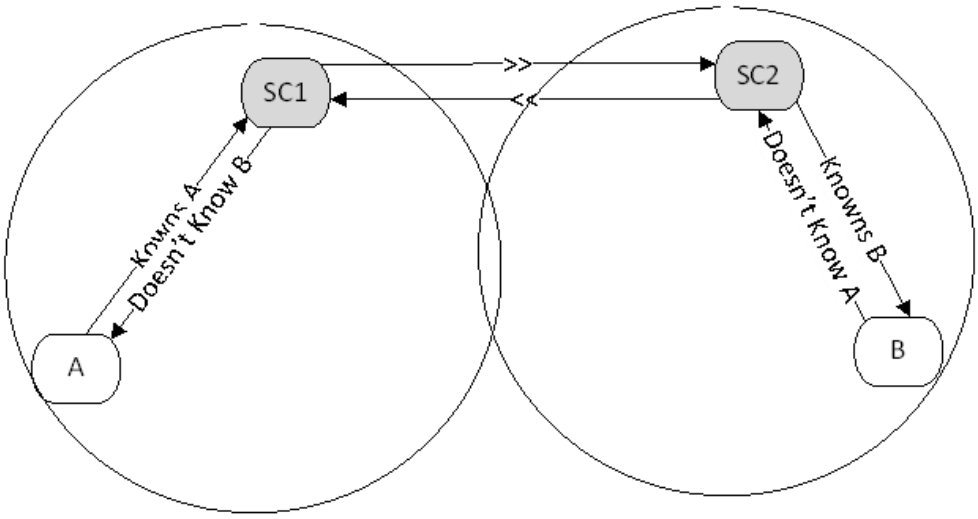

Figure 3.9 Privacy-aware Communication over Different Overlays

To be able to fully explain the routing algorithm and how a message is forwarded from one point to another, we define the data types and attributes of the main entities.

Service Centre Key (*SCKey*). Each Service Centre is assigned with a key *SCKey* that is 160 bits and generated by hashing the public key of the Service Centre using SHA-2. It dynamically maps to the live nodes within the overlay. The peers within the Service Centre are known to each other and to the service Centre however, their identities are not known to any other Service Centres outside of their group.

Source Node (*srcID*): each *srcID* represents an instance of a peer in the overlay network where the message is initiated. The *nodeID* is assigned to peers randomly using a 160 bits *identifier* space. The length of *nodeID* should be long enough to preserve and maintain the uniqueness of the *nodeID*. The construction of the *nodeID* can be generated by hashing the public key of the node using SHA-2. Each node has an *identifier* mapping it to the neighbours and the Service Centre. In defining the routing process, the *nodeID* is converted to a *srcID*, identifying the message source. The node identifier is associated with the Service Centre that it belongs to. This makes the local routing within the same cluster efficient and secure as well as determining the destination of a routed message by mapping the destination to its associated Service Centre. The *srcID* includes the public key of the peer that originates the message and sends it to the associated Service Centre to be forwarded to the destination node. Once it is advertised locally, it will not pose any privacy issues.

Destination Node (*destID*) – the target node identifier, which has the same attributes as any other node. This information is attached to a message when the 'node handler' forwards the message to the intended destination.

Message (*messageID*) – the identifier of the payload to be forwarded by a Service Centre.

NeighbourSet – every node within SEP maintains a list of its neighbours. This facilitates coordination for the node handler function of the Service Centre by providing proximity information about member nodes. Friendly nodes share this information as soon as they join the network.

Node Handler: every node is assigned a *nodeID* and a transport address upon joining the network. These are used for routing and message delivery by the node handler function. The node handler is responsible for obtaining information from the Naming Table and coordinating with different Service Centres to route a message from a source to its destination. Figure 3.10 shows the relationships between the different classes of 'node handler' function.

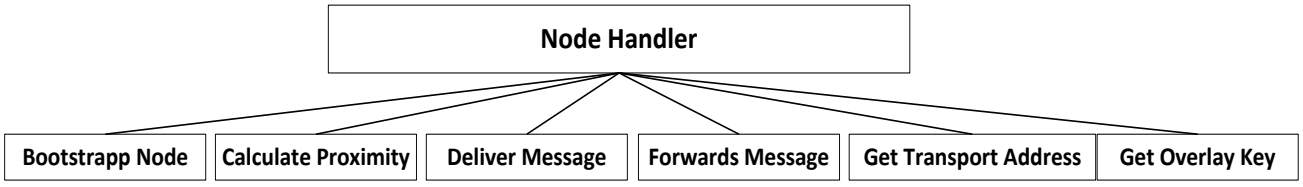

Figure 3.10 Class Diagram of Node Handler

The solution to the problem of privacy is achieved using the structure of the network group, membership management by the Service Centre and the lookup algorithm that maintains the anonymity of users. Within most unstructured P2P systems, the decisions about routing and packet replication are accomplished at either network routers (Skype) or at end hosts (NICE). SEP takes a different approach and assigns those roles and responsibilities to a trusted entity: The Service Centres. Since the Service Centre is an elected member of the group of friendly users, the *nodeID*s of the source and destination are not passed to anyone beyond the associated group community. In order to route a packet from one user to another we define the following algorithm shown in Table 3.3.

Table 3.3 Pseudo Code for Packet Routing

/ A is the node and G is the group */*
1. *Node A wants to send a request for a resource – a file – which exists at node B.*
2. *Node A encrypts the message using the public key of B and forwards it to SC_1.*
3. *SC_1 decrypts the messageID and checks whether it is a local node or not based on the desID.*
4. ***if** it is a local node **then***
5. *SC_1 diverts the message to node B and informs node A of the locality of the destination node*
6. ***else***
7. *SC_1 identifies the associated SC_2, hashes the messageID with the destination Service Centre public key.*
8. *SC_1 forwards the messageID to SC_2.*
9. *SC_2 receives the message and payload, decrypts the messageID using SC_1's public key.*
10. *SC_2 identifies the next destination based on the partly known desID*
11. ***if** the node is NOT within SC_2's group **then***
12. *Bounce back the message with an error.*
13. *Sends an acknowledgment to its neighbours.*
14. *Updates the Naming Table in SC_2.*
15. ***else***
16. *Forwards the payload to node B.*
17. *Node B receives the message and check for signature of node A.*
18. *It then check the signature using the public key of A and its own private key.*

In our framework, we suggest that before a query is run, the source and the destination nodes and the routing path must be in a '*clear*' and '*ready*' state to avoid failed lookups and redundant traffic. This is regularly checked and update by the Service Centre using heartbeat and maintenance messages. Considering the high cost of a single query within a large-scale network, this will improve the network efficiency as well as reducing latency. The proposed lookup scheme maps keys to values through a 'Naming Table' within each Service Centre. If the state of the destination source is in an '*active*' state, then the overlay grants the look-up and creates a path from the route to the destination either directly or through an available route within an adjacent overlay. The only way to determine that the destination node is not in an '*active*' state is through its Service Centre. If the destination node is not in an active state or not available for any reason, there are two possibilities: the destination Service Centre wakes it up using a

heartbeat message and completes the forwarding process, or removes the destination node from its Naming Table and informs the Service Centre that the destination node is not reachable. If the destination node is a network resource, the destination Service Centre forwards the message to an alternative source.

3.3. Scalability

The group member generation policy defines our design for topological growth of the network. Group members form a cluster of friendly users and invite trusted acquaintances until the cluster reaches its maximum capacity. The overlay topology grows exponentially by creating another cluster adjacent to an existing one once reached the maximum capacity, choosing a Service Centre for the new cluster. The network overlay forms a logical link over the physical underlying network. In contrast to other overlay expansions where nodes are randomly attached to access hosts or routers, SEP administers the membership process to maintain security and privacy. This involves the addition of only trusted nodes to existing groups to maintain community trust. Furthermore, it maintains network balance by enforcing merge and split functions, which contribute to network efficiency. Figure 3.11 demonstrates that a new network overlay is created adjacent to the existing one, replicating existing network resources and services.

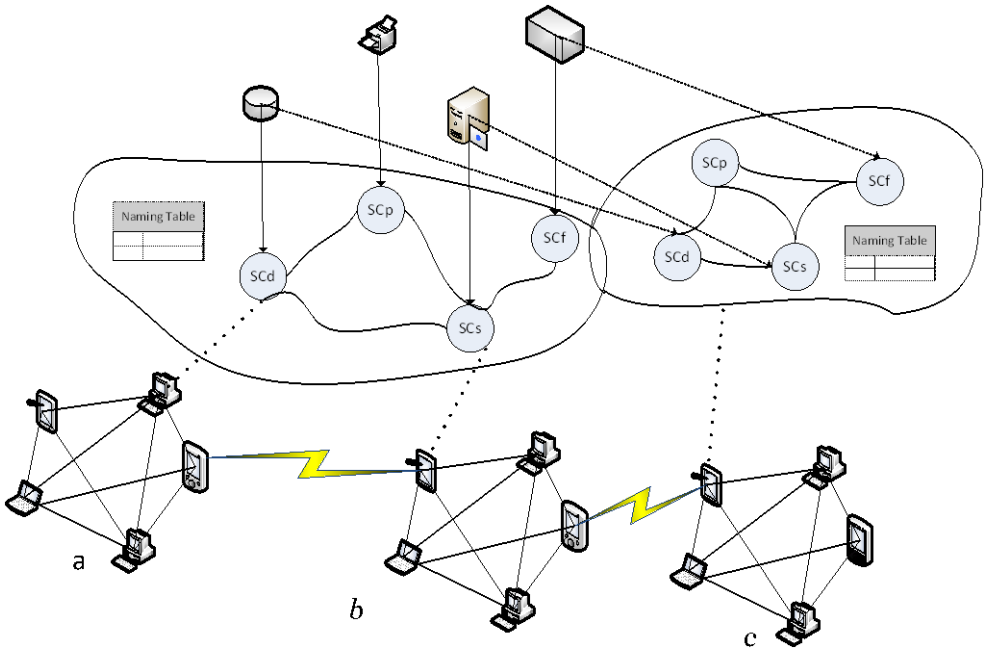

Figure 3.11 Extension of Network Overlay to Accommodate New Members

The network resources are allocated to an overlay as a virtual network to extend the network functionality. Common examples of virtual or physical nodes can be found in Cloud Services

and P2P networks. Although such devices are accessible by every node across the network via different interfaces, further interaction with such entities requires physical communication.

Additional Service Centres are created as the number of users within the system grows. This will support system scalability by allocating extra resources with minimum infrastructure or policy modification.

Network maintenance and high bandwidth consumption has always been an issue within a scalable system. The SEP system bootstraps nodes with common interests to the same group. As such, it is highly likely that the communication is done locally within the friendly peers. SEP organises nodes into a few Service Centres with large group sizes. This ensures low maintenance cost in unicast and multicast applications because of small short links. This further improves network efficiency and effective membership management of the nodes.

3.4. Privacy

Freenet, which is first developed by Ian Clarke for anonymising search on the Internet (Clarke *et al.*, 1999), was designed to provide a tool to promote free speech and discussions, allowing the expression of social political views by human rights dissidents and by those who fight for freedom of speech especially in oppressive communities. Clarke believed that the World Wide Web is a highly decentralised storage system in which search is coordinated by Domain Name System (DNS) that leaves traces of user routing information with service providers. Clarke stated that the regular Internet made it too easy to keep track of user information by providers, for instance, location (Kak, 2011).

In SEP, the distribution of the keys follows the technique used in Freenet; randomly generated keys distributed over nodes. The path of trust within Freenet enables two non-direct nodes to communicate with each other. Within SEP, this path is generated and governed by the Service Centre, while maintaining the anonymity of users. The path also provides efficient routing information, service discovery, membership updates and naming consistency improving usability, integrity and availability of the system. As stated in Chapter 4, there is a fundamental problem with Freenet, which places a limitation on the scalability of the network and subsequently, routing efficiency. The depth search for a data object may go to the destination with no trusted path. It might be true because the initial overlay for Freenet was established as a small community of trusted users to exchange data objects. Nonetheless, in a scalable system, the network may expand greatly with the addition of new nodes. In Freenet there is no

mechanism for shifting and re-arranging data objects in case a member leaves or fails. Therefore, there is no guarantee that the lookup for a data object will lead to a successful retrieval or that searches will complete in a timely manner (Kak. 2011).

Within SEP, the unstructured physical layer of the nodes and network links is organised as a well-balanced overlay where a diverse path is offered by a Service Centre if the routing process has exceeded the Time-to-Live (TTL) threshold. The *TTL* avoids infinite search and the *hop-to-live* implemented by Clarke *et al.* (1999) rejects vising a node twice ensures anonymity within a look up process.

3.5. Security & Resilience

The proposed framework provides a cost-effective and network-aware topology solution to acheive scalability by accommodating a large number of nodes and replicating network resources respectively. Therefore, the topology of the existing network stays intact and self-scaling. Maintaining the scale-free property of unstructured networks improves percolation of the network in network membership (Deng *et al*., 2011) and ensures availability. Such networks are resilient against random attacks (Barabasi *et al*, 2000). If an attacker knows nothing about the network, he must destroy every member to be able to disrupt the network operation (Gallos *et al*, 2005). However, having reliable information about high degree nodes within the network makes them candidates for targeted attacks.

SEP provides an efficient self-healing algorithm if the current Service Centre fails for any reason. Constant updates of the SEP topology ensure interoperability of the system and maintain integrity and availability. If a Service Centre fails or becomes unavailable, a backup leader replaces the current leader. This replacement process is considered to be completed within a minimum time and effort to reduce the impact on the network operation. The algorithm replaces the Service Centre as many times as possible, as long as the number of the existing group of users does not fall within the threshold that may trigger the *merge* function.

Providing a diverted path or offering an alternative path for communications with broken physical links or when the initial network path is not available is similar to the one proposed in Resilient Network Overlay (Anderson *et al.*, 2002). It provides a certain level of resilience and self-healing when facing a legitimate problem. It is convenient because autonomous and decentralised systems are independent of the central servers therefore, failure of only one will not affect the system operation significantly.

Using the clustering co-efficient to select a node to be entrusted by other users to facilitate data flow and communication has been considered as a way to reduce risk of membership change attacks (Seibert *et al.,* 2008). El Defrawy *et al.* (2007) reported a number of exploitations in P2P systems such as Bit Torrent, where an attacker sabotages the neighbour selection mechanism. In this way, an attacker forces large number of peers to believe in existence of and exchange information with an arbitrary node on the Internet. We believe such attacks are omitted by direct selection of neighbours with the clustering co-efficient. In other words, the neighbouring nodes with common interests share information locally maintaining the security by implementing a transient trust within neighbours. Such an approach has been tested by Seibert *et al*. (2008). Seibert and colleagues (2008) proposed a clustering co-efficient algorithm to prevent such attacks. Preventing risks at such an early stage is crucial for a privacy observed and secure P2P system. Furthermore, implementing clustering co-efficient improves efficiency in P2P networks where membership changes lead to failed lookups and high bandwidth consumption (Banerjee *et al.,* 2002).

3.6. Trust

The privacy and trust properties of SEP are based on the crucial hypothesis that group formation is founded on trust and that the community group members trust each other to some degree. The main limitation of this method is that it might be subverted by misbehaving nodes or nodes with malicious intent, for example acting as sleeping agents.

Malicious nodes can hinder interoperability by obstructing vote-based decisions such as Service Centre election. Other possibilities can include sabotaging split or merge functions. Malicious nodes with a high degree and high computational power with potential of becoming a Service Centre can join the group, build up their reputation until they become Service Centres at a suitable opportunity, gather, and misuse users' information. The possibility of such a case is not plausible but it depends on the level of trust a member has in forming a community trust. We assume that the formation of friendly relationships and confidence is based on a genuine trust and no misappropriation of such belief is going to occur within the group members. The only to mitigate a possible failure is to identify misbehaving nodes, removing it from the group and inform neighbouring nodes of this decision.

Even in real life, we are – normally – careful in choosing a friend and consider some attributes such as trustworthiness and common interests. We might trust with a new friend with whom we

are travelling around the world with our luggage, but we certainly do not share details of our financial affairs. Therefore, the SEP scheme intends to maintain the integrity of communication by proposing appropriate encryption mechanisms applied to the messages interchanged between peers. Each associated Service Centre is aware of identities of the member nodes in its group, their whereabouts and probably their associations, but their communications with other nodes in different groups will remain totally private and confidential.

3.7. Summary

In this chapter, the Secure, Efficient and Privacy-aware (SEP) architecture is presented. A novel topology construction and management is presented to form a trust-based community of users to provide scalability and autonomy to large-scale P2P systems. A new and inclusive leader election method is presented to maintain privacy using community trust. Furthermore, we described the details of the search and lookup algorithm using Service Centres, which provides anonymity to peers and maintains efficient P2P communications.

The next chapter presents the implementation strategy of SEP using a discrete P2P network simulator – OverSim – and provides an outline of our simulation results. It outlines design rationale in order to define the performance metrics to analyse and evaluate the proposed framework.

4. Implementation of SEP Framework

In this chapter, we present the implementation of the SEP framework using the OverSim (Baumgart *et al.*, 2007) network simulator. We use the experimental methodology to achieve our objectives and implement the simulation scenarios and test plans derived from the system design rationale. Furthermore, we include performance metrics to validate our research hypotheses with a plan to compare the produced results with other unstructured P2P systems in the next chapter. The testbed provides an opportunity for us to model, implement and measure a scalable P2P system and collect various statistics to allow us to validate our proposed framework.

4.1. Implementation Methodology

For the implementation of our proposed framework, we have focused on system scalability, security and user privacy issues within large-scale unstructured P2P systems. We analyse and evaluate the scalability and performance of the proposed scheme using OverSim, an open source and discrete network simulator built on top of OMNet++ network simulator.

Our network-aware topology construction approach is aimed at providing scalability and autonomy for unstructured communication of file sharing or broadcasting P2P systems. We also demonstrate that this ensures the integrity and heterogeneity of the system by providing equitable access and maintaining state consistency. The equitable access provides constant maintenance and update the state on every node within the topology.

Furthermore, we implement a novel anonymous search and broadcast algorithm using network-aware group leaders within the unstructured P2P system. Again, the aim is to create an overlay topology to support file sharing, search and broadcast functionalities. In dealing with confidentiality, our focus is user privacy, which is achieved by providing anonymity. Wherever appropriate, some trade-offs have been considered to explain the system constraints and justify the proposed design.

4.2. Network Simulator

A network simulator is a software tool that is used to model network events and evaluate the behaviour of a computer network and displaying the output in textual or graphical format. The network simulator can add virtual networking capabilities via network overlay to derive network

experiments on different scenarios and can be used to validate proposed models and frameworks. There has been much debate about whether network simulators are the right tools to validate results, especially for small scale configurations and calculations of execution time (Soren, 2007). However, in a scalable network with 1,000+ nodes, it would be almost impossible to create an environment for modelling future wireless ubiquitous networks and test availability, communication and response times using real machines and network components. The use of network simulators to validate published research has also been growing and several techniques have been developed to improve the credibility of the results (Soren, 2007). Table 4.1 illustrates some network simulators that have been used by researchers and academics to validate their results.

Table 4.1 Survey of the Most Used Network Simulators – Number of Times appeared in a paper (Henderson, 2009)

Simulators	**NS2**	**OPNET**	**QualNET/GloMoSim**
TRANSPORT LAYER & ABOVE	123 (75%)	30 (18%)	11 (7%)
NETWORK LAYER	186 (70%)	48 (18%)	31 (12%)
MAC & PHYSICAL LAYERS	114 (43%)	95 (36%)	55 (21%)

Each network simulator has particular capabilities, advantages and disadvantages. A simulation scenario may involve using more than one simulator. Sometimes one simulator is used to generate the results and another to analyse and compare the results. We chose OverSim because of the flexibility and ease of implementation, the modular layered structure and the many overlay protocols that are already included in the package. Furthermore, our choice is strengthened by the visualisation support, bootstrapping support and look up functions embedded within OverSim.

4.3. OverSim

OverSim is an open-source discrete-event simulator built on top of OMNET++ (Baumgart *et al.*, 2007). OverSim is capable of simulating overlay networks with many P2P overlays models such as Chord, GIA and Pastry. OverSim is well documented and supported, structured as object-oriented C++ programing, and offers visualisation tools and debugging to validate P2P topology construction and routing algorithms. To enable the implementation of new protocols, OverSim comes with many common functions and features that are useful for implementing overlay protocols such as:

- **Message handler:** Uses RPC and is facilitated by the Base Overlay Class that implements structured P2P protocols, a generic lookup class and API Key Based Routing (KBR) protocols. Many routing models such as iterative, recursive, semi-recursive, full recursive and source-routing-recursive are implemented using the KBR protocols.
- **Flexibility:** OverSim allows simulation and development of structured and unstructured overlay networks.
- **Visualisation support:** The interactive GUI and OMNET++ features provide a framework for visual inspection of code, a debugging environment, network topology visualisation and the ability to examine routing tables and messages.
- **Scalability**: The existing examples implementations provided with OverSim enable researchers to compare results with existing approaches. OverSim is designed to simulate large-scale networks. A network of 100,000 nodes has successfully been simulated using OverSim (Baumgart *et al.*, 2007).
- **Statistics**: OverSim enables the collection of simulation results and statistics such as hop count, number of packets sent, received or dropped as well as successful delivery or failure of communications. The output results can be exported in CSV or Octave format to be analysed later on. Python Script support is included for post processing the results and generation of gnuplot output.
- **Applications:** OverSim also includes several overlay applications such as Application Layer Multicast (ALM), Scribe, DHT and SimMud.
- **Churn**: Within a P2P networked environment, nodes join the network, participate in network operation or services, use or share resources and then leave independently. Churn is defined as the independent leaving or joining of nodes during network operation (Stutzbach, 2006). Most of the file-sharing or content distribution P2P systems rely on user contribution, affecting network structure and service delivery directly. Furthermore, churn can have an effect on network resilience and interoperability especially within the systems whose interoperation and security heavily relies on high degree nodes. OverSim uses different churn generators for simulating static and dynamic network environments, to accommodate custom configurations and the use of different parameters to reflect different node behaviours. Churn generators in OverSim are an important feature for initialising a network and creating a network topology by bootstrapping the joining nodes until the initialisation phase is complete. Furthermore, they incorporate the collection of simulation statistics such as transition and measurement time.

In order to understand the different churn approaches, their definitions and effects on different P2P overlays, the following list describes the different churn implementations provided by OverSim.

a. **No churn:** Represents a static P2P network where the number of nodes does not change. Nodes are added to the network in the initialisation period by the bootstrapping process until the defined number is reached.
b. **Life-time churn:** Similar to 'no churn', but nodes are given a time-to-live. Each node's lifetime is assigned randomly upon their arrival and a node departs once its lifetime is reached. The average lifetime is set using the *'LifeTimeMean'* parameter measured in seconds. The *'lifeTimeDistName'* parameter is used for defining the lifetimes of the nodes.
c. **Random Churn:** Nodes join, leave or migrate randomly. Nodes are assigned a random number and nodes behave based on the number. To restrict the nodes' behaviour to the defined parameters, nodes are given the probability of the three states. This enforces the network configuration based on three probabilities, namely creation probability, migration probability and removal probability. These probabilities are distributed randomly based on the network topology, scale and growth model. If we assume the join probability is 70%, then the probability of the node leaving or migrating will be 30%. The sum of those probabilities should not exceed one.
d. **Pareto Churn:** A node's lifetime is assigned in the same way as for the '*life-time churn'* case, but as a two-stage process. Pareto churn was originally proposed as a response to the heterogeneity of lifetime churn. Some nodes spend a substantial amount of time in the network, share content, and contribute to the network operation. In contrast, there are nodes that contribute a little and spend a minimum amount of time as part of the network. Pareto is a custom-made churn used to analyse user behaviour and assign churn based on user activities (Yao *et al.*, 2006).

4.4. SEP System Design Rationale

The implementation scenarios we have chosen are focused on running the SEP framework to evaluate two distinct characteristics, namely: topology construction and network scalability, and the privacy-aware lookup process. Within these characteristics, we outline the design rationales in order to critically analyse the proposed scheme. To be able to evaluate the network infrastructure, scalability, security and resilience of the SEP, we constructed and evaluated a

hybrid overlay design. This hybrid overlay created an unstructured P2P systems organised into clusters to form and maintain scale-free property as explained in section 2.2.3.

In order to evaluate the various features of the SEP scheme, we define a variety of performance metrics that we will measure the system against, and which we are able to determine from the simulation results. The next sections explain in detail these metrics and their relationship with the overall objectives of SEP.

4.4.1. Stability

Since the system is intended to handle a large numbers of nodes, it is important to analyse and understand the system stability characteristics. We evaluate and analyse topology stress to determine the network stability during membership change. Membership change includes nodes leaving, joining and failing randomly. We compare the network stability in various scenarios: with a low, medium and high numbers of nodes using various configurations and initialisation times. This helps us determine how the topology is able to handle the different operations under different numbers of nodes with different churn rates. From our simulation results we can compare the cluster stability when applying dynamic topology adaptation and clustering. To be able to evaluate the system stability we define two specific metrics, namely *link stress* and *topology stress*.

Link stress represents the physical connection between the nodes and how membership changes can affect system operation. To evaluate the link stress, we measure the power-law distribution of nodes derived from scale-free property of the topology. We generate the number of links to each Service Centre, which represents the node distribution in the topology. The number of links are calculated using the direct connection between Service Centre and member nodes.

For the topology stress, we measure the recovery time in the event of Service Centre failure. We conduct several experiments to see how quickly the system recovers from a Service Centre either ungracefully leaving or unexpectedly failing within both a small group and large-scale system. Furthermore, we observe how quickly the system regains balance and the scale-free property once the high degree node becomes unavailable. In addition, join retries need to be considered in analysing why a node join request is rejected and how node join re-tries are handled within the topology. We define membership change as a metric to evaluate the membership management of the topology, which has direct effect on system stability. It is measured to evaluate how the system can accommodate new resources once the existing nodes leave or fail.

The unit of calculation is considered as the time taken from a node leaving or failing until the topology responds to the issues with a new member replacement.

A node departure can occur because of a failure or when a node simply chooses to leave. Any departure, which involves leaving the group without informing the associated Service Centre is classed as an 'ungraceful leave'. The membership update is accomplished by obtaining membership status through a heartbeat or using neighbours' report messages. This is when an ungraceful leave is detected. As soon as an ungraceful leave is detected, the steps taken to replace it are as follows

1. The node is deleted from the member node list in the Service Centre's naming table
2. An addition to the group capacity is added to the Service Centre's records.
3. The system prepares to accept a join request.

To measure the membership changes in the system we measured the average time between each create and delete. This means a topology with *n* nodes should maintain network membership by looking at the total number of existing members and add a new member as soon as a node departs the group. This is achieved by constantly sending heartbeat messages and receiving acknowledgment messages between Service Centres and group members.

4.4.2. Scalability

Preferential Attachment (Barabási -Albert, 2002) in a power-law distributed network can be used to bootstrap incoming nodes to a node with high degree. However, applying this would lead to some nodes having too many members – "the rich get richer" – and cause a system bottleneck. Furthermore, this would introduce new scalability challenges such as bandwidth distribution and membership management. To overcome these scalability challenges, we use the proportionate degree-distribution method (Fotouhi & Rabbat, 2013) to accommodate group members within different Service Centres. Our aim is to ensure the distribution of Service Centres and member nodes will follow a scale-free property, thereby maintaining topology scalability. To maintain the scale-free property we define metrics such as the number of node limitation where we limit the maximum number of nodes allowed in the group, maximum and minimum hops allowed within a message re-diversion and topology flexibility where group split and merge is performed. To achieve better efficiency and security, we limit the number of nodes allocated to a Service Centre. In order to stress the topology, we measure the changes to the

power-law distribution as the network grows. Furthermore this ensures better distribution and load balancing, which are the main factors to ensure topology scalability.

4.4.3. The Average Shortest Path

The shortest path between two nodes is the smallest number of hops a packet can take to get from source to destination. In other words, for nodes A and B, if Y is the set of all cyclic paths between A and B, and for $y \in Y$ we use $|y|$ to represent the length of the path y (number of hops), then the shortest path length $l_{A,B}$ between A and B is be given by:

$$l_{A,B} = \min\{|y| : y \in Y\} \tag{4.5}$$

This reflects the network efficiency as the shorter is the distance, the less time a packet will take to reach from the source to its destination. Furthermore, the existence of the average shortest path within community of trusted acquaintances contribute to the security of the system.

We measure and record the number of hops from the data source to the destination node. To assess the quality of the data path, we measure the shortest path length for communications when data packets are transmitted through different links within the topology along with the number of packets lost, number of responses for a query (response count) and failed routes as a result of the destination node being unavailable.

4.4.4. Control Overhead

Network overhead represents the maintenance cost of the network operation in terms of the quantity of data packets sent or received to maintain the network. These packets include transmissions for group refinement, wakeup call messages, join and leave request messages within the network. Within SEP, the network uses maintenance, acknowledgment, instruction and aggregate messages for different operations. The accumulation of these messages is considered as control overhead. We compare the ratio of operation and maintenance packets for different groups under different churns and configuration settings. We evaluate the effectiveness and efficiency of the SEP topology and membership policy when large numbers of nodes are organised in different clusters. We argue that the overhead enforced on the system is justified to some degree if user privacy and system security are well maintained. However, in order to achieve a lower management overhead, we employ an aggregate approach where multiple groups are managed by Service Centres with constant local wakeup calls and sign in messages to keep state consistency up-to-date. For example, SEP uses an alternative route path if a Service

Centre fails. We measure the extra bandwidth required to replace the system as well as the message-forwarding cost at the application level. Furthermore, we measure packets lose when the destination becomes unavailable because of a Service Centre failure.

To be able to maintain user anonymity we use additional communication and verification. To provide security and confidentiality, we encrypt the exchanged messages, which imposes extra bandwidth on the system. The extra bandwidth is generated because of additional verification and acknowledgment to accomplish better user anonymity. We use asymmetric encryption methods for communications, which increases the data size as compared to the original clear text or the output from a symmetric cypher, resulting in greater bandwidth than the unsecured or symmetric case.

We record the maintenance costs caused by encryption as the data packets exchanged between nodes as verification messages and carry out an evaluation of it. In addition, pro-active state management is an important design goal. We achieve this by using local and pre-defined time intervals to control aggregate messages to keep state consistency within the group. We measure the bandwidth consumption within the system, including heartbeat messages, join and leave request messages and any other maintenance cost.

4.4.5. Security & Resiliency

System reliability represents the system security and its ability to recover from a random or targeted failure. Scale-free networks are resilient to random attacks but prone to targeted attacks especially if the attack is focused on high degree nodes. Targeted attacks can affect the security and interoperability of the system by directing attacks at these high degree nodes. As a high degree node has increased responsibilities, it will be relied on more as part of the overall topology. Service Centres are therefore likely to be the focus of targeted attacks.

We use various metrics to evaluate the reliability of the SEP scheme in terms of security and interoperability. To evaluate system security and the self-healing properties of the topology, we simulate targeted and random attacks on Service Centres and measure the recovery time: how quickly a Service Centre is replaced after a point of failure and how long it takes to re-gain the scale-free topology. Fault detection before the system recovery is done by exchanging ping/pong messages locally within the Service Centre group.

4.5. SEP Topology Structure

OMNET++ allows the use of multiple churn generators for a network simulation. This means that, depending on the topology defined; multiple churn generators can be used in a single simulation. This is useful when implementing the topology construction algorithm of SEP because, diverse group of users are evaluated using different churn generators.

The SEP protocol uses structured negotiations based on Service Centres for topology construction. However, application of the search and broadcasting model uses an unstructured P2P topology where users can join and leave freely. Therefore, there are two different churn generators, one for the Service Centres and one for the other nodes within the network. A trace file can be loaded in to OverSim to control and manipulate the nodes entering and leaving the network. Figure 4.1 shows the modular architecture of OverSim.

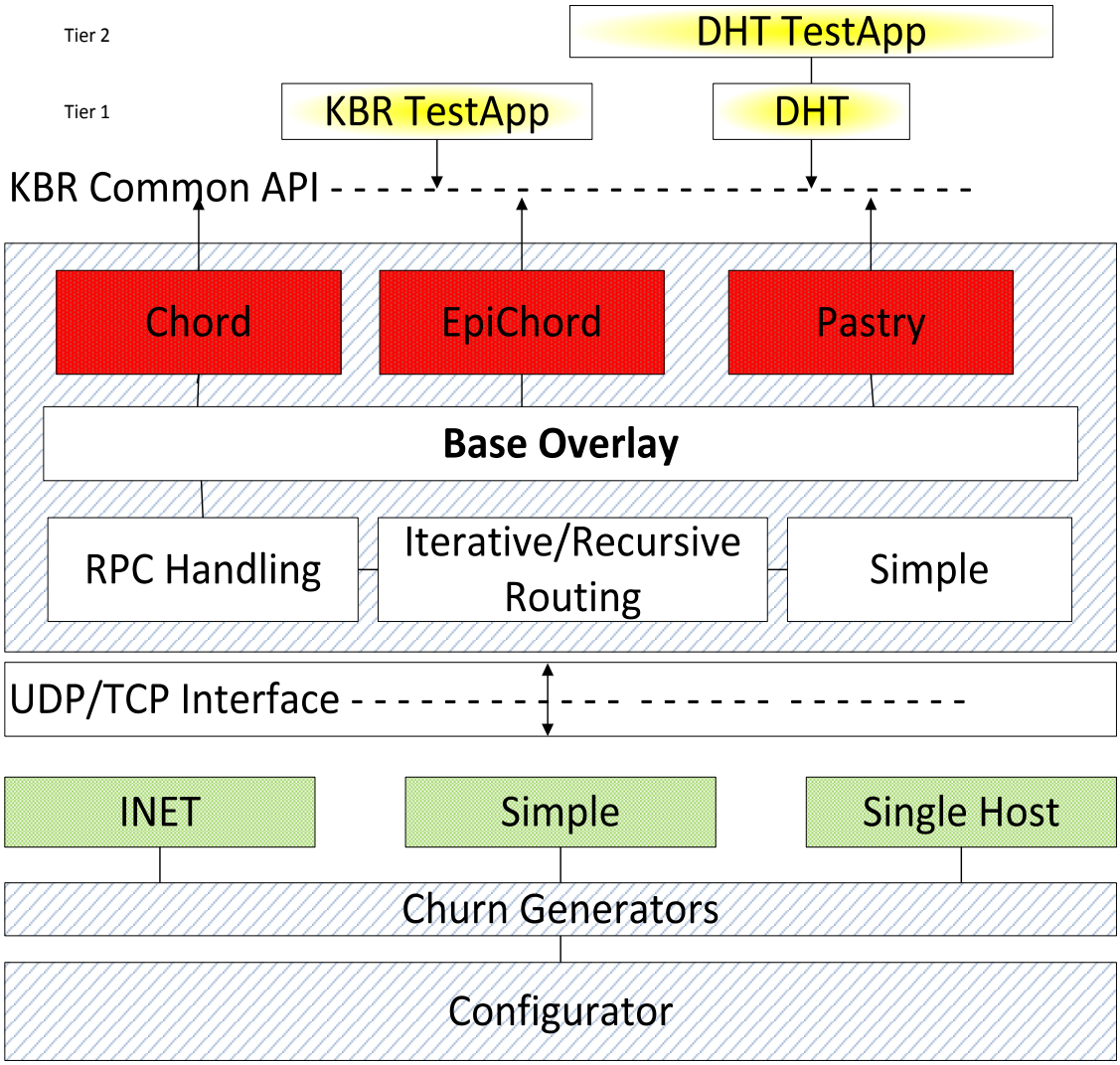

Figure 4.1 OverSim Architecture (Baumgart et al, 2007)

The topology of SEP is incorporated with the Base-Overlay within OverSim structure. The maintenance of the protocol is dictated by the underlying infrastructure of OverSim. Figure 4.2 shows the layered structure of the SEP topology integrated within the OverSim architecture.

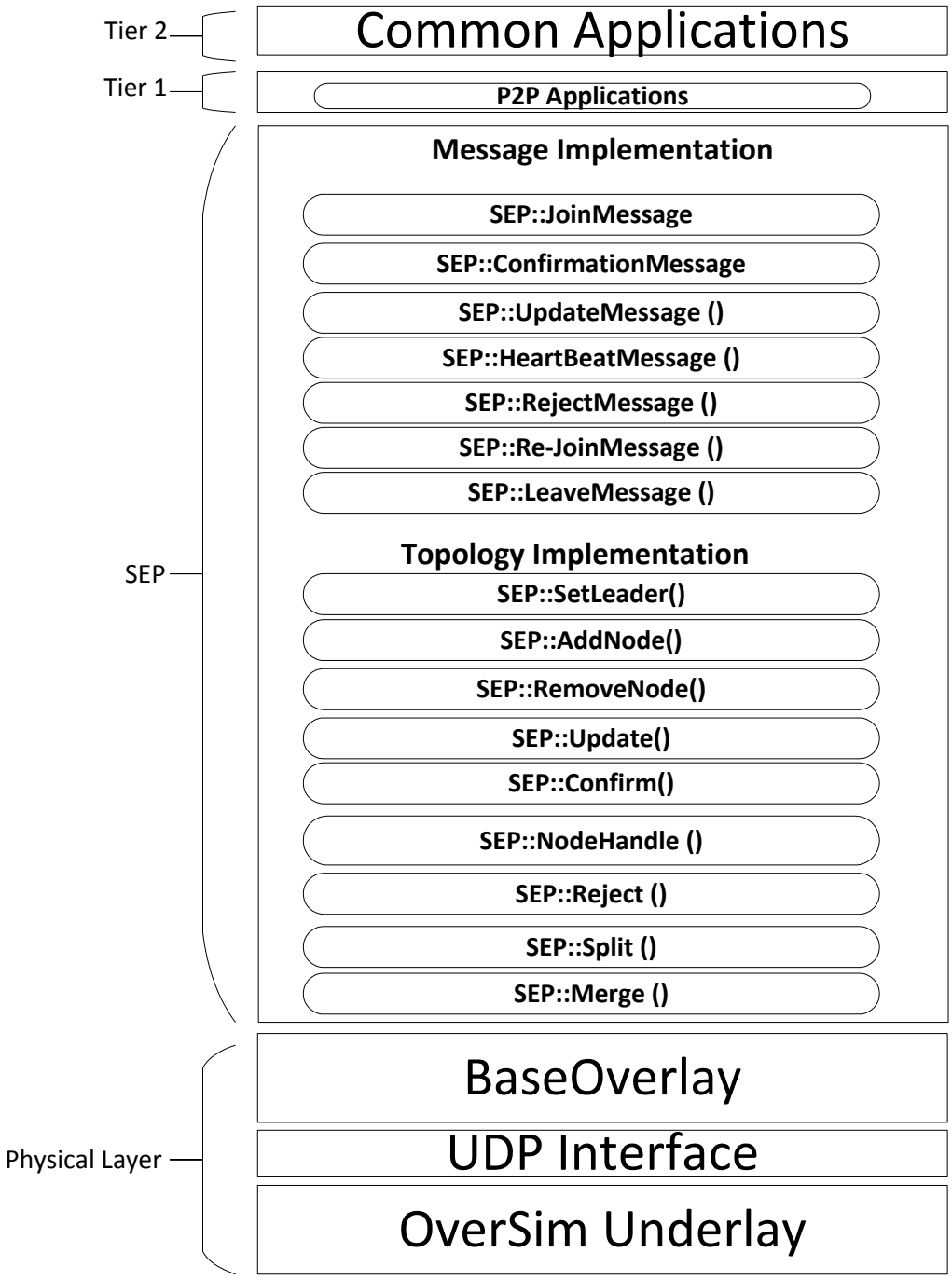

Figure 4.2 Layered Architecture of the SEP Design

The topology implementation of SEP incorporates with the BaseOverlay in OverSim Framework. The topology is implemented over the BaseOverlay of the OverSim architecture as shown in Figure 4.2.

4.6. Simulation Strategy and Constraints

In this section, we present the implementation strategy and simulation constraints. We also justify our chosen simulation settings and configurations in terms of time, size of the network, size of the group and other considerations. Some experiments were carried out with different configurations to those presented here, however the results of these have not been included because they did not display notable differences from similar or other configuration settings.

4.6.1. Number of Runs

We have selected ten runs for each set of experiments performed. We have justified the choice of the number of runs with Confidence Intervals performed for each experiment as explained in section 4.4. To manually analyse the results and evaluate the possibility of any changes within a larger number of runs, we also performed a set of simulations with the same seed and over 30 runs. We compared the accumulated results to the original sample of 10 runs, and found no statistical difference. Based on this we continued performing 10 runs for each set of experiments.

4.6.2. Simulation Time

In order to test the system, we initially set the simulation to run over a 600 seconds period and with a network of 100 nodes. However, we increased this to 2,000 seconds because we found the bootstrapping of nodes for simulations with larger numbers of nodes was taking longer than the session time, producing no statistics. To achieve accurate results for our simulations we ensured that the bootstrapping time would not take more than 1% of the simulation time. We altered the settings to record the statistics only after the bootstrapping process had completed. However, if we were to evaluate the network stability and inclusion of the bootstrapping session it would provide a better understanding of the topology stability. For other scenarios, the statistics and mean of the results are calculated after the initial period of overlay topology creation. Some systems implemented in OverSim such as Chord and GIA support short

bootstrapping, but some systems such as Koordle do not. SEP supports simultaneous join requests as well as short bootstrapping. For fairness and to improve the accuracy of the experiments, we adjusted the initial creation time to 0.1 seconds for 100 and 500 nodes, 0.01 seconds for simulations over 1000 nodes and 0.001 for simulations of 10,000 nodes and above. In addition, 10 simulation runs for over 10,000 nodes with two other systems would require an overwhelming amount of memory as much as 50GB. In the following, we describe some of the information captured.

We have run a single simulation with 10,000 and set the initial bootstrapping time to 0.001 seconds included in the complete simulation time of 2,000 seconds. It took just over 10 minutes of simulation time to complete the bootstrapping and start the statistics recording. This equates to half the simulation time being spent on bootstrapping the member nodes.

4.6.3. Number of nodes

In order to obtain performance metrics – described in the next section – we ran experiments with 100 nodes and incremented the size of the network by 100 nodes for each experiment. We continued until reaching a simulation run with 1,000 nodes. We used this strategy in order to understand the nature of the results as the network scaled. This also maintains the ratio of Service Centres to numbers of groups to maintain the scale-free property of the network that our work is based on. The OverSim developers claim to have tested simulations with up to 100,000 nodes (Baumgart et al., 2007). However, we were unable to perform simulations with over 10,000 nodes.

When attempting to perform an experiment with one run incorporating 20,000 nodes the simulation crashed before the bootstrapping session was complete. The reason for the crash was that the allocated memory for the simulation for that many nodes was not sufficient. We have evaluated the trend of the results produced by our experiments using different numbers of nodes and found it to be consistent with a linear trend. Therefore, there is no evidence to believe that the simulation with 100,000 nodes would have produce different results compared to the simulation with 1,000 nodes.

4.6.4. Experimental Platform

We used a desktop machine with Windows 7 Operation System Enterprise Edition 64-bit with Intel Core i7-3770 CPU 3.4GHz processor and 16GB RAM for all of the simulations. We

performed most of the simulations on desktop. We installed OMNET++ 4.4, OverSim-2012 and the INET-2011 framework on both machines. The simulation time was slow in real time for the desktop; however, this resulted in no difference in the outputs recorded.

4.6.5. Simulation Settings

We have developed a number of different simulation scenarios using OverSim to analyse and evaluate the design rationale and objectives using the performance metrics defined in Section 4.6. The scenarios are defined by altering the input settings for OverSim[1]. The system's inputs and outputs are defined using the SEP modules for different applications and layers such as the TCP and UDP layers. Furthermore, the following configurations have been applied for the simulations:

- We run the simulation for 10 minutes for a topology of under 1000 nodes and 20 minutes for over 1,000 nodes. The default churn generator is set to '*NoChurn*' for the Service Centres and *'Pareto'* for the remaining nodes with lifetime means set to 1800 seconds.
- Since we plan to simulate up to 1000 nodes, we set the number of Service Centres to 10 for each simulation. This means that for a simulation with 100 nodes each of the 10 Service Centres will manage 10 members. For a simulation of 500 nodes each Service Centre will manage 50 members and for a 1,000 nodes simulation each with manage 100 nodes.
- We use Application Layer Multicast (ALM) and GIASearchApp applications to perform the simulations and to evaluate network robustness. To test for stability, we have disabled probability of leader rejection by members for SEP. We also use *Scribe* for some simulations for the Tier1 application layer as defined in the OverSim architecture to evaluate multicasting capabilities of SEP.

4.7. Summary

This chapter presented the implementation strategy to evaluate the objectives of the SEP. It explains the implementation methodology with justification of the network simulator choice to validate the research objectives. It then identifies the design rationale in order to plan an effective implementation strategy to generate simulation scenarios. We present simulation settings, configuration information and limitations we had to include in order to analyse and evaluate different characteristics of SEP topology.

[1] Defined in the omnetpp.ini and default.ini configuration files.

5. Performance Evaluation of SEP Framework

In this chapter, we analyse and evaluate the design rationale of the SEP framework based on the simulation results and performance metrics discussed in Section 5.1. We evaluate the security and privacy requirements based on three main properties: *availability*, *integrity* and *confidentiality*.

Designing a semi-structured P2P system such as SEP for security and privacy concerns is an important practice as we encounter increasing numbers of violations of privacy and personal spaces (Barnett & Raab, 2006 and Gross & Acquitsi, 2005). As mentioned earlier in Chapter 4, security and privacy are often overlooked within unstructured P2P systems. In previous chapters, we presented our scalable and network-aware topology construction inspired by Small World networks for enhancing the security and privacy of the system by harnessing existing trusted relationships.

Although the main objective of our proposed framework is to provide security and privacy for a scalable unstructured P2P topology, other metrics and design motivations such as stability and performance are presented to explain the system trade-offs and to justify the proposed scheme. The availability and integrity of the system is analysed and balanced against efficient and effective membership management and communication within the SEP framework. This is presented under the topology stability Section 4.4.1. We presented the simulation results and compared them with the multi-tiered tree type clustered overlay topology, NICE. Many related work suggest that NICE is the best Application Layer Multicast overlay designed in terms of scalability, performance and effectiveness (Li *et al*., 2005; Banerjee *et al.*, 2002; Krause & Hubsch, 2010). Therefore, we evaluate the SEP system by comparison with the NICE design, highlighting security and privacy concerns where appropriate, to validate the proposed scheme. The confidentiality of the system is analysed by establishing privacy concerns and considerations and the need for user-oriented and privacy observed services.

Scalability issues have been highlighted in unstructured and Gnutella-type networks (Adamic *et al.*, 2001) which in turn, affects the security of the system. In other words, scaling the unstructured P2P systems with autonomous services introduces security challenges. These issues are exercised in the SEP framework with an eye on privacy and maintaining the system performance to an acceptable level. We analyse and validate the scalability issues using the modelling techniques and properties existing in Small World networks with a power-law

distribution of node degrees. Furthermore, we evaluate the load balancing and network growth using a degree-proportionate distribution technique. The developed network-aware topology construction in SEP can be implemented within unstructured multicast and unicast applications.

We assess the validity of the system rationales and evaluate the system performance and its security. In addition, the evaluation appraises the privacy observation of the SEP framework in response to current alternative ubiquitous system examples, namely unstructured P2P overlay systems.

5.1. Performance Metrics

In this section, we present the performance metrics. Different qualitative and quantitative metrics are considered in line with the project objectives in order to map those metrics to the SEP design rationale for performance evaluation and analysis;

5.1.1. Membership Change

The network-aware topology construction algorithm maintains topology membership by responding to changes in the groups. This includes nodes leaving or failing. We evaluate the effect of the membership change in network stability and link stress. In order to evaluate the topology stability described in Section 4.4.1, we use membership change in order to evaluate the topology management of SEP. We define the membership change as the ability of the system to allocate the member nodes after a node failure or departure. We calculate the membership change as the time taken to add a new member once an existing member of the group is failed or has left the group.

5.1.2. Topology Recovery Time

This metric is used to analyse the recovery time when a Service Centre fails or leaves ungracefully. The network-aware topology construction maintains the scale-free property of the network by replacing the Service Centre if it ungracefully leaves or fails. This metric is calculated from the time of the Service Centre failure to the time the system replaces it, making all of the services available within the group. The metric is defined to evaluate the system stability and topology stress as described in Section 4.4.1 of the design rationale.

5.1.3. Node Distribution

The membership management strategy ensures the conditional preferential attachment of nodes to the appropriate Service Centre in order to fairly distribute and allocate member nodes. The node distribution metric is considered to analyse the node stress and evaluate the effect of node stress in topology scalability. Furthermore, the effective distribution of nodes ensures load balancing, which is explained in Section 3.3. To be able to analyse the node stress, we calculate the clustering co-efficient of Service Centre to member nodes, described in Section 2.2.6. We define the clustering co-efficient as ratio of number of links to the number of nodes within the group. If the node distribution of nodes forms a scale-free topology with maximum CC of one as shown in Section 2.2.6, it will satisfy the scalability element of the design rationale. We define the scale-free element of the topology as a condition if the network growth model follows the degree-proportional probabilistic and exhibit a power-law distribution.

5.1.4. Forwarded Message Maintenance

This metric is used to analyse the effectiveness of the topology clustering, and evaluate the message-forwarding algorithm by Service Centre. This metric presents the trade-off between anonymous routing and the control overhead. The anonymous communication and message-forwarding is explained in network-aware message-forwarding Section 3.2. The messages maintenance cost is calculated as the sum of the bytes as result of the exchange of the messages between nodes.

5.1.5. Hop Count

We define the Hop Count as the number of nodes a packet should visit in order to get from its source to the destination. The hop count evaluates the ability of the system to find and maintain the shortest path in communications as explained in Section 4.4.3. We calculate the number of nodes that a packet the Service Centre takes from its source to the last node as the destination of the route.

5.1.6. One-way-latency

We define the one-way-latency to evaluate the efficiency of the topology construction, which in turn contributes to the design rationale set out in Section 4.4.3 that ensures shortest paths in end-to-end communications. We observe the time expected to deliver a packet at the destination and compute the maximum delay in delivering the message as the difference between them.

5.1.7. Application Forwarding Maintenance

This metric is used to evaluate the performance of the SEP topology construction as a base overlay to handle different applications. It evaluates the effect of an application on the overall topology maintenance as explained in Section 4.4.4 and calculates as the sum of bytes as result of running application over the SEP overlay.

5.1.8. Packet Drop Rate

The packet drop rate analyse the effectiveness of the clustering of the topology by allocating Service Centre and to evaluate the integrity of the system as explained in Section 4.4.5. We calculate the packet drop rate as the difference between the sent packets and the successfully received ones at the destination node.

5.1.9. Join Request Byte Count

In order to join a group, a node should send request to the service Centre. We define the join request byte as the cost of the process in order to evaluate the control overhead described in Section 4.4.4. We record the cost of the join request to be able to evaluate the effect of the membership change on maintenance cost. In case of a Service Centre failure, SEP nominates the backup Service Centre to take its place. However, some nodes may try to join other groups. Sending join requests to a Service Centre generates extra overhead, especially if the request is initiated after a Service Centre failure.

5.1.10. Average Response Count

The clustering strategy of the proposed scheme not only improves the effectiveness of the end-to-end communication, but also improves the security and resiliency as explained in Section 4.4.5. To be able to analyse the effective use of short paths, we define *average response count*. The *average response count* is calculated by observing the successful delivery rate of the sent packets at the destination by counting the number of messages arrived back at the source node. We define the average responses received from the destination nodes as an acknowledgment of successful delivery of the packets.

5.1.11. Disconnection Ratio

The disconnection ratio is considered to analyse the topology aggressiveness in response to random or targeted attacks and to evaluate the topology security and resiliency as explained in Section 4.4.5. The disconnection ratio is defined as a mean to calculate the system failure in

managing node membership. When a Service Centre fails randomly or due to an attack, the member nodes are directed to connect to a new Service Centre or join the neighbouring group. In some cases, node members fail to re-instate their links to any group and disconnect from the network. We measure the average disconnection ratio as result of the change within each group. We determine the *disconnection ratio* by calculating the number of nodes that fail to sign in to a Service Centre after a Service Centre failure, group merge or split.

Table 4.2 summarises the different features of the SEP scheme, which we have evaluated and the defined metrics for the validation of each component.

Table 5.1 Performance Metrics

	Stability	**Scalability**	**Average Shortest Path**	**Control Overhead**	**Security & Resiliency**
Membership Change	●				
Recovery Time	●				
Node Distribution		●	●		
Forwarded Message Maintenance				●	
Hop Count			●		
One-way Latency					●
Application Forwarding Cost				●	
Packet Drop Rate		●			●
Join Request Cost				●	
Average Response Count		●	●		
Disconnection Ratio					●

5.2. Confidence Intervals

In order to evaluate the performance of SEP in comparison with other P2P protocols, we ran several simulations and compared the results to other unstructured overlay networks. We ran simulations using a variety of churns, numbers of nodes and parameters for all of the systems

under investigation. We ran 10 different sets of simulations for each scenario and calculated the mean values and associated confidence intervals. Simulation seeds are set with the corresponding run number from 0 to 9. The confidence intervals allow better understand of the sample distribution of the overall system performance.

Statisticians use confidence intervals to express the degree of uncertainty associated with a sample statistic. A confidence interval is an interval estimate combined with a probability statement. A confidence interval consists of taking a sample and finding the mean value of that sample to estimate the population mean. Using the confidence interval, we can calculate the margin of error within our simulation to validate the significance of the results. Suppose S represents the set of samples and $|S|$ is the number of samples. We calculate the mean $\bar{x}$, standard deviation σ, margin of error ε and confidence interval ci as follows.

$$\bar{x} = \frac{1}{|S|}\sum_{x \in S} x \tag{5.1}$$

$$\sigma = \sqrt{\frac{1}{|S|}\sum_{x \in S}(x - \bar{x})^2} \tag{5.2}$$

$$\varepsilon = Z^* \times \left(\frac{\sigma}{\sqrt{|S|}}\right) \tag{5.3}$$

$$ci = \bar{x} \pm \varepsilon. \tag{5.4}$$

Where Z is determined based on the level of confidence being considered. There are four common levels of confidence Z^* used in our experiments and given in Table 5.2.

Table 5.2 Common Confidence Intervals to determine the 'Margins of Error'.

Level of confidence	**Z^*-value**
80%	1.28
85%	1.44
90%	1.64
95%	1.96
99%	2.58

We aimed at achieving a 95% level of confidence. This means that the margin of error ε for the system is represented be 5% of the samples that we have examined during the experiment. To calculate the confidence interval, we used the mean value of the results and the number of experiments carried out to justify that the simulation results actually represent 95% of the represented sample. We have calculated confidence intervals for every set of experiments we

have performed. The confidence interval pertains to what would happen if we carried out a large number of experiments and constructed large-scale data value. If we repeated the experiment *t* times, then we would expect that 95% of the confidence intervals would contain the mean of the produced results.

5.3. Simulation Results and Evaluation

In this section, we present the experiments based on the implementation methodology outlined in Section 4.1 and include the results generated by different simulation scenarios. We map each simulation scenarios to the performance metrics outlined earlier to validate the design rationales and evaluate the objectives of the project.

5.4. Topology Stability

In order to evaluate topology stability, we define two metrics namely: Membership Change for analysing node stress as explained in Section 5.1.1 and topology recovery time to analyse topology stress as explained in Section 5.1.2. Table 5.3 outlines the simulation settings and summary of the configurations for this experiment.

Table 5.3 Simulation Settings

Parameter	**Value**	**Parameter**	**Value**
Number of nodes	100 nodes	Application Type	ALM Test App
Simulation time	1000s	Max Key Length	100 bytes
Initial phase creation interval	0.1s	Message Delay:	60s
Churn type:	Pareto	Heartbeat intervals	5s
Lifetime mean	100s	Message size	100bytes
Max responses	10	Query Interval	2s
Max number of Service Centres	10	Service Centre Capacity	10

5.4.1. Experiment 1 (A): Membership Change

We perform Experiment 1(A) to evaluate topology stability as described in Section 4.4.1. Nodes are allocated a lifetime mean distributed uniformly within the topology.

In this experiment, we set the number of existing nodes and expect that the membership management will maintain the numbers of group membership to be able to ensure topology stability. We observe the average number of nodes at different time lines to evaluate membership changes within the timeline of the simulation. The network-aware topology construction changes the bootstrapping interval proportional to the number of the join requests every Service Centre receives. Once a node leaves the network, the system replaces it with new node in order to maintain the network membership. This evaluates the stability of the system in terms of membership management. Figure 5.1 shows the total number of nodes plotted within the timeline across the lifetime of the simulation.

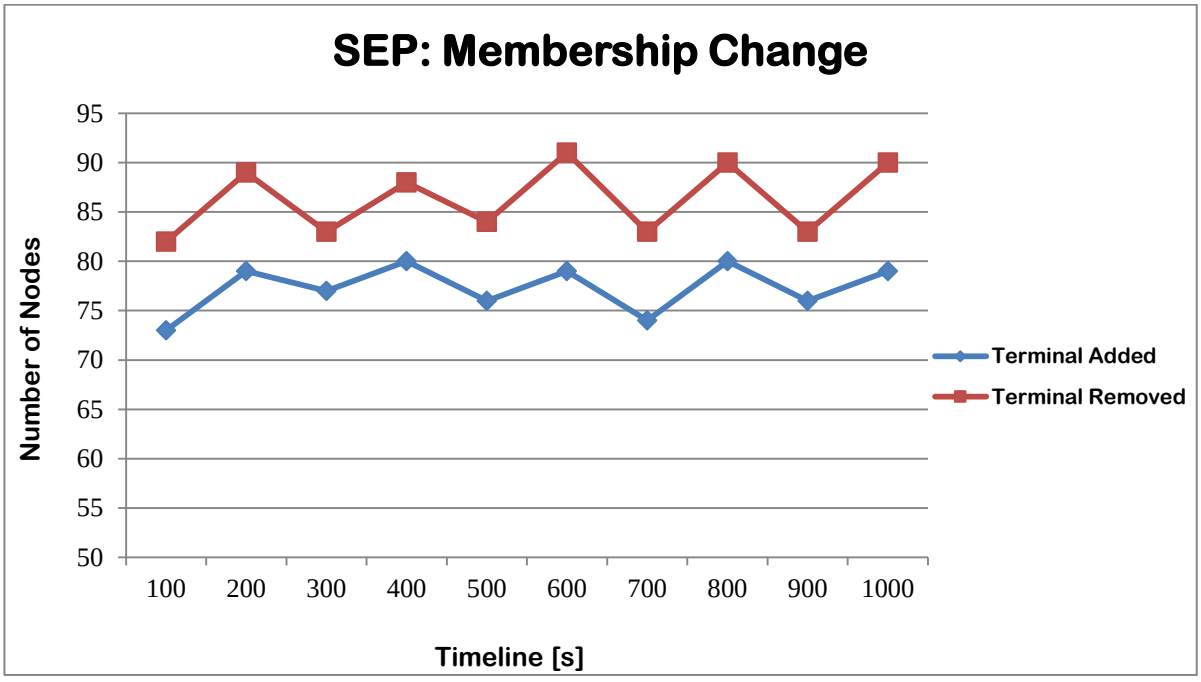

Figure 5.1 Average Membership Change in SEP

The blue lines show the timelines of the added nodes, whereas the red lines are the timeline for node leaves and node failures. The time log shows the steady and consistent membership management for our proposed SEP framework. This means that the network-aware topology management maintains the group membership with effective replacement of the network resources.

To be able to compare the effectiveness of membership management in SEP, we evaluate the performance of NICE system with similar settings and configurations. We observed the membership change over the timeline to see how NICE implements the membership

management and membership recovery as explained in Section 2.3.1.5. Figure 5.2 shows the results recorded during the experiment.

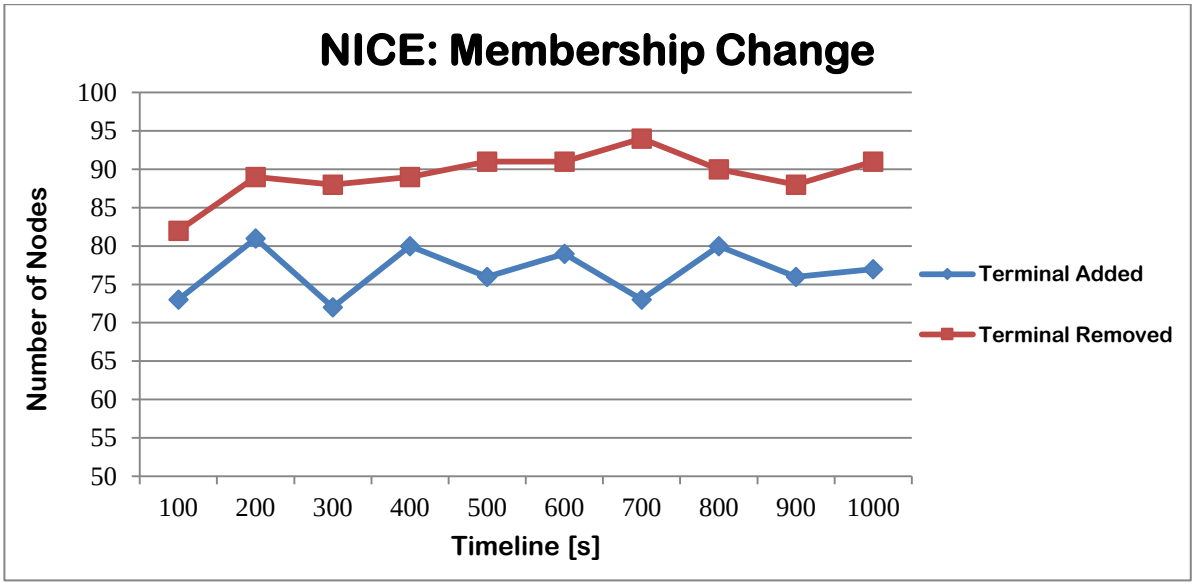

Figure 5.2 Average Membership Change in NICE

The blue time line indicates the replacement in response to the node failure during that period. This means that NICE takes longer to replace failed or left nodes.

It can be noticed from Figures 5.1 and 5.2 that SEP maintains the number of nodes effectively within the group and replaces the failed nodes in a timely manner since the Service Centres directly maintain membership information and constantly monitor the node status. Furthermore, this improves the availability of the nodes in the network. The node replacement trend in NICE becomes more effective overtime since it uses neighbouring nodes to report failed or left nodes. Nonetheless, it suffers effective response to membership change and maintain the topology membership where neighbour cooperation is limited.

To evaluate the stability within more scalable network, we increased the number of nodes to 1,000 and the simulation time to 1,000 seconds. Figure 5.3 plots the simulation results for the average of membership changes for SEP and NICE over the simulation time.

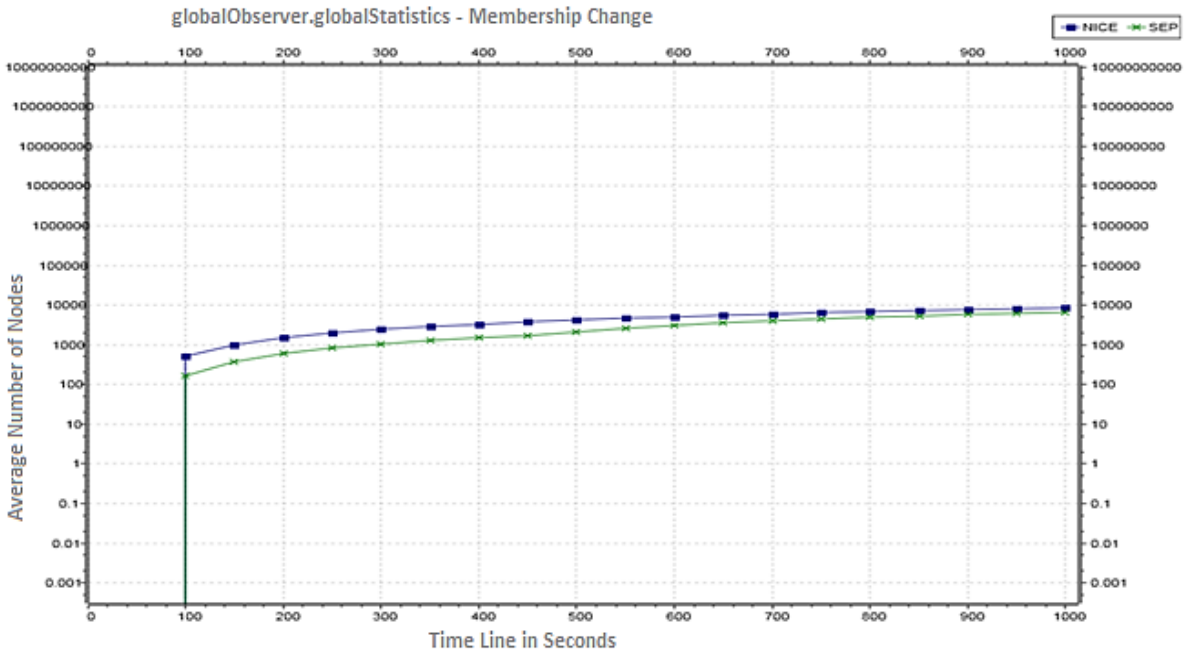

Figure 5.3 Topology Stability - Membership Change

As demonstrated in the Figure 5.3, the trend of the membership changes on both systems shows a steady line, which can be interpreted as a liner relationship between membership change and topology stability. However, SEP outperforms NICE in terms of topology stability and membership management. The number of nodes in NICE always stays higher than SEP showing that additional nodes are connected to each group. This means that NICE fails to maintain the group clusters within the defined limit. Exceeding the cluster capacity will cause topology stress. Furthermore, this may lead to resource starvation if the system is overwhelmed by additional requests.

5.4.2. Experiment 1 (B): Topology Recovery Time

In this experiment, we evaluate the topology stress in terms of system stability defined in Section 4.4.1. Topology stress evaluates how quickly the topology construction algorithm defined in Section 3.1 repairs a network by replacing the Service Centre when they fail or leave ungracefully.

Each Service Centre acts as a super node within the group, maintaining direct link with group members as well as other neighbouring Service centres. If a Service Centre leaves without informing the group members or fails, the topology construction algorithm replaces it by electing new leader as outlined in Section 3.1.1. We define the *recovery from failure* metric as explained in Section 5.1.2 to evaluate the process. The metric is calculated as the time difference

between a Service Centre failure and its replacement. Figure 5.4 is a representation of the effective system recovery with Pareto churn applied to the Service Centres shows the sum of the statistics recorded during the simulation.

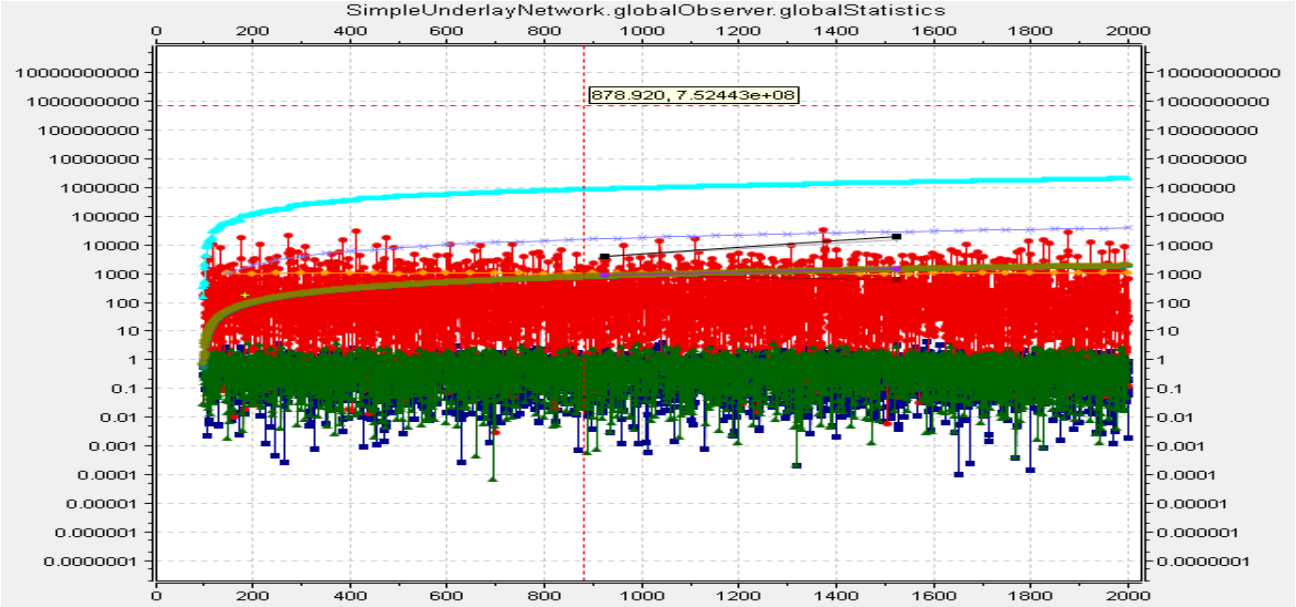

Figure 5.4 SEP Topology Recovery under Pareto Churn of Service Centres

The green lines represent the average ‘delete’ and the red lines indicates the average ‘create’ times for the topology management of 1,000 nodes during a simulation of 2,000 seconds.

The Service Centre change starts from t = 100 seconds. The times between ‘deletes’ and ‘creates’ shown in Figure 5.4 are consistent as the SEP topology effectively replaces the Service Centres once they fail or leave. The average number of nodes stays at a flat rate of 1,000 as shown by the yellow line in the figure 5.4. In other words, the group membership stays constant as the Service Centre always maintains the group membership.

We perform simulations with similar configuration and settings for NICE. The NICE cluster replacement pattern is comparable to SEP, replacing every failed cluster leader as shown in Figure 5.5. The timeline between ‘deletes’ and ‘creates’ for the NICE topology with 1,000 nodes simulated over 2,000 seconds is uneven comparing to the SEP topology. This means that, although the cluster leader recovery in NICE is as effective as SEP, but it is not as consistent as shown in Figure 5.5.

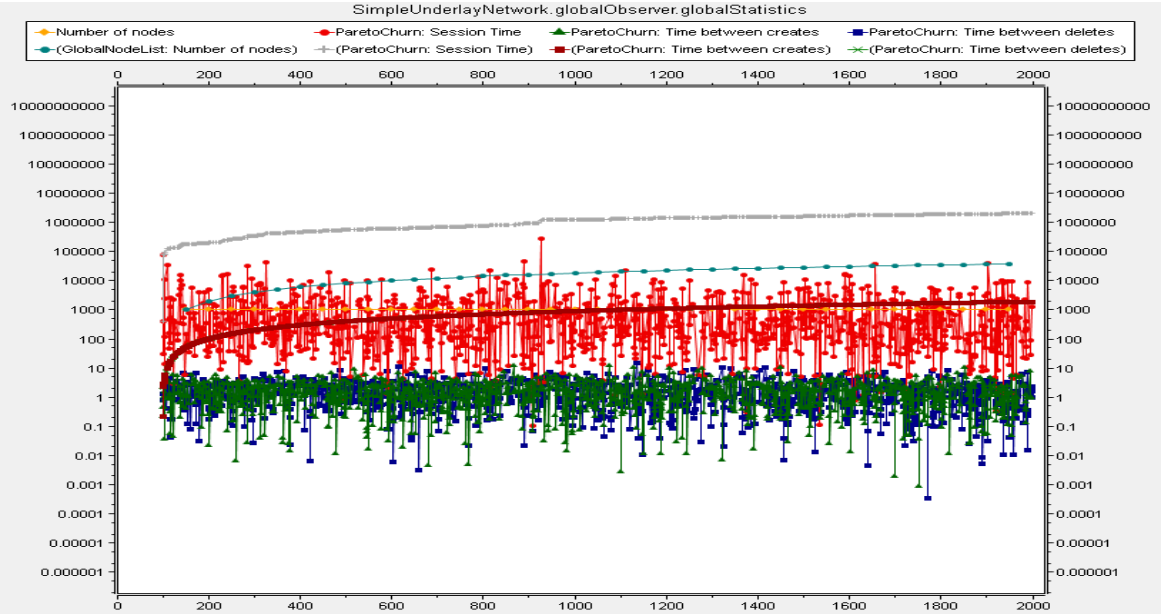

Figure 5.5 Network Stability in NICE – Cluster Leader Recovery

To be able to see the effectiveness of the approach, we have extracted the 'delete' and 'create' times for the simulation timeline for both SEP and NICE. Figure 5.6 shows the moving average for the timeline where a Service Centre is removed and then replaced over a period of 2,000 seconds.

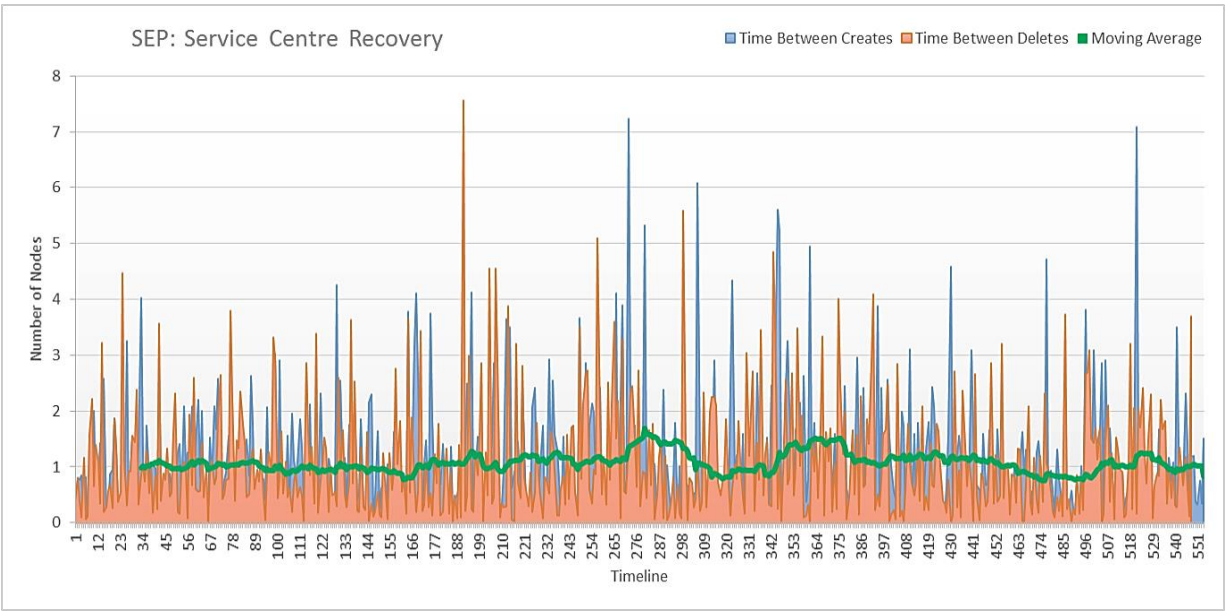

Figure 5.6 System Reliability – SEP Topology Recovery

Figure 5.7 demonstrates the moving average for cluster leader replacement for NICE.

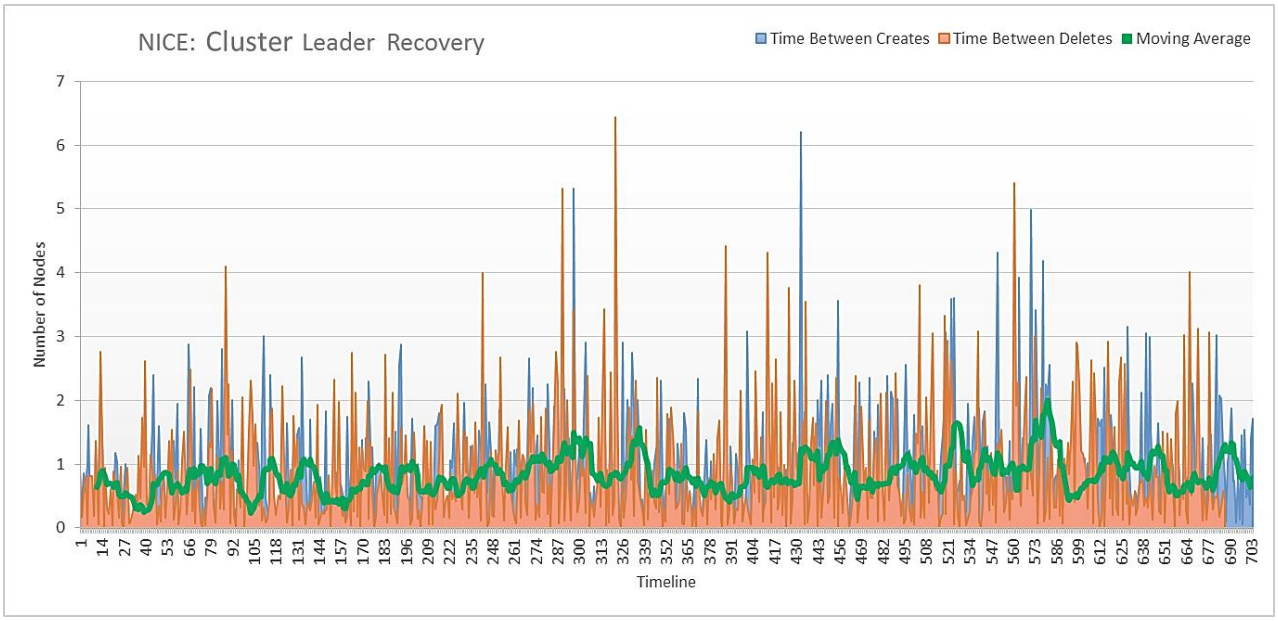

Figure 5.7 System Reliability – NICE Topology Recovery

The difference between the patterns of the moving average for the two topologies can be seen within the above two Figures 5.6 and 5.7. The moving average time for the NICE topology is more uneven than the SEP topology. This means, in practice, that the consistency in replacing the cluster leader in NICE is not as efficient as SEP in terms of recovery time from failures.

During the experiment to test the topology stability within NICE and SEP, we have concluded the following observations. First, both systems were resilient in terms of availability. There were no packets dropped because of overwhelming requests. Secondly, we found that setting the initial mobility delay to 0.1s produced good stability with both systems. Thirdly, changing the payload from 100KB to 500KB did not affect the system performance and statistics significantly.

To measure the effect of the power-law distribution and scalable clusters of users and evaluate how the network performs under different loads, we measured the network stability as an indication of how efficient the load distribution and membership management are. To measure the efficiency of the topology, we measured the power-law distribution characteristics by recording the connectedness of the nodes to Service Centres and calculating the links to determine whether the node distribution follows a power-law property.

Node stress measures the topology stability in relation to the number of attached overlay terminals to the Service Centre. The power-law property of the network is maintained by the

Service Centres attracting member nodes and retaining them by sending heartbeats at constant intervals.

We first defined the maximum members allowed in a group, the initial join and member churns within the given time scale using the OMNET++ configuration. We ran the SEP topology with an initial 500 nodes and waited until the bootstrapping process started. We then disabled the grouping algorithm and started the initial bootstrapping without a topology. Figure 5.8 demonstrates the network with distributed nodes and no topology.

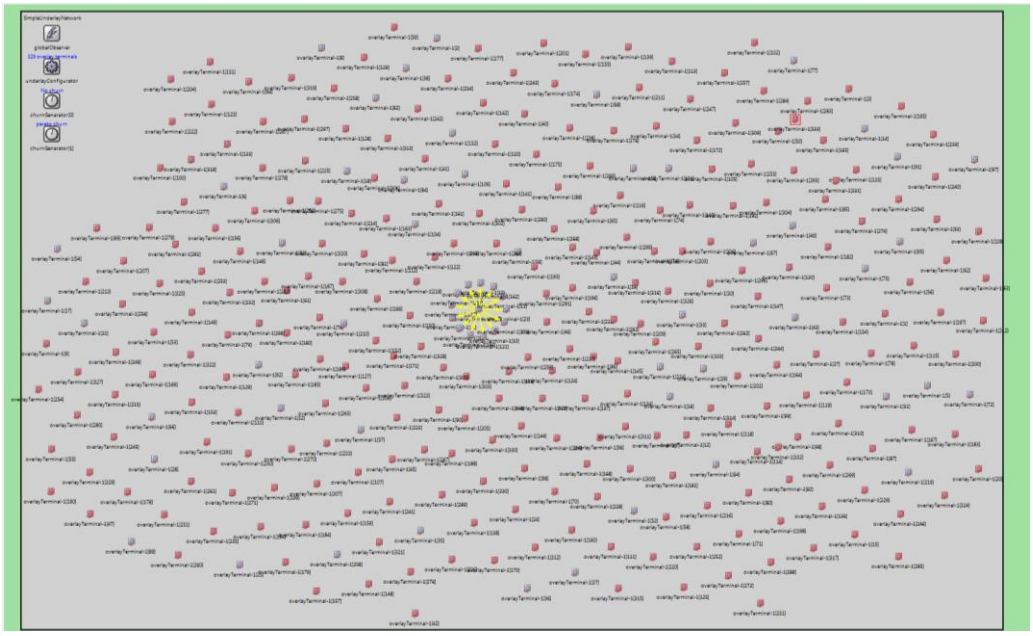

Figure 5.8 Topology Free Arrangement of Member Nodes

We then applied the clustering algorithm to organise member nodes as a group and assign them to a Service Centre upon joining the network. We define the Service Centre capacity as 500 nodes with no churn. Figure 5.9 is a screen shot of the topology interface after a join operation.

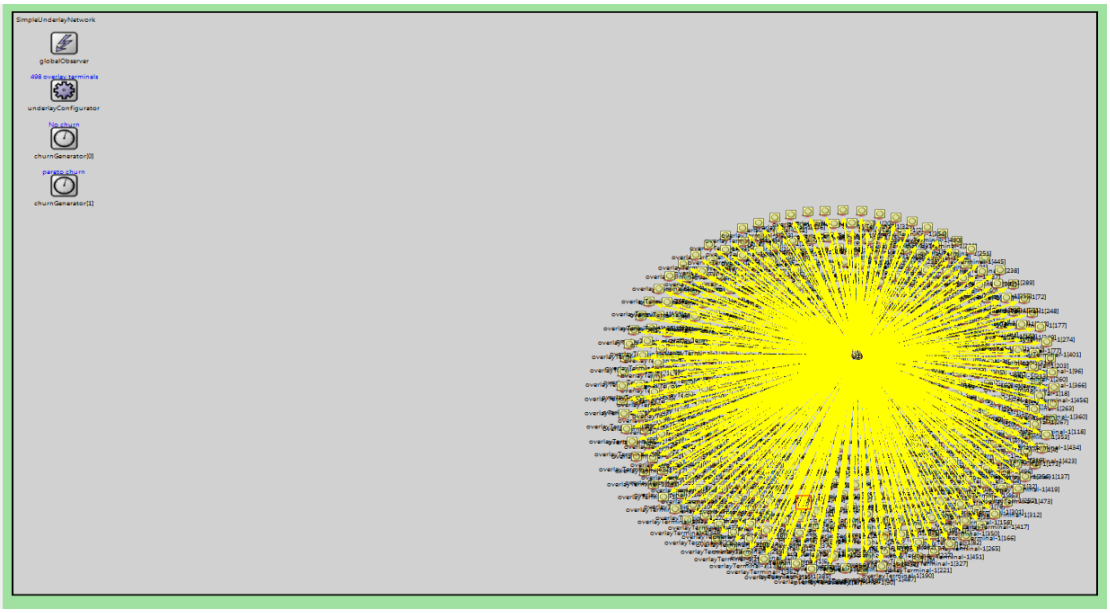

Figure 5.9 Grouping Node Members using Service Centre

We collected statistics while initialisation of SEP topology before it is stable to analyse the network stability and network cluster quality. After bootstrapping of 100 nodes, the topology showed in Figure 5.10 was formed after 100 seconds of simulation.

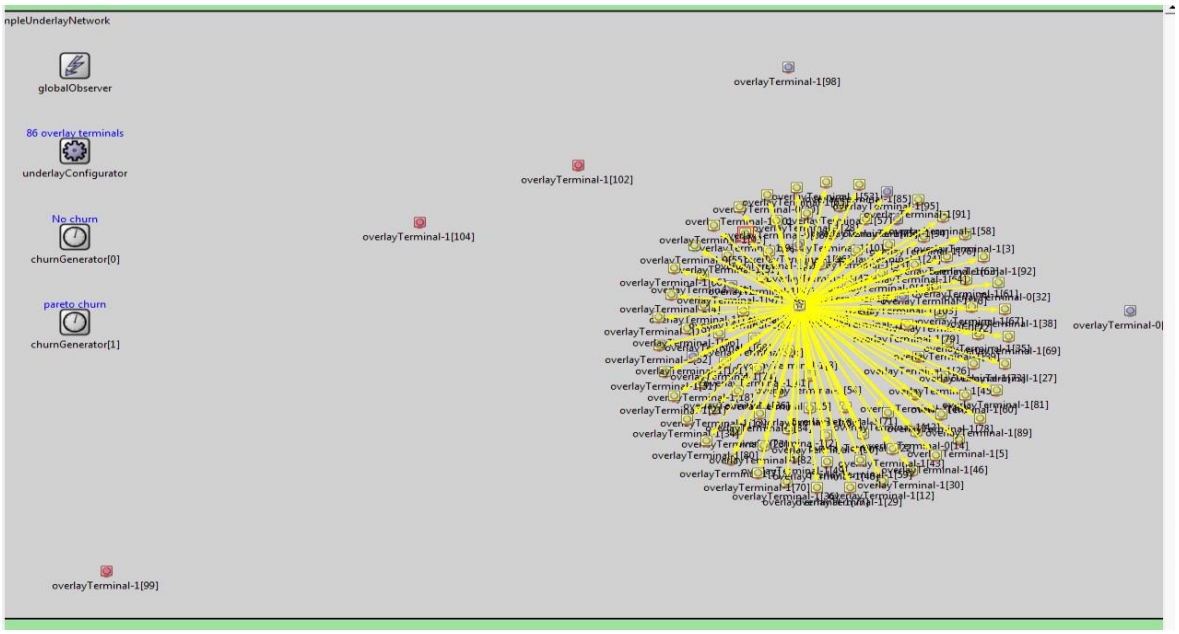

Figure 5.10 Topology with Clustering Co-efficient of Zero

A Service Centre can be overwhelmed by a large number of users subsequently claiming bandwidth within an overlay network. To manage this, the Service Centre monitors the network balance by frequently sending heartbeat messages to the members and updating membership

changes accordingly. *Merge* and *split* functions maintain load balancing and sustain the network overhead when the situation is determined due to membership changes.

GIA uses preferential attachment to divert the network traffic to nodes with the highest capacity. Consequently, the preferential attachment will move most of the incoming traffic to the node with greatest capacity, overloading the cluster, while the node with second best capacity is left with only a few links. Figure 5.11 shows two clusters established within a GIA topology with 300 members.

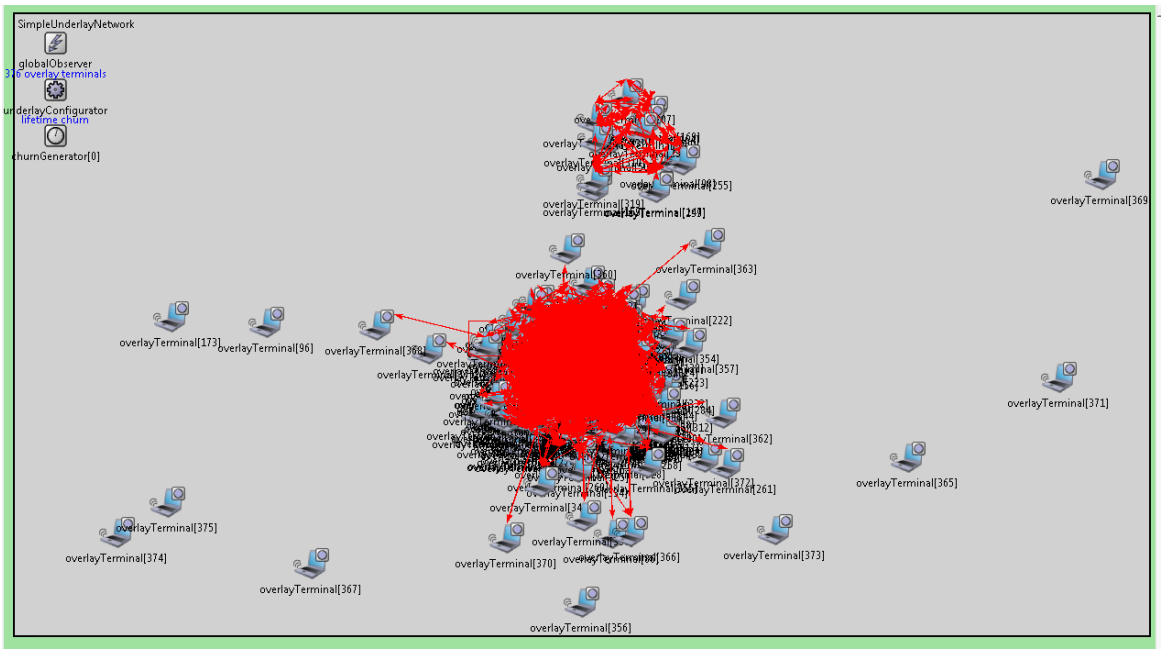

Figure 5.11 GIA Super Node Topology

More than 85% of the nodes are connected to the node with the highest capacity and the highest satisfaction level, while only 15% of the nodes are connected to the second cluster. Around 5% of the member nodes are either not connected, or have left the system.

In a scalable GIA type system, the network topology fades away from uniformed distribution because of the lack of control of the location of the selected super nodes as shown in Figure 5.11. As a result, GIA suffers from load balancing in terms of node and resource distribution. This will have significant impact on resource availability and end-to-end communications.

NICE uses Hierarchical-tree type node distribution, where cluster leaders are located at the top of the hierarchy as demonstrated in Figure 5.12.

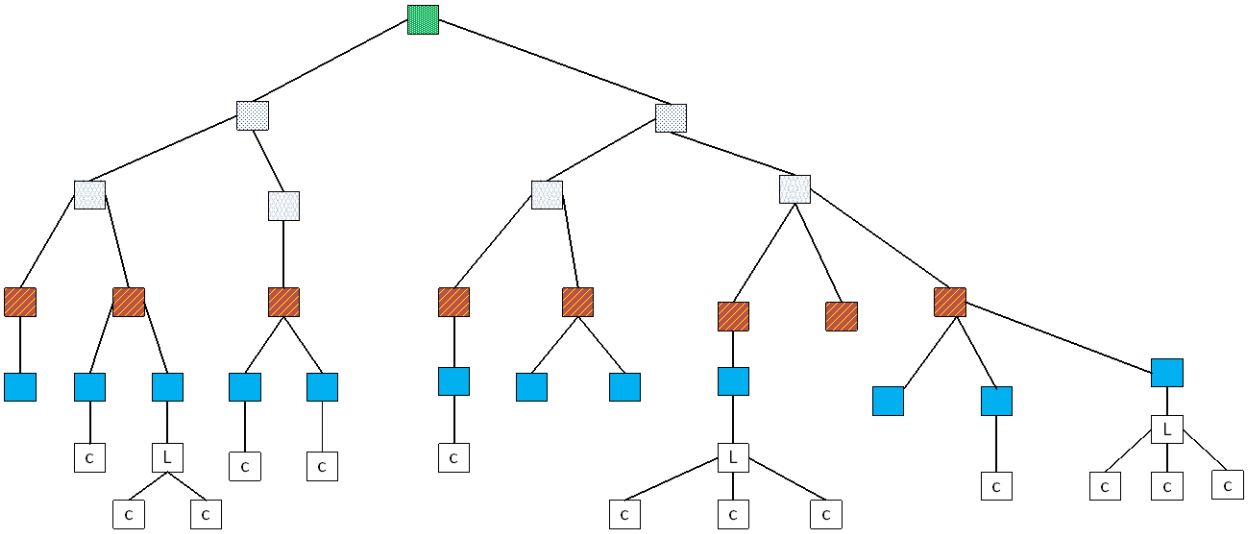

Figure 5.12 - NICE Hierarchy-Tree Topology

The cluster leaders are elected based on their topological location as described in Section 2.3.1.4. The arrangement of nodes and their cluster leaders are the effective approach in multicasting within each individual hierarchy-tree. However, it introduces challenges such as resiliency and efficiency. We explain and evaluate the effect of such approach in terms of efficiency in Section 5.5.1 and resiliency in Section 5.8.2.

5.5. Topology Scalability

We evaluated the SEP topology using the network growth model described in Section 3.3 and the scalability design explained in Section 4.4.2. To be able to evaluate the scalability of SEP, we measure the node stress and topology stress within a power-law distributed model and scale-free topology.

The main objective of this research was to achieve optimised scalability using a power-law distribution to generate a scale-free network. We model the SEP topology as an undirected graph $G = (V, E)$, where V is the set of member nodes and E is the set of links between the nodes within the group. We analyse and evaluate the SEP network to show that the implemented network prototype exhibits Small World properties. To achieve a scalable topology, we present a qualitative analysis of SEP in achieving a topology with a sustainable power-law distribution of nodes. Using node connectivity and link stress, we present the connectivity distribution to analyse and evaluate the design hypotheses that the network-aware topology construction exhibits and preserves a power-law structure.

5.5.1. Experiment 2 (A): Node Distribution.

The topology construction algorithm creates a new group, assigns a Service Centre to them and attaches the nodes that join to the new Service Centre to form a cluster. We perform an experiment to evaluate the effective distribution of nodes. Using the degree-proportionate distribution and preferential attachment of nodes explained in Section 2.2.4, we model how SEP distributes nodes to achieve better scalability by maintaining scale-free property. We define the *node distribution* metric to evaluate the effective use of preferential attachment. We determine the node distribution by calculating the clustering co-efficient of nodes within each Service Centre. After completing a simulation run of a network with 200 members, the resulted topology is shown in Figure 5.13.

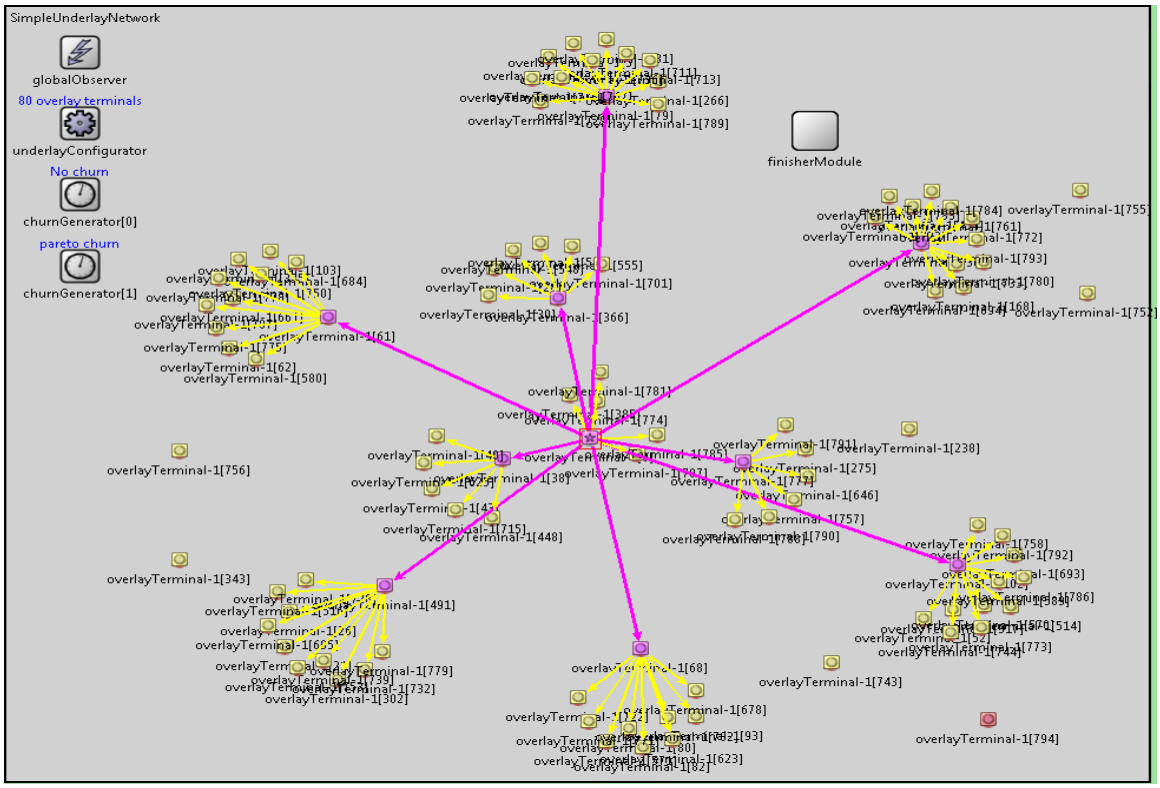

Figure 5.13 Power-law Distribution is SEP

As explained in Section 2.2.3, although the preferential attachment is an important element of a small world network, which retains scale-free property, its application may lead to a long tail or random network. As such, we use clustering co-efficient in order to enforce the conditional preferential attachment explained in Section 3.1 to maintain the scale-free property of network.

In order to achieve better model growth and scalability, we structure the topology by distributing the nodes to be proportionate to the number of Service Centres. To avoid overloading a Service

Centre and inappropriate implications of preferential attachment, we limit number of nodes allowed to attach each Service Centre. As the Service Centre reaches it maximum limit, the split function is initiated to accommodate newly joined nodes. Thus, the network will follow a power-law distribution and nodes will be connected proportionate to their degree.

To be able to measure the node stress, we calculated the ratio of the number of network nodes to the overall number of Service Centres created. If we define the network size to be between k and $10k - 1$, for a network of 100 nodes there will be at most two Service Centres. This is further illustrated via our simulation results shown in Figure 5.14.

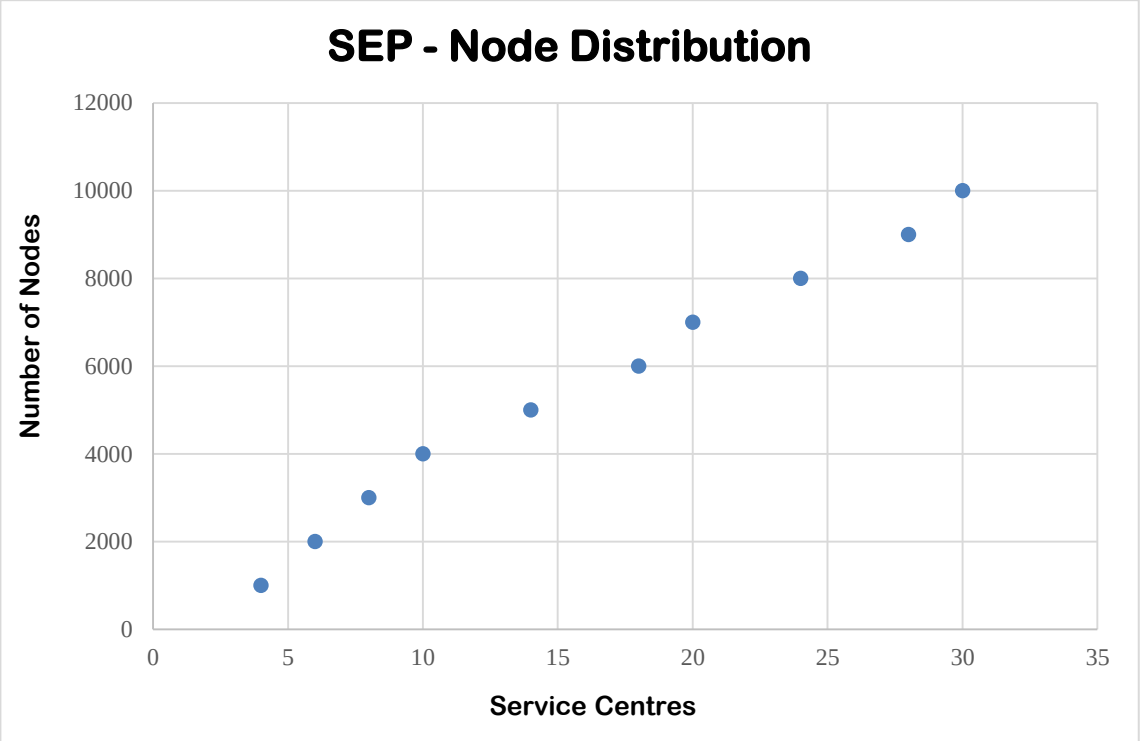

Figure 5.14 Node Stress in SEP

In order to predict the future behaviour of the topology in terms of node distribution and model the network growth, we perform regression analysis to establish the data trend line. Performing a trend function and regression analysis of the data presented in Figure 5.13 generates the results shown in Figures 5.14.

Table 5.4 summarises the residual output for the data collected from the experiment.

Table 5.4 The Residual Output - Prediction of the Node Distribution Trend

RESIDUAL OUTPUT			
Observation	*Predicted Number of Service Centres*	*Residuals*	*Standard Residuals*

1	9989.114	10.886	0.035
2	9338.517	-338.517	-1.101
3	8037.325	-37.325	-0.121
4	6736.133	263.867	0.859
5	6085.537	-85.537	-0.278
6	4784.344	215.656	0.702
7	3483.152	516.848	1.682
8	2832.556	167.444	0.545
9	2181.960	-181.960	-0.592
10	1531.363	-531.363	-1.729

The regression analysis compares the relation between two variables. The residual represents the discrepancy between the predicted and real values (Gelman & Hill, 2006). In our case we consider *X* – the dependent variable – to be the number of nodes, and *Y* – the independent variable – to be the number of links. Using the regression analysis, we interpreted the relationship between *X* and *Y* and generated the scatter plot shown in Figure 5.15.

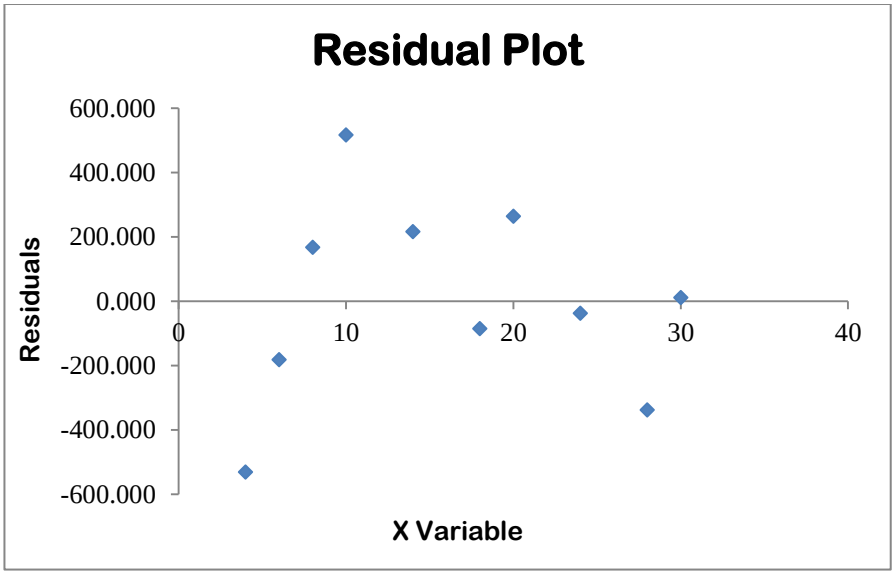

Figure 5.15 The Relationship between Nodes and Service Centres

To be able to find the best fit, we performed a regression analysis of the data and generated the trend line for the node distribution. The node residuals are scattered all around the graph as shown in Figure 5.15. Now, we can determine the power relationship between the variables and therefore can draw the trend line as shown in Figure 5.16.

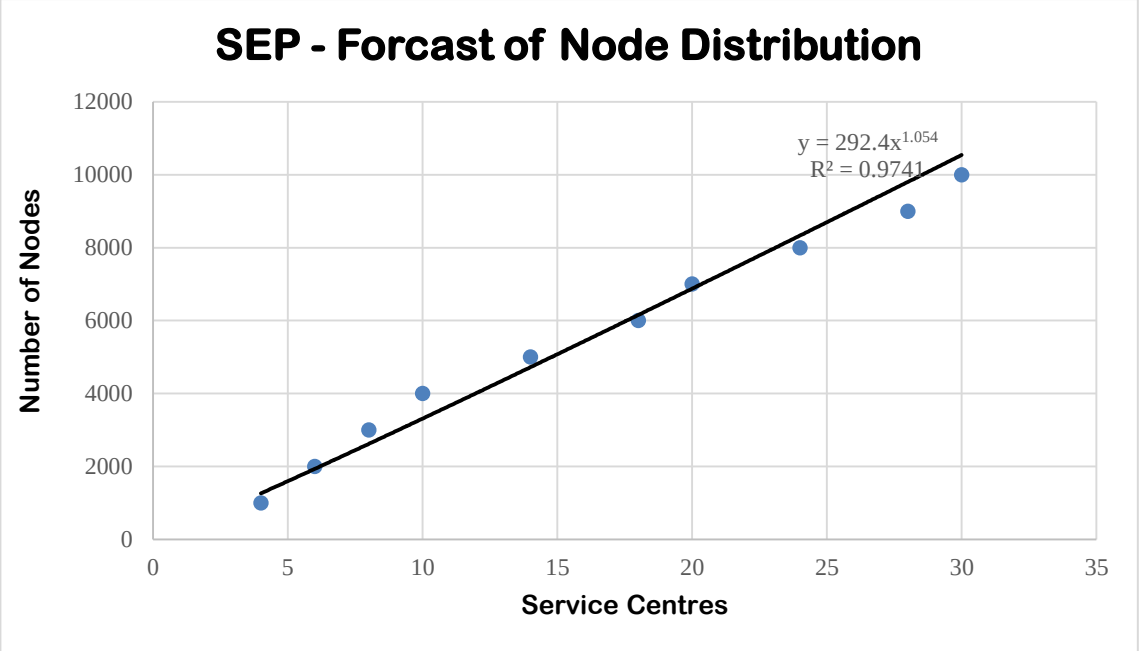

Figure 5.16 – The 'Goodness of Fit' for Node Distribution Prediction in SEP

The R^2 in Figure 5.16 is the statistical relationship between two events (Gelman & Hill, 2006) within the network growth process, namely the number of joining nodes to a group and the number of links currently active within the group. In other words, it represents the proportion of the variation in number of nodes, which is explained by number of Service Centres.

The number of active links are referred to the connection between Service Centre and their nodes which we deduce the number of Service Centres. In Figure 5.16, we use the R^2 value to interpret the relationship and to describe the '*goodness of fit*' for the set of experiments we have undertaken. R^2 value varies between 0 and 1, where 1 represents the perfect fit. In other words, all of the variations close to 1 are inherently represent a model of good fit, although possibility of a perfect fit is unlikely.

We compared the number of nodes to the degree distribution of nodes accommodated at each Service Centre. We recorded the number of links to each Service Centre and calculated their ratio to the total number of Service Centres to demonstrate the power-law distribution of the nodes within the topology. The result shows many nodes with a few links and a few nodes with many links, which exhibits a power-law property as demonstrated in Figure 5.17.

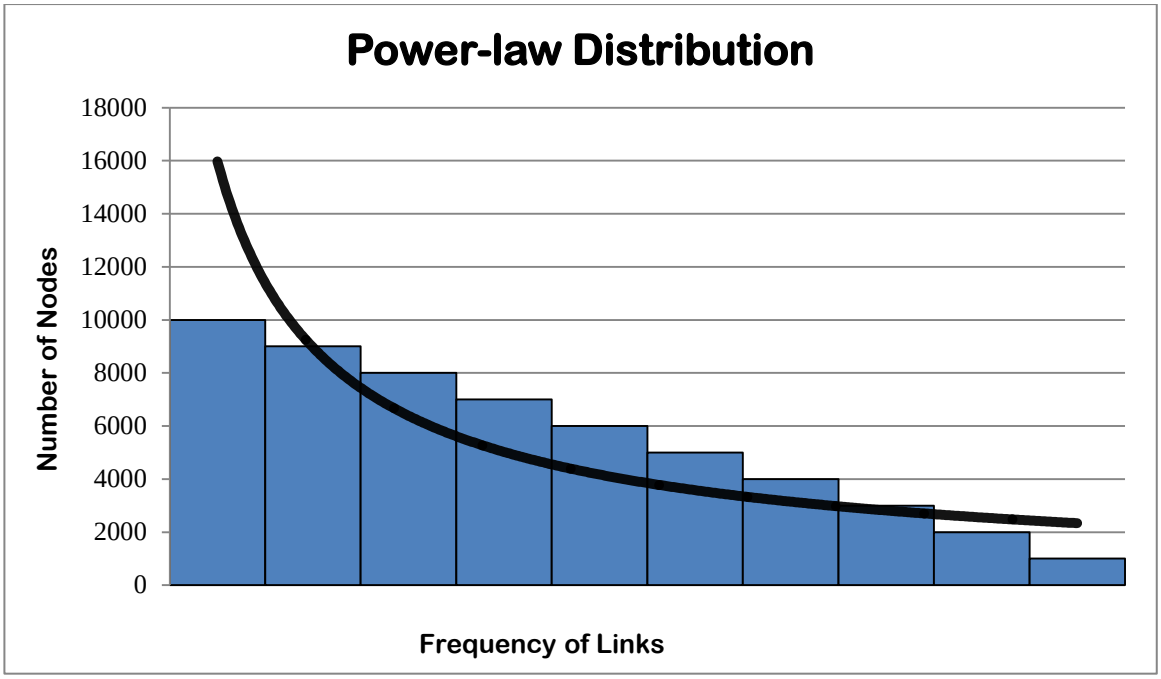

Figure 5.17 Power-law Distribution in SEP

To be able to prove the fact that the node distribution follows a power-law, we use a trend function and calculate the trend line derived from the data. In order to do so, we plot the residual values of the data and concluded a power trend line within the node distribution.

We compared the node distribution of SEP with the most effective multicast topology NICE. The NICE distribution follows a multi-tree clustering topology where every tree is assigned a cluster leader at level L_0. Every layer has a cluster leader, which forms a cluster over the existing layer L_1. Finally, the cluster leader within L_1 in the centre of the cluster is selected to serve as a rendezvous point. The dimension of the clusters is determined by the number of adjacent neighbours at each layer which in turn is used to decide when to initiate a cluster split or merge process. We observed the ratio of cluster leaders in total to the number of the nodes accommodated in the NICE topology. The results are shown in Figure 5.18.

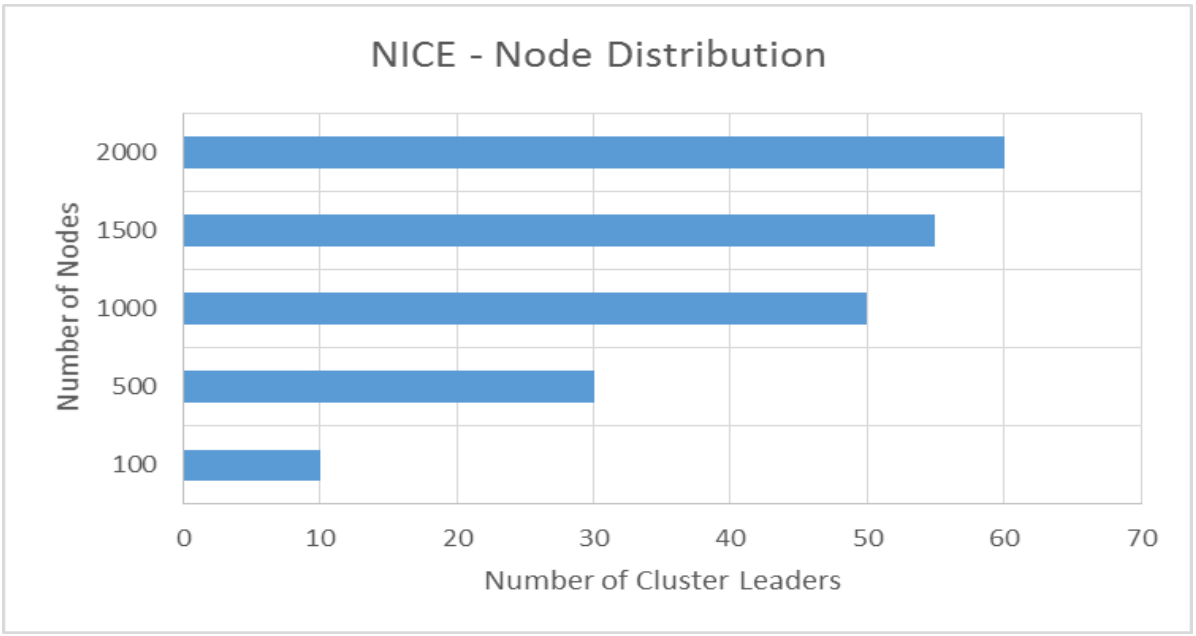

Figure 5.18 NICE Node Distribution

We calculated the residual analysis of the data using regression testing and found the residual distribution pattern as demonstrated in Figure 5.19.

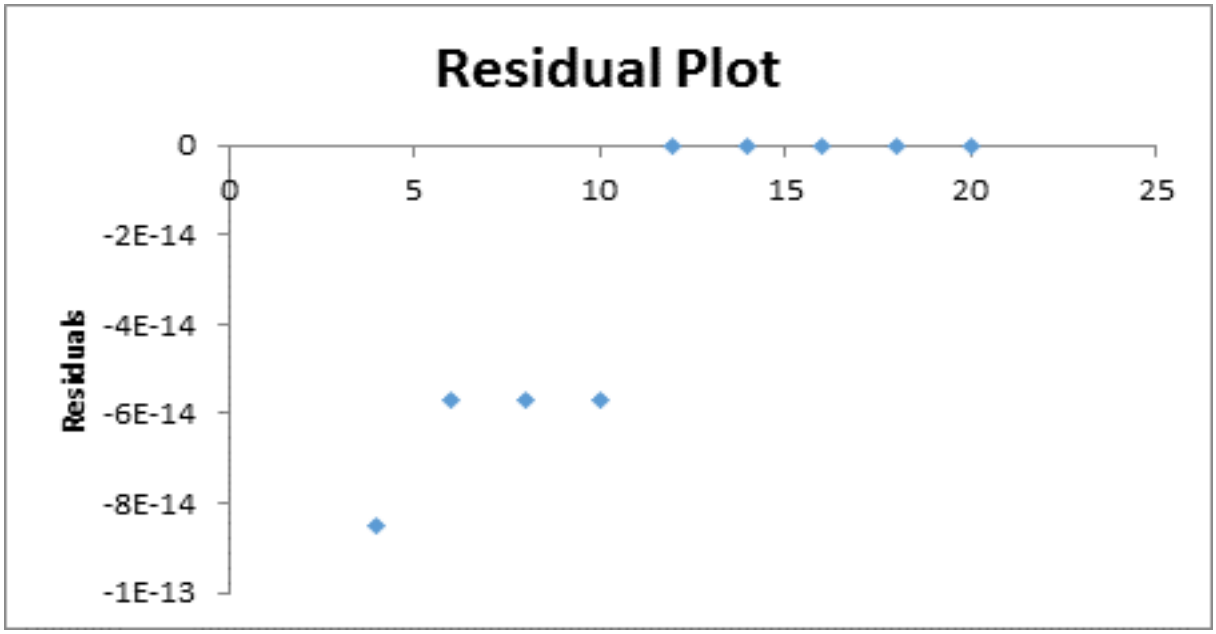

Figure 5.19 NICE Node Distribution Residual Plot

The residual plot shown in Figure 5.19 shows the relationship trend between cluster leaders and ordinary nodes within the tree-hierarchy distribution model of NICE. The node distribution residual plot for NICE in Figure 5.15 is scattered in a way that represents polynomial relationship (Gelman & Hill, 2006). Using the analysis, we can determine the trend of the cluster leader-node relationship as shown in Figure 5.20.

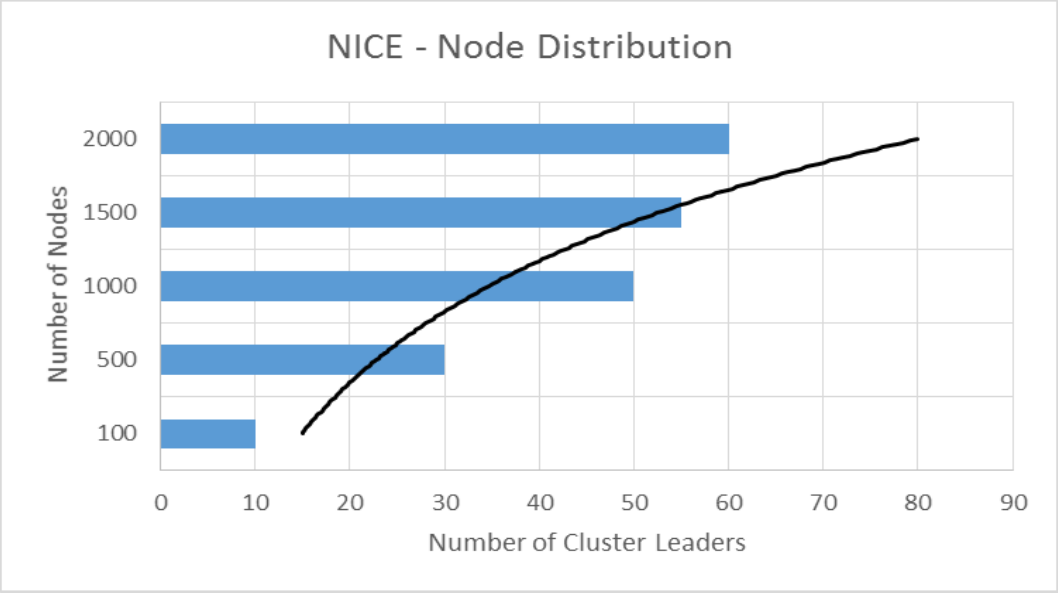

Figure 5.20 NICE Node Distribution Trend line

The size of the network and the density of the neighbours has a direct effect on the number of cluster leaders in NICE. Due to the effective forwarding capabilities of the cluster leaders, they contribute significantly to efficient multicasting and ensuring a low redundancy rate in terms of failed communications. NICE organises member nodes in large groups of cluster leaders with associated small numbers of member nodes. As such, random failures are more likely and the impact of cluster leader failure is greater. Therefore, it may have significant impact on successful packet delivery ratio, failed lookups and additional network bandwidth. We demonstrate these effects and explain these metrics later on in this section.

SEP on the other hand, organises the member nodes in groups proportionate to the size of the network and assigns a Service Centre to each group. Therefore, random failures will not have significant impact on overall interoperability of the network.

SEP uses conditional preferential attachment to model the network growth and to maintain a power-law distribution of member nodes' links. To achieve the design rationale and overcome the traditional problems arising from preferential attachment, we use the proportionate degree-distribution technique to accommodate group members within different Service Centres. To maintain system scalability, we ensure the prototype achieves scale-free properties. The simulation results show that SEP successfully sustains a power-law distribution and therefore scales well.

Furthermore, SEP handles the topology stress better than NICE. The topology adaptation recovers from random failures in a timely manner. In order to evaluate the topology stress, we measure the Scale-free properties as the network grows. For the node stress, we measure the number of the groups and number of entries for each group to indicate that SEP achieves better distribution and load balancing, which are the main factors for ensuring topology scalability. To be able to evaluate the scalability of the system using the data derived from the simulation results, we perform regression testing. Regression analysis will prove that the topological structure of the SEP remains scale-free. Table 5.5 summarises the regression statistics for topology observation in Experiment 2(A).

Table 5.5 Regression Statistics

Regression Statistics	
Multiple R	0.994834042
R^2	0.98969477
Adjusted R^2	0.988406617
Standard Error	325.9949082
Observations	10

The R^2 in Table 5.5 is the statistical relationship between node distribution and Service Centre. It determines the 'goodness of fit' as explained earlier and determines the proportion of the variation in number of Service Centres, which is derived by number of nodes. The number of active links are referred to the connection between Service Centre and their nodes which we deduce the number of Service Centres.

More importantly, the network growth model described in Section 4.4.2 is predicted to follow the power-law distribution. In other words, we expect the network topology will stay scale-free regardless of number of nodes. Figure 5.15 is a scatter plot of the link distribution between Service Centres and member nodes, which shows a power-law distribution of the nodes to ensure better scalability. To be able to find the trend line for the data, we have calculated residuals for the produced results.

The power-law distribution of the nodes is in line with the design rationale and objectives in regards to modelling the network growth as explained in Section 2.2, validating the probability analysis of degree distribution. Figure 5.21 demonstrates the degree distribution of SEP topology. The analysis of node distribution and its relationship to Service Centre appointment shows the degree distribution within the network. Comparing the links within the topology

shows that there are many nodes with few links. However, the analysis shows that there are only a few nodes within the system with many links. This is the true characteristics of a power-law distribution as explained in Section 2.2.5.

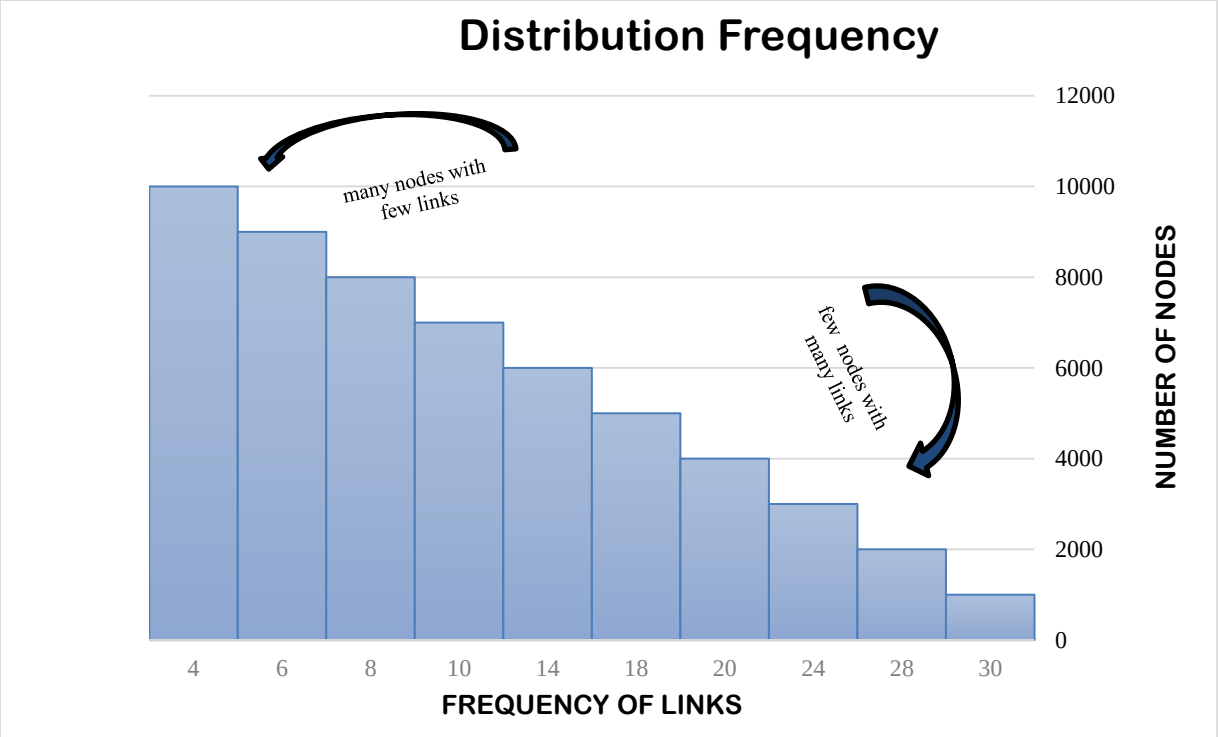

Figure 5.21 Scale-Free Distribution of Nodes in SEP

Simulation results show that the number of links stayed proportionate to the number of Service Centres with 100 nodes. After scaling the topology and performing an experiment with 1,000 nodes, the ratio of the Service Centre to the node distribution stayed relatively the same and scale-free property of the network was sustained.

We observed that using different types of churn engines cause slight changes to the topology stability with 1,000 nodes. While setting the node distribution to Service Centre ratio as 10:1, the R^2 displayed variation from 9.1 to 9.8. This was due to some nodes being rejected from entering any group and failing to acknowledge or interact with Service Centres to maintain stable links. However, this change was insignificant and had no impact on the network operation as a whole.

5.6. Average Shortest Path

In this section, we analyse the ability of the proposed framework in finding and maintaining the shortest paths in communication in order to evaluate the design rationale explained in Section 4.4.3. In a peered approach, the average shortest path will stay as low as possible preventing the long tail communications. The Service Centres serve as intermediary nodes to divert requests to the right destination in the routing and lookup process. They act as a network overlay on top of the logical network using live trusted links. The average shortest path not only ensures efficient (Ying *et al.*, 2010) and effective communications, but it improves the security (Cohen, *et al.*, 2003) within the communications.

5.6.1. Experiment 3 (A): Hop Count

We define *hop count* as a metric to analyse the effectiveness the SEP in finding and implementing the average short path as explained in Section 4.4.3. We consider the *hop count* as the number of steps a message takes from its originating source to reach the desired destination. We describe the step as the nodes are visited during the routing process. Therefore, we observe the path length as representation of hop count. To be able to compare the results, we also observed the average hops for an equivalent NICE topology. Figure 5.22 shows the average hop count for both systems within different network size.

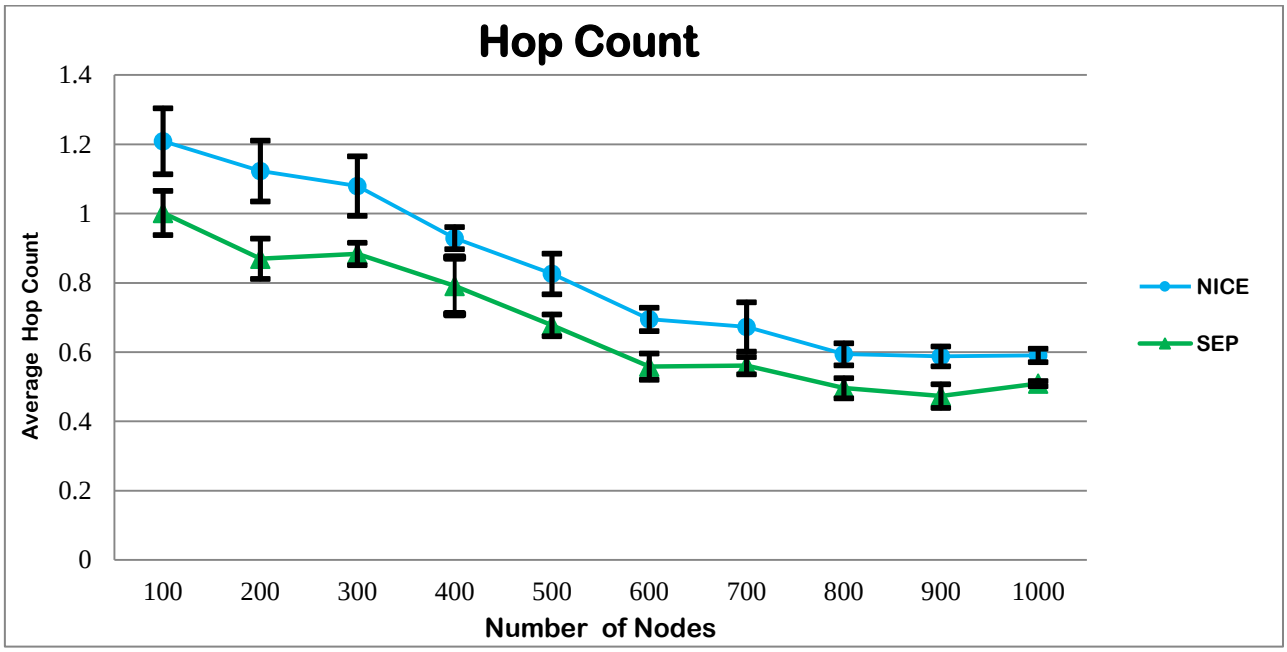

Figure 5.22 Overlay Path Length

Using regression analysis of the data, we produced the line fit plot shown in Figure 5.23.

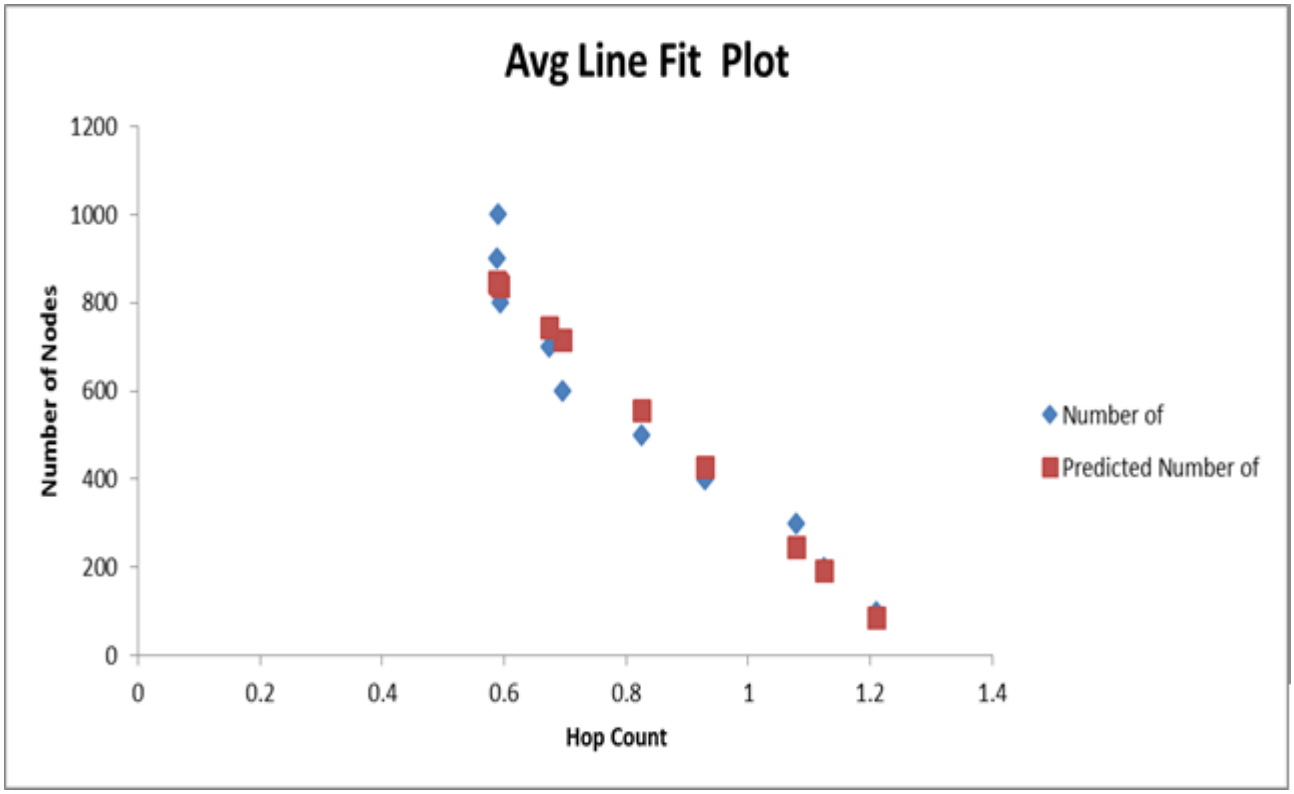

Figure 5.23 - Line Fit Plot for Hop Counts

Figure 5.244 shows the residual plot for the best fit, which represents the relationship between number of nodes and hop count.

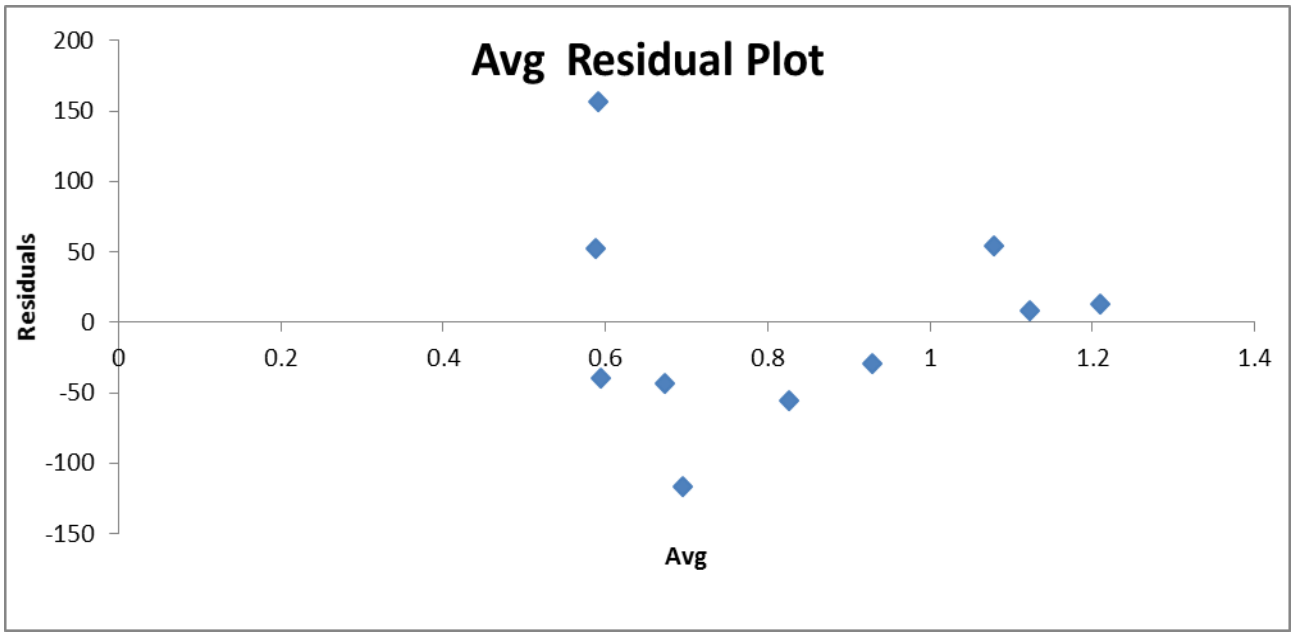

Figure 5.24 Residual Plot of Hop Count

The way the residual plot is scattered on Figure 5.24, and because the average *hop count* will never be 0, we can conclude that the trend of the *hop count* shows a logarithmic pattern. Figure 5.25 shows the forecast trend line for the average *hop count* for the NICE and SEP topologies.

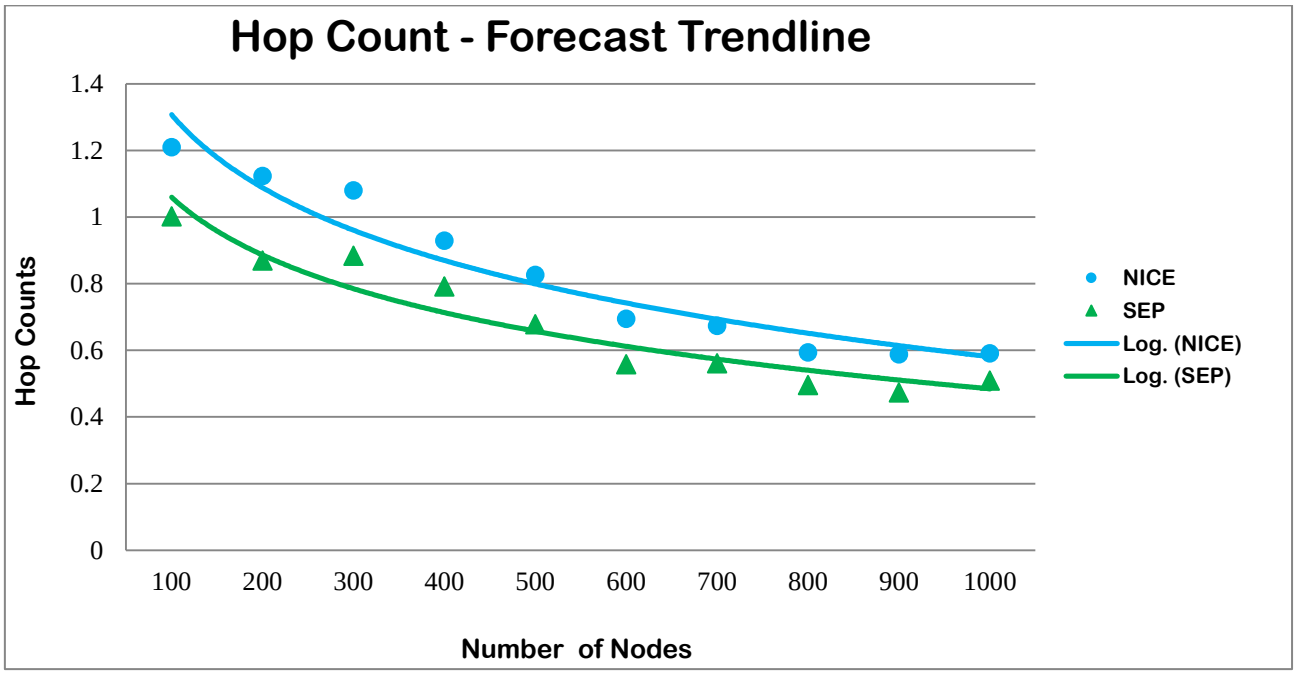

Figure 5.25 Hop Count Trend line

SEP outperforms the NICE topology in terms of achieving lower hop count, improving efficiency. As shown in Figure 5.25, both systems improve the average hop count as the number of the nodes increase. In other words, the average shortest path stays steady even with significant increases in the number of nodes. One way to explain this can be explained is that the shortest path is identification of high degree nodes (Cohen, *et al.*, 2003) makes the routing process efficient by singling out the cluster leaders and directing the messages to them. Furthermore, the use of neighbouring information and user cooperation in routing and broadcasting in communications. This feature is better implemented within a highly populated topology where availability is guaranteed. In SEP, this is achieved by collaboration between Service Centres which ensures an alternative shortest paths if the initial link becomes unavailable or broken. The suitability of this concept and topology design is explained in Section 3.2.

Random walks in power-law networks naturally gravitate towards the high degree nodes implemented in systems such as GIA (Chawathe et al., 2003), but better scaling is achieved by intentionally choosing high degree nodes (Adamic et al., 2001). By choosing a Service Centre as a high degree node within a network-aware topology to administer efficient search and

broadcasting, we replace the random-walks and blind searches with a more effective communication channel and bias search and broadcast to use the shortest paths.

The proposed framework is suited to a large-scale dynamic system where network resources are distributed over large numbers of users. By employing a small-world network model and state management, the shortest link is maintained to ensure routing efficiency and resource availability.

5.7. Control Overhead

We observed different experiments to evaluate the control overhead encountered by SEP within different scenarios as defined in Section 4.4.4. First, we calculated the effect of membership change and node failures on the control overhead. We calculated the bandwidth cost generated as a result of node disconnection during membership changes and compared this to the situation where no membership change has taken place.

In the second experiment, we analysed the effect of the topology size on the control overhead. We observed the maintenance cost for forwarding messages within different network size. Through this experiment, we were able to evaluate the path length distribution for different network dimensions and the effect on the topology maintenance. We then compared the generated results with maintenance cost in NICE.

5.7.1. Experiment 4 (A): Join Request Cost

The topology management maintains the integrity of the system by accommodating member nodes and replacing the Service Centres if they fail or leave ungracefully. A Service Centre is replaced by a back-up Service Centre, if it leaves the network. The replacement process also involves exchanging acknowledgment messages between peers and the Service Centre. During the Service centre replacement, some nodes disconnect from the group or try to join other groups due to conflicts of interest or failing to acknowledge and approve the change. The same issue happens during the *split* and *merge* operation.

We evaluate the effect of such scenarios by calculating the join request cost. We measure the bandwidth cost of node disconnections where a join request is made subsequently.

When a node is disconnected from a group, it needs to re-join the group or may join different group. Re-joining the group requires an exchange of messages between the node and the Service Centre of the group it is trying to join. In order to evaluate the control overhead of the join

request resulting from a membership change, we observed the join request cost incurred by the process for SEP.

We calculated the join request cost as the byte counts and compared it to the cost when there is no membership change. Figure 5.26 shows the average byte count for the join requests during a simulation of 1,200 seconds.

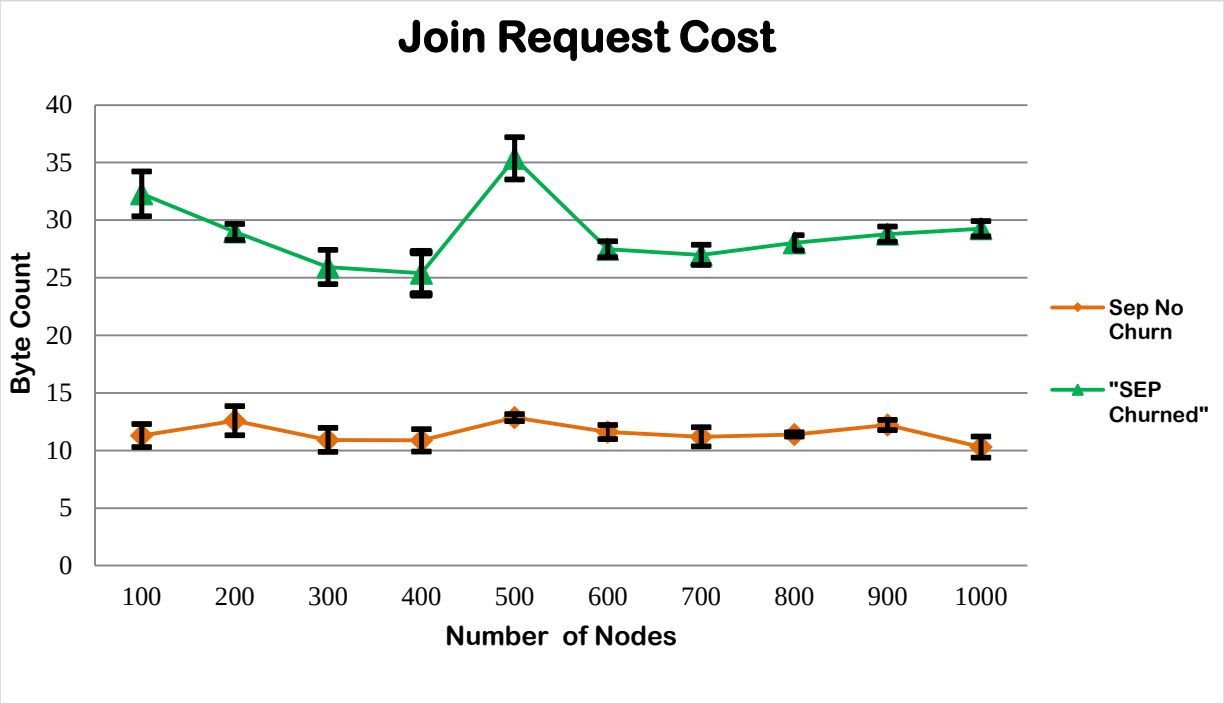

Figure 5.26 Join Request Cost

The cost of a join request is significant particularly if there is a membership change or a failure in the network. Therefore, this requires careful consideration. As shown in figure 5.24, the membership change enforces extra cost on network operation.

To be able to evaluate and justify the design rationale, we measured the control overhead incurred by node disconnections in SEP and compared this to the equivalent results that were generated for NICE. Figure 5.27 show the join request cost for EP and NICE where the network deals with random membership change as result of member nodes node or cluster leader failure.

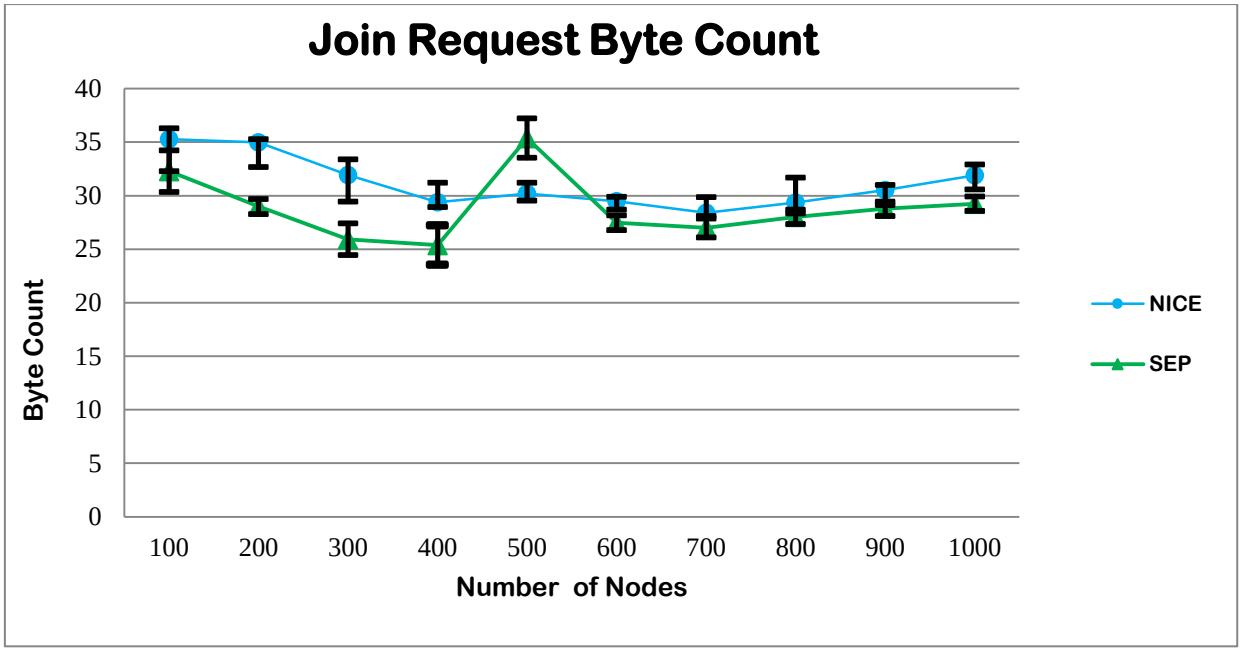

Figure 5.27 Comparison of Join Request Cost in SEP & NICE

Figure 5.27 shows that the join request cost for SEP is comparable to NICE within larger size networks (500 and above). However, it outperforms NICE within smaller size networks (400 nodes and below).

Within SEP, a Service Centre is nominated by the system and elected by group members with close ties, common interests and friendships. In a technical sense, this includes nodes within the same or neighbouring group, as well as close topological location. The Service Centre is also responsible for facilitating node joins and governing the membership table after a node failure or a graceful leave. If a Service Centre is rejected by the majority of the nodes, the system replaces the nominee with the one whose attributes comes as second best. This is most likely the case within *merge* operations where a group of nodes need to join another group geographically close and most likely sharing a common interest or where their interests are close to each other. Disputes are unlikely within a *split* operation where a group of nodes which reaches its maximum capacity attempts to split in two, but it is possible. In most application multicasts, this function has been disregarded. This may bring conflict of interests, security and privacy issues within systems.

SEP accounts for the probability of Service Centre rejection and forwards the nodes to neighbouring clusters or removes them from the group. This will not affect Service Centre operation if the majority of the nodes exchange acknowledgment messages and confirm the leadership. If group *A* with the minimum defined number wants to join group *B* and group *A*'s

leader's attributes and capacity is higher than that of *B*'s leader, then group *A*'s leader with minimum members will be selected as the new Service Centre. There is a good chance that the majority of existing members will reject the new Service Centre. We define that the Service Centre for group B will maintain leadership and new members acknowledge and confirm the decision.

In Figure 5.27, the maintenance cost for SEP within a topology with 500 nodes increases considerably. This is because of the cost of a *merge* operation which kicks in when the group size reaches 500. The *merge* and *split* requests generate extra maintenance costs for the network that is crucial for membership management and integrity. Considering the benefits of the *merge* and *split* on the network efficiency and effectiveness, the extra overhead is justifiable.

5.7.2. Experiment 4 (B): Message-forwarding Cost

In the previous experiment, we measured the control overhead on topology efficiency through observation of the effect of the membership management. In this experiment, we measure the effect of the scalability on the control overhead and evaluate how clustering the network enforces additional cost to the interoperability of the topology.

As explained in Section 3.2, the network-aware message-forwarding algorithm administered by the Service Centre ensures efficiency and effectiveness using average shortest paths and privacy-aware route and broadcasting. Within an autonomous and unstructured P2P system, this generates additional cost in order to cooperate and coordinate those processes. We analyse and evaluate the message-forwarding maintenance cost.

To measure the maintenance cost for message-forwarding, we do not consider membership changes. We have observed and collated the message-forwarding cost for both systems as displayed in the Figure 5.28.

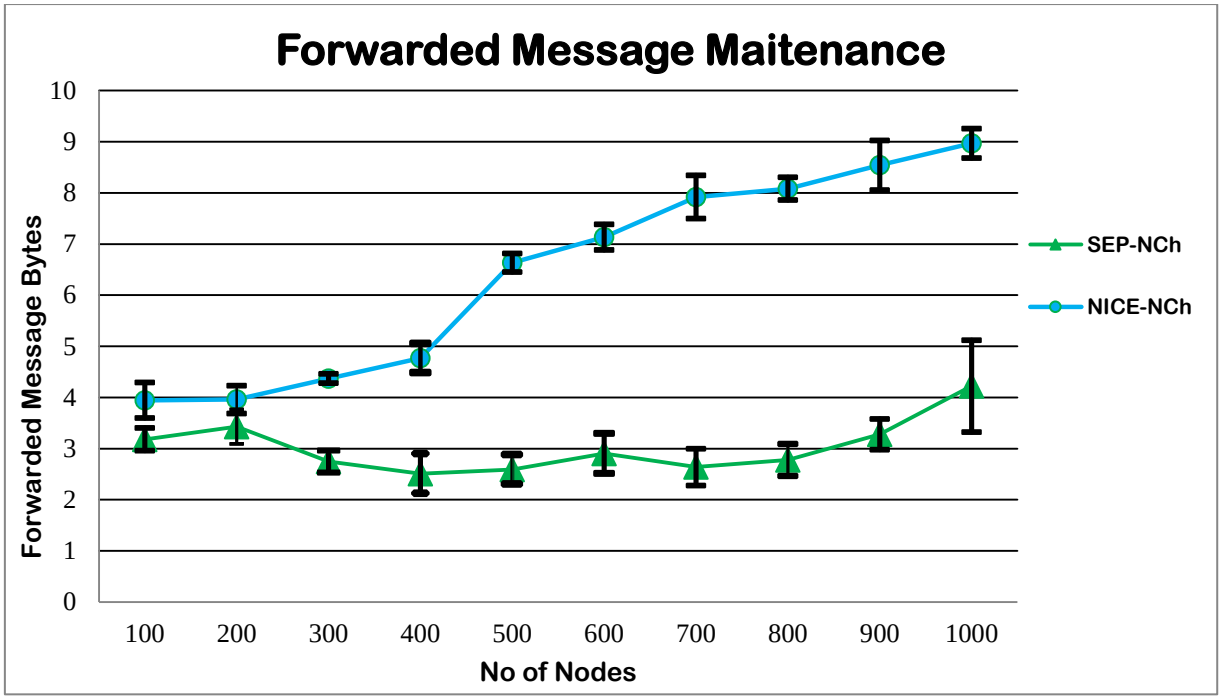

Figure 5.28 Maintenance Cost on Message-forwarding

The figure suggests that maintenance costs for NICE are lower for small network sizes (less than around 300 nodes) and comparable to SEP, but that for larger network sizes (around 300 nodes and above) the efficiency of NICE decreases rapidly. In contrast SEP achieves relatively consistent performance in terms of maintenance costs, and so has a lower maintenance cost than NICE for larger (around 300 nodes and above) network sizes.

In order to contact a node at the higher end of the hierarchical-tree, a NICE message must be routed through every layer of the hierarchical-tree, which involves exchanging acknowledgment messages, which cost network bandwidth. However, SEP performs better as the maintenance messages are routed through only two Service Centres. Using the direct communication, the shortest path and a lower hop count make the search, broadcasting and messages forwarding more efficient comparing to NICE.

Figure 5.29 shows the trend line for the maintenance cost of message-forwarding for both systems.

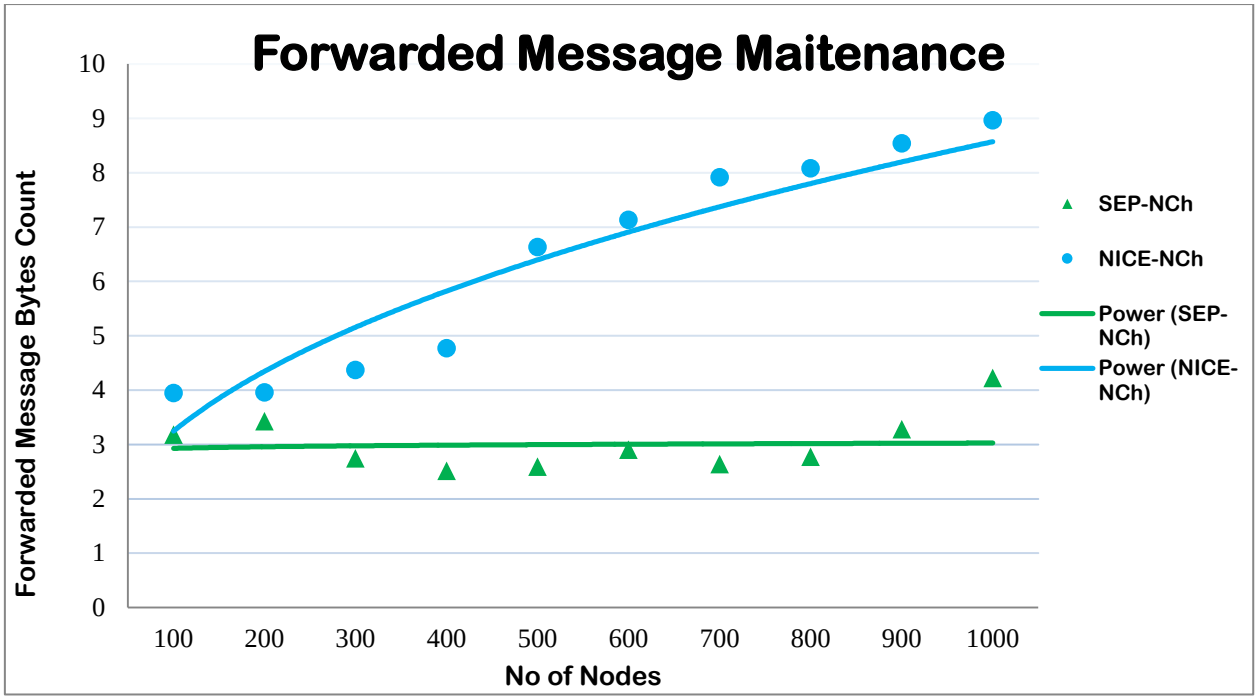

Figure 5.29 Maintenance Cost Trend line

The maintenance cost increases in NICE in contrast to SEP where the cost is predicted to stay constant. This is because of the scale-free effect of the network growth as explained in Section 2.2.3. Each Service Centre maintains an updated list of group members and effectively forwards incoming and outgoing messages. Instead of using a flooding type routing and visiting every node to forward a message, SEP uses a biased routing in cooperation two Service Centres, which act as super nodes. The messages This represents the maintenance cost for different topology sizes, which determines the efficiency of the network-aware message-forwarding as explained in Section 3.2 of the SEP design.

5.7.3. Experiment 4 (C): The Effect of Topology Management on Maintenance

In this experiment, we measure the cost enforced application forwarding ALM is a multicast application, which broadcasts a message indiscriminately to every member node within the network.

We measure the message-forwarding maintenance for the ALM application and compare it for both SEP and NICE. Figure 5.30 shows the average maintenance cost for forwarding routed messages when the system has to deal with group leader replacement.

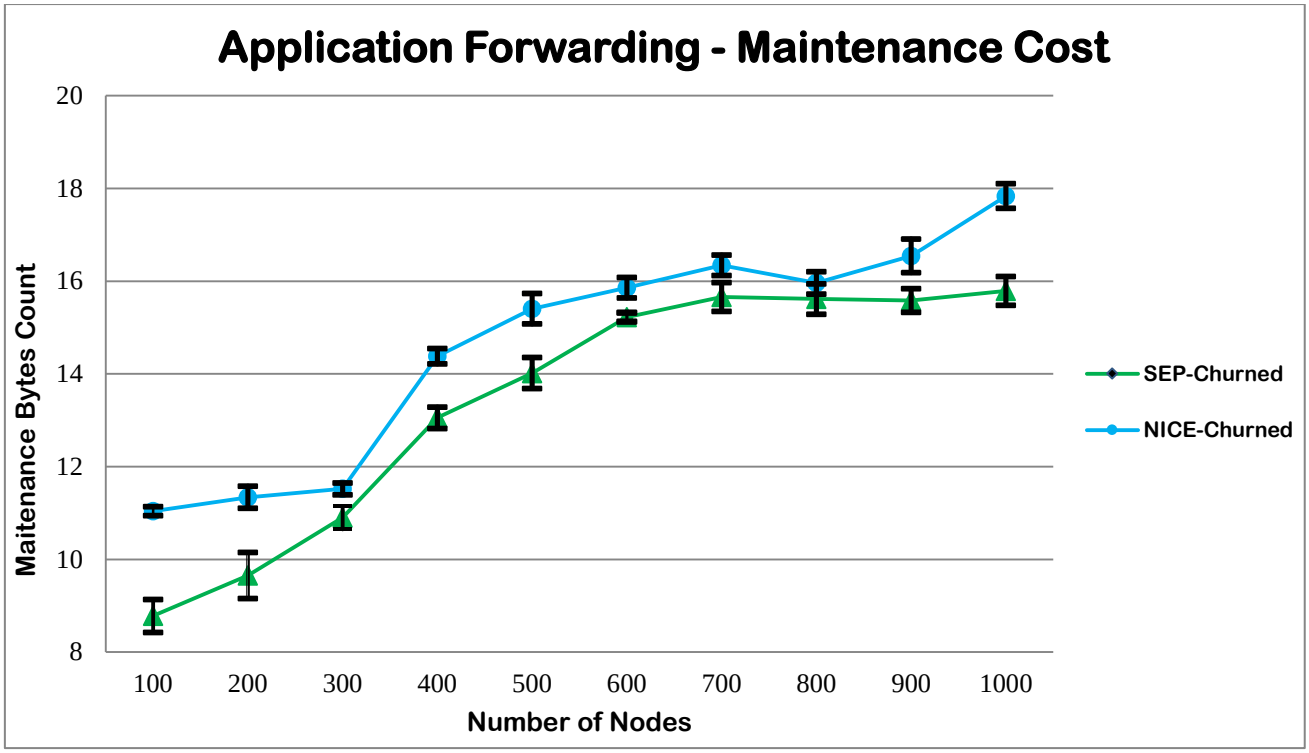

Figure 5.30 Maintenance Cost for Application Forwarding with Pareto Churn

For these experiments, we used the same settings of Experiment 4 (B) regarding the topology size. The Service Centre within a group administers the message forwarding efficiently by using the cluster co-efficient techniques and maintains the shortest path.

The maintenance cost within the network is considered as the number of membership update messages exchanged within the group, which is calculated as byte counts as explained in Section 5.1.8. The maintenance cost for application forwarding increases for both systems as the network size grows. This is expected as the simulation results indicate that SEP scales better with a large number of nodes and is good with partitioning and self-organising of the nodes. We achieved two bytes improvement over NICE in case of 1000 nodes. This improvement will have larger impact when the number of nodes grows significantly.

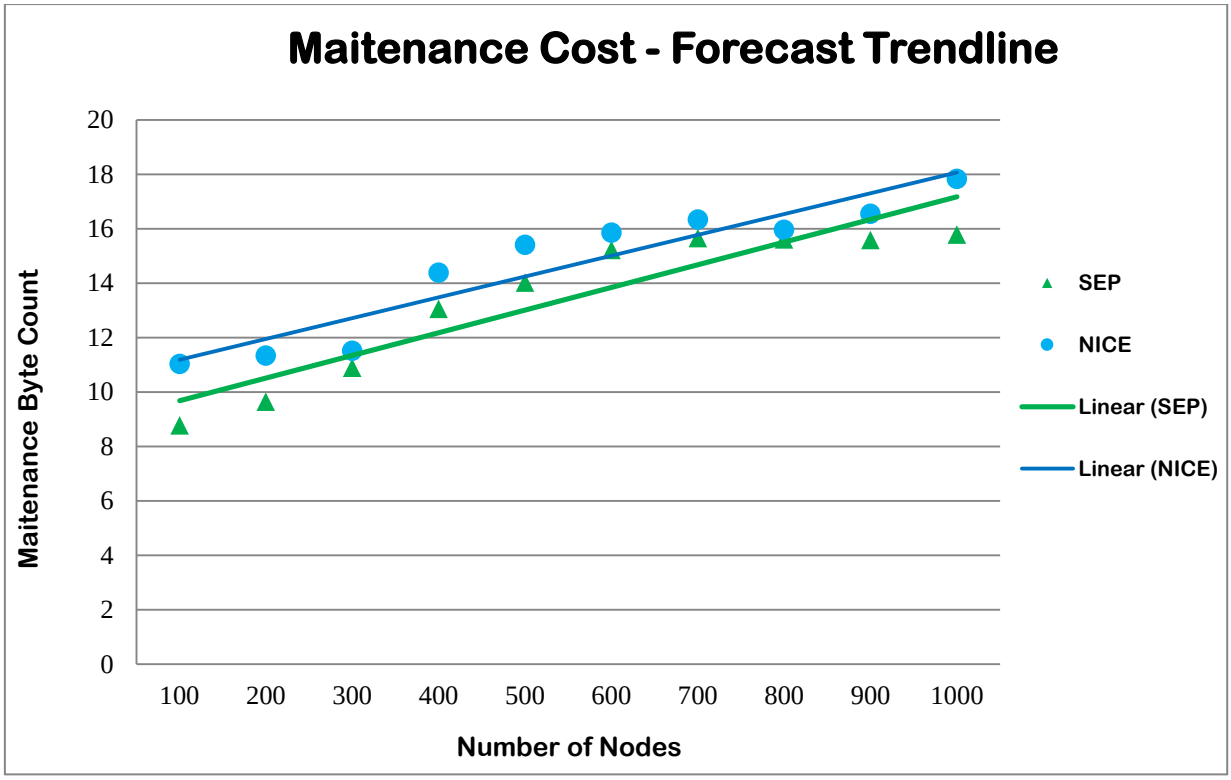

Figure 5.31 Maintenance Cost Forecast

As predicted, network maintenance increases as the number of nodes goes up. This is the same for both NICE and SEP. In NICE the system maintenance is managed through heartbeat messages exchanged with all members by the Rendezvous point. This is similar to a client-server model, therefore sharing the same characteristics in terms of latency and operation overhead. The NICE maintenance cost increases proportionate to the number of nodes. We revisit the maintenance cost evaluation demonstrated in Figure 5.31. NICE starts with a reasonable maintenance cost for 100 nodes and it follows the same or a lower pattern until the network dimension grows. As soon as the number of cluster leaders is increased, the maintenance cost jumps up significantly.

The SEP maintenance cost on the other hand is distributed amongst different Service Centres. The autonomy of the groups provides efficient and cost effective membership management. The distances for the heartbeat messages are shorter and the latency is less than for NICE. Since the maintenance is managed and administered by distributed Service Centres at a local scale, the maintenance increase is proportional to the number of Service Centres. This starts with higher maintenance cost compared to NICE for smaller topology size, but it stays steady as the *k* value is increased.

The maintenance cost includes the node join, leave and fail overhead imposed on the system throughout the operation. The cost of leader selection and leaders leaving ungracefully are comparable in both NICE and SEP, assuming the leader rejection is not too high in SEP. If the leader rejection process occurs more often than expected with the SEP system, it forces many negotiations, nominations and exchange of messages. A possible reason for leader rejection is where nodes, which hold the majority of the group with, low levels of confidence in the nominated Service Centre. Another reason could be misbehaving nodes or malicious nodes trying to disrupt the leader selection process.

5.8. Security & System Resiliency

When a Service Centre fails or leaves, the system replaces it with a backup Service Centre. The effective management of the operation will reduce system recovery time; improve efficiency and subsequently, security of the system. We performed experiments with different numbers of nodes to evaluate recovery from a Service Centre failure in SEP and compared it against cluster leader failure in NICE. When we simulate a Service Centre leaving the network, we do this as an ungraceful leave or complete fail, i.e., there is no opportunity to warn other nodes in advance.

5.8.1. Experiment 5 (A): Reliability – Average Response Count

When an overlay node ungracefully leaves or fails within a Service Centre, it will have no significant impact on the overall topology maintenance or interoperability of the overlay. This is because the low degree nodes are not important for system maintenance or operation. However, a Service Centre failing or leaving the system may lead to interruption of packet delivery, message-forwarding and look up operations as well as failure to manage nodes joining and leaving. The topology construction algorithm considers replacing the Service Centre with a backup leader once the Service Centre decides to perform a graceful leave. However, an ungraceful leave means that the Service Centre fails or leaves without sending a graceful leave message as a pre-warning.

In SEP, the failed Service Centre is proactively replaced with an already nominated backup node. The Service Centre exchanges messages between nodes, periodically updating membership information and group maintenance on Naming Table. If the heartbeat messages are not received from the Service Centre by the scheduled time, the system replaces the Service Centre with a backup node and asks member nodes to confirm the appointment. To evaluate

system reliability, we measure the level of system capability to recover from Service Centre failures.

To be able to evaluate the topology efficiency, we measure the average response count for the queries performed within SEP. When a query is initiated, every recipient acknowledges it. We have used *GIASearchApp* (Chawathe *et al.*, 2003), a Tier 1 application to perform queries and observed the number of responses. We compared the statistics to the NICE topology. We collected these reply messages and considered their quantity as the response count. Appendix 2 is the simulation setting to observe and collate the response counts during the simulation. The simulation results are presented in Figure 5.32 shows the average value of the response count for SEP and NICE.

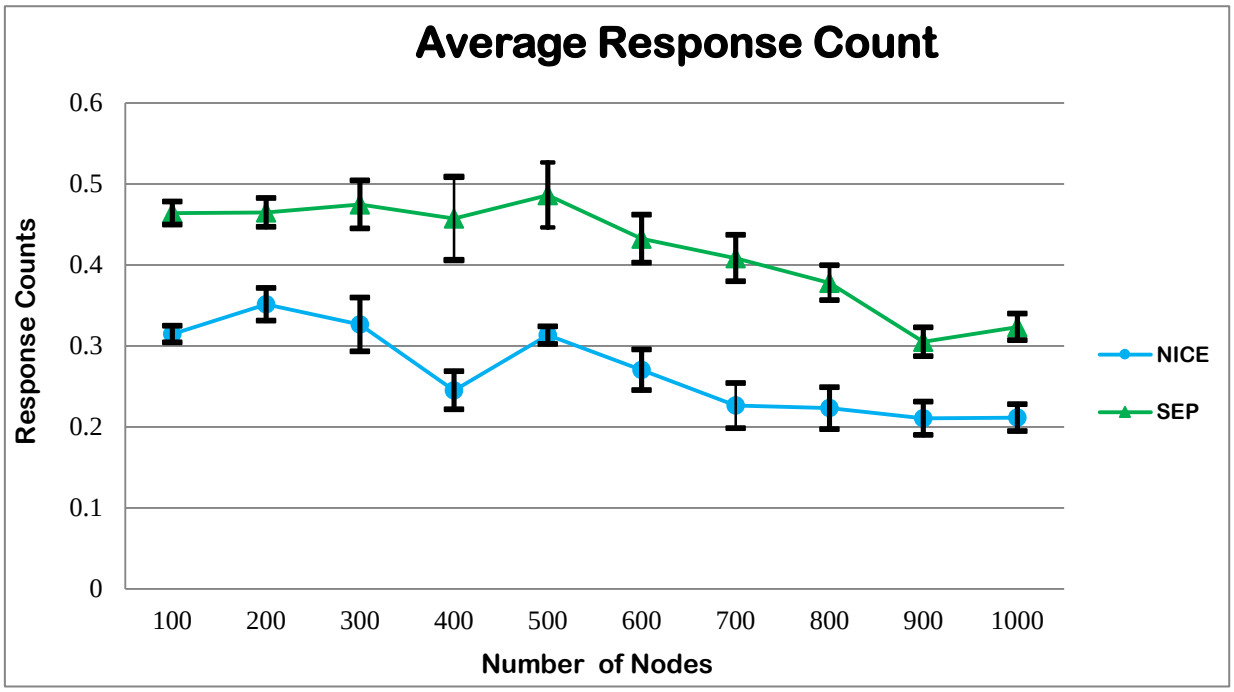

Figure 5.32 Average Query Response Count

We then perform a regression analysis in order to determine the data trend in the results as shown in Figure 5.33.

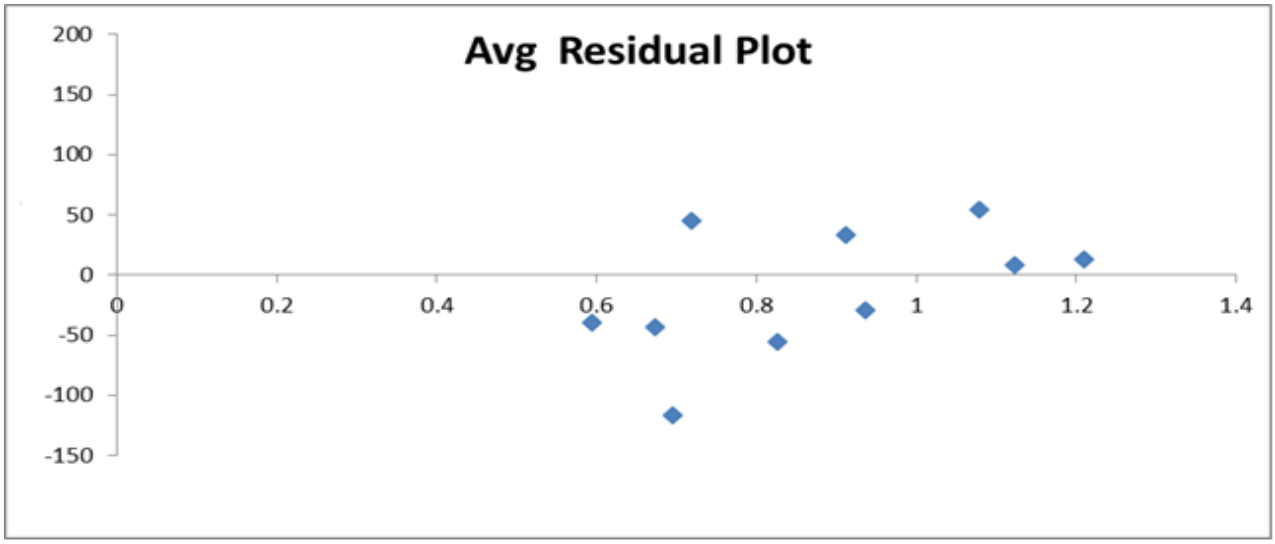

Figure 5.33 Residual Plot - Average Response Count

The way the residual plot is scattered in Figure 5.33, we can we conclude there is a logarithmic relationship between the number of nodes and the average response count for queries in SEP and NICE. As shown in Figure 5.30, SEP always receives the highest rate in average response counts. The confidence intervals shown on Figure 5.32 also show that this is true 95% of the times. From the residual analysis of the data presented an the residual plot, we can see that the response count starts with significant increase, stays relatively within lower rate compared to the initial experiment and levels out at a steady rate afterwards. Figure 5.34 shows the trend line and forecast of the average response count for both SEP and NICE.

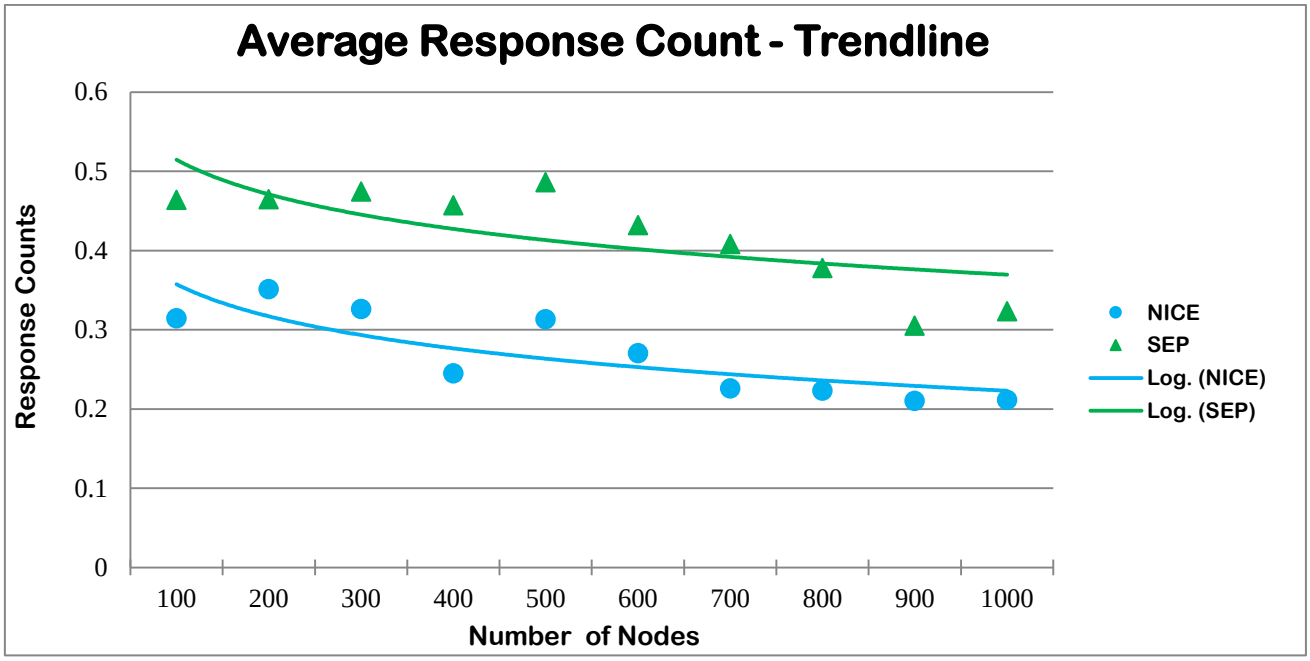

Figure 5.34 Trend line of Average Response Count

NICE has a three-layer tree-topology construction where a single node is assigned a leadership responsibility. A node leader is selected if it is at the centre of a group. A rendezvous node is selected from the second layers within the group leaders if the leader is at the centre of the leader's cluster. This means the Rendezvous node on the higher tree layer is the same one who is at the centre of its own cluster. This provides an efficient search and broadcasting is achieved efficiently. If a cluster leader fails, the system calculates the location of the existing members and selects the node which is located in the middle of the cluster as a leader. NICE does not consider failure of a Rendezvous point, and treats any leader failure as normal and performs a replacement operation using the algorithm. Considering the Rendezvous point is responsible for the most of the membership management and interoperability, any failure will have a significant impact on the network. Even if the failure is recovered in a timely manner, the distribution of the maintenance cost and recovery cost imposes a big overhead to the system.

SEP on the other hand distributes the overall membership and forwarding responsibility to Service Centres with complete autonomy. This means any Service Centre failure will have an impact on a local and small scale. For SEP the scale of the security impact will be a fraction of that compared to NICE.

Consider a 1,000-member group, where it is divided into two SEP groups and managed by two Service Centres. In NICE the Rendezvous point is responsible for the whole network operation. Therefore, the impact will be twice as great as for SEP, assuming the recovery time and maintenance cost are comparable.

The *GIASearchApp* (Chawathe *et al*., 2003) was suitable for this experiment as it tries to find the highest degree node to forward messages. Upon failure of a super node, the system must seek either an alternative route to divert the message or wait until the super node is replaced. The latter is the best option for preserving user privacy. This is because the *hop-to-live* implemented by Clarke *et al.* (1999) prevents a node vising the same node twice ensures anonymity within the process.

SEP maintains membership locally. It is crucial that the Service Centre has enough capacity and resources to deal with the maximum number of nodes predicted. The self-healing property of SEP in terms of Service Centre replacement, group dimension maintenance and membership refinements ensure fault tolerance.

5.8.2. Experiment 5 (B): Resiliency - Packet Drop Rate

In this section, we perform an experiment to test the system resiliency and its ability in repairing the scale-free property of the topology under random attacks. We use Scribe as a Tier 1 application running on top of the SEP and NICE overlay topologies. We plan to apply churn engines on the cluster leaders to emulate the attacks on the network, which leads to Service Centre failure.

The packet delivery process fails in two situations namely; the source Service Centre failure and destination Service Centre unavailability. We observe the effective delivery of the packets in order to evaluate the topology construction algorithm and the design hypothesis where the algorithm ensures self-healing of the topology in a timely manner. We collate the number of UDP packets and calculate the average packet drop rate for both overlay topologies as a result of leader failures or destinations not being available.

Figure 5.35 shows the average number of UDP packet drops for different network sizes because of unavailable node destinations, where network members join and leave as scheduled.

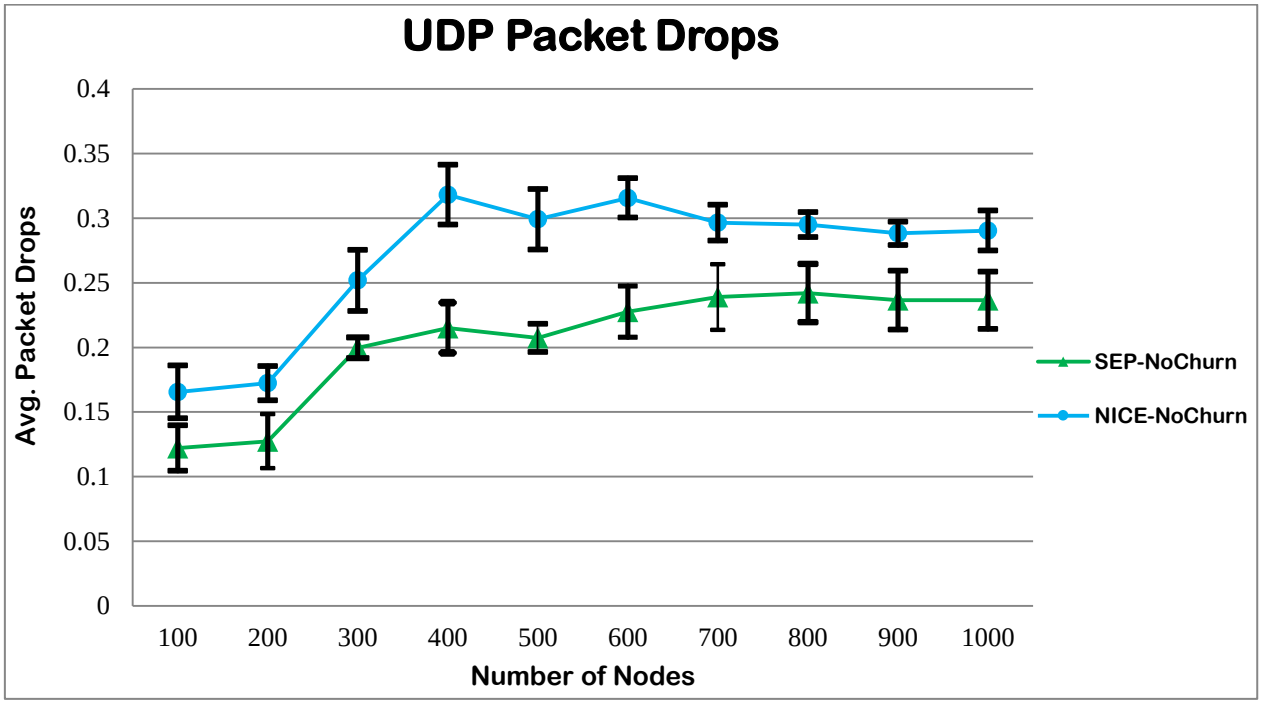

Figure 5.35 Average Number of Packet Drop Rate with No Churn

The membership change within a group has no significant impact on the communication or packet delivery as it is achieved using P2P communication. However, packet drops as a result of the destination being unavailable mean that the Service Centre for the destination node is

unable to acknowledge and forward the packet due to a failure or ungraceful leave. Figure 5.36 is the trend line for UDP packet drop rates for both systems.

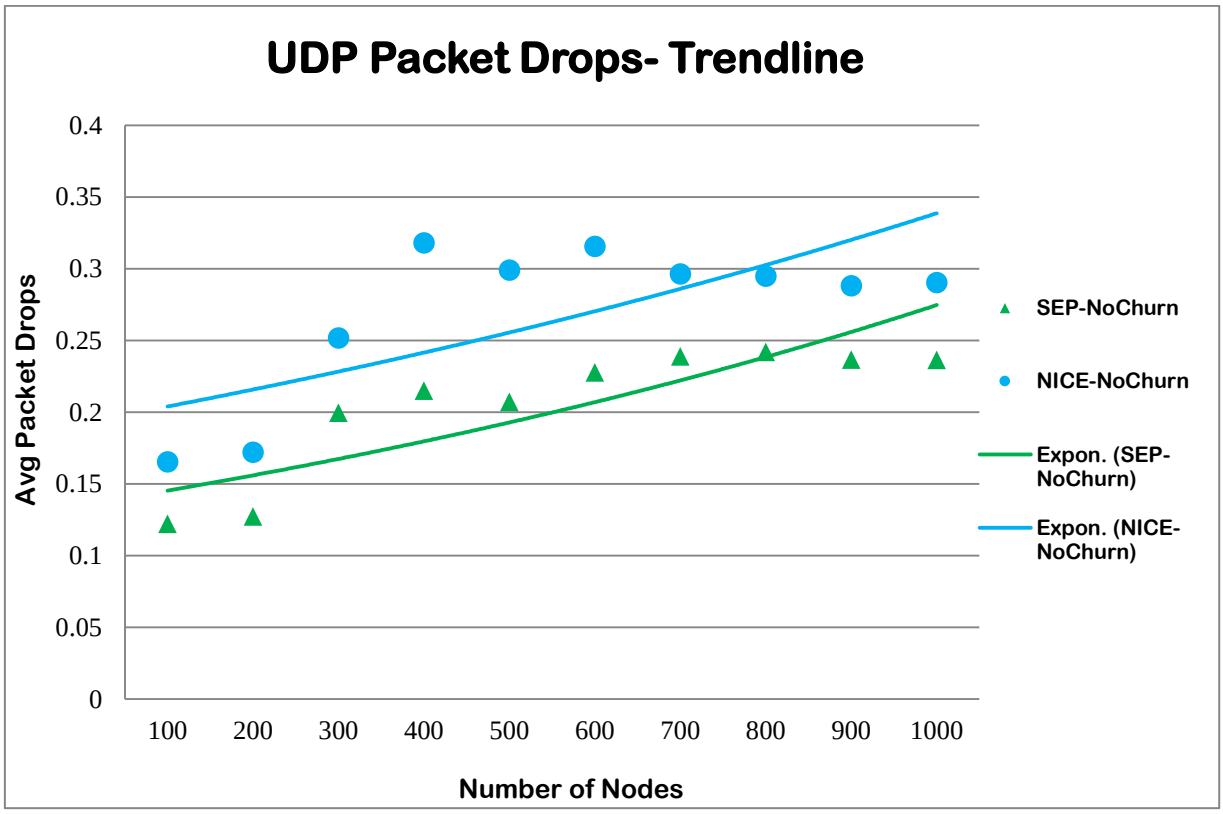

Figure 5.36 The Trend line for Packet Drop Ratio

The experimental results indicate that SEP outperforms the NICE topology in terms of effective topology recovery. The effective recovery from failures improves successful packet delivery. Therefore, not only this improves the integrity of the communications, but it prevents bandwidth redundancy.

In order to emulate the targeted attacks and evaluate the effective recovery of the topology, we performed an experiment to systematically remove Service Centres. We used the *Pareto* churn engine for the experiment. In order to evaluate the integrity of the system we compare the simulation result t the best known multicast P2P overlay, NICE. Figure 5.37 demonstrates the simulation result for both systems.

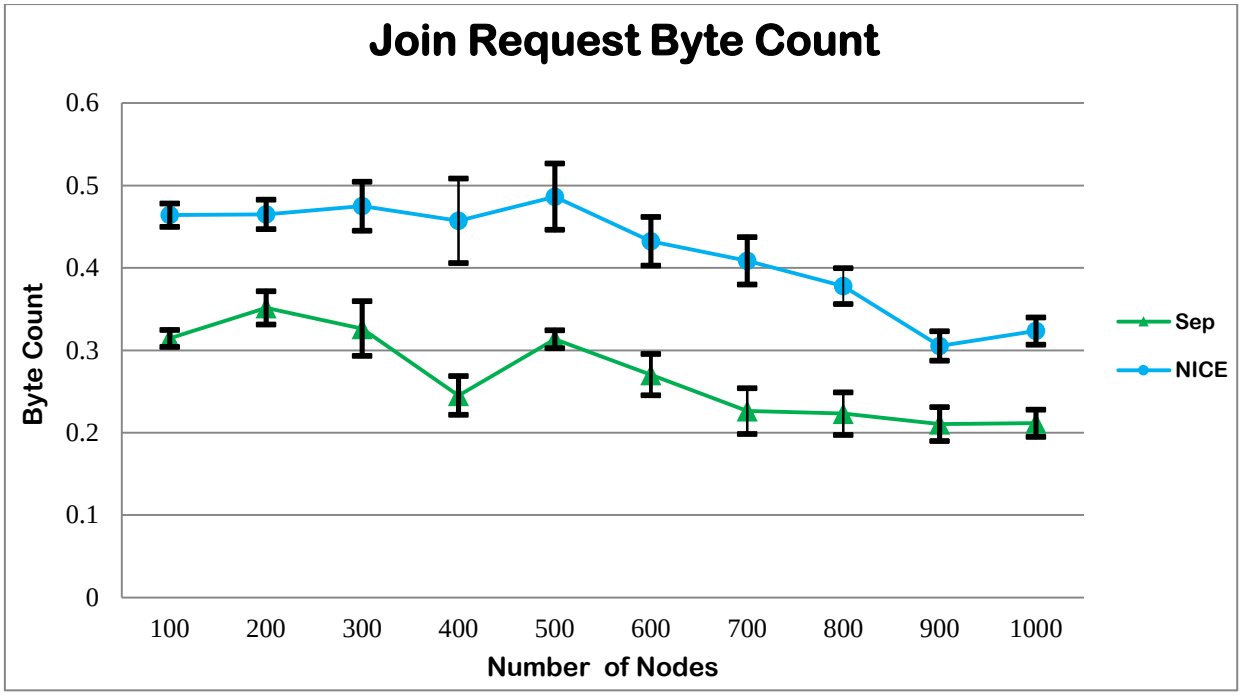

Figure 5.37 The Effect of Service Centre Failure on Packet Drops – Pareto Churn

As shown in Figure 5.37, SEP outperforms NICE in terms of integrity and interoperability of the topology while being targeted by an attack. We can conclude that SEP is much more reliable and effective in recovery from a targeted attack comparing to NICE.

To be able to have a better understanding of the implication of experiment 5 (B), we extracted the additional statistics for both topologies as shown in Table 5.6. The table shows the comparison of statistics recorded for both systems with an average of 1,000 nodes over a 2,000 second simulation.

Table 5.6 The Effect of Service Centre Failure on Packet Delivery Ratio

	Mean number of nodes	Packet drop due to unavailable destination	Time between deletes	Time between creates	Maintenance bytes
SEP	1012.84	22.7881	0.985994 s	0.950398 s	84.93256
NICE	1018.94	28.60925	1.707631 s	1.711116 s	73.23192

The statistics show the mean number of packets dropped due to destination nodes being unavailable. The result shows that the packet drop is considerably higher in NICE than SEP. The difference might not seem statistically significant at first in terms of drop ratio, but the average time between creates and deletes is shorter in SEP as shown in Table 5.6. This means the drop ratio and subsequently redundant bandwidth will be higher over longer operation time

with larger number of nodes. However, the maintenance cost is higher in SEP due to the higher number of message intervals sent during the membership change and the housekeeping process.

We measured the message delivery delay to evaluate the significance of the statistics presented in Table 5.6. We measured the message delivery delay within multicast message dissemination as a result of Service Centre failure compared it to NICE as shown in Figure 5.38.

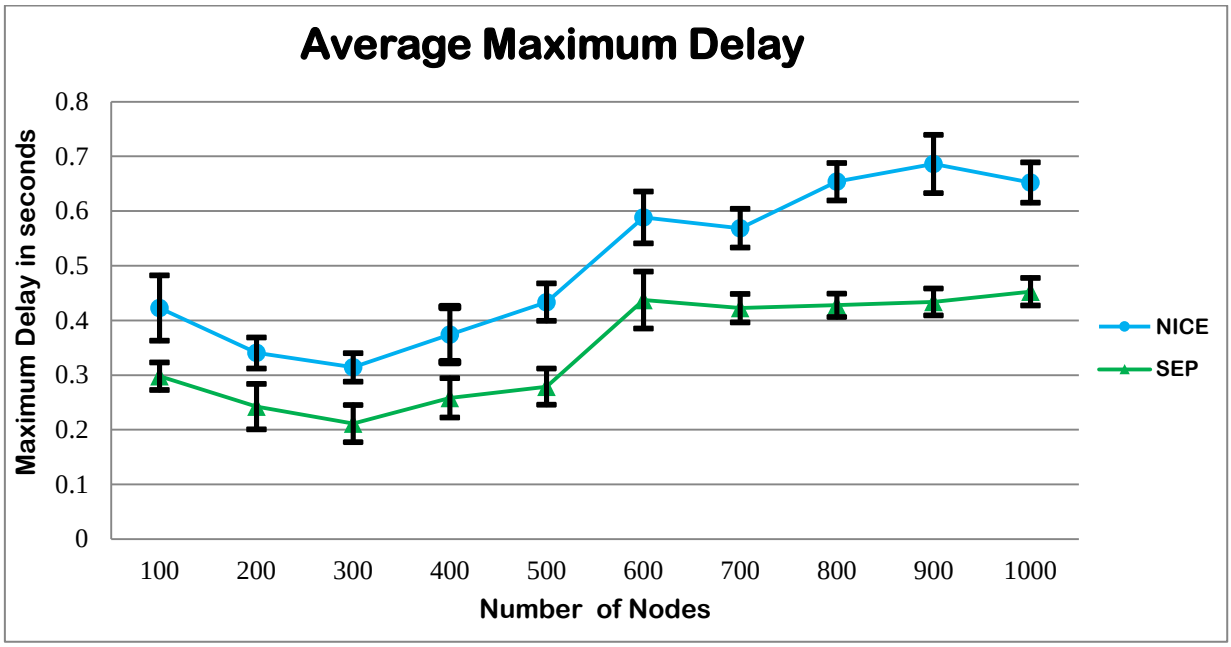

Figure 5.38 One-way Latency Time in seconds for Multicasting

Figure 5.39 shows the trend line analysis of the one-way latency within SEP and NICE.

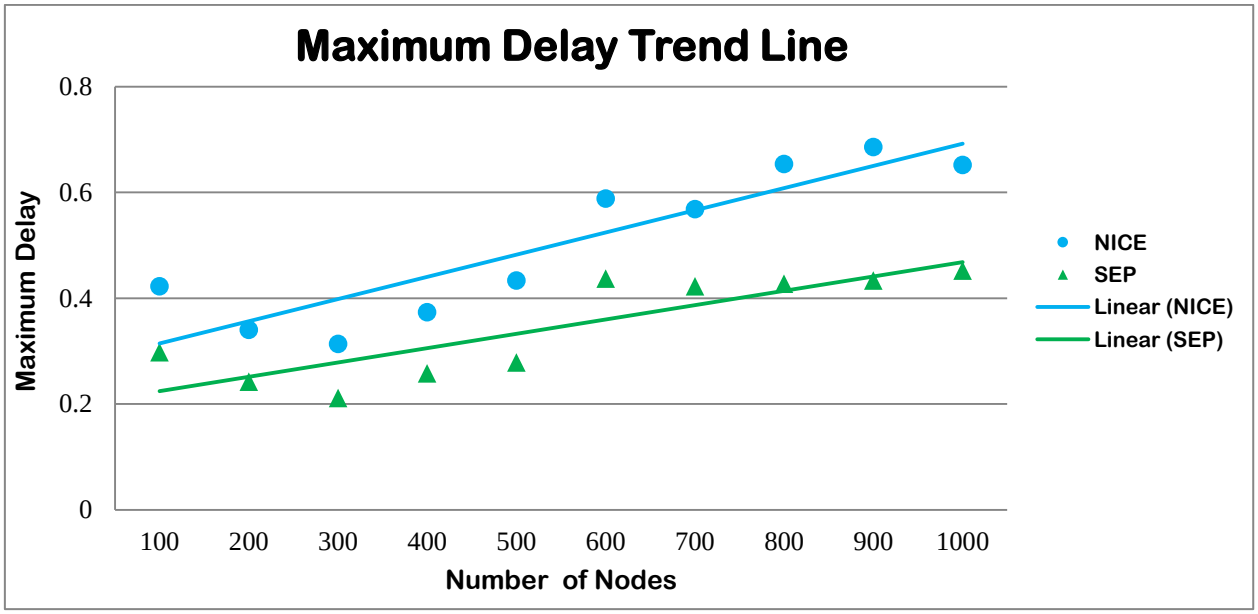

Figure 5.39 Trend line for Maximum delay

The trend line shows that the delay time increases linearly for both systems as the number of the nodes within the network grows. However, the average delays for SEP always stay lower making it more reliable than NICE in terms of end-to-end communications.

5.8.3. Experiment 5 (C): Disconnection Ratio

We performed this experiment to evaluate the aggressiveness of the topology in response to random attacks. The topology aggressiveness is the ability of the topology construction algorithm to maintain the system integrity by administering the *split* and *merge* operation as well recovery from a Service Centre failure. We perform an experiment to analyses the topology management to maintain the integrity of the group membership and to evaluate the self-healing characteristic of the topology to ensure system security and resiliency as explained in design rationale, section 4.4.5.

In this experiment, we measure the average node disconnection ratio to measure the aggressiveness of the topology based on the size of the cluster. We define the node disconnection as an instance where a node fails to join or register within a group. Apart from a graceful leave, a node is disconnected from the network within three distinct operations, namely Service Centre failure, group *merge* or *split*. We randomly remove Service Centres to emulate the random attacks on the network. We observe the average number of disconnected nodes as a result of the Service Centre failure. Figure 5.40 shows the average number of disconnections within different network sizes.

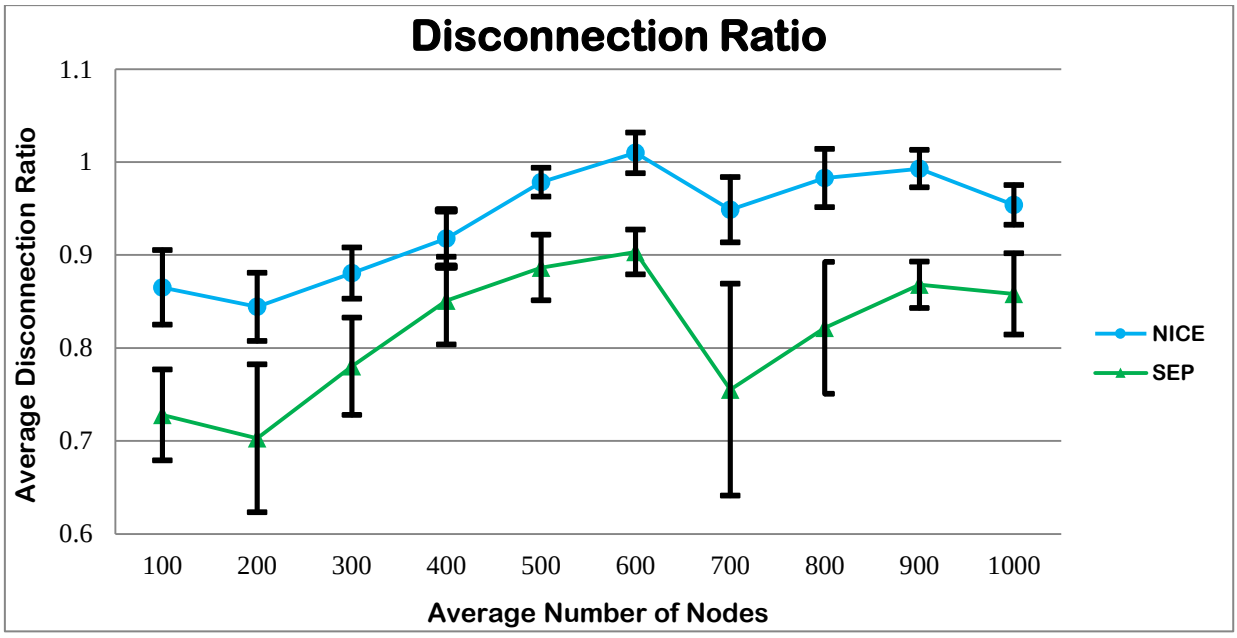

Figure 5.40 Topology Aggressiveness – Average Node Disconnection Ratio

Figure 5.40 shows that even though the confidence interval in SEP fluctuates in comparison to NICE, it is more resilient compared to NIC in terms of disconnection ratio of members under random attacks. SEP appoints Service Centres proportionate to the number of the nodes. The degree distribution in SEP ensures power-law, maintaining a few Service Centres allocates with many nodes attached to them. As discussed in Section 2.2.5, such networks are prone to targeted attacks but resilient to random attacks. The topology management will ensure that the failed Service Centre is replaced by a node with similar characteristics. Considering the autonomy of the Service Centres, failing one, will not have significant impact on the other groups or the topology as a whole. However, due to complexity of the tasks such as *merge*, *split* and misbehaving nodes that may cause disruption in leader selection or membership management process, the random failures are inevitable. As such, it is vital to analyse the implication of such failures on the system security.

In NICE, the 'rendezvous' point is responsible to assign, replace and maintain cluster leaders as well as their cluster members. When a cluster leader fails, it is replaced by another node closest to it in terms of topological location. The member nodes are redirected to the closest cluster leader by the 'rendezvous' point. Failure of a cluster leader has only impact on limited number of nodes since NICE distribution includes many cluster leaders with few members within each cluster. However, when a rendezvous point fails, it affects the whole network and its sub-modules. In this experiment we did simulate a rendezvous point failure. Therefore we assume the topology aggressiveness and the results extracted from the experience does not take into account the rendezvous point failure.

NICE defines network dimensions by setting the maximum number of neighbours a node can have. Therefore, the tree can grow exponentially, spreading with high density of population. If the leader at the root of the tree fails it will affect the whole population within that cluster. The hierarchical-tree design in NICE is vulnerable to targeted attacks as explained in section 2.2.3. Since there is no limit to the membership numbers within different sections of the hierarchical tree, failing a cluster disconnects all of the members within the tree.

The experimental results shown in Figure 5.40 demonstrate that SEP handles topology aggressiveness better and outperforms NICE in terms of member retention ratio in dealing with random attacks. Throughout the experiment, the average disconnection ratio of SEP remains lower than that of the NICE topology. The better handling of topology aggressiveness in SEP will also have a positive effect on the control overhead of the topology.

5.9. Summary

In this chapter, we presented the results generated from the experiments and carried out analysis in line with the system rationales using the performance metrics that were defined in Section 5.1. Furthermore, we evaluated the experiment results and collated statistics using different analysis tools and techniques in order to assess the validity of out design hypotheses and accomplishment of research objectives. The generated results then were compared to the most effective and reliable unstructured P2P system.

6. Conclusion and Future Work

Ubiquitous Computing has promised that the conventional desktop computer will disappear and replaced by tiny, integrated digital interfaces interacting with humans. The advances of the Internet and emerging technologies and solutions such as wireless and low cost networking have made interconnection of those devices possible. This brings the paradigm of IoT, which leads to ubiquitous use of electronic services and data explosion. The interconnection of many network infrastructures creates a large-scale or global network with dynamic change of members, policies and services. Managing different features within such a large-scale network requires pro-active planning and careful feasibility studies to fulfil system requirements as well as addressing the emerging challenges.

Scalability resolutions in P2P networks focus on identifying and mitigating system bottlenecks. This includes improving and maintaining system performance using the existing resources after the addition of new users or entities. Without an actual network load and implementation, it is hard to predict system bottlenecks and plan for mitigation. Moreover, scalability brings different issues and new challenges within user oriented systems such as IoT and critical systems. The prediction of network growth and operation under different circumstances are achieved using probability theories, test beds or simulation environments. In this work, we have utilised an abstraction of a large scale unstructured P2P network system to model system security and resiliency, performance and interoperability. The outcome is then generalised to the rest of the system to validate the proposed framework.

Within a scalable network, the spread, mobility and granularity of nodes, and the dynamic architecture of the network, make resource management and arrangement of nodes complex (Li *et al*., 2010). Topology management should consider cost, time and space as well as privacy, fair access, confidentiality, integrity and availability of resources. Managing network resources and communications within such distributed systems becomes more complicated, with important tasks such as membership management, routing, topology choice, service access and state management becoming increasingly challenging. The traditional client-server arrangements within centralised systems using low-level protocols have now been replaced by autonomous mobile hosts and dynamic protocols over ubiquitous decentralised systems. Using these low-level protocols, nodes can communicate with each other and make independent decisions of the network management system.

The interconnection of autonomous computers and isolated communication networks enables new services and applications to form distributed networks (Panda *et al*., 2011). Despite the typical centralised nature of computer networks, a distributed network operates more efficiently and effectively over a mix of workstations, LAN servers, wireless networks, regional, Web and other servers (Papers *et al*., 2010). As the size of the distributed network grows, managing network resources, access control and security become more complex due to the dynamic and rapid change of network structure, state and flexibility.

Secure communication and confidentiality, efficiency, fault tolerance, availability and integrity of the resources are the main concerns of scalable distributed network algorithms. Furthermore, they should maintain state consistency, resource consistency, privacy, resiliency and response to intrusion as well as functionality and interoperability of the network.

There are several ubiquitous applications to address the challenges facing scalable ubiquitous networks. However, those solutions are not inclusive. In particular, they do not support efficient service discovery and performance testing (Edwards & Grinter (2001); Panda *et al.*, 2011; Dixon *et al.*, (2011); and Greenberg *et al.*, 2009). Throughout this project, several weaknesses and major flaws of scalable ubiquitous systems have been identified within the current frameworks and applications (see Chapter 2). Those systems may fulfil the requirements of a ubiquitous system environment and address technological challenges to some degree (Edwards & Grinter, 2001). However, some elements of user-oriented system design and security have been overlooked. There is no comprehensive approach to address all of the challenges facing dynamic changes of scalable network structure with hundreds of devices and services joining, leaving or failing within the system. In addition, the privacy concern in a user-oriented environment has been given less attention. We proposed a novel network-aware topology construction and membership management scheme to address resiliency and integrity of the scalable unstructured ubiquitous systems such as P2P overlays. By enforcing the network to follow a power-law distribution of nodes, organising the network members and different entities becomes efficient and cost effective (Li *et al*., 2010).

The topology management process usually aims at maintaining fairness, but this is not the case within the current ubiquitous system developments. Applications and users demand network resources in real time without complicated configuration. While the price of storage media has gone down significantly within the past few years, we do not deal with a resource-limited network. We rather focus on how to allocate those resources to achieve better performance and

security. Therefore, the four essential aspects of resource allocation, namely task allocation, membership management, anonymous communication and resiliency have been the focus of this project.

The rising cost of data traffic and the need for efficient communications and improved management of systems have created pressure to rollout efficient and effective communication methods and address dynamic change of members within ubiquitous P2P networks. This work uses a novel topology construction and management scheme with network-aware lookup and broadcast techniques to initiate efficient communications. We make effective use of the shortest paths within the Ubiquitous Computing networks without the need for complex changes to the network topology, policy or procedures. A simple mesh-based overlay is proposed to maintain minimum hop search and a lookup mechanism using Service Centres. A novel privacy-concerned leader election algorithm is proposed to preserve user anonymity and communication security. Considering the high cost of failed queries within scalable networks, this work improves network efficiency and reduces latency.

The interactions and communications within a ubiquitous computing environment involve generating sensitive and personal data. Providing an infrastructure to maintain security and efficiency as well as interoperability within such ubiquitous systems has been the focus of businesses, service providers, academia and the research community. The development and current advances of such broad objectives have been discussed within this work and many research questions have been highlighted. Using different modelling techniques, mathematical theorems, system and application scenarios and a simulation environment, this work contributes to the current knowledge with a novel approach and robust experimental evaluation. The approach considers development limitations as well as current advances in the area of ubiquitous systems.

Network overlays add additional layers on top of the existing networks with indirect mapping or virtualisation to provide service to a more scalable domain. The proposed framework forms several network overlays to address scalability issues within a decentralised P2P system. It supports routing, addressing, security and mobility and the dynamic changes in the network such as node addition, re-configuration and failures. The proposed scheme is fault tolerant, scalable and provides an effective methodology for self-organisation of the nodes. We evaluated the proposed methods using experimental analysis and discovered that the developed framework

SEP scales well, offers practical partitioning and is effective in terms of self-healing and self-organising of resources.

During this work, many concerns have emerged regarding the efficiency and privacy within ubiquitous systems. Privacy is an issue that changes from one environment to another, considering cross border laws and legislation as well as many guidelines. Therefore, the introduction of a comprehensive standard and guidelines to include every aspect of privacy may be a near-impossible task. Nonetheless, this poses a challenge to the future of ubiquitous systems.

6.1. Topology Construction

The network-aware topology construction is a core element of the SEP design. In this section, we present an overview of the topology construction and bootstrapping processes, which contribute to system scalability. SEP organises existing members into groups of trusted users and nominates a Service Centre to act as a super node to administer routing and forwarding tasks. Although this is inspired by the clustering co-efficient property explained in Section 3.6, the intention is to leave member nodes to form a community of users who can communicate with each other without globally advertising their identity. The user's anonymity is observed from the very basic elements of the system, which is the initialisation phase. Within the initialisation phase, member nodes are promoted to vote a trusted member of the community with higher processing power and degree distribution as leader, thereby creating a Service Centre. If a member node is not happy with the nomination, it can leave the group and join another group, which it may have common interests with. Group members are required to confirm the election until their confirmation is acknowledged. After the creation of the first Service Centre and the registration of group members, they can invite friends into the group to expand the group membership. If a group member fails to acknowledge and confirm the selection, it will be removed from the group and will need to request to join again if it decides to join later.

Having multiple Service Centres within the P2P network ensures heterogeneity of the design with full support for any decentralised system. The experimental results showed effective group and membership management and multicast data path reliability by providing additional guarantees using alternative routes.

In Scribe and NICE, the location information is used to select a cluster leader. A node, which is located in the middle of the topological location, is assigned as cluster leader. This means a node with lower capacity may become a cluster leader. Such an approach may cause system bottlenecks compromising network performance. SEP takes a different approach to this issue by including the computational power and available bandwidth as parameters in nominating a Service Centre. Furthermore, the conditional preferential attachment in node distribution maintains effective node arrangement. In the next section, we explain how this improves network balance in terms of resource distribution.

6.2. Topology Stability and Load Balancing

As we have mentioned earlier, ensuring a symmetric network topology is a major challenge while designing a P2P network. Load balancing is considered for the distribution of network traffic and resources amongst the member nodes. Clustering the network is the simplest and efficient way of distributing network resources to achieve the best load balancing. The current most effective and efficient solutions for unstructured P2P systems include hierarchical topology (GIA) and hierarchical-tree topology (NICE).

The hierarchical-tree topology in NICE is an efficient clustering solution for unstructured P2P, which supports multicast applications. It organises the nodes into hierarchical trees, allocating the nodes located at the centre of the tree as super nodes shown in Figure 5.12. The *cluster leader allocation* algorithm in NICE is unbiased and only considers the distance vector of nodes as a metric when making a decision.

GIA on the other hand implements different approach and directs the queries over the topology to the nodes with higher degree. Although this may provide effectiveness in terms of improved communications nonetheless, it may create system bottlenecks by sending overwhelming number of requests to particular nodes. Moreover, using the preferential attachment where high degree nodes attract more links from other nodes leads to unbalanced networks in terms of node distribution as demonstrated in Figure 5.11.

The power-law distribution of node in SEP as shown in Figure 5.13, maintains scale-free property as well as ensuring effective load balancing. This property contributes towards system resiliency and low overhead in end-to-end communications.

6.3. Topology Scalability

While designing the distribution topology for a P2P system such as the Internet P2P streaming, two architectures are usually utilised: tree-based and mesh-based architectures (Seibert, Fahmy, & Nita-rotaru, 2008). In the Tree-based structure, members explicitly choose their parent (Hosseini *et al.*, 2007). A Tree-based overlay constructs a hierarchy of nodes, which can be administered by their parents. This provides simple routing topology and effective membership management. The Tree-based method has many advantages over other methods such as selecting a leader with adequate required resources, direct control over the network and, most importantly, the members select their leader from the known members in the network (Hosseini *et al.*, 2007). However, tree-based overlays cannot scale well. Multi-tree overlays such as Chunky-spread (Venkataraman *et al*., 2006) have been introduced to address this issue. Chunky-spread uses a random graph with proportionate load target to improve load-balancing issues. Each node needs to know information about its neighbour such as maximum load number and its neighbouring nodes' constraints. If a parent node receives 50% more load than anticipated, then the node does not transmit any data. This can affect the interoperability of the system.

On the other hand, in a mesh-based approach, the overlay facilitates the communications in an unstructured manner with information about subsets obtained from the membership server (Seibert *et al*., 2008). Mesh-based systems are resilient to membership changes and produce high performance with heterogeneous bandwidth capabilities. Seibert *et al*. (2008) have measured – through experiments – that mesh-based overlays perform better than the tree-based ones.

While choosing the best network topology, the SEP framework aims to provide a balance between two distinct metrics namely: maintaining the average shortest path and reducing the number of hops in lookups, thereby reducing end-to-end delays. Such an approach has not been implemented or documented yet (Hosseini *et al*. 2007). Furthermore, routing data packets using Service Centres maintains the anonymity of the P2P communications. To achieve the first requirement, SEP uses the clustering method discussed in Chapter 3. The second requirement is achieved by using an administered routing protocol with one-hop or minimum-hop communication. The routing algorithm in explained in detail later on in this chapter.

The main advantage of the mesh-based P2P system is efficiency in terms of bandwidth consumption (Hosseini *et al*., 2007 and Seibert, Fahmy, & Nita-rotaru, 2008). Assuming that most of the users have an acceptable internet connection, and given the security and privacy

considerations, the Tree-based method is similar to the scale-free network in terms of node distribution. In SEP, we have implemented a scale-free network, which is a different variation of the Tree-based topology management to simplify membership changes and to implement the proposed effective routing algorithm for maintaining user privacy.

Our experiment results show that the SEP protocols is scalable, efficient and resilient to random attacks. To validate the components of the system, we tested the system scalability using the system's ability to handle link distress and topology stress. To do this, we measured the topology structure using random graphs as explained using the Erdös-Rényi (1959) model.

The first step in implementing the SEP framework is to construct a scalable overlay topology, in order to organise a Gnutella-like unstructured network into a clustered group of users where the network overlay can scale to accommodate a network at Internet scales. Topology construction includes arrangement of members as groups of nodes with common interests and to nominate a Service Centre to act as a group leader. The network starts with the initial membership management and constructs a cluster until it reaches its maximum defined capacity. It then grows with a similar configuration to accommodate further nodes up to the Internet scale.

The topology construction algorithm starts bootstrapping the nodes and nomination of Service Centres to connect the nodes to the cluster until the initialisation period is completed as shown Figure 5.13. The topology construction algorithm follows conditional preferential attachment of nodes for membership management and node distribution and degree-proportional probabilistic (Fotouhi & Rabbat, 2013) to model the future network growth.

The topology construction experiment has two stages to evaluate system scalability. It is based on a power-law distribution of nodes and the ability to cope with network stretch and membership changes within the clustering co-efficient model. Membership change is governed by different churns and network stretch is assessed by changing the network size and seeing how the network convergence properties are affected by it.

6.4. Membership Management and System Resilience

The paradigm shift from client server to distributed scalable P2P ubiquitous systems makes cooperation more important and feasible than coordination. As the unstructured P2P network becomes an autonomous system, user contribution and cooperation play an important role in terms of interoperability of the network. This is considered as a major factor for successful

lookup and communication mechanisms in unstructured and scalable P2P systems such as GIA and Gnutella. User presence, especially the presence of those with high value attributes such as processing power and memory, which may take on the role of being Service Centres, is key to the successful operation of SEP. The cooperation and active contribution is not a major issue within the SEP framework since the user groups are formed based on trusted relationships and friendly associations. Member nodes' common interests and positive reputation are the basis of a group membership. These factors are important parameters in the Service Centre nomination and appointment where the majority of members participate in the voting process to select a node as a group leader. Therefore, member nodes are expected to make an active contribution to the community group to ensure interoperability and availability.

Nodes within SEP have an affiliation motive to the community group to share information or facilitate in the sharing of information. These are the main instincts that drive formation of clustered community groups. We can see examples of this motivation in Web communities such as Yahoo Groups, Google Groups and chat rooms. Free riders are one of the main obstacles in successful and efficient communication in cooperative communities (ADAR *et al.*, 2000). However, we almost eradicate the possibility of free riding by assigning administrative roles to Service Centres and constantly monitor them using sign in or wake up calls. As such, fault tolerant communication and lookup protocol is guaranteed to some extent within the proposed system.

The uptime for a user with high capacity and high degree can have a direct influence on system operation. Therefore, the key for success in such systems is client participation. In an unstructured system such as Gnutella, the median uptime for clients is 60 minutes (Saroiu *et al.*, 2002). In the SEP system, the Service Centres play an important role in providing crucial services to their group members. However, we assume Service Centres stay active and live for a reasonable amount of time and inform the system on graceful leave to reduce inconsistency and overhead.

Generic network-level routing protocols do not address application specific faults and therefore only legitimate problems with paths or physical links are considered (Anderson, 2002). The integration of the average shortest path and network dimension ensures the efficiency of the resource allocation. The integrity and state consistency within the network will maintain the interoperability of the system.

In this project, the trusted relationships are not formed based on existing Small World network theories; on the contrary, it has been treated as a base for building and maintaining a trusted community. The trusted relationships within SEP group members not only contributes to network interoperability through user cooperation in terms of leader election, but it ensures system resiliency and user privacy through contribution in terms of state management.

6.5. Future Works

This work is an experiment driven research rather than a pure literature review. Due to the inherent limitations of evaluating real world networks and the considerable quantity of reference material, we used network simulation to implement our design goals and validate our research hypotheses. This provides an understanding of current developments, as well as the challenges facing Ubiquitous Computing systems. This research has revealed that current tools and technologies do not support privacy within scalable ubiquitous networks. Considering the ubiquitous use of the systems that we reviewed, the analysis we carried out and the experiments we conducted generated more questions. Considering the ubiquitous use of the P2P applications and rising concerns for system security and user privacy, it is crucial to address those issues. Given the scope of the project and time limitation, addressing all of the challenges would not be possible. Therefore, in the following, we identify the directions for future work following this project.

6.5.1. Multiple Groups Membership

The main objective of the anonymity proposed in SEP is to maintain user privacy. SEP strives to anonymise user's identity as much as possible without compromising efficiency and effectiveness. It includes advertising node state only at a local scale and withholding user's identity from anyone outside the group in search and broadcasting. The topology construction algorithm introduced in the SEP framework limits node membership to only one group. In order to join a group, a node should make its attributes and affiliation known to its Service Centre. The system ensures the correctness of the membership list by comparing the list of nodes to detect discrepancies. Unlike declared community groups and attributes publication (Khambatti *et al.*, 2002), SEP uses the existing associations to form groups. The advertisement and discovery are achieved locally for members of the group. If a member is located outside of the group, the communications and message forwarding are administered by the Service Centre,

maintaining user anonymity. For future direction, we will look into the possibility of multiple group membership and evaluate its effect on network interoperability as well as user privacy.

6.5.2. Efficient Cryptography & Misbehaving Nodes Solutions

The additional overhead on the SEP operations is justified with the aim of improving security, system resiliency and user privacy. The system uses public key infrastructure. Each Service Centre is responsible for providing and distributing the digital certificates to individual users after they join a group. For future work, we will be pursuing an efficient key management strategy to replace public key encryption mechanism and certificate based key distribution to improve efficiency and overhead.

Misbehaving nodes or sleeping cells may raise privacy and security concerns to SEP system. This is one of the main challenges that cannot be completely rectified. This is true in human relationships as well. Nodes may change their behaviour as a result of changes in their interests. However, the fear of misbehaving or suspicious nodes should not prevent community trust. In human relations, it has been established as social norm that we have to be cautious in choosing friends. However, a small group of nodes or a high degree node acting maliciously may have catastrophic impacts on not only user privacy, but the system operability. For future direction, we need to conduct a threat analysis to outline the implications of such scenario and propose security mechanisms as well as robust detection and prevention methods.

6.5.3. Real World Overlay Protocol Deployment

We plan to implement the SEP framework to be deployed with different real world overlay protocols and applications such as Skype. Skype is one of the most efficient applications for end-to-end communication that utilises fully distributed resources of its users in order to provide improved communications. We would like to include Skype implementation within our framework design and use the clustering technique within Skype. This was out of scope of our work. In addition, this was not possible due to the unavailability of the Skype documentation and source code. However, this can be resolved by inclusion of several machines within different locations and setting up Skype nodes in order to evaluate the effect of node and topology stress as explained in chapter 4.

6.5.4. Unicast Protocols with Cache Replacement

Freenet uses cache replacement in order to provide anonymity to the users who share content online. The success or even the failure of the performed queries is not guaranteed. We believe that, the cache replacement technique may improve the anonymity and at the same time improving the efficiency and reduce the control overhead. Although the design limitations and lack of scope for better scalability in Freenet prevent ubiquitous deployment of the application, the concept of the user privacy within autonomous systems is appealing. Freenet does not assign any role or responsibility to a specific user. This provides robustness to the system and makes it reliable against targeted attacks at the same time introducing inefficiency. We will consider the cache replacement capability within SEP unicast protocol to improve privacy for autonomous users and increase the efficiency of the lookup process and end-to-end communications.

6.6. Summary

This chapter concludes the thesis with summary of the findings and brief evaluation of the results generated from the experiments. It highlights the research challenges we have addressed in this work. Furthermore, it presents the future directions that can be taken following our work in this project.

References

Aberer, K. (2005). “Managing trust in distributed environments,” *Proceedings. International Conference on Pervasive Services 2005* (IEEE Cat. No. 05EX1040), p 4.

Access, S. (2014). Internet Society Global Internet Report 2014. Available on http://www.internetsociety.org/sites/default/files/Global_Internet_Report_2014_0.pdf. [Retrieved September 2014].

Adamic, L, A. Lukose, R, M. Puniyani, A, R. and Huberman, B, A. (2001). “Search in Power-Law Networks”. *Phys*. Rev. E 64, 046135.

ADAR, E., AND HUBERMAN, B. A. (2000), Free Riding on Gnutella. *First Monday, Internet Journal* (Oct.). Available at http://www.firstmonday.dk/issues/issue5_10/ adar/index.html.

Albert, R, Jeong, H and Barabási, A.-L. (2000). “Attack and Error Tolerance of Complex Networks”. *Nature*, (406):378.

Albert, R. (2005). Scale-free networks in cell biology. *Journal of Cell Science,* 118(Pt 21), 4947–57. doi:10.1242/jcs.02714.

Albert, Réka; Barabási, Albert-László (2002). "Statistical mechanics of complex networks". *Reviews of Modern Physics* 74: 47–97.

Al-Muhtadi, J. S. Chetan, a Ranganathan, and R. Campbell, R. (2005). “Super spaces: a middleware for large-scale pervasive computing environments,” *IEEE Annual Conference on Pervasive Computing and Communications Workshops*, pp. 198-203.

Andersen, D., Balakrishnan, H., Kaashoek, F., & Morris, R. (2002). Resilient overlay networks. *ACM SIGCOMM Computer Communication Review,* 32(1), 66. doi:10.1145/510726.510740

Anderson, D. Balakrishnan, H. Kaasshoek, F and Morris, R. (2002). ‘Resilient Overlay Networks, *Master's thesis, Department of EECS, MIT*. http://nms.lcs.mit.edu/projects/ron/.

Arabo, A. Shi, Q. and Merabti, M. (2009). Context-Aware Identity Management in Pervasive Ad-hoc Environment, *International Journal of advanced Pervasive and Ubiquitous Computing.* PP, 29-42.

Arabo, A. Shi, Q. and Merabti, M. (2009). Context-Aware Identity Management in Pervasive Ad-hoc Environment, *International Journal of advanced Pervasive and Ubiquitous Computing.* PP, 29-42.

Arabo, A. Shi, Q. and Merabti, M. (2012). Privacy Preserving Identity Management in Pervasive Ad-hoc and Context Sensitive environment, *Journal of Ambient Intelligence and Humanized Computing.*

Baeza-yates, R & Cambazoglu, B. B. (2014). 'Scalability and Efficiency Challenges in Large-Scale Web Search Engines'. *Disclaimer Dis*, 1–90.

Bahl, P., and Padmanabhan, (2000). V. RADAR: An in-building RF-based user location and tracking system. *In Proceedings of IEEE Infocom*, Los Alamitos, pp. 775–784.

Ball, P. (2014). 'Wisdon of Crowd': The Myths and realities'. *www.bbc.com*. [Retrieved July 2014].

Bamberger, Walter (2010). "Interpersonal Trust – Attempt of a Definition". *Scientific report*, Technische Universität München. Retrieved 2011-08-16.

Banerjee, S. Bhattacharjee, B. and Kommareddy, K. (2002). "Scalable Application Layer Multicast," *in Proceedings of conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM'02)*, vol. 32, no. 4, pp. 205–217.

Barabási, A. (2002). Linked: The New Science of Networks. Perseus, Cambridge, MA

Barabasi, A. Albert, R and Jeong, H. (1999). Mean field theory for scale-free random networks, *Physica*. A 272. 173-187

Barabási, A. Bonabeau, E. (2003). Scale-free Networks, *Scientific American*

Barabási, A.(2003). "Linked: How Everything is Connected to Everything Else and What It Means for Business, Science, and Everyday Life." *New York: Plume*.

Baset, S. a, & Schulzrinne, H. G. (2006). An Analysis of the Skype Peer to Peer Internet Telephony Protocol, 1–11.

Baumgart,I. Bernhard, H and Krause, S (2007). "OverSim: A Flexible Overlay Network Simulation Framework". *Proceedings of 10th IEEE Global Internet Symposium (GI '07) in conjunction with IEEE INFOCOM 2007*, Anchorage, AK, USA.

Bazli, B, Llewellyn-Jones, D. Merabti, M. (2014). 'Privacy Concerns within Scalable P2P Systems', *in proceeding of, World Symposium on Computer and Network & Information Security.*

Bazli,B. Llewellyn-Jones, D. Merabti, M. (2011). 'Using Network Infrastructure to enhance Security and Trust within Ubiquitous Computing Network', *13th Symposium on the Convergence of Telecommunications, Networking and Broadcasting, PGNET*, Liverpool, UK.

BBC News. (2009). Scots swine flu cases confirmed". Archived from the original on 30 April 2009. [Retrieved 27 April 2009].

Bennett, C. J., & Raab, C. D. (2006). *The governance of privacy: Policy instruments in global perspective*.

Bondi, André B. (2000). "Characteristics of scalability and their impact on performance". *Proceedings of the second international workshop on Software and performance - WOSP '00*. p. 195. doi:10.1145/350391.350432. ISBN 158113195X.

Boritz, J. Efrim. (2005). IS Practitioners' Views on Core Concepts of Information Integrity. *International Journal of Accounting Information Systems. Elsevier*.

Boukerche, A. Yonglin Ren. (2008). "A trust-based security system for ubiquitous and pervasive computing environments," Computer Communications, v 31, n 18, p 4343-51, 18 Dec.

Castells, M., (2010). The Information Age: Economy, Society and Culture Volume 1: The Rise of the Network Society. 2nd ed. Oxford: Wiley Blackwell.

Cavoukian, A. (2001). Taking Care of Business: Privacy by Design. Toronto. Retrieved from http://www.ontla.on.ca/library/repository/mon/2000/10296375.pdf [Accessed Nov 2013]

Chawathe, Y., Ratnasamy, S., Breslau, L., Lanham, N., & Shenker, S. (2003). Making gnutella-like P2P systems scalable. Proceedings of the 2003 Conference on Applications Technologies Architectures and Protocols for Computer Communications SIGCOMM 03, 25, 407. doi:10.1145/863955.864000

Chen, G. (2004). "Solar : Building A Context Fusion Network for Pervasive Computing," *Security*.

Chen, R and Yeager, W. (2001). "Poblano. A Distributed Trust Model for Peer-to-Peer Networks," *Sun Microsystems.*

Chung, Y. (2012). "Distributed denial of service is a scalability problem," *ACM SIGCOMM Comput. Commun*. Rev., vol. 42, no. 1, p. 69.

Clarke, I. (1999). Freenet: A Distributed Anonymous Information Storage and Retrieval System, available at http://freenetproject.org/freenet.pdf.

Clauset. Aaron, (2011). "Inference, Models and Simulation for Complex Systems", Lecture Notes.

Cohen, R. Havlin, S. and ben-Avraham, D. (2003). "Efficient Immunization Strategies for Computer Networks and Populations," Physical Review Letters, vol. 91.

Dame, N, (2002) “Statistical mechanics of complex networks,” World Wide Web Internet and Web Information Systems, vol. 74.

Deng, K., Hu, K., & Tang, Y. (2011). Evolving network models under a dynamic growth rule, 5. Physics and Society. Retrieved from http://arxiv.org/abs/1108.1597

Dimartino-Marriott, Martin (2009). "Comment: Darren Brown’s Interpretation of the Wisdom of Crowds". MartinBlueprint.co.uk. [Retrieved June 2013].

Dionne, S. D., & Dionne, P. J. (2008). Levels-based leadership and hierarchical group decision optimization: A simulation. The Leadership Quarterly, 19(2), 212-234.

Dixon, C., Uppal, H., Brajkovic, V., Brandon, D., Anderson, T. and Krishnamurthy, A. (2011). ‘ETTM: a scalable fault tolerant network manager’. *In Proceedings of the 8th USENIX conference on Networked systems design and implementation* (pp. 85-98). USENIX Association.

Douceur, J. Mar. (2002) The Sybil attack. In Proceedings of the First International Workshop on Peer-to-Peer Systems.

Duboc, Leticia; Rosenblum, David S.; Wicks, Tony (2006). "A framework for modelling and analysis of software systems scalability". Proceeding of the 28th international conference on Software engineering - ICSE '06. p. 949. doi:10.1145/1134285.1134460. ISBN 1595933751.

Dwyer, C. Hiltz, S, R. and Passerini, K. (2007) “Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace,” *Proceedings of the Thirteenth Americas Conference on Information Systems*, Keystone, Colorado.

Dyke, C, V and Koç, Ç, K. 2003. “On Ubiquitous Network Security and Anomaly Detection,” *Manager*, pp. 374-378.

Edwards, W and Grinter, R. (2001) “At Home with Ubiquitous Computing: Seven Challenges,” *Proc. 3rd Int’l Conf. Ubiquitous Computing, Lecture Notes in Computer Science 2201*, Springer-Ver- lag, Berlin, pp. 256–272; www.parc.xerox.com/csl/members/grinter/ubicomp.pdf.

El Defrawy, K. Gjoka, M. and Markopoulou. A. (2007). Bottorrent: Misusing bittorrent to launch ddos attacks. *In Proc. of USENIX* – SRUTI.

Erdős, P.; Rényi, A. (1959). "On Random Graphs. I". Publications Mathematics 6: 290–297.

European Directive. (2013). "What about the "EU Cookie Directive"?". WebCookies.info.

Fall, K. & Varadhan, K., (2011). The ns Manual. *The VINT project*, (3), p.434. Available at: http://discovery.bits-pilani.ac.in/discipline/csis/virendra/bitsc481/ns_doc.pdf.

Faloutsos, M. Faloutsos, P and Faloutsos, C. (1999).“On power-law relationships of the Internet topology,” *ACM SIGCOMM Computer Communication Review*, vol. 29, no. 4, pp. 251-262.

Flake, G, W. Lawrence, S. Giles, C, L and Coetzee, G, M. (2002). Self-Organization and Identification of Web Communities. *In IEEE Computer*, 35(3), 66- 71

Fotouhi, B., & Rabbat, M. G. (2013). Degree Correlation in Scale-Free Graphs. Statistical Mechanics; Data Analysis, Statistics and Probability; *Physics and Society*. doi:10.1140/epjb/e2013-40920-6.

Fox, L. (2013). NSA Spying Included Major Internet Giants, Washington Post, *http://www.usnews.com/news/articles/2013/06/06/washington-post-nsa-spying-included-major-internet-giants.* [Retrieved July 2014].

Gallos, L, K. Cohen, R. Argyrakis, P. Bunde, A and Havlin, S. (2005), Quantifying Network Nulnerability, *Phys. Rev. Lett*. 94, 188701.

Garg, V. K. (2004). Leader Election, 3, 209–219.ISBN 047143230X

Gellersen, H, W. Beigl, M. Krull, H. (1999). “The MediaCup: awareness technology embedded in an everyday object,” Handheld and Ubiquitous Computing. *First International Symposium, HUC'99. Proceedings* (Lecture Notes in Computer Science Vol.1707), p 308-10.

Gelman, A. and Hill, J. (2006). ‘Data analysis using regression and multilevel/hierarchical models’. *Cambridge University Press.*

Gomm R, Hammersley M, Foster P. (2000). ‘Case study method: Key issues, key texts’. *Sage Publications*, London.

Gonz´alez,M, C, Hidalgo,C, A. and A.-L. Barab´asi, (2008). ‘Understanding individual human mobility patterns’. *Nature* 453, 779–782.

Goyal, P. Harrick, M. and Cheng, H. (2009). ‘Start-time Fair Queueing: A Scheduling Algorithm for Integrated Service Packet Switching Networks’. *Technical Report – 96 -02. Department of Computer Science.* University of Texas at Austin

Greenberg, B, A. Hamilton, J, R. Kandula, S. Kim, C. Lahiri, P. Maltz, A. Patel, P. and Sengupta, S. (2009). “VL2 : A Scalable and Flexible Data Center Network,” Access, vol. 09, pp. 95–104.

Gross, R., & Acquisti, A. (2005, November). Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society* (pp. 71-80). ACM.

Gupta, A. Liskov, B. and Rodrigues, R. (2003). “Efficient Routing for Peer-to-Peer Overlays.”

H. Institutes and L. Sciences, (1979). “Scale- free networks in cell biology,” Physics.

Haladjian, R. (2006) "Violet press release -- Nabaztag's platform has buckled under the weight of all the new Rabbits!".

Han, S, W. Y. B. Yoon, Y,B. Youn, H, Y. (2004) “A new middleware architecture for Ubiquitous Computing environment,” Second IEEE Workshop on Software Technologies for Future Embedded and Ubiquitous Systems, pp. 117-121.

Harris, David; O'Boyle, Michael; Warbrick, Colin (2009). Law of the European Convention on Human Rights (2nd ed.). New York: Oxford University Press. pp. 549–556. ISBN 978-0-406-90594-9.

Hawley, K. (2008). Trust, Distrust and Commitment 1. pp,1–39.

Hayes, B. 2000. Graph Theory in Practice: Part II. American Scientist. 88(2): 104-109.

Hayrynen, T. (2005). “The Barabasi-Albert Scale-Free Model,” pp. 1-17

He, Y., Perkins, D. & Huang, B., (2008). S-Box : A Scalability Analysis Framework for Ad Hoc Routing Protocols. pp.572–578.

Henderson, T. (2009). ‘Improving Simulation Credibility through Open Source Simulations’. *Simutools Conference*. University of Washington

Henshaw, J. (2013), Complex systems, The Encyclopaedia of Earth. [Retrieved June 2014].

Hieronymi, Pamela (2008): ‘The Reasons of Trust’, Australasian Journal of Philosophy, 86.2: 213-236.

Hightower, J., & Borriello, G. (2001). Location systems for Ubiquitous Computing. Computer, 34(8), 57–66. doi:10.1109/2.940014

Hill, R. Al-Muhtadi, J. Campbell, R. Kapadia, A. Naldurg, P, and a Ranganathan, A. (2004)“A Middleware Architecture for Securing Ubiquitous Computing Cyber Infrastructures,” IEEE Distributed Systems Online, vol. 5, no. 9, pp. 1-1.

Hoff, B. (2012). “Overlay Networking: vLANs for the Cloud”. Innovation in Action, Interview by Arthur Cole. Avaialvle at [http://www.conference.cn/En/Conference.asp?ArticleID=1006] [accessed October 2014].

Holland. R, Dalton. A, (2003), The University of Tennessee, Centre for Profitable Agriculture,

Hosseini, M. Ahmed, D. T, Shirmohammadi. S, and N. D. Georganas. N. D, (2007). “A Survey of Application-Layer Multicast Protocols,” Communications Surveys & Tutorials, IEEE, vol. 9, no. 3, pp. 58–74.

Hsiao-Hwa Chen (2007), The Next Generation CDMA Technologies, John Wiley and Sons, pp. 105–106, ISBN 978-0-470-02294-8.

ICAEW. (2011). BUILDING TRUST IN THE DIGITAL AGE : RETHINKING PRIVACY, PROPERTY and security. Page 11-12

IETF. (2011). “HTTP State Management Mechanism – Overview”. April 2011.

Ithiel, P. Kochen, M. (1979). Contacts and Influence. Social Networks.

Jackson, T (1996). "This Bug in Your PC is a Smart Cookie". Financial Times. [Retrieved April 2014].

Jacob, E., & Orters, P. M. (2012). Spatial preferential attachment networks: power-laws and clustering coefficients ¨, pp, 1–25.

Jahanbakhsh, K. Shoja, G and King, V. (2010). “Social-Greedy: a socially-based greedy routing algorithm for delay tolerant networks”. In Proceedings of the Second International Workshop on Mobile Opportunistic Networking (MobiOpp '10). ACM, New York, NY, USA, 159-162. DOI=http://dx.doi.org/10.1145/1755743.1755773

Jakubowski, M. Venkatesan, R. and Yacobi, Y “Quantifying Trust,” pp. 1-9.

Jakubowski, M., Venkatesan, R. & Yacobi, Y. (2010). “Quantifying Trust”. Microsoft Research, p.1-9.

Janson, S., Lavault, C., & Louchard, G. (2008). Convergence of some leader election algorithms. arXiv preprint arXiv:0802.1389.

Jawad, M. Serrano-alvarado, P and Valduriez, P. (2013).“Supporting Data Privacy in P2P Systems Table of Contents,” pp. 1–51.

Jeffery. R. (2010). The Web means End of forgetting. New York times, 19th July

Jinshan Liu, Valérie Issarny, (2007). “An incentive compatible reputation mechanism for Ubiquitous Computing environments,” International Journal of Information Security, v 6, n 5, p 297-311.

Joseph, Claudia. (2014). “Google Glass: Is this the Death of privacy?”. The New Zealand Herald. June 29th.

Joshi, Rajive, (2011), Data-Centric Architecture: A Model for the Era of Big Data, [retrieved from www.drdobbs.com on July 2014].

Kagal, L. Finin, T. and Joshi, A. (2001). "Trust-based security in pervasive computing environments," Computer, vol. 34, pp. 154-7.

Kak, A. (2001) “Small World Peer-to-Peer Networks and their Security Issues”, Purdue University, Lecture Notes. Vol 2.

Keerthi, T. Bandara, A. Price, B. and Nuseibeh, B. (2013). Distilling Privacy Requirements for Mobile Applications. In: 36th International Conference on Software Engineering (ICSE 2013), 31 May - 7 June 2013.

Khambatti, M. Ryu, K. & Dasgupta, P. (2002). ‘Peep-to-Peer communities: formation and Discovery’. Arizona State Universitye.

Kleinberg, J, M. (2000). “Navigation in a Small World”. Nature 406, 845.

Kleinberg, J. 2000. Navigation in a Small World. Nature, 406:845.

Kochen, M (ED.). (1989). The Small World. Norwood, NJ: Ablex.

Krause, S and Hubsch, C. (2010) “Scalable Appliction Layer Multicast Simulations with OverSim”, Institute of telematics, University of Karlsruhe, Germany, IEEE Communications.

LaMarca, A., Chawathe, Y., Consolvo, S., Hightower, J., Smith, I., Scott, I., Sohn, T., Howard, J., Hughes, J., Potter, F., Tabert, J., Powledge, R., Borriello, G., and Schilit, B. (2005). Place Lab: Device positioning using radio beacons in the wild. In Proceedings of the International Conference on Pervasive Computing (Pervasive 2005), pp. 116–133. Munich, Germany.

Lamb, D, J. (2009). Developing a Global Observer Programming Model for Large-Scale Networks of Autonomic Systems, Doctorate Thesis. UK.

Lao, L. Cui, J. Gerla,M and Maggiorini, D. (2005). “A Comparative Study of Multicast Protocols: Top, bottom, or in the Middle?, Technical Report. Computer Science Department. UCLA.

Laudon, K. Traver,C and Guercio, C. (2008). E-commerce: Business, Technology, Society. Pearson Prentice Hall. ISBN 9780136006459.

Li, Y. Tian, C. Diggavi, M, C. and Calderbank, R. (2010). Network resource allocation for competing multiple description transmissions. IEEE, Trans. Comm. 58, 5. pp. 1493-1504.

Li, Y. Tian, T. Diggavi, S. Chiang, M and Calderbank. A. (2010). “Network resource allocation for competing multiple description transmissions,” IEEE Trans. Commun., vol. 58, no. 5, pp. 1493–1504.

Liu, L., Yu, E. & Mylopoulos, J., 2003. Security and privacy requirements analysis within a social setting. Proceedings. 11th IEEE International Requirements Engineering Conference, 2003.

Living, P and Links, R. (2000). “EasyLiving,” no. 2000, pp. 2000-2001.

Llewellyn-Jones, D. Merabti, M. Shi, Q. & Askwith, B. (2009). Trusted Digital Rights Management in Peer-to-Peer Communities. Developments in eSystems Engineering (DESE), Second International Conference on, 211–219. doi:10.1109/DeSE.2009.54

Lua, E, K. Crowcroft, J. Pias, M. Sharma, R and Lim, S. (2005). "A Survey and Comparison of Peer-to-Peer Overlay Network Schemes," *IEEE Comm. Surveys and Tutorials*, vol. 7, no. 2.

LV, Q., CAO, P., COHEN, E., LI, K., AND SHENKER, S. (2002). Search and Replication in Unstructured Peer-to-Peer Networks. In Proceedings of 16th ACM International Conference on Supercomputing (ICS’02) (New York, NY, June 2002).

Marsh, Gerald (2011): ‘Trust, Testimony and Prejudice in the Credibility Economy’, Hypatia, a Journal of Feminist Philosophy 26.2, 280-93.

Marvel, Seth A.; Martin, Travis; Doering, Charles R.; Lusseau, David; Newman, M. E. J. (2013)The small-world effect is a modern phenomenon. Cornell University Library.

Masticola,, S. . Bondi, A, B. and Hettish, M. (2005). Model-based scalability estimation in inception-phase software architecture. In Proc. ACM/IEEE 8th Int’l Conference on Model Driven Engineering Languages and Systems, pages 355–366.

Mathias, N. and Gopal, V. (2001). "Small Worlds: How and why," Physical Review E, vol. 63, pp. 12

McCallion, J. (2014). Apple: Celeb Photo breach wasn’t iClouds fault. www.pcpro.co.uk. [Retrieved September 2014].

McGeer, Victoria (2008): ‘Trust, Hope and Empowerment’, Australasian Journal of Philosophy, 86.2: 237-54.

McKnight, D. H., and Chervany, N. L. (1996). The Meanings of Trust. Sciedubocntific report, University of Minnesota.

McLuhan, Marshall (1962). The Gutenberg Galaxy : the making of typographic man. Toronto, Canada: University of Toronto Press. p. 293. ISBN 978-0-8020-6041-9.

McLuhan, Marshall.(1987). “Letters of Marshall McLuhan”. (Oxford University Press, 1987) p254.

Modarres, M. Kaminsky, M. Kristove, V. (1999). Reliability Engineering and Risk Analysis. ISBN 0-8247-2000-8, Library of Congress Catalog. Online Version.

Morozov, E. (2011). The net delusion: The dark side of Internet freedom. New York, NY: Public Affairs.

MSDN, Microsoft, Design for Scalability, (2003), [Retrieved from www.msdn.microsoft.com on June 2014].

Mu, B and Yuan, S. (2010). "A method for evaluating initial trust value of direct trust and recommender trust," Computer Design and Applications (ICCDA), 2010 International Conference on, vol.2, no., pp.V2-185,V2-190, 25-27.

Nguyen, D. T., Nguyen, B. Le, & Vu, D. L. (2009). Improving Freenet's Performance by Adaptive Clustering Cache Replacement. 2009 IEEE-RIVF International Conference on Computing and Communication Technologies, 1–7. doi:10.1109/RIVF.2009.5174645

Nguyen, D. T., Nguyen, B. Le, & Vu, D. L. (2009). Improving Freenet's Performance by Adaptive Clustering Cache Replacement. 2009 IEEE-RIVF International Conference on Computing and Communication Technologies, 1–7. doi:10.1109/RIVF.2009.5174645.

Nikiforakis, N. Acar, G. (2014). Browse at Your Own Risk. IEEE Spectrum. August Version.

Noulas, A. Scellato, S. Lambiotte, R. Pontil, M. and Mascolo, C (2012). "A tale of many cities: Universal patterns in human urban mobility. PLoS ONE 7, 1–10 (2012).

Nowostawski, M., & Foukia, N. (2007). Social Collaboration, Stochastic Strategies and Information Referrals. 2007 IEEE/WIC/ACM International Conference on Intelligent Agent Technology (IAT'07), 416–419. doi:10.1109/IAT.2007.100

Number, O. M. G. D., Associated, S., & Files, N. M. (2011). OMG Unified Modeling Language TM (OMG UML), *Superstructure*, (August). [Retrieved August 2014].

O'Connor, Patrick D. T. (2011), Practical Reliability Engineering (Fourth Ed.), John Wiley & Sons, New York. ISBN 978-0-4708-4462-5.

Panda, G, K. Tripathy, B, K. and Jha, S, K. (2011). "Security Aspects in Mobile Cloud Social Network Services," Int. J. vol. 2, no. 1.

Papers, R and Meng, J et al,. 2008. "Communications and Networking," vol. 2, no. 1.

Patel, J. Teacy, W,T,L. Jennings, N,R. and Luck, M. (2005). "A probabilistic trust model for handling inaccurate reputation sources," presented at Third International Conference on Trust Management, iTrust 2005, Paris, France

Patterson, S. & Bamieh, B. (2010). 'Leader Selection for optimal network coherence. Proceeding of the IEEE Conference on Decision and Control, 2692- 2697

Pfleeger, C. Pfleeger, S. (2006), Security in Computing, 4th Edition, Prentice Hall, NJ. US. ISBN:013035548-8.

Portmann. M, Sookavatana. P, Ardon. S. and Seneviratne, (2001), A. The cost of peer discovery and searching In the Gnutella peer-to-peer file sharing protocol. In Networks, 2001. Proceedings. Ninth IEEE International Conference. Pages 263–268.

Ranganathan, P, (2011). From Micro-Processors to Nanostores, Rethinking data-centric Systems, (January), pp.39–48.

Redner. S ,Krapivsky, L. F, (2008). "Evolving (Preferential Attachment) Networks", Lecture notes, Boston University.

Renesse, R. Van, Birman, K. P., & Vogels, W. (2003). Astrolabe : A Robust and Scalable Technology For Distributed System Monitoring , Management , and Data Mining, pp. 1–43.

Resnick, P. (2002). "Trust Among Strangers in Internet Transactions : Empirical Analysis of eBay' s Reputation System," Most.pp. 1-26.

Ripeanu, M. (2001). Peer-to-peer architecture case study: Gnutella network. Proceedings First International Conference on Peer-to-Peer Computing, 1–11. doi:10.1109/P2P.2001.990433

Ritter, J. (2001). Why Gnutella Can't Scale. No, Really. Available on http://www.cs.rice.edu/~alc/old/comp520/papers/ritter01gnutella-cant-scale.pdf. [Retrieved December 2013].

Rowstron, A. and Druschel, P.(2001). "Pastry : Scalable, distributed object location and routing for large-scale peer-to-peer systems". IFIP/ACM International Conference on Distributed Systems Platforms, Germany, pages 329-350.

Ruohonen, K. (2013), Graph Theory, PDF access from http://math.tut.fi/~ruohonen/GT_English.pdf in December 2013

Sabater, J and Sierra, C, (2002). "Reputation and social network analysis in multi-agent systems," *presented at First International Joint Conference on Autonomous Agents and Multi-Agent Systems*, AAMAS '02, New York, NY, USA.

Sabater, J and Sierra, C, (2005). "Review on computational trust and reputation models," *Artificial Intelligence Review*, vol. 24, pp. 33-60.

Saroiu, S., Gummadi, P. K., & Gribble, S. D. (2002). A Measurement Study of Peer-to-Peer File Sharing Systems. Network, 2002, 152. Retrieved from

[http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.74.7773&rep=rep1&type=pdf]

Saunders, M., Lewis, P. and Thornhill, A., (2003). Research methods.

Schank, T & Wagner, D. (2004). Approximating Clustering Coefficient and Transitivity, University of Karlsruhe, Project file, http://i11www.iti.uni-karlsruhe.de/_media/projects/spp1126/files/sw-acct-05.pdf, retrieved June 2014

Schilit, B. Adams, N. and Want, R. (1994)."Context-aware computing applications". IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'94), Santa Cruz, CA, US. pp. 89–101. CiteSeerX: 10.1.1.29.5833.

Seibert, J., Fahmy, S., & Nita-rotaru, C. (2008). "Won"t You Be My Neighbor ?' Neighbor Selection Attacks in Mesh-based Peer-to-Peer Streaming. Computer. doi:10.1.1.154.8235

Sen, A. and Wang, J. 2004. "Analysing Peer-To-Peer Traffic," vol. 12, no. 2, pp. 219–232.

Sen. Rockefeller. (2011). "Get Ready for a Real Do-Not-Track Bill for Online Advertising". Adage.com

Siegemund, F. 2004. A Context-Aware Communication Platform for Smart Objects. In Pervasive Computing: Second International Conference, PERVASIVE 2004, volume 3001 of LNCS. Springer-Verlag.

Soldatos, J. Pandis, I. Stamatis, K. Polymenakos, L and J. Crowley, J. (2007). "Agent based middleware infrastructure for autonomous context-aware Ubiquitous Computing services," Computer Communications, vol. 30, no. 3, pp. 577-591.

Søren, A. Peter, G. W. (2007). "Stochastic Simulation: Algorithms and Analysis". Springer. Series: *Stochastic Modelling and Applied Probability*, Vol. 57.

Srinivasan, R. (2013). Complex Networks, Lecture Notes PDF (www.ma.utexas.edu/users/rav/ComplexNetworks/ComplexNetworks.Lecture12.Notes.pdf). [Accessed June 2014].

Stajano, F, (1992). Security Issues in Ubiquitous Computing .0000, pp.1–34.University of Cambridge Computer Laboratory.

Stoica, I. (2004). Overlay Networks, *Lecture Notes*, University of California, Berkeley, pp, 1–20. [Retrieved June2014]

Stoica, I. Morris, R., (2003) "Chord: A Scalable Peer-to-Peer Lookup Protocol for Internet Applications," IEEE/ACM Trans. Net., vol. 11, no. 1, pp. 17–32.

Stutzbach, D. (2006). Understanding churn in peer-to-peer networks, proceedings of the 6th ACM SIGCOMM, 189. Doi:10.1145/1177080.1177105

Surowiecki, J. ‘The Wisdom of Crowds’. (2005). ISBN: 978-0385721707, Anchor Publishers, US

Taubenberger, J.K and Morens, D.M. (2006). “1918 Influenza: the mother of all pandemics.” Emerging infectious diseases, vol. 12, no. 1, pp. 15-22.

Tsang. P and Smith, S, W. (2008). “PPAA : Peer-to-Peer Anonymous Authentication (Extended Version),” Science.

Varga, A. (2001). “The OMNET++ Discrete Event Simulation System,” Proc. of the European Simulation Multi conference. http://whale.hit.bme.hu/omnetpp/

Varshavsky, A., & Patel, S. (2010). ‘Location in Ubiquitous Computing’, *Chapter 7*. 285–320. Available at *http://abstract.cs.washington.edu~shwetak/classes/cse590p/notes/location_preview_draft.pdf*

Vega, T. (2010). "New Web Code Draws Concern Over Privacy Risks". *The New York Times*. [Retrieved July 2013]

Venkataraman, V. Yoshida, K. and Francis, P. (2006). Chunkyspread: Heterogeneous unstructured tree-based peer-to-peer multicast. *In Proc. of IEEE ICNP*.

Virendra, M. Jadliwala, M. Chandrasekaran, M. and Upadhyaya, S. (2005). “Quantifying trust in mobile ad-hoc networks,” *International Conference on Integration of Knowledge Intensive Multi-Agent Systems*. pp. 65-70, 2005.

Vogt, H. (2005). ‘Small Worlds and the Security of Ubiquitous Computing’. *Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks*, 593–597. doi:10.1109/WOWMOM.2005.98

Vogt, H. (2005). Small Worlds and the Security of Ubiquitous Computing. *Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks*, 593–597. doi:10.1109/WOWMOM.2005.98.

Walia, N. Zahedi, F.M. (2013) "Success Strategies and Web Elements in Online Marketplaces: A Moderated-Mediation Analysis of Seller Types on eBay," *Engineering Management, IEEE Transactions* on , vol.60, no.4, pp.763,776.

Warren and Brandies. (1890). “The Right to Privacy”. 4th Harvard Law Reviews 193.

Watts, D, J. and Strogatz, S, H. June. (1998) . “Collective dynamics of ‘small-world’ networks.” *Nature*, vol. 393, no. 6684, pp. 440-2.

Wei, Y. Wang, C. Chu, Y. and Chang, R. (2012). "A Secure and Stable Multicast Overlay Network with Load Balancing for Scalable IPTV Services*," Int. J. Digit. Multimedia. Broadcast.* pp. 1–12.

Weinstock, C. B., & Goodenough, J. B. (2006). On System Scalability, (March).

Weiser, M and J. S. Brown, J, S. 1996. "T H E C O M I N G AG E O F CALM TECHNOLOGY 1," Technology, vol. 1, no. July, pp. 1-17.

Weiser, M. (1991). The Computer for the 21 century. *Scientific American*, 265(3), p.94-104.

Weiser, M. (1993). Hot topics-Ubiquitous Computing. Computer, 26(10).

Wellman, B and Hampton, K. (1999). "Living Networked in a Wired World". *International Journal of Urban & regional research*. vol. 28, no. 6, pp. 1-12.

Xiao, W. Qin, Y. and Parhami, B. (2007). "Extended Clustering Coefficients of Small-World," pp. 67-73, 2007.

Xiaowen Chu, Xiaowei Chen, Kaiyong Zhao, Jiangchuan Liu. (2010). "Reputation and trust management in heterogeneous peer-to-peer networks," Telecommunication Systems, v 44, n 3-4, p 191-20.

Yalagandula, P., & Dahlin, M. (2004). Research Challenges for a Scalable Distributed Information Management System, pp,1–18. [Retrieved July 2014].

Yang, J. Shi, J. Jin, Z and Zhang, H. (2002). Design and implementation of a large-scale hybrid distributed graphics system, Proceedings of the Fourth Eurographics Workshop on Parallel Graphics and Visualization, September 09-10, 2002, Blaubeuren, Germany.

Yao, Z., Wang, X., & Loguinov, D. (2006). Modeling Heterogeneous User Churn and Local Resilience of Unstructured P2P Networks,pp, 1–34.

Zhang, H. and Goel, A (2004) "Using the small-world model to improve Freenet performance," Computer Networks, vol. 46, no. 4, pp. 555-574, Nov. 2004.

Zhang, Y. Rajimwale,A. Arpaci-Dusseau, A. and Arpaci-Dusseau, A. (2014). "End-to-end Data Integrity for File Systems: A ZFS Case Study" (PDF). *Computer Sciences Department, University of Wisconsin.*[Retrieved June 2014].

Zheng, J. Y. Qin, J. Zhu, and X. Li, (2008). "Constructing Trust Networks Based on Small-World Theories," *The 9th International Conference for Young Computer Scientists*'. pp. 1957-1962.

Zhu, H and Huang, Z, X. (2004). "Navigation in a Small World with local information." *Physical review. E, Statistical, nonlinear, and soft matter physics*, vol. 70, no. 3 Pt 2, p. 036117.