A Trustable Architecture over Blockchain to Facilitate Maritime Administration for MASS Systems

Yang Wang[a,c], Peng Chen[b,c], Bing Wu[a,c], Chengpeng Wan[a,c] and Zaili Yang[d]

[a] *Intelligent Transportation Systems Research Center, Wuhan University of Technology, China.*

[b] *School of Energy and Power Engineering, Wuhan University of Technology, Wuhan, China.*

[c] *National Engineering Research Center for Water Transport Safety, China.*

[d] *Liverpool Offshore, Logistics and Marine Research (LOOM) Institute, Liverpool John Moores University, UK.*

Abstract: Maritime Autonomous Surface Ship (MASS) is widely deemed as the future of global shipping. The cyber vulnerability has however been identified as an emerging problem and a potential barrier influencing MASS development. This paper, through the investigation of the fundamental trust problem with regards to the cyber security of MASS systems, aims to develop a blockchain-based scheme for the trust management of MASS. The innovative idea of using blockchain within the MASS context is that the mobile entities in the MASS operational environment constitute a decentralized opportunity network, which makes blockchain an appealing tool to provide a solution to evaluating and maximizing the trust over the dynamics of the entities. This paper elaborates the mechanism by which the MASS entities participate in keeping the main chain. Firstly, the paper illustrates how the Belief of Trust (BoT) among the entities is encoded and assembled into the chain, to allow MASS entities to have an initial judgement towards another entity before they get acquainted. Secondly, at the consensus layer of blockchain technique, it addresses how the witness, who has a temporary right of producing a block and append it to the chain, can be elected among the nodes and how to incent the nodes to maintain the blockchain from a proof-of-stake perspective. Finally, this paper describes how the MASS entities can use the certificate dependence information to evaluate the trust transition in the MASS operating environment. Typical scenarios are delineated to show the procedure of certificate inquiry, handover of controls between maritime supervision centers and shore-side remote control centers in case of the occurrence of unexpected events. The findings provide any entity in an MASS network with an effective solution to evaluating the degree of trust he can have for any targeted node/participant. They can therefore help choose better (more trustable) nodes to maintain the MASS network's knowledge of evidence to judge the trust on an unknown member.

Keywords: Trustworthiness management, Blockchain, MASS, Decentralized entities, Cyber security, Maritime Security

1. Introduction

Maritime Autonomous Surface Ship (MASS)[1] has been keenly envisioned by industrialists, academic scholars as well as governmental bodies[1]. As early as 2012, European Union launched the research project *Maritime Unmanned Navigation through Intelligence in Networks* (MUNIN)[2], aiming to provide a pioneering concept and prototype for unmanned ships. Since then, The R&D progress of MASS seems to be proceeding at a high speed. In 2016, Rolls Royce initiated a research program, *Advanced Autonomous Waterborne Applications* (AAWA), together with a number of European partners from industry and academic community. In 2018, *Safer Vessel with Autonomous Navigation* (SVAN) was started by following AAWA. In 2019, SVAN came out with the first full autonomous ferry, *Falco*, who began her voyage between the islands near Turku, Finland.

The technological upgrading in MASS will obviously not be confined to individual ships. Instead, practice towards MASS will elicit the technological evolution of maritime administration and supervision, as well as the technological ecosystem in shipping worldwide. AAWA[3] aids to envisage how operators in a shore control center can monitor and control the remote ships, revealing a new paradigm for maritime operations in the era of MASS. In this process, shore-side control centers became the key components of the whole maritime panorama.

Motivated by the enthusiasm for high autonomy in shipping, researchers have devoted much effort on the development of the technologies relating to navigational intelligence, such as collision avoidance, route planning, and situation awareness etc. Recently, there is an increasing concern about the safety issue of using MASS systems[4]. At the current stage, the accident data of MASS are scarce[5]. The domain researchers can, through the analysis of traditional maritime accidents, principally understand the potential accident occurrence in the scenarios of autonomous shipping, and develop the corresponding risk-control measures[6][7]. Li et al focus on the collision risk for the MASS system[8].Vos et al survey the statistics of the maritime accidents during 2000-2018, and analyze how these scenarios could be like if the ships are replaced with autonomous ships[9]. Vos et al give an intuitive view about the anticipation of decreased losses in the maritime industry when the traditional navigation is evolving towards the MASS.

With the fast development of MASS research and prototype ship implementation in real world, World Maritime University predicts that by year 2040, autonomous ship under supervision will account for 15% of the total ships worldwide [10]. In this technical evolution, the digital community is expected to take its shape from the growing number of the autonomous ships. As the population of autonomous ships continues to increase, the necessity of cyberspace will in turn influence conventional ships and promote their adaptation to the digital community.

According to the IMO definition on the four autonomy levels (ALs) of autonomous ships, it is evident that the long-term evolution of MASS from low to high ALs should undergo chronic iterations both in technology and in management. This entails an intriguing question in an MASS system, i.e., how to deal with the communication and trust management among the participants? To fully understand this, we take account of the following three observations in the MASS system: (1) There will be no vocal command and control loop (i.e. VHF) between the maritime

[1] Given the large number of abbreviations used in this paper, a list of acronyms is presented in Appendix 1.

administration and the autonomous ship, whereas the maritime supervision has to be realized by digital means; (2) There will be a shore-side remote control center for autonomous ships, which makes the digital maritime administration a less flatten structure; and (3) In a highly digital maritime administrative scenario, interaction among entities of maritime participants calls for authenticated identification and communication, thus more sophisticated techniques are required. These radical changes imply that the safety issues in the era consist of not only the traditional maritime accidents in the operational aspect, but also the challenges from the cyber security[11].

In the traditional maritime routine practice where voice-based communication dominates, people usually need not doubt the genuineness about the calling and answering over the public channel. However, in the MASS scenario, the aforementioned problems call for prudent treatment against malicious entities. To make things tangible, a realistic way is to resort to the conventional solutions to information security. Theoretically, asymmetric encryption and the digital certificate technology have provided a solid foundation for identification, authentication, tamper-proof validation and confidentiality if necessary[12].

Nevertheless, the actual implementation of conventional information security methods in practical maritime environment proves to be challenging. Firstly, the connectivity of an MASS entity network is highly dynamic and instable. This implies that any asymmetric encryption-based approach has to be realized under an opportunistic circumstance, where additional considerations should be taken in contrast to its implementation in reliable network infrastructure such as the Internet. Secondly, since the navigational data exchange is of high mobility, there is no clear-cut border to define the session or transaction for the data bulk among the entities. Meanwhile, the records of the exchanged data across the network are massive and increasing in term of volume, whereas these data are not designated to specific nodes in the MASS network for storage. Thus, data acquisition rests on a peer-to-peer style, which further demands a quick and reliable way to manage trustworthiness of data distribution. Such challenges reveal two research questions :(1) What is the relation between the traditional information security and the trust management? and (2) How to propose a new methodological architecture that enables to tackle the relation between the traditional information security and the trust management?

In light of the above, this paper aims to develop a blockchain-based methodology for the trust management among the participants of an MASS system to ensure its cyber security. To achieve the aim, this paper is organized in 5 sections and their interaction is descried in Figure 1. More specifically, Section 1 is the background introduction about an MASS system, and briefly explains why cyber security is a prominent problem in an MASS system. Section 2 describes the formation of an MASS system, analyses the key technical features of blockchain, identifies the cyber security requirements of an MASS system and explores the major difficulties in the trust management in an MASS system. In Section 3, a blockchain-based methodology for the cyber security of an MASS system is developed. It first expounds the CA-based solutions to the data level protection and the basic trustworthiness warranty. Furthermore, the question on how to maintain a fundamental trust structure over certificate trees is answered. Finally, it delineates the blockchain sketch to support trust management that simultaneously take into account the incentive, fairness and stability. Section 4 provides a series of experimental studies by simulating an opportunistic MASS network to demonstrate the feasibility of the methodology. Section 5 concludes the paper.

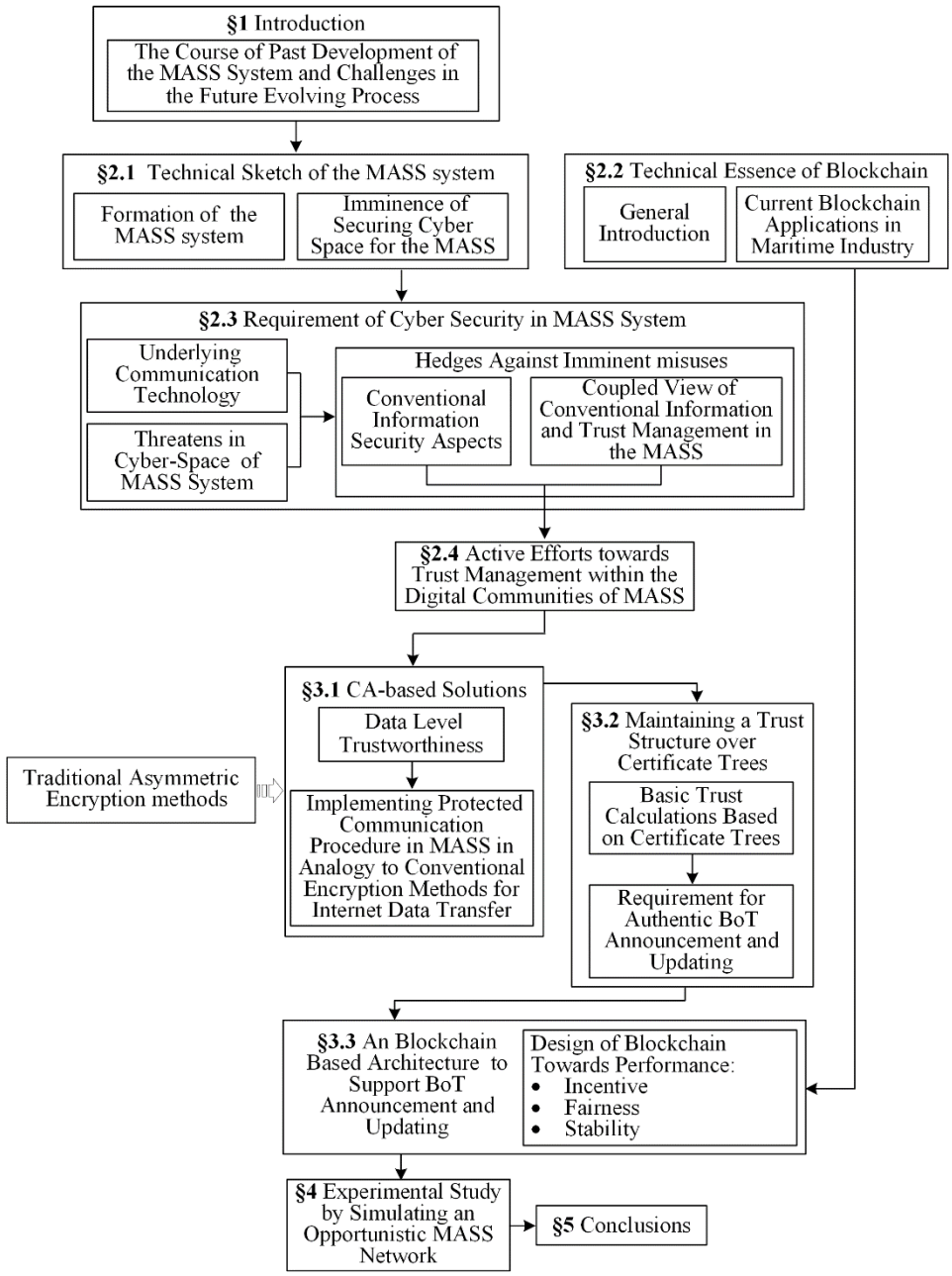

Fig.1. The flowchart of the structured modules.

2. Technical formation of an MASS system and its cyber security concerns

2.1 Composition of an MASS network

To fully describe the architecture of an MASS network[13][14], the entities are categorized into three types, as depicted in Fig.2 below. In fact, three major types of stakeholders can be found in the MASS network as follows, and each instance of the stakeholder/entity is modeled as a node in the network.

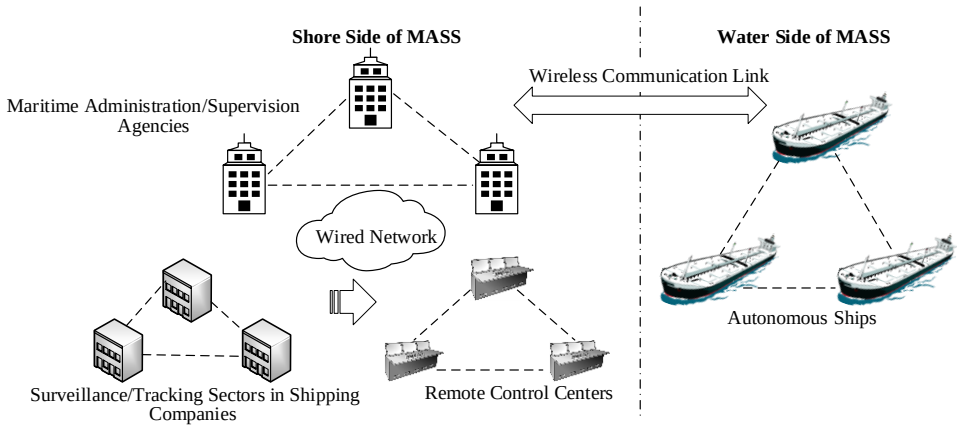

Fig.2. Categories of entities in MASS network.

At the shore side of MASS, Maritime Administration Agencies (*Type I node*s) usually represent the government body, and their routine task is to supervise the vessel traffic in the water and keep it in a safe order[15]. Shipping companies are the second major type of the stakeholders. For these entities, tracking the position and the real status of the ships is one of their main concerns. In the MASS era, shipping companies and their remote control centers are conceptually highly coupled, since the autonomous ships are supervised or operated by the shore-side control centers. Therefore, remote control centers (*Type II node*s) become the actual entities within the MASS network, through which a shipping company can track and control its ships at sea. At the waterside of MASS, autonomous ships are termed as *type III nodes*. This study focuses on the high levels of autonomous ships defined by the IMO, where the ship-shore and ship-ship communication is processed and perceived by machine instead of human.

Principally, the data flow in an MASS network inherits most of the functions of data exchange in a conventional ship network, including, instructions, status announcing, control signaling, inquiry/answers and coordination messages etc. The significant difference between the MASS network and the conventional peri-ship communication lies in the digitalized and structured data formation. The digitalization in the MASS elicits a cyber-enabled distributed system, which is more vulnerable to malicious behaviors. Considering the profound transition from traditional shipping to MASS systems, it will not bring out a complete view of the safety issue in the MASS system, if we simply project the traditional maritime accident occurrence onto the MASS scenario context[16][17]. Particularly, one of the key safety issues in MASS is cyber security, which is not conspicuous in the traditional maritime system[18][19]. It is evident by the cyber security accidents in other sectors (e.g. unmanned aerial vehicles), which shed light on analyzing the loopholes in the MASS system regarding to the cyber reliability[20]. The challenges facing MASS cyber security include (1) for a detected autonomous vessel at sea, how to determine its true identification and its controllers or the entity in charge; (2) for any data exchange to aid navigational, how to authenticate its true issuer; and (3) how to store and trace the context of the data exchange procedure and make such data undeniable and unambiguous.

The current experimental MASS lays emphasis on the machine intelligence in building the system to make it feasible, and probe the way that machine intelligence can replace human and take over tasks onboard. In this process, the cyber security becomes crucial to ensure the safety of using machine intelligence on ships. However, three are few cyber security studies of MASS in

the current literature. To address the cyber security in the highly digitalized context of any MASS system, we have to develop effective solutions to ensuring the ship identity and data genuineness and the reputation management (e.g. evaluation of the trustworthiness) of MASS behaviros.

2.2. Blockchain technology in the maritime industry

In recent years, blockchain emerges as one of the most prominent technologies in the domain of information and data management. Intensive attention from researchers has been drawn to blockchain not only for the sake of the exquisite technological ideas behind, but also due to its commercial success in cryptocurrencies such as Bitcoin[21]. Conceptually, blockchain has two features, namely a decentralized structure and distributed storage[22][23]. The ancestor of the blockchain-based network can date back to the peer-to-peer (P2P) network where content of interest is disseminated mutually without any centralized and designated server. A P2P network works well in the scenarios where there is not a strong need for maintaining unique and tamper-proof global data[24]. However, when the P2P network needs to support data-critical applications like financial accounting, additional mechanisms have to be designed to ensure that the decentralized nodes can do as well as the centralized approach does. As the shared ledger is introduced into the P2P network to secure the global uniformity of sensitive data, the blockchain technology become the most feasible way to achieve the goal.

Apart from the research on the fundamental and inherent problems related to the generic blockchain technology, such as the performance[25], scalability and incentive mechanisms[26], researchers also conduct the investigations on the applications of blockchain technology to various socio-technical systems. Due to its basic features, the blockchain technology can fit the scenarios with the following characteristics as a potential solution to managing critical data. (1) There are massive participants/users in the system; (2) There are transaction or interactions among the participants/users; (3) There are no predefined hierarchy among the participants/users, and there are no compulsory administrative rules to govern the participants/users. As a result, blockchain has also been exploited in many fields other than cryptocurrencies, including personal data storage[27], smart vehicle network[28], health care[29], smart grid[30] etc.. It demonstrates the commendable strength of blockchain in treating data exchange in scenarios with massive and interactive users. In this paper, the blockchain is utilized to solve the trustworthiness management of MASS systems[31].

Considering their salient technical strengths, blockchain-based approaches are developed and applied in the maritime industry in recent years. Maritime supply chains are one of the hotspot fields within this context. For instance, tracing the logistics of cargos during the shipping procedure can be realized by blockchain[32][33]. Another important application in the shipping industry is to replace the current paper-based workflow with the stream of tamper-resistant digital document among all the stakeholders[32]. This feature can be of special benefit for the escrow of container booking and bill of lading in container transportation. Furthermore, blockchain shows its competence in dealing marine insurance[34], since the status of the targeted asset can be recorded in blochchain for underwriters' on-demand check. Zhou et al. survey the factors that influence the application of blockchain in the maritime industry[35]. Using interviews and questionnaires, the challenges and opportunities of using blockchain technology in the maritime industry are also analysed in this study. Petkovic et al propose a macro framework of blockchain

application for the data sharing in the maritime industry[36]. Munim et al survey the blockchain technology designed for the maritime applications[37].

The findings from the previous studies reveals two common features. Firstly, the advantage of blockchain is mostly exploited from a commercial perspective for business of shipping. Secondly, while the participants are in need of cooperation to complete a business transaction, they all express their concerns on the trustworthiness of their partners. Blockchain technique thus provides a mechanism in which any digital operation from each participant is under the supervision of all other participants.

2.3. Communication technology and cyber security requirements in MASS

The acute demand for ship-ship and ship-shore digital communication has constantly been driving the technical evolution in the maritime domain[38]. There are various means for maritime communications, such as VHF/AIS, satellite, and 4G/5G carrier (ISP) networks. Among these technical solutions, some are endorsed by the IMO while the others are utilized through private agreements. VHF has been the prevailing terrestrial communication technique for decades. Besides, satellite communication, like INMARSAT, is the supplementary communication method for ocean-going ships[39].

It is obvious that conventional VHF/AIS shows less competence in an MASS system. Firstly, the vocal calling in VHF is based on analogue signal and hence does not suit for autonomous ship. Secondly, the AIS channel saturation often occurs in waters where maritime traffic is high. In this case, AIS packets are discarded randomly, causing the degrading of communication reliability for AIS participants. Thirdly, the bitrate of AIS is too low to carry the control or coordination information in MASS. Taking these drawbacks into account, the IMO and ITU are working together on a VDES technology to provide higher speed for ship-ship and ship-shore digital communications. VDES brings out a flexible and appealing solution for ship-ship and ship-shore digital communications. Compared to current VHF/AIS, terrestrial VDES offers much higher transmission rate that supports denser data flow. At the same time, VDES can also contain satellite-based data linkage to the current INMARSAT. Therefore, VDES greatly enables the data communication capabilities for an MASS system. Unfortunately, cyber vulnerability remains unaddressed in VDES designs.

Regarding to the much concerned cyber threats, Table 2 describes the most imminent malicious exploitation of the loopholes in the cyberspace of an MASS system, which are newly developed with reference to those in other modes of autonomous vehicles in the literature. Although each attack is ascribed to certain types of defects in cyberspace protection, the actual occurrence of an attack could be caused by the combination of multiple factors. Table 2 omits the severe scenario in which a compromised autonomous ship changes into a physical menace to other ships. In Table 1, lacking of identity authentication, message authentication and trust censorship are among the majority of causes that contribute to possible cyber attacks. This suggests that, to bring out countermeasures, such issues as identity validation, data verification and trust crediting have to be well addressed in MASS. By inheriting the conventional information security techniques, PKI, certificate and digital signature can be incorporated into an MASS system to solve the first two aspects. As for trust crediting, a new framework is developed in Section 3 for which a certificate scheme makes fundamental contributions for reputation accounting and trustworthiness evaluation.

Table 1
Imminent misuses perceivable in cyberspace of MASS.

Misuse model	Causal vulnerabilities	Description
Remote ship hijacking[40]	Lack of encryption Lack of identity authentication	An adversary takes control of the remote ship.
Eavesdropping[41]	Lack of encryption Broadcast style	An adversary wiretaps the communication of an entity to learn sensitive information.
Forged identity[42]	Lack of identity authentication	An illegal entity uses forged identity to evade maritime supervision or release disinformation.
Denial of service[43]	Lack of access control	An adversary deliberates to saturate the targets with spam requests, depriving them of the normal functioning.
Sybil attack[44]	Lack of identity authentication Lack of trust censorship	Somewhat like the forged identity model, an adversary fabricates a number of fake identities to act according to its will, thus illegally gaining influence in the system.
Good mouth/Bad mouth[45]	Lack of message authentication Lack of trust censorship	The adversaries deliberate to label a malicious entity as a good one or vice versa.
Replay attack /Impersonation attack[46]	Lack of message authentication Lack of protocol check	An adversary records a communication session and replays the same content to a target at a later point in time, causing the state disorder of the victim or other deception.
False information dissemination[47]	Lack of trust censorship	An adversary announces fictitious information for selfish purpose.

Trust management is an extended cyber security issue, and it deals with the upper level security judgement or policy for accessing the interactions among the MASS entities. Fig.3. demonstrates the principles of communication and trust management for an MASS system. It admits that human involvement for lower ALs can be the complementary means to cover unexpected cases. In contrast to the macro view of trust management illustrated in Fig. 3., Fig.4. shows a layered model from the perspective of a single entity. The figure illustrates the correlations of the conventional information guidelines and the trust management, and it also explains why trust management is highly dependent upon the leverage of certificate. It is notable that three databases are sketched in the figure. As for the databases *Maritime Safety Policy* and the *Cyber Security Policy*, they are private databases that locate in each individual entity in an MASS system. These databases determine the logic how an individual entity should act in the cyberspace of MASS.

The database *Ledger* is however a global database that stores the reputation of the participating entities. How to develop the global database based on the fact that no perfect mutual trust is available remains unclear. To make a comparative view, the cyber security in other domains of autonomous transportation systems are selected as follows, including the trust management in smart vehicles. Lai et al. delineate the security problems in the VANET[48]. Onieva et al. and Garg et al. investigate a security framework in vehicular networks from the perspective of edge computing[49][50]. Tan et al. build a fuzzy logic based empirical knowledge to assess the trustworthiness values for participants in vehicular networks[51]. Tangade et al. propose a hybrid cryptography scheme that supports incentive in crowd trust management[52]. Guo et al present a blockchain-based hierarchical framework to facilitate trust authentication in vehicular network[53].

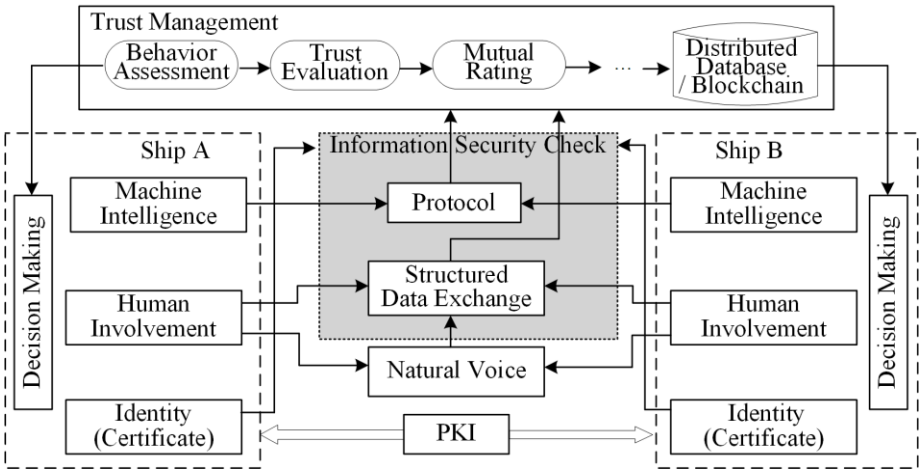

Fig.3. General model of communication and trust management for an MASS system.

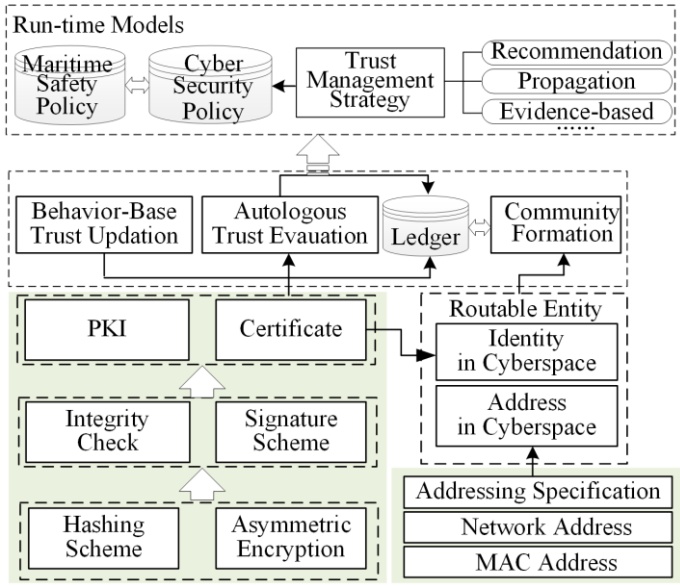

Fig.4. Trust management and the underlying conventional information security functionalities.

2.4. Trust management within the digital communities of MASS

As the entities in a digital community are independent individuals with autonomous decision-making capabilities, the trust among the entities will significantly affect the activities that involve reciprocal interactions. Trust originally stands for the subjective belief about the behaviors of a particular entity. When two or more entities are participating in a mission or task, the degree of trust can influence the evaluation or preference of the individuals[54]. This is especially of real implication in an MASS system, where opportunistic encounter calls for multilateral intentional actions, for instance, in the multi-ship collision avoidance scenarios.

Forming a global trust structure in a highly dynamic and opportunistic MASS system is indeed very challenging. Firstly, an individual can only have the straightforward trust assessment for a limited number of other entities over time. This suggests that, for any given entity, the direct

pairwise trust assessment between the entity and its peers only constitutes a *local* trust relationship. Therefore, to calculate the trust relationship between two arbitrary entities, the local trust relationship should be first combined[55], and then one can find some paths of trust to connect the two entities and reason how trust can propagate along these paths[56]. The next challenge lies in the lack of third-party to act as a notary in a digital community, where there is not a centralized or authorized body to be a globally accepted trustee. In an opportunistic environment, no entity is appointed as an official agent to provide trust report. Hence, the trust assessment between two entities, who are not familiar with each other, should be conducted based on the known and reliable information. Such information is often presented in piecemeal since the known assessment is usually pairwise. In this scenario, an entity will likely have different clues of trust calculation by considering the trust transfer along the advertised trust assessment, resulting in certain incongruity as for the point-to-point trust assessment[57]. Within this context, it is highly demanded to develop an acceptable trust fusion model to enable trust level assessment among the entities in MASS. It will also aid the development of a collective trust complexion that best reflects the irregularly announced individual trust assessment[58].

The incentive of participating in the trustworthiness recognitions is another indispensable factor that matters in forming a smart community of digital agents. Fundamentally, MASS is a cyber-physical system (CPS) with cooperative computing environment in the cyber part. Nevertheless, the crowdsourcing style of trust assessment can give raise to the varying extent of willingness to contribute to the public affair. For instance, if the proportion of the free-riding participants in the system is high, structuring a trust-based digital community will be difficult[59]. In real world applications, the incentive is an actually required option to promote the development of a digital community. The typical example is the Bitcoin blockchain, in which there is a reward by a mount of bitcoin to the winner of the competing miners who try to be the block-creator[21]. However, in an MASS system, the incentive is not so explicit as a cash-like reward. In most research work, the reward is an incremental score, whereas the total score possessed by an entity can suggest its reputation rank in the community[60]. Two methodological concerns emerge regarding to designing the incentive in the system. Firstly, the incentive scheme should keep a good trade-off between the fairness and the efficiency, particularly, the polarization of trust score should be averted; secondly, while indirect reciprocity prevails in incentive design, measures have to be taken to prevent misuse of the incentive, for instance, bidding up the trust score by collusion. From the perspective of theoretical probing, researchers usually resort to game theory to model the incentive problem in the cooperative environment[61]. The game framework attempts to describe the underlying motivation of the participants to make contribution or not. The entities have rationales to judge their payoffs, i.e., maximizing the profit at the lowest cost. In this context, incentive mechanism can be interpreted as the change of payoff, and various forms of games are investigated by researchers, such as repeated game[62], Bayesian game[63] and Stackelberg game[64].

In an MASS system which consists of a population of independent entities with autonomous decision-making capabilities, the social behavior among these entities will be clearly demonstrated. Compared to the traditional pure computing systems such as grid or cloud computing, the MASS system features a real-world and physical interaction between the entities, for instance, the encounter of ships. For any two entities, the event-based and real-world contact will have strong impact on the trust evaluation between the two peers. Furthermore, the updated and reinforced trust perception among the entities can make a major factor to shape the social behavior within the

MASS system. Some patterns of evolutional social characteristics are observable in the digital society driven by trust assessment or reputation indication. They include 1) trust agglomeration: the forming of small groups in which the group members have higher trust with each other in contrast with the entities outside the group[65]; 2) self-organizing scenario: the entities tend to setup an ad hoc group or alliance to cope with some specific tasks, aiming to make the most advantage or to pass through the hard situation[66]; and 3) the formation of reputation hierarchy: when trust or reputation is used as a scale to quantify the position of an entity inside a community, a hierarchical structure of the entities will come into being, and the upper level of the structure is more stable than the lower level[67]. In an MASS system, whether these characteristics will demonstrate any new appearance remains as a research question to answer. Accordingly, several methodologies are employed to model the social behaviors in digital community. To describe the social network and the dynamic relationship among the entities, analysis is usually conducted upon graphs or network[68]. As a result, the features of trust, such as symmetric/asymmetric, propagation/updating, transitivity/non-transitivity, can be formulized by the nodes and edges. Furthermore, dynamics equations are utilized to express the evolutionary behavior within the population[69]. With regard to the collective social behavior in MASS, the opportunistic nature of the system makes it difficult to directly employ the named traditional network models.

3. A new architecture framework for the trustworthiness evaluation in MASS

3.1. Connecting certificate authorities (CAs) within an MASS network

A new architecture framework is developed in this section to evaluate the trustworthiness of entities in MASS. It is outlined by 1) defining the CAs in MASS and 2) incorporating asymmetric encryption methods in the new communication procedure in MASS.

Currently, the asymmetric encryption is the dominating information security paradigm in various sectors such as Internet and mobile payment. Therefore, adopting the asymmetric encryption to solve the information security issue in MASS is the most promising way and hence investigated in this section. To realize asymmetric encryption in an MASS network, CAs are indispensable for identifying the entities, and they act as the foundation of the overall trustworthiness edifice for MASS. It is evident that CAs are currently not incorporated into an MASS network since they do not explicitly interoperate with the MASS nodes. Taking into account this note, we define the aforementioned Type I, Type II and Type III nodes as *ordinary entities nodes* or *MASS entities/nodes* to distinguish them with CAs.

A CA can issue certificates for both other CAs and the ordinary MASS nodes. Furthermore, some CAs have strong prestige to issue certificates for themselves, and these CAs are called *root CA*s. Thereafter CAs in this paper are categorized into root CAs and the non-root ones, which are called intermediate CAs. Each CA hosts its own certificate to identify itself. In this paper, the CAs and the MASS entities bear the following attributes, and these assumptions will not undermine the generality of the CA system:

(1) Each CA or entity possesses only one certificate issued by itself or another CA;

(2) The relationship of *issuing/issued* between the ordered node pairs <CA,CA> or <CA, ordinary entity> constitute a *tree* structure, in which the former element in the ordered pair is the parent of the latter. The root of the tree is a root CA, while other nodes are either a CA, or an ordinary entity. Meanwhile, each non-root node in the tree has *one* parent, which is a CA node. It

is obvious that in this way all the CAs and MASS entities are organized in individual trees, and the roots of the trees are the root CAs;

(3) Any entity in an MASS network is supposed to associate with at least one of the CAs, i.e. the issuer of his certificate. Moreover, by checking the issuing chain from his certificate and tracing upwards, it is easy to locate the root CA to which the entity is inherently linked. This is to say, the entity should *fully* recognize all the ancestor CAs beyond his certificate issuer along the tree. Nevertheless, an entity can choose to recognize other CAs even if its certificate has no connection with the CAs. It is also reasonable that once an entity recognized a CA, he is potentially willing to recognize all the nodes in the entire tree, but with different beliefs depending on their positions in the tree. Based on the creative role of CAs, new communication procedure in MASS is developed by incorporating asymmetric encryption methods. From the perspectives of operational practice and data exchange, MASS and conventional ships have shown significant difference[70]. A new communication procedure in MASS is developed by 1) analyzing the cyber vulnerability of the current technologies onboard ships and 2) revising their use within the context of MASS to endorse trustworthiness evaluation and management. By incorporating CAs into the MASS system, communication procedure in MASS can be re-devised in analogy to the off-the-shelf protecting routines in Internet where asymmetric encryption methods are widely employed. From the perspectives of operational practice and data exchange, MASS and conventional ships have shown significant difference[70]. A new communication procedure in MASS is developed by 1) analyzing the cyber vulnerability of the current technologies onboard ships and 2) revising their use within the context of MASS to endorse trustworthiness evaluation and management.

(1) AIS-like broadcast and status advertisement in MASS

In conventional navigation routines, AIS messages are the most important data exchange among the ships at sea and also for the shore-side surveillance [30]. The AIS messages are currently in plaintext, without the hash of the content and the signature of the sender. In this situation, the AIS datagram can easily be tampered or forged, and an AIS datagram can also be denied by a nominal sender. In the newly designed CA-based framework, an upgraded version of AIS for status advertisement, particularly, the position/heading/velocity announcement will be developed. It is called upgraded because the anticipated AIS-analogous technology should bear longer payload that can carry the traditional content as well as the digest and the signature. For instance, the size of an ASM datagram can be three times larger than the length of the traditional AIS messages, reaching a maximum 28.8kbps transmission rate.

Fig.4 illustrates the data exchange procedure, with respect to the de facto common information security treatment. Both the sender and the receivers follow a routine of asymmetric encryption-based genuineness and authenticity checking. This emphasizes the importance of maintaining a global enquiring mechanism of certificates. It is noteworthy that the procedure in Fig.5 shows the most desirable case, whereas there are other possible branchings of data process in the receiver end that contain verification failures. The disposition of these cases is supplemented as follows. For the failure of step ② in the receiver end, the receiver should treat the ship as an unidentified object and continue to process the data; For the failure of step③or④, the datagram should be discarded, and the receiver should resort to other means (such as ARPA) to trace the motion of the vessels in the neighboring waters.

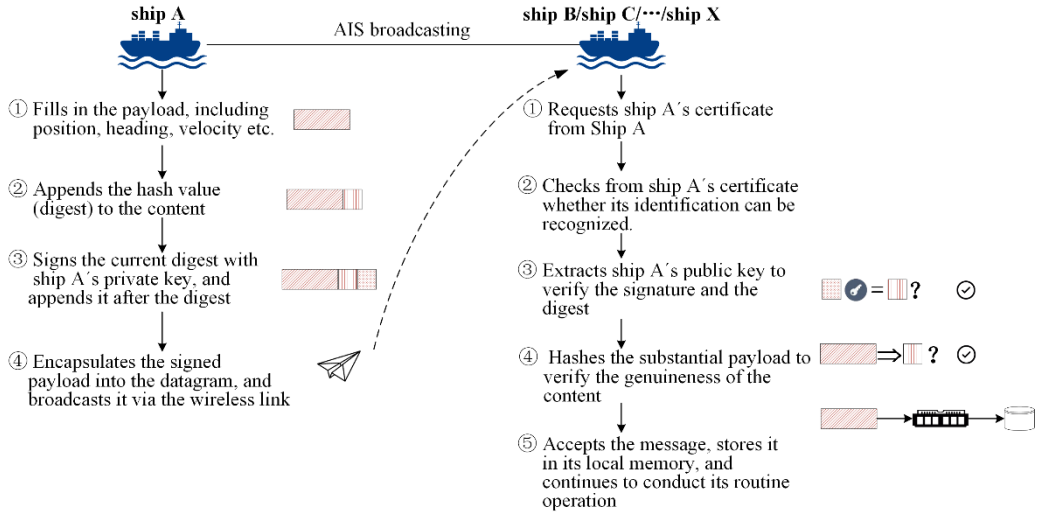

Fig.5. The revised implementation of AIS-like broadcast and the verification process in MASS.

(2) Ship-ship coordination (unicast)/shore-ship supervision and control (unicast)

In an MASS system, data transmission by unicast between the entities should also be the prevailing form of communication, which is in sharp contrast with the current state-of-art communication mode. Some typical scenarios include ship-ship coordination and shore-ship supervision. In the former case, a ship can communicate with another ship nearby to jointly tackle risky situations (e.g. the collision avoidance). In the latter case, shore-side agencies, such as remote-control centers, would connect and get the control of an autonomous ship at sea, or send ad-hoc instructions to the ship.

The principle of anti-spoofing in the unicast mode is almost the same as in the broadcast mode, except that in the unicast mode, the recommended way to strengthen the security is to use enciphered text, compared to the plaintext in the broadcast mode. To implement the digest-signature-encipher operation, the two entities should have a handshaking phase to exchange their certificates. If the volume of data transmission is heavy, the two sides can negotiate for a symmetric encryption scheme and the session key, with the negotiation itself being protected by the asymmetric encryption. Fig.6 illustrates the naive shore-ship handshaking for data transmission.

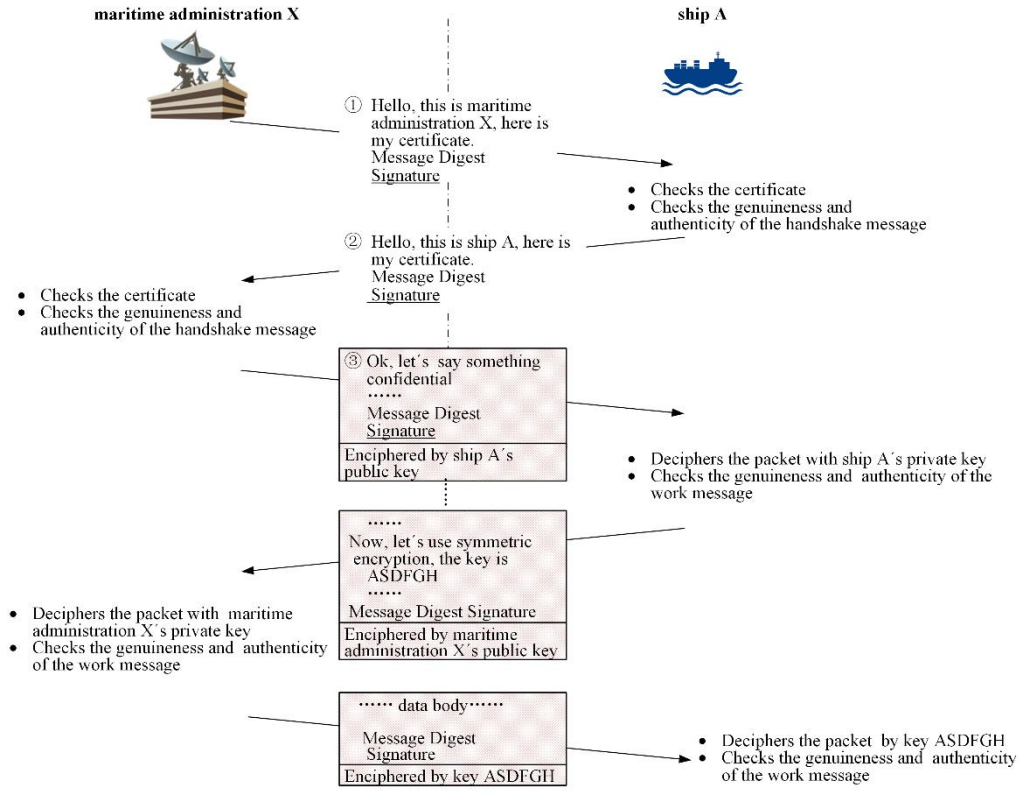

Fig.6. A naive shore-ship handshaking procedure for data transmission in MASS.

(3) Scenarios of relayed communication

In an MASS network, there will be more sophisticated scenarios that combine a sequence of interactions across different types of nodes. These convoluted interoperations are pervasive in the MASS system due to its highly cyber-dependent environment. A complete task that involves successive interactions between multiple MASS nodes is defined as a *transaction*, and one interaction that takes place between two nodes is called a *session*. Obviously, the implementation of a transaction constitutes a series of sessions. This will give rise to the relayed communication along a sequence of nodes, which still elicits the trustworthiness concerns. Apparently, the regularly used transactions suggest that an MASS system should allow for a less flattened operational structure, and it calls for a chained protection of trustworthiness. In the conventional navigation communication, VHF-based oral callings are usually granted without stringent authenticating the true identities of the caller and the callee. Nevertheless, in an MASS system, CA-based relayed communication should be elaborated to eliminate the risk of malicious interception.

Fig.7 demonstrates an envisioned scenario for an autonomous ship with the IMO autonomy level 3 (AL3), called *ship A*. The traffic supervision sector of the regional maritime administration observes that *ship A* deviates from the traffic separation scheme; *ship A* is in an autonomous steering mode, and it will keep on cruising until the remote control center directly takes over the control, or the chief officer takes over the control with the consent of the remote control center.

Under this situation, all the data exchange is achieved by enciphered unicast, based on the certificates, which is obtained in the handshaking phase.

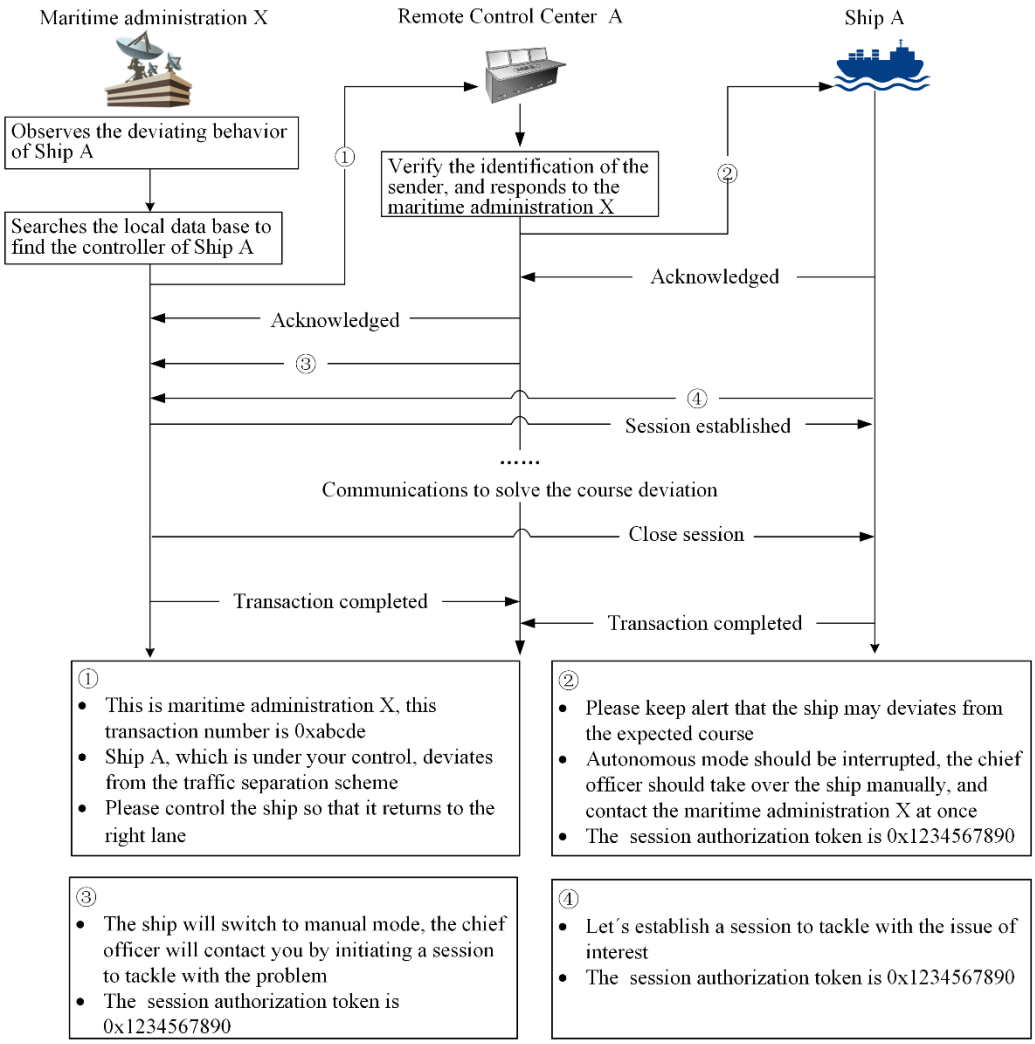

Fig.7. The implementation of a typical transaction in MASS.

3.2. Maintaining a trust structure over certificate trees in an MASS network

The success of MASS cyber depends on certain information from a global network perspective, including the certificates, the affiliation relationship and the credibility of the nodes, etc. This elicits two levels of trustworthiness management. At the data level, trustworthiness refers to the traditional aspect of digital security such as data integrity, privacy and non-deniability; at the performance level, the trustworthiness of an entity relates to its reputation during the navigational activities, and how its peers would recognize its behavior. The two levels of trustworthiness are highly coupled, and this section focuses on the CA-based infrastructure that underlies the cryptographic techniques for solving the data level trustworthiness.

In the past decade, IP based ad hoc network has been fully addressed in the communication/ networking research[71], with emphasis on routing, QoS and network capacity. Therefore, it is reasonable to foresee that the MASS nodes make up an *ad hoc* network by using the state-of-art underlying technologies[72], which support data transmission with a lower bound of bandwidth. Again, it should be borne in mind that this ad hoc network has much confined ability of connection between the peers therein, in sharp contrast with that of the Internet. Each MASS node should have its unique cyber address with the uniform format, and is denoted by $\mathrm{Addr}_i = NetworkAddress_i \| Hash(PubKey_i)$. This notation means that the address of node$_i$ in the cyber space is the catenation of its network address (typically, the IP address) and the hash value of its public key, both of which are of fixed length. It is worth mentioning that node$_i$ holds a certificate issued by one CA, and its public key is written in the certificate.

In terms of inquiry and storage of certificates, it is easy to exchange certificate, but difficult to verify it in the MASS system. To verify a certificate, a node should firstly have the certificate of the issuer, and secondly, the node should trust the issuer. This will further reveal two problems: (1) While the direct certificate exchange is straightforward, as depicted in Fig.8, how to inquiry or search for the issuer's certificate remains unclear; and (2) If a node does not directly trust the issuer specified in the certificate, what should it further do to trust the certificate's holder?

Fig.8 demonstrates the relationships among the CAs (in boxes) and MASS nodes (in ellipses), these trees are called *Relationship Trees of Certificate Nodes*(RTCNs), in which each CA or MASS node can be identified by a unique certificate. It is noted that CAs are not incorporated into an MASS network since they do not explicitly interoperate with the MASS nodes. Within this context, the following judgments are made:

(i) Node2 and Node3 should fully recognize CA-A022, CA-A02 and CA-A0;

(ii) Node2 and Node3 both have a certificate issued by CA-A022, hence they should highly trust each other;

(iii) Node1 and Node3 are connected by CA-A02 and CA-A022, hence they should have trust with each other, which is weaker than that of Node2 and Node3;

(iv) If Node3 also recognizes a CA in the CA-B0 tree, say CA-B021, it can trust Node4 to some extent;

(v) If Node3 does not recognize any of the CAs in CA-B0 tree, Node3 cannot trust Node4.

As for the quantitative description of the degree of trust, formal definitions are formulated below.

Definition 1: For any two nodes$node_1, node_2$in a tree, there is a determined path in the tree that connects the two nodes, and we denote the path by $\mathrm{Path}(node_1, node_2)$, which consists of all the nodes and links along the path from $node_1$ to $node_2$ without any repetition of nodes or links. Furthermore, we denote all the nodes in tree, along the path by $\mathrm{PathPoint}(node_1, node_2)$.

Definition 2: In the aforementioned RTCN, each non-leaf node is a CA, which may have one or many child(ren), indicating that the node issues certificate(s) to the child(ren). Each leaf node is an ordinary MASS node. For a leaf node *node$_i$*, the path connecting the leaf node to the root node is called the node's *inherent train of trusted CAs* (ITTCs), denoted by $\mathrm{ITTC}(node_i)$, allowing we ignore that the leaf node is not a CA.

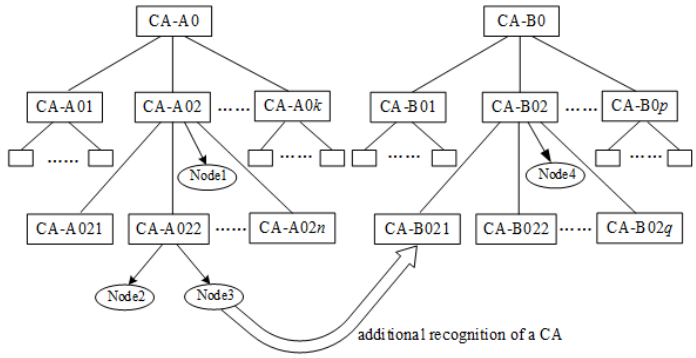

Fig.8. The trust relationship among CAs and MASS nodes.

To make it succinct, when referring to a CA or an MASS node, its certificate is equally used to identify its identity. Because each CA or MASS node is uniquely holding its own certificate, ITTCs equally stands for the sequence of certificates corresponding to each of the node.

In the simple case of inner- RTCN, some basic terminologies and results are adumbrated by focusing on the uni-RTCN in which there is only one root CA that acts as the trust source. Let $node_i$,$node_j$be two nodes inside a RTCN, according to the definition of ITTC, it can be written that

$$\mathrm{ITTC}(node_i) = \mathrm{PathPoint}(node_i, root)$$

Particularly, when *node*$_i$ and *node*$_j$ are the leaf nodes, there may be an overlapped section of their ITTCs. Within the overlapped section of their ITTCs, the CA that is located at the far most from the root node is called the *nearest common CA*(NCC), denoted by $\mathrm{NCC}(node_i, node_j)$. It can also be easily proved, that the NCC of two leaf nodes is unique. In Fig.5, CA-A02 is the NCC of Node1 and Node2.

Definition 3: For any two leaf nodes within a RTCN, *node*$_i$ and *node*$_j$, the number of links from *node*$_i$ to their NCC is called *direct trust length* (DTL) *of node*$_i$ *given node*$_j$, denoted by $\mathrm{DTL}(node_i|node_j)$.

Therefore, the quantitative formulation of degree of trust between two MASS nodes can be elaborated as follows.

Definition 4: Given a RTCN, for any two leaf nodes in the tree, *node*$_i$ and *node*$_j$, *node*$_i$'s prior belief of trust (BoT) for *node*$_j$ is calculated as $\mathrm{PriBoT}(node_i \to node_j) = \lambda^{\mathrm{DTL}(node_j|node_i)}$, where $0<\lambda<1$ is a constant. Here BoT stands for the extent to which the own side would trust the other.

$\mathrm{PriBoT}(node_i \to node_j)$ indicates how much *node*$_i$ would trust *node*$_j$. In the context, when one node attempts to trust another, we call the former node the *credence giver* (CG), while the latter node the *credence recipient* (CR). The constant λ reflects the alertness of an MASS node in regards of trust transition. To keep the current work simple, we assume it is a global constant for every MASS node. It can be seen that *node*$_i$'s BoT for *node*$_j$ does not necessarily equal to *node*$_j$'s BoT for *node*$_i$. This asymmetric BoT occurs even in our daily life as well.

After that the definitions and models about the trust transmission are given in a single RTCN that encompasses CAs and MASS nodes, more general cases can be taken into consideration where multiple RTCNs coexist. In fact, the example illustrated by Fig.7 has shown the essential principles for the association of multiple RTCNs. In the real world, there can be a number root CAs, and these root CAs are highly reputable and independent with each other.

For a root CA, due to its high authority, its certificate is self-issued, and this certificate is positioned at the top of the CA/certificate edifice. Since each none–root CA has a unique certificate issued by its superior CA and that the root CAs are mutually independent, the RTCNs are disjoint in pairwise. In this context, any MASS node should belong to one of the RTCNs.

Let$node_i$,$node_k$be two nodes that belong to different RTCNs, i.e.,$node_i \in \mathrm{RTCN}_1$, $node_k \in \mathrm{RTCN}_2$. In such a scenario, we have

$$\mathrm{ITTC}(node_i) \cap \mathrm{ITTC}(node_k) = \phi$$

Accordingly, $\mathrm{NCC}(node_i, node_k) = \phi$.

In order for $node_i$ to trust $node_k$ with some degree, $node_i$ should recognizes some certificate in RTCN_2. Let $node_p \in \mathrm{RTCN}_2$ be the node identified by a certificate which is recognized by $node_i$, $node_p$ is called $node_i$'s *trust contact point* (TCP) in RTCN_2. In fact, $node_p$ acts as the intermediary of trust that $node_i$ can anchor, so that $node_i$ can trust other nodes in RTCN_2 with high confidence. By overriding the use of symbols, we denote the *node*$_i$'s prior BoT for *node*$_p$ by $\mathrm{PriBoT}(node_i \to node_p)$, which is a subjectively estimated value indicating the cross-RTCN trust between two nodes. Thus for any $node_q \in \mathrm{RTCN}_2$, the *node*$_i$'s prior BoT for *node*$_q$ can be calculated by

$$\mathrm{PriBoT}(node_i \to node_q) = \mathrm{PriBoT}(node_i \to node_p)\mathrm{PriBoT}(node_p \to node_q)$$

After the BoT is calculated, the next step is to inquiry CA over an MASS system. When two or more MASS entities try to launch a communication session, the first thing is to check the identity of the entities, which is written in their certificates. By finding the certificate affinity through the certificate dependence thread, the MASS entities establish the trust connection and complete the procedure of trust transition. The following steps should therefore be fully undertaken.

(1) In the inner-RTCN case, the NCC of two nodes surely exists, equally, the path that connects the CG and CR can be found in the RTCN;

(2) In the cross-RTCN case, the point path that connects the CG and CR consists of two successive segments, i.e., the trust link between the CG and the TCP, and the trust path between the TCP and the CR;

(3) When CG node tries to verify the certificate of a CR node, the complete sequence of certificates along the path is supposed to be obtained for the CG to validate CR.

In this trust transition process, two assumptions are set to answer two questions below.

Assumption 1: Each MASS node hosts in its local storage all the certificates of its ITTCs besides its own certificate.

Assumption 2: If an MASS node additionally trusts an MASS entity (i.e. the TCP), in another RTCN, it hosts in its local storage all the certificates of the TCP's ITTCs.

Question 1: By what means the CG can tell whether there exists a path to a particular MASS node, to ensure the node to be a CR?

Question 2: How the CG should obtain the sequence of certificates for the validation through the dependence thread?

These assumptions are deemed rational because 1) an MASS node can usually acquire its ITTCs when it applies for its certificate from an intermediate CA or root CA. Retaining the ITTC will make the node be convinced of its own validity; and 2) when an MASS node trusts a certificate outside its own RTCN, the node actually means to partially recognize the RTCN of the certificate

(TCP). Therefore, the node is supposed to possess one branch of the RTCN to which the TCP belongs. For instance, the node can acquire the ITTCs from the TCP directly.

A secured MASS network needs gossiping protocols. *As introduced previously, the global RTCNs constitute separate trees, the root nodes of the trees are independent root CAs that are self-certified. In an MASS network, each node should participate in the gossiping across the network, by periodically advertising his ITTCs to his real-word neighbors. It is noted that the gossiping is conducted in an insecure context, thus further measures should be taken to refine the gossips.* Fig.9 demonstrates the implementation of the gossiping protocol. Each MASS node will have increasing neighbors. The left part of Fig.9 shows the main payload of the gossip. The left part shows the peer-to-peer gossiping case, in which the payload is encrypted by the receiver's public key. Optionally, analogous to the current AIS, gossiping can also be implemented by broadcast, in which the payload will not be encrypted. This is to say, only the integrity of the payload can be checked in the broadcast scenario.

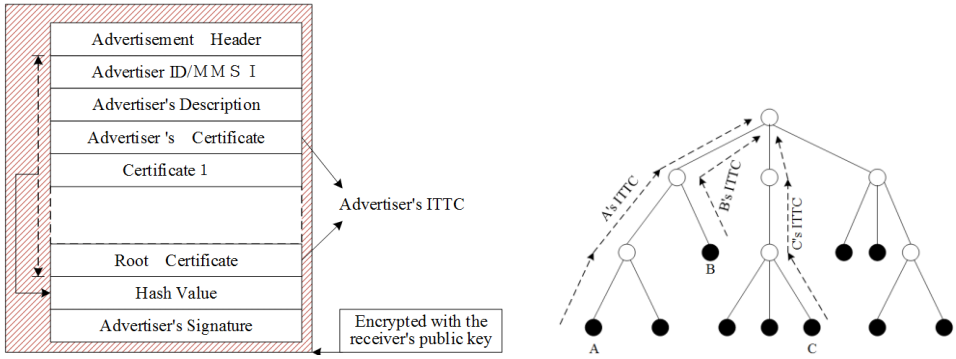

Fig.9. The main payload of the gossip over an MASS network and principles of ITTC advertisement.

The advertisement header is the public information about the entire advertisement body. Usually, the header contains the version number, the length of the message, the number of certificates in the ITTC carried in the message, timestamp etc. The Advertiser ID or MMSI is the identification of an MASS node, since there should be a universal naming organization available in the MASS network that can provide the globally unique identity code for all types of the node, analogous to the current MMSI code for ships. The next field, Advertiser's Description, consists of the concise introduction to the MASS node, usually in the "attribute = value" form. After this field, all the CAs in the advertiser's ITTC are appended to the body, starting from the advertiser's own certificate to its root CA's certificate. Afterwards, the hash value of the fields from Advertiser ID/MMSI to the root certificate are computed and attached to the message body. Finally, the hash value is signed with the advertiser's private key.

3.3. Blockchain to facilitate trust perception over an MASS network

The essential mechanism of implementing a blockchain-based approach to tackle the trust management in an MASS network includes:

(1) There will be some nodes engaged in forming blocks and announcing it to all MASS nodes, and the block carries the fluctuation of trust assessment for a node that is in need for MASS operation;

(2) The delegation of a group of MASS nodes is elected and has the qualification of being the ledger poster, who will append the block to the existing chain, and broadcasts the new block to other nodes;

(3) There should be an incentive to encourage the MASS nodes to vote for the witness, and there also should be a reward to the witness who builds the block and appends it into the chain.

To form and manage the blockchain in MASS, a proof-of-stake based election of witnesses is needed. The core idea behind the blockchain is that a node should use a chance to re-evaluate the BoT of another node, whereas the chances for a node to update the BoT are limited in a period. Thus the chances can be analogous to the deposits in the node's account. Each MASS node is endowed with an initial amount of credits to participate in the trust ecology evolution in MASS. When we treat the chances as credits, it is apparent that the MASS network will sustain a global ledger to record the expenditure of a credit and the surplus of credits for each MASS node.

Updating the BoT of a specific MASS node and adverting it to the whole MASS will make concrete contribution to forming the overall trust linkage among the MASS nodes. Thus, the more credits an MASS can hold, the more discourse it will have to exert influence on the trust ecology. It is therefore necessary to leverage blockchain to publish the dynamic evaluation of the BoT with regard to the real-world behavior. Fig.10 describes the main steps for the delegation of the proof-of-stake procedure in an MASS network, while their details are presented as follows.

(1) The process of updating the board of *witnesses*. A *witness* is a node who is authorized to build a block and append it to the blockchain. There are multiple *witnesses* endowed with this privilege, and they actually exercise such functions in a round-robin way. The board of witnesses should be regularly revised so that the members will not serve the board permanently. To make the timely revision smooth, only a portion of the board will exit and be replaced by new incomers. Suppose at a due time the current board is to be updated, the youngest witness, the launcher, sends out a voting appeal to an MASS network under the permission of the present board.

(2) A receiver of the appeal should check the nodes which are known. Each receiver will recommend up to $\boldsymbol{K}$ candidates outside the current board to be the new witnesses, bearing in mind that not all candidates can be finally elected. Whenever the receiver recommends a node to be the witness, it pays one credit into the credit pool. If a receiver does not recommend any candidates in his reply, he will pay no credits. In particular, if the receiver does not reply to the launcher's appeal, he will be not involved in the voting group. When a receiver replies to the launcher, he will sign his decision with his private key.

(3) The launcher then receives replies from other nodes. The launcher will conduct some statistic analysis. First he sorts all the nodes with respect to the credits they received from others in the current turn. The top $\boldsymbol{\Gamma}$ nodes that gain the most votes in this round of voting will become the new witnesses in replace of the current $\boldsymbol{\Gamma}$ witnesses with the highest service age. For the nodes who have invested credits to the winners, they will be rewarded by the credits in the pool. Therefore, if a non-witness node can recommend more witnesses into the board, it can gain more reward. On the contrary, if the nodes it recommends are not actually elected as the members of the board, the credits they pay will not produce any return.

(4) The launcher of the voting declares the voting statistics to all the nodes, including the winners of the voting, i.e., the top $\boldsymbol{\Gamma}$ nodes, their recommender list and the new board of witnesses. In addition, the transfer of credit will also be announced so that the rewarding process is

supervised. Since every node has been signed in the voting process, the announcement released by the launcher is undeniable. In this way, the revised board will be recognized by all nodes.

(5) The revised board of witnesses manage the blockchain in a round-robin manner. Once a witness is in its turn to be the block-producer, it will construct a block and uses gossip protocol to let all the nodes know the block. The witness should conduct the following major tasks. First, all the witnesses should reach an agreement about the runtime parameters of the blockchain, such as the frequency of producing blocks, the constant $\boldsymbol{K}$, $\boldsymbol{\Gamma}$, the maximum block size. Second, the witness should also be rewarded with credits every time when he produces a block, and at the same time, there is an aging mechanism so that witness serves the position for a limited time. Third, if a witness fails to produce a block in time, the next witness should take over the task instantly. This scenario usually occurs when some witnesses are accidentally offline.

(6) For a non-witness node, once it receives a voting appeal, it is supposed to respond to the appeal by recommending the nodes it trusts. As aforementioned, from the perspective of a given node, the trust evaluation for other nodes can be expressed by PriBoT or its revision, i.e., the re-evaluation of BoT. While the PriBoT can be calculated by static RTCN structures over an MASS network, the re-evaluation of BoT is subjectively rated according to the behavior of the MASS entities that is perceived by the CG.

Fig.10 illustrates the main principles of proof-of-stake and the witness election model.

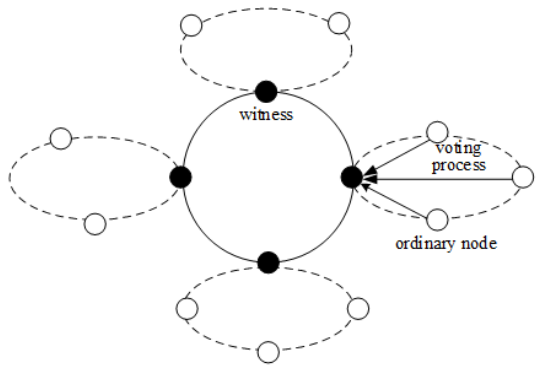

Fig.10. Principle of proof-of-stake by voting for a witness.

Gains and expenditure of credits in an MASS network constitutes a liquidity cycle, which associates some asset-like features with the credits, and makes them analogous to the currency circulation. This furthermore adds another motivation to utilize blockchain to model the trust formulation in the MASS ecosystem. The features of the credits in MASS include.

(1) The origination of a credit

There are three ways to obtain credits. First, when a node joins an MASS network, it is initially endowed with a fixed amount of credits. Second, each node will also be given credits with the elapse of time. Third, when a witness successfully adds a block into the blockchain, the witness will be rewarded by some credits. If there are enough credits in the public credit pool, the witness will withdraw the predefined amount of credits as the reward; in case there are not enough credits in the pool, the witness can create some original credits make itself fully rewarded. Hence, credits can be the incentive to become a witness. Overall, the total credits in an MASS network increase with time.

(2) The credit pool and the stake

In the witness election process, the non-witness node will conduct an investment. While each node recommends up to $\boldsymbol{K}$ witness candidates, it has to pay one credit for each recommended candidate. The credits are cast to the public credit pool. If the recommended node can be enrolled as the highest recommended $\boldsymbol{\Gamma}$ witness candidate, the recommender can take back multiplied credits from the pool. In this way, credits can also be regarded as the stake of non-witness. On one hand, a non-witness is encouraged to recommend the most competitive candidates to gain credits; on the other hand, it is less likely for a non-witness to gain credits by purely broadening his recommendation of witness candidates.

(3) Cost of submitting a claim of BoT re-evaluation

Once an MASS node is obliged to announce its BoT towards another MASS node, it should make this claim by initiating a transaction, which will be loaded into the blockchain by some witnesses. To do so, the node has to pay a credit. This is to say, if an MASS node has no credit, he has to wait until a credit is granted by time elapse, so that the node can make the claim. In spite of the cost of submitting a claim, we can easily see the counterbalance of the expenses. The node can increase its popularity since its claim will be recorded in the blockchain and can be inquired and referred to. This will enhance its chance of being recommended as a witness.

Fig.11 illustrates the layout of a block in the blockchain. The block is divided into block header and block body, with the block header having fixed length. The block header is hashed so that it can uniquely identify the block. The previous header points to the latest block before the current block, thus, all the blocks are linked into the chain. The block is produced by a witness, who is a member of the current board of witnesses. The witness and its cyber address thus are written into the block header. Other fields of the header include the timestamp, which indicates the time of forming the block; the length of the block body, which varies with the number nodes in the group; the signature, which covers the whole block header. Finally, the block header contains the Merkle tree root, which is adopted from the Bitcoin block. Each claim of credit/BoT change is treated as a *transaction*. When they are not yet on the chain, transactions of this kind should be collected by the current presiding witness to be written on the block, before the block is finally assembled on the chain. In the block body, the transactions are hierarchically hashed through a binary tree structure from leaf to top. The Merkel tree root thus stores the top-most hash value as the fingerprint of all the transactions.

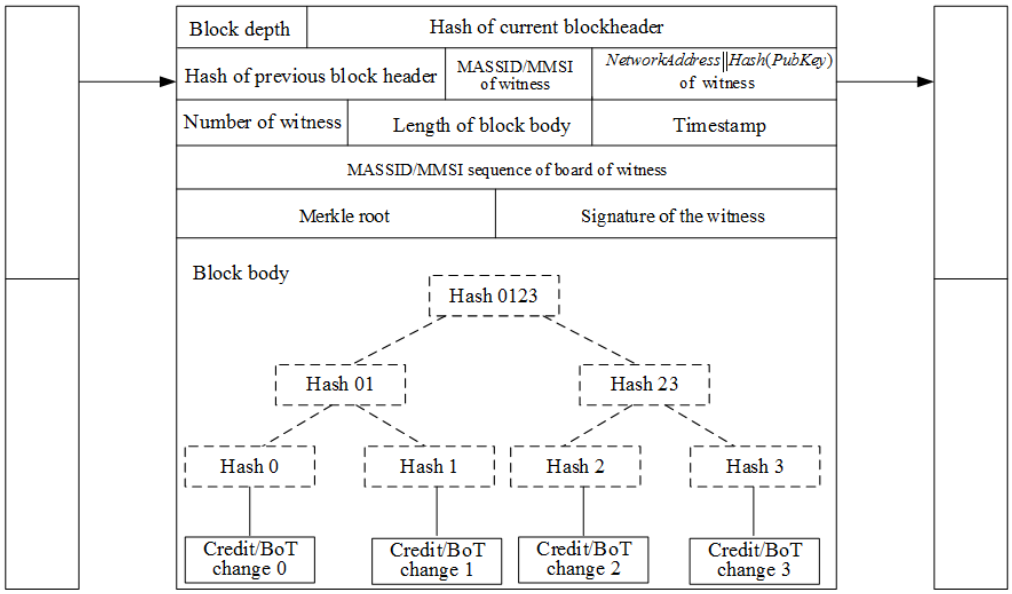

Fig.11. Layout of a block in the blockchain.

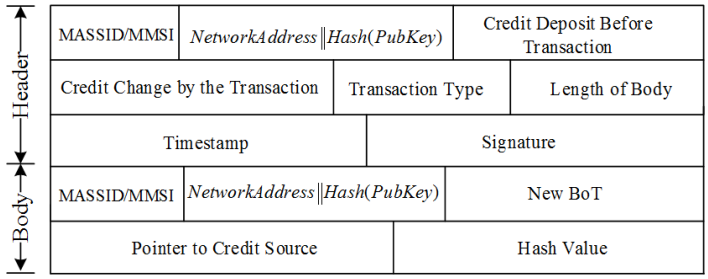

Fig.12. Structure of a node's typical transaction.

The structure of a transaction is depicted in Fig.12. Again, the structure is divided into header and body. The fixed-length header contains the identity of the claimer, and the credit it has owned. Other fields include the timestamp, the length of the body and the claimer's signature about its decision. Moreover, since the transaction usually causes change of credit possessed by the claimer, there is a field indicating the gain or loss of the credits. There can be several types of transactions. Most typically, the claim for BoT re-evaluation is frequently used to update the trust connection among the MASS nodes, and a BoT claim costs the claimer a credit. The body of transaction is dependent on its type. Fig.12. uses the claim for BoT re-evaluation as a demonstration. First, the target MASS node of the BoT should be recorded, together with the value of the new BoT, which is a real number between 0 and 1. The pointer to credit source indicates which credit is to be paid by the claimer to the public pool, and it will be recycled and be drawn as the income for other nodes when it is needed.

4. Experimental results and discussion

In this section, the behaviors of a number of MASS nodes are simulated and examined. The motions of these nodes constitute an opportunistic network[73], where encounters or departures among the MASS nodes occur continuously and randomly, so that the formation of the network are constantly on the change. For two specific MASS nodes, an encounter may lead to the updating of PriBoT. Therefore, the opportunistic network of MASS nodes will give rise to sustained transactions of BoT revision, which will be contained in blocks and be added to the blockchain.

Other than the opportunistic encounters and departures, RTCNs offer more stable relationship that MASS nodes can be associated. Hence, under the devised experimental circumstances, the MASS nodes are the leaf nodes located in several RTCNs. Additionally, some malicious nodes are constructed to simulate the real-world malevolent users. For instance, an autonomous ship controlled by an illegal group may disguise as a normal ship. Since the malicious ship does not have a legal certificate, it has to forge an entire ITTC to make its identification more seemingly convincing to other MASS entities. With this in mind, the experiment simulates a fake RTCN to participate in the evolution of trust ecology. Since the root CA is forged, all the leaf nodes are illegal MASS entities. The ordinary RTCNs (left-side) and the fake RTCN (right-side) are depicted in Fig.13.

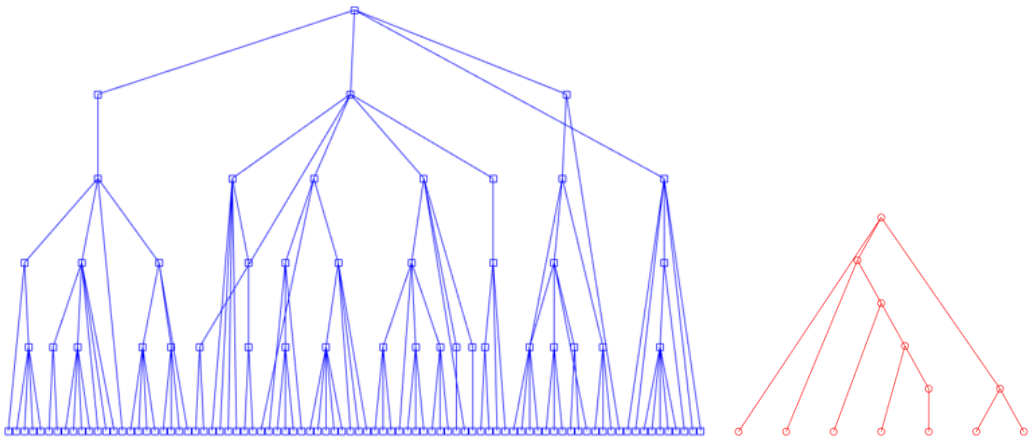

Fig.13. The typical ordinary RTCN and the fake RTCN.

4.1. Setups of the experimental scenarios

The outlines of the experimental design are first elaborated to generate meaning results.

(1) The MASS nodes. 8 RTCNs are randomly generated, including 1 fake RTCN. For an ordinary RTCN, there are 100 to 120 leaf nodes standing for the MASS entities, while for the forged RTCN, the number of leaf node ranges from 5 to10, representing forged MASS entities. The distance from the leaf node to the root node varies from 1 link to 4 links. Each leaf node is assigned a value indicating its *moral*, i.e., the extent of being a good inhabitant in an MASS system. Initially, each MASS node is endowed with 5 credits, so that it can conduct the BoT revision or invests in the witness election process.

(2) The opportunistic network. The simulation is divided by continual time phases. In each phase, the MASS nodes are partially selected so that encounters can occur among them. Specifically, in each phase, the leaf nodes are fractured into 16×16 groups. The rationale is based on the generation of an opportunistic network, which will be elaborated afterwards. Upon an encounter, there is a probability of *willingness*, $\boldsymbol{w}$=0.1, that one node may update its BoT

towards the other entities and advertise this transaction by spending 1 credit. In this simulation, the revised BoT is based on the moral of the target entity with random fluctuation of $\pm 20\%$ by an even distribution, which is aimed to reflect the deviation of BoT evaluation. It is worth mentioning that the BoT revision can be made either inside a RTCN or across two RTCNs. Each phase will last 240 minutes, and in the next phase, all the above the procedure will repeat independently. The claims of BoT revision will be triggered immediately after an encounter, with probability $\boldsymbol{w}$.

(3) 21 witnesses will be initially randomly selected in a chronological order from all the leaf nodes of the 8 RTCNs. Every 24 hours, there will be a voting launched by the youngest witness. The launcher will call for recommendation of new witness. The ratio of reply to the voting appeal is 80% among the non-witness nodes. Herein, $\boldsymbol{K}$=20, i.e., in each reply, the recommender will nominate up to 20 witness candidates by paying one credit for each of them. These replies are also treated as transactions as they involve credit transfer and recycling. The launcher will collect the replies and produce new blocks containing these recommendation transactions. Finally, $\boldsymbol{\Gamma}$ is assigned with 7, i.e., the 7 out of 15 winners with the highest votes will replace the 7 out of 10 witnesses with the longest service time. In case of excessive candidates with equal votes to compete the 7 seats, the candidates with higher BoT will break the tie. The nodes whose recommendation list includes the winner(s), will get a reward of 10 credits per winner.

(4) The witnesses will produce blocks in turn every 30 minutes. This is to say, a block contains all the transactions in the last 30 minutes that are not written on the chain. Once a witness generates a block, it will get a reward of 8 credits. Every node will be granted one credit every 12 hours so that it can have the basic right to broadcast a BoT if it feels obliged, or to invest on someone hoping to make it a witness.

To generalize the encounters among the entities in an MASS system, a simulation of opportunity ad-hoc network is conducted, as demonstrated in Fig.14. All encounters are modeled by a square, and is divided by $n \times n$ sub-squares. Initially, the entities are evenly located in all the sub-squares. The type I and Type II entities are fixed nodes denoted by solid circles, while the Type III entities (i.e. autonomous ships) will move to the neighboring sub-squares in predefined time intervals, Δ, with equal probabilities. Additionally, for each moving autonomous ships, according to the experience of crews, the average time of encounter meeting with another entity, T, regardless of fixed type or autonomous type, is also set as predefined values. The encounter occurs random only within the entities in the same sub-square for a given Type III entity, and the average encounter interval T follows an exponential distribution.

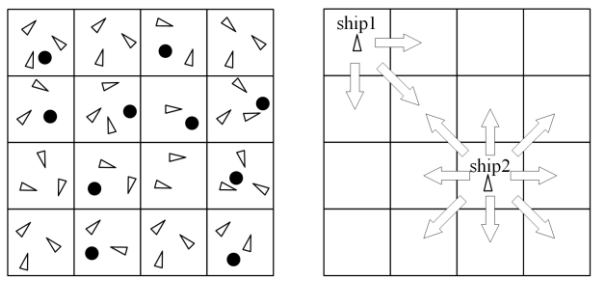

Fig.14. The construction of opportunistic ad-hoc network among the entities

In this simulation, 566 entities are generated, of which 50 are fixed entities. With this configuration, Table 2 summarizes the encounter occurrences under the combination of various inputs. These results can provide an apparently reasonable manifestation of opportunistic

encounters under the circumstance of gradual space/time transitions. The block generation time, 30 minutes, is chosen to level off T so that a block is produced when most ships can have an encounter with another entity. Short block-generation time, such as 10 minutes in Bitcoin, are not applicable given the transaction pace and population size in the MASS network is significantly lower than that of Bitcoin. Next, this paper employs the configuration listed in the fourth row with italics and bold typeface to carry out the follow-up experiments.

Table 2
The statistical feature of encounters in an opportunistic ad-hoc network simulation (one sample).

T (min)	Num of sub-squares	Δ (min)	Total encounters among the entities every 30 min
30	8×8	30	560
30	8×8	60	561
30	8×8	90	551
30	***16×16***	***30***	***450***
30	16×16	60	380
30	16×16	90	300
60	8×8	30	279
60	8×8	60	278
60	8×8	90	278
60	16×16	30	251
60	16×16	60	262
60	16×16	90	203
90	8×8	30	185
90	8×8	60	185
90	8×8	90	185
90	16×16	30	144
90	16×16	60	152
90	16×16	90	136

4.2. Strategies used in the delegated proof of stake

On receiving a voting call for the new witness election, the ordinary MASS should recommend some MASS nodes. There are multiple factors that can affect the options of recommendation.

(1) The cost and the reward

Since the cost of recommending an MASS node is one credit, the voting node should have budget to make this recommendation. In the experiment we conduct, each voting node will use half of its current amount of credits to recommend the nodes it trusts. However, now that totally there are only seven nodes to be the winners, the chance of earning credits is low for most non-witness nodes.

(2) Recommending the most trustable nodes

For a non-witness, it will endeavor to recommend the most trustable nodes. Normally, the estimation of BoT is based on two types of calculations. 1) If the own node does not know the target nodes, the BoT can be derived purely from the affinity of the two nodes by the scheme introduced in Definition 4; and 2) if the own node knows the target node very well, for instance, by direct encounter, the own node can easily give its BoT to the target. However, as long as the BoT is updated, it would elicit consequential BoT changes.

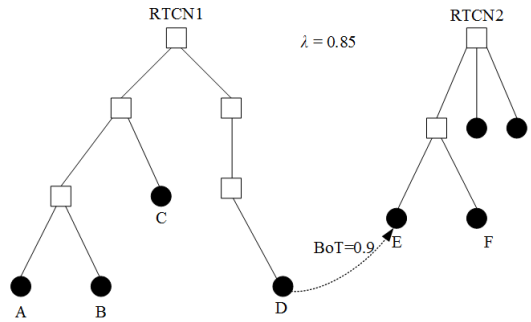

Fig.15. The nodes outside the RTCN may have higher BoT from the perspective of node D.

Fig.15. shows an instance to demonstrate this situation. Node D initially does not know Node E. If there is an encounter between node D and E occurs, and D rate the BoT(D→E)=0.9, then from the perspective of Node D, the BoT towards F and other leaf nodes should change accordingly. Particularly, if λ=0.85, node D would trust E and F rather than A, B, and C, although the affinity with A, B, and C is higher. This is to say, if D decides to recommend two nodes to compete for the witness, the candidates will be E and F in the other RTCN.

4.3. Main results and their implications

The blockchain provides a decentered mechanism so that each MASS node can evaluate the trustworthiness of other peers through continually opportunistic interactions. These interactions can occur in such scenarios as shore-ship communication, ship-ship encounter or the contact between remote control center and the other ships, etc. Trustworthiness over the MASS nodes makes MASS nodes show more salient features of social network. In an MASS network, the trustworthiness is influenced by two factors, i.e., the RTCNs and the BoT carried in the blockchain. From our experimental study in Sections 9.1 and 9.2, some prominent results can be obtained.

The credits of a node reflect its extent of freedom to recommend a candidate into the witness board, and to advertise the BoT of a specific entity to a whole MASS network. Hence, the amount of credits an entity possesses indicate the influencing power of the node. Fig.16 shows the credits distribution among the 566 nodes. The left part is the distribution percentile of the first 5 days, and the right part is the distribution percentile over 30 days. Since every node will regularly receive 2 credits every day, the total amount of the credits is rising. We can see that as time goes on, the credit inequality tends to level off. Nevertheless, the actual credit inequality remains significant.

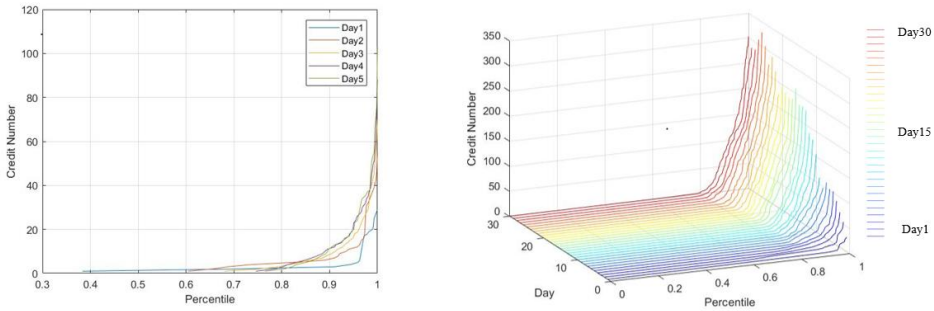

Fig.16. Credits distribution among the nodes over time.

For instance, at the 30th day, even the inequality has been harmonized in some sense, the 80 percentile still correspond to the mere 34% of the top holder's credits.

The next key issue is about the dynamic properties of the witness board that constitutes the temporary keepers of the blockchain. The left part of Fig.17 shows all the nodes that have ever

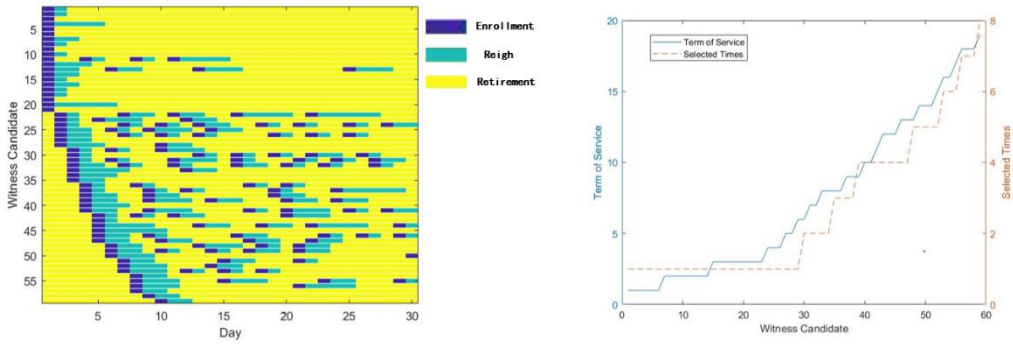

Fig.17. The enrollment and retirement of the witnesses.

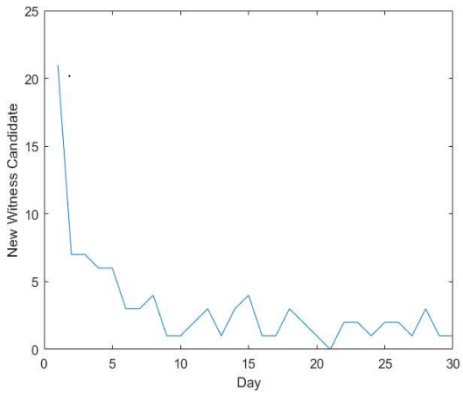

Fig.18. The number of the new comers that have never been enrolled in the witness board.

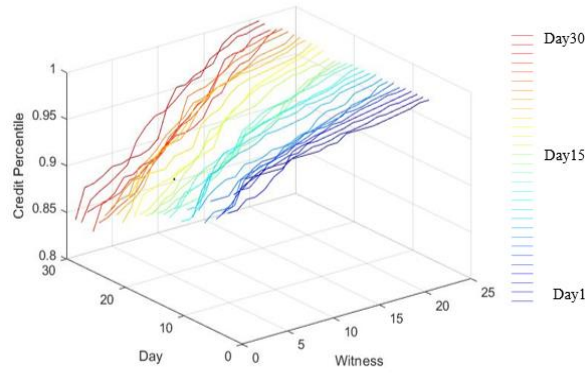

Fig.19. The percentile of credit owned by the witnesses and their evolvement over time.

been enrolled into the witness board, including the 21 randomly selected witnesses in the origin. Totally there are 34 witnesses apart from the initial 21 witnesses entering the board. Considering the total 566 MASS nodes, these 59 witnesses form a rather small group, implying a highly concentrated circle that draws the trust from large mass nodes. In Fig.17, a blue rectangle refers to a new comer to or re-entering to the witness board, while a green rectangle refers to the witness that continues to serve the board in the current term. The yellow rectangle refers to retirement from the board. The right part of Fig.17 shows two curves. The solid line is the distribution of service term of the 59 candidate after sorting, while the dotted line is the times of (re-)entering the witness board. Of all the witnesses, we can see that half of them serve more than 10 days in the witness board during the 30-day period of simulation, and also half of them enter the witness board repetitively for over 5 times. It suggests that among all the 59 candidates, there exist some patriarch-like nodes that are highly trusted and occupy the seats for long time.

Fig.18 shows the number of "absolute" new comers to the witness board. Here the term *absolute* stands for the new comer that has never been enrolled before. The curve in Fig.17

suggests that the major portion of witnesses demonstrate early appearance. This is to say, if an MASS node is not a witness in the first 20 days, it is less likely that he will become a witness afterwards. Fig.19 shows the situation of credit possession regarding the witness board after sorting. The vertical axis corresponds to the percentile of the credit owned by a witness, compared to the whole MASS nodes. The curves show that most witnesses have high positions in terms of credit retention. The credit percentile will go even higher with time.

The evolving of trust among the MASS nodes is another issue of interest. Initially, if there is no encounter occurred, the BoT can simply be deduced by the structure of RTCNs, which is pieced together by the ITTCs in the gossip messages. In other words, each node has no information about the other nodes except for the RTCNs initially. As opportunistic encounters accumulate, some nodes may send out the BoT towards the nodes in another RTCN, enabling the cross-RTCN trust evaluation.

Fig.20 depicts the recommendations for and from the nodes outside RTCNs during each voting procedure over the 30-day collective social behaviors. The left part of the figure refers to the ratio of recommendation from the nodes outside the RTCN where the receiver locates in. The horizon axis demonstrates the percentile of the receiver in terms of the ratio. It can be seen that as times elapses, a node can receive more votes from the nodes outside the RTCN. The same pattern also becomes obvious if and when we change the perspective to the recommendation sent out, as shown in the right part of Fig.20. This phenomenon suggests that

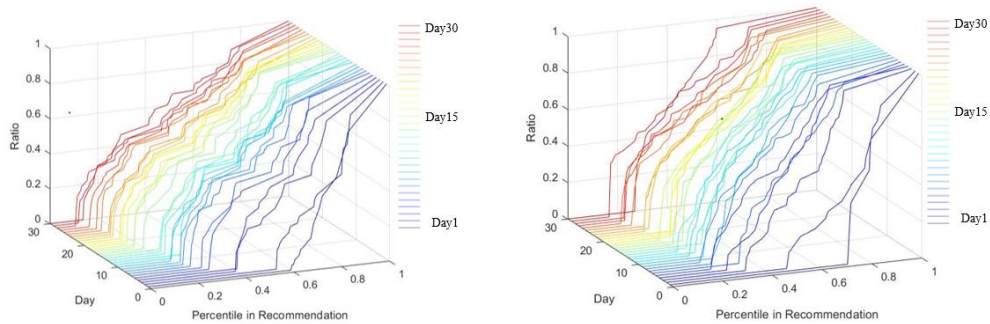

Fig.20. The ratio of recommendation for and from the nodes outside RTCNs.

the BoTs carried in the blockchain help broaden the range of MASS nodes whose trust can be evaluated by others. Even there are no encounters occurred, a node is able to deduce the trustworthiness of some unacquainted nodes.

As the reciprocal BoTs are disseminated over the blockchain, the mutual trust among the MASS nodes keeps evolving. For an individual node, it will keep and update the list of known nodes ranking by their trustworthiness. These nodes may or may not have direct contact with him. As for the nodes which do not have direct contact with the given node, their trustworthiness is estimated by the affinity along the RTCNs. A question can be raised, that is, how good the nodes which are mostly trusted by other nodes, could be. Fig.21. shows two major aspects of the question. The left part of Fig.21 surveys the average credits of the nodes that are recommended by every individual node, and the right part surveys the average moral value. From the curves over time horizon, we can see that, of the recommended nodes, those who have very high credit possession and high moral will constitute increasingly larger portion as time elapses. This phenomenon suggests that, besides direct contact that makes two nodes have straightforward evaluation of trust

towards each other, the BoTs can help ordinary nodes to have the accurate evaluation of trust rationally even if the two nodes are in separation.

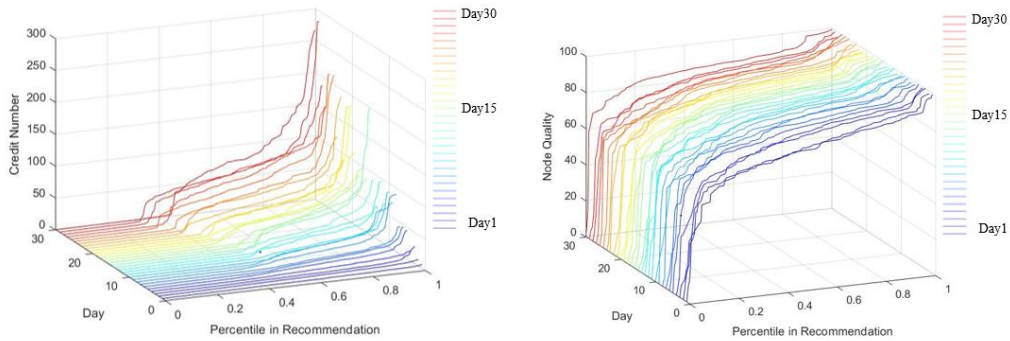

Fig.21. The properties of nodes that on the top of trust list for the ordinary MASS nodes.

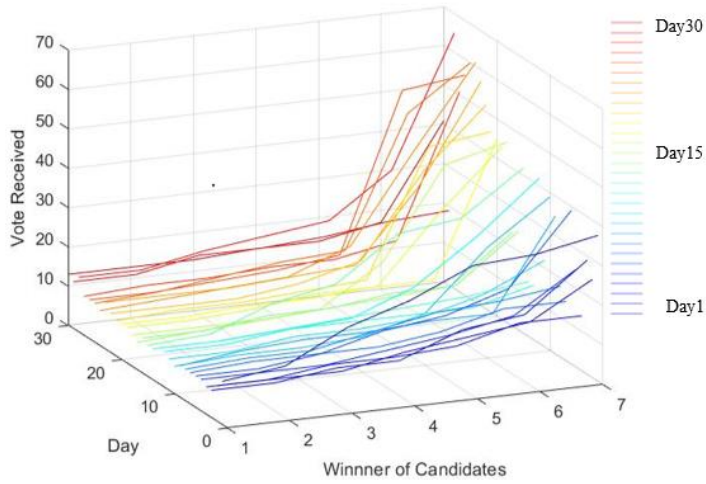

Fig.22. The needed votes to become a witness over time.

In this experimental study, “bad nodes” with forged certificates are deliberately added in the network, as depicted in the right part of Fig.13. For these bad nodes, the whole system cannot discriminate them from normal nodes if every bad node has good behavior. However, since the RTCN tree is small, as long as a low BoT is released towards one of the counterfeit nodes, all the other counterfeit nodes will degrade in trust evaluation accordingly. Also in the experiment, it is evident that even there is a collusion among the bad nodes, none of them is able to become a witness. Fig.22 shows the votes needed to be the winners among all the recommended nodes. The minimum number of votes to win is 35 in the first witness election. As time elapses, the minimum number goes higher rapidly. Therefore, it is evident that the 7 bad nodes are too week to make a force in the proof of stake mechanism.

5. Conclusion

This paper reveals why the trust management in an MASS system is vital yet challenging, and how it can be solved through the mean of a traditional asymmetric encryption approach. The key features of an MASS network constitute a major obstacle for the application of the traditional solutions to information security. Specifically, there is not a centered agency with enough public trust in the MASS community to lead PKI and the related inquiry services, especially under the opportunistic and dynamic environment of the MASS network. Using the developed architecture blockchain can be effectively used to compensate for such defects exposed by the conventional methods in the MASS system. The proposed asymmetric encryption enabled cyber space in an MASS system, and the associated robust scheme can effusively facilitate trust management in an MASS system. By incorporating the certificate edifice into MASS, blockchain can be used as a virtual global data center to store the BoT among the MASS entities. The experimental results show that the blockchain based method can be effective in dealing with the intangible asset in distributed and non-hierarchy network environment through experimental proof.

This paper also expounds the relation of traditional information security and the trust management. Particularly, digital certificate is leveraged to be the connection of the traditional information security and trust management. It is due to that (1) the traditional information security deals with the *data level security* such as privacy, integrity, authentication etc., which can be regarded as *hard* security. The public key in certificate can facilitate these treatments by using asymmetric encryption methods; (2) the trust management deals with the reputation or behavior level security by rating the degree of subjective belief about the rightness of an entity, which can be regarded as *soft* security. The certificate is used to uniquely identify an entity therein.

Blockchain is utilized to record the dynamic subject trust perception for each entity towards other entities, without presuming a central database recognized by all. By block generation and advertisement, every entity can effectively perceive and sort the trustworthiness among the participant across an MASS network. Proper strategy can therefore be adopted for an individual entity to cope with navigational practice. As a result, the social attribute of the socio-technical system is strengthened for the MASS community, aiming to achieve an autonomous governance over the population of MASS entities. This method is of particular merit in an MASS system where a centralized administration agency is not available.

To further improve the proposed approach, further research could be conducted to address the limitations that (1) the proposed scheme does not take into account the instable network connection among the MASS nodes, and the gossip may not reach and cover a large portion of MASS nodes; (2) the produced block may not necessarily be synchronized across a whole MASS network; (3) the majority of the investigated MASS system must not be malicious entities, although it at large should reflect the reality in the shipping industry.

Acknowledgements

The work presented in this paper is cosponsored by China National Key Research and Development Plan (Project/Task No. 2018YFC0810400/05) and Funds for International Cooperation and Exchange of the National Natural Science Foundation of China (Grant No.51920105014) and EU H2020 ERC Consolidator Grant programme (TRUST Grant No. 864724).

References

[1] IMO. IMO takes first steps to address autonomous ships. Press Brief 2018; 2:99–100. http://www.imo.org/en/MediaCentre/PressBriefings/Pages/08-MSC-99-MASS-scoping.aspx (Accessed by May 25, 2018).

[2] Burmeister H-C, Bruhn W, Rødseth ØJ, Porathe T. Autonomous unmanned merchant vessel and its contribution towards the e-navigation implementation: the munin perspective. International Journal of e-Navigation and Maritime Economy 2014; 1:1–13. https://doi.org/10.1016/j.enavi.2014.12.002.

[3] Rolls Royce. Rolls royce future shore control centre 2017. https://www.youtube.com/watch?v=ALwx5VP8kWA. (Accessed by March 17, 2017).

[4] Wróbel K, Montewka J, Kujala P. System-theoretic approach to safety of remotely-controlled merchant vessel. Ocean Engineering 2018; 152:334–345. https://doi.org/10.1016/j.oceaneng.2018.01.020.

[5] Xiaoyang W, Shuai J, Qiang M, Tan KC. Tugboat scheduling for container ports. Transportation Research Part E 2013; 49:217–249. https://doi.org/10.1016/j.tre.2020.102071.

[6] Wróbel K, Montewka J, Kujala P. Towards the assessment of potential impact of unmanned vessels on maritime transportation safety. Reliability Engineering and System Safety 2017; 165:155–169. https://doi.org/10.1016/j.ress.2017.03.029.

[7] Ramos MA, Thieme CA, Utne IB, Mosleh A. Human-system concurrent task analysis for maritime autonomous surface ship operation and safety. Reliability Engineering and System Safety 2020; 195. https://doi.org/10.1016/j.ress.2019.106697.

[8] Li M, Chen L, He Y, Huang Y. A rule-aware time-varying conflict risk measure for MASS consideringmaritime practice. Reliability Engineering and System Safety 2021; 215. https://doi.org/10.1016/j.ress.2021.107816.

[9] Vos JD, Hekkenberg JR, Banda OVA. The Impact of Autonomous Ships on Safety at Sea – A Statistical Analysis. Reliability Engineering and System Safety 2021; 210: 107558. https://doi.org/10.1016/j.ress.2021.107558.

[10] Schröder-Hinrichs JU, Song DW, Fonseca T, Lagdami K, Loer K. Transport 2040: Automation, Technology, Employment. The Future of Work 2019. https://doi.org/10.21677/itf.20190104.

[11] Bolbot V, Theotokatos G, Boulougouris E, Vassalos D. A novel cyber-risk assessment method for ship systems. Safety Science 2020; 131. https://doi.org/10.1016/j.ssci.2020.104908.

[12] Siboni S, Sachidananda V, Meidan Y, Bohadana M, Mathov Y, Bhairav S, et al. Security testbed for internet-of-things devices. IEEE Transactions on Reliability 2019; 68:23–44. https://doi.org/10.1109/TR.2018.2864536.

[13] Goerlandt F. Maritime autonomous surface ships from a risk governance perspective: interpretation and implications. Safety Science 2020; 128. https://doi.org/10.1016/j.ssci.2020.104758.

[14] Chang CH, Kontovas C, Yu Q, Yang Z. Risk assessment of the operations of maritime autonomous surface ships. Reliability Engineering and System Safety 2021; 207. https://doi.org/10.1016/j.ress.2020.107324.

[15] Wróbel K, Montewka J, Kujala P. Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels. Reliability Engineering and System Safety 2018; 178:209–224. https://doi.org/10.1016/j.ress.2018.05.019.

[16] Zhang M, Zhang D, Yao H, Zhang K. A probabilistic model of human error assessment for autonomous cargo ships focusing on human–autonomy collaboration. Safety Science 2020; 130. https://doi.org/10.1016/j.ssci.2020.104838.

[17] Fan C, Wróbel K, Montewka J, Gil M, Wan C, Zhang D. A framework to identify factors influencing navigational risk for Maritime Autonomous Surface Ships. Ocean Engineering 2020; 202. https://doi.org/10.1016/j.oceaneng.2020.107188.

[18] Utne IB, Rokseth B, Sørensen AJ, Vinnem JE. Towards supervisory risk control of autonomous ships. Reliability Engineering and System Safety 2020; 196. https://doi.org/10.1016/j.ress.2019.106757.

[19] Thieme CA, Utne IB, Haugen S. Assessing ship risk model applicability to Marine Autonomous Surface Ships. Ocean Engineering 2018; 165:140–154. https://doi.org/10.1016/j.oceaneng.2018.07.040.

[20] Sedjelmaci H, Senouci SM, Ansari N. A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks. IEEE Transactions on Systems, Man, and Cybernetics: Systems 2018; 48:1594–1606. https://doi.org/10.1109/TSMC.2017.2681698.

[21] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system 2008. https://bitcoin.org/bitcoin.pdf. (Accessed by November 1, 2008).

[22] Yuan Y, Wang FY. Blockchain and cryptocurrencies: model, techniques, and applications. IEEE Transactions on Systems, Man, and Cybernetics: Systems 2018; 48:1421–8. https://doi.org/10.1109/TSMC.2018.2854904.

[23] Lei A, Cruickshank H, Cao Y, Asuquo P, Ogah CPA, Sun Z. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet of Things Journal; 4:1832–1843. https://doi.org/10.1109/JIOT.2017.2740569.

[24] Li JS, Chao CH. An efficient P2P content distribution system based on altruistic demand and recoding dissemination. IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and HumansYear 2010; 40:1083–1093.https://doi.org/10.1109/TSMCA.2010.2044881.

[25] Yu G, Zha X, Wang X, Ni W, Yu K, Zhang JA, Liu RP. A unified analytical model for proof-of-x schemes. Computers & Security 2020; 96. https://doi.org/10.1016/j.cose.2020.101934.

[26] Wang EK, Liang Z, Chen CM, Kumari S, Khan MK. PoRX: A reputation incentive scheme for blockchain consensus of IIoT. Future Generation Computer Systems 2020; 102:140–151. https://doi.org/10.1016/j.future.2019.08.005.

[27] Chen Z, Zhu Y. Personal archive service system using blockchain technology: case study, promising and challenging. IEEE International Conference on AI & Mobile Services (AIMS) 2017; 93-99. https://doi.org/10.1109/AIMS.2017.31.

[28] Dorri A, Steger M, Kanhere SS, Jurdak R. BlockChain: a distributed solution to automotive security and privacy. IEEE Communications Magazine 2017; 55:119–125. https://doi.org/10.1109/MCOM.2017.1700879.

[29] Kuo TT, Kim HE, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association; 24:1211–1220. https://doi.org/10.1093/jamia/ocx068.

[30] Luo F, Dong ZY, Liang G, Murata J, Xu Z. A distributed electricity trading system in active distribution networks based on multi-agent coalition and blockchain. IEEE Transactions on Power Systems 2019; 34:4097–4108. https://doi.org/10.1109/TPWRS.2018.2876612.

[31] Chawla C. Trust in blockchains: Algorithmic and organizational. Journal of Business Venturing Insights 2020; 14:1–8. https://doi.org/10.1016/j.jbvi.2020.e00203.

[32] Kshetri N. 1 Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management 2018; 39:80–90. https://doi.org/10.1016/j.ijinfomgt.2017.12.005.

[33] Foerstl K, Schleper MC, Henke M. Purchasing and supply management: From efficiency to effectiveness in an integrated supply chain. Journal of Purchasing and Supply Management 2017; 23:223–228. https://doi.org/10.1016/j.pursup.2017.08.004.

[34] Gatteschi V, Lamberti F, Demartini C, Pranteda C, Santamaría V. Blockchain and smart contracts for insurance: Is the technology mature enough? Future Internet 2018; 10:8–13. https://doi.org/10.3390/fi10020020.

[35] Zhou Y, Soh YS, Loh HS, Yuen KF. The key challenges and critical success factors of blockchain implementation: Policy implications for Singapore's maritime industry. Marine Policy 2020; 122:104265. https://doi.org/10.1016/j.marpol.2020.104265.

[36] Petković M, Mihanović V, Vujović I. Blockchain security of autonomous maritime transport. Journal of Applied Engineering 2019; 17:333-337. https://doi.org/10.5937/jaes17-22740.

[37] Munim Z, Duru, O, Hirata E. Rise, Fall, and Recovery of Blockchains in the Maritime Technology Space. Journal of Marine Science and Engineering 2021; 9. https://doi.org/10.3390/jmse9030266.

[38] Aslam S, Michaelides MP, Herodotou H. Internet of ships: a survey on architectures, emerging applications, and challenges. IEEE Internet of Things Journal; 7:9714–9727. https://doi.org/10.1109/JIOT.2020.2993411.
[39] Geng S, Liu S, Fang Z, Gao S. An agent-based clustering framework for reliable satellite networks. Reliability Engineering and System Safety 2021; 212:107630. https://doi.org/10.1016/j.ress.2021.107630.
[40] DNV-GL. Cyber security resilience management for ships and mobile offshore units in operation. 2016.
[41] Wang P, Wu X, He X. Modeling and analyzing cyberattack effects on connected automated vehicular platoons. Transportation Research Part C: Emerging Technologies; 115: 102625. https://doi.org/10.1016/j.trc.2020.102625.
[42] Cho JH, Swami A, Chen IR. A survey on trust management for mobile ad hoc networks. IEEE Communications Surveys and Tutorials 2011; 13:562–583. https://doi.org/10.1109/SURV.2011.092110.00088.
[43] INMARSAT. Cyber Security Requirements for IMO 2021.
[44] Park S, Aslam B, Turgut D, Zou CC. Defense against Sybil attack in the initial deployment stage of vehicular ad hoc network based on roadside unit support. Security and Communication Networks 2013; 6:523–538. https://doi.org/10.1002/sec.679.
[45] Movahedi Z, Hosseini Z. Trust-distortion resistant trust management frameworks on mobile ad HOC networks: A Survey. IEEE Communications Surveys & Tutorials 2015; 18:1–1. https://doi.org/10.1109/COMST.2015.2496147.
[46] Li W, Song H. ART: An attack-resistant trust management scheme for securing vehicular ad HOC Networks. IEEE Transactions on Intelligent Transportation Systems 2016; 17:960–969. https://doi.org/10.1109/TITS.2015.2494017.
[47] Mejri MN, Ben-Othman J, Hamdi M. Survey on VANET security challenges and possible cryptographic solutions. Vehicular Communications 2014; 1:53–66. https://doi.org/10.1016/j.vehcom.2014.05.001.
[48] Lai C, Lu R, Zheng D, Shen XS. Security and privacy challenges in 5g-enabled vehicular networks. IEEE Network 2020; 34:37-45. https://doi.org/10.1109/MNET.001.1900220.
[49] Onieva JA, Rios R, Roman R, Lopez J. Edge-assisted vehicular networks security. IEEE Internet of Things Journal 2019; 6:8038–8045. https://doi.org/10.1109/JIOT.2019.2904323.
[50] Garg S, Singh A, Kaur K, Aujla GS, Batra S, Kumar N, et al. Edge computing-based security framework for big data analytics in VANETs. IEEE Network 2019; 33:72–81. https://doi.org/10.1109/MNET.2019.1800239.
[51] Tan S, Li X, Dong Q. A trust management system for securing data plane of Ad-Hoc Networks. IEEE Transactions on Vehicular Technology 2016; 65:7579–7592. https://doi.org/10.1109/TVT.2015.2495325.
[52] Tangade S, Manvi SS, Lorenz P. Trust management scheme based on hybrid cryptography for secure communications in VANETs. IEEE Transactions on Vehicular Technology 2020; 69:5232–5243. https://doi.org/10.1109/TVT.2020.2981127.
[53] Guo S, Hu X, Zhou Z, Wang X, Qi F, Gao L. Trust access authentication in vehicular network based on blockchain. China Communications 2019; 16:18–30. https://doi.org/10.23919/j.cc.2019.06.002.
[54] Fan X, Liu L, Li M, Su Z. GroupTrust: Dependable Trust Management. IEEE Transactions on Parallel and Distributed Systems 2017; 28:1076–1090. https://doi.org/10.1109/TPDS.2016.2611660.
[55] Lu X, Baraldi P, Zio E. A data-driven framework for identifying important components in complex systems. Reliability Engineering and System Safety 2020; 204:107197. https://doi.org/10.1016/j.ress.2020.107197.
[56] Liu G, Wang Y, Orgun MA, Lim EP. Finding the optimal social trust path for the selection of trustworthy service providers in complex social networks. IEEE Transactions on Services Computing 2013; 6:152–167. https://doi.org/10.1109/TSC.2011.58.
[57] Wu J, Li X, Chiclana F, Yager R. An Attitudinal Trust Recommendation Mechanism to Balance Consensus and Harmony in Group Decision Making. IEEE Transactions on Fuzzy Systems 2019; 27:2163–2175. https://doi.org/10.1109/TFUZZ.2019.2895564.

[58] Zhang P, Zhou M. Security and Trust in Blockchains: Architecture, Key Technologies, and Open Issues. IEEE Transactions on Computational Social Systems 2020; 7:790–801. https://doi.org/10.1109/TCSS.2020.2990103.
[59] Feldman M, Lai K, Stoica I, Chuang J. Robust incentive techniques for peer-to-peer networks. Proceedings of the ACM Conference on Electronic Commerce, vol. 5, 2004, p. 102–111. https://doi.org/10.1145/988772.988788.
[60] Ding X, Guo J, Li D, Wu W. An Incentive Mechanism for Building a Secure Blockchain-Based Internet of Things. IEEE Transactions on Network Science and Engineering 2021; 8:477–487. https://doi.org/10.1109/TNSE.2020.3040446.
[61] Liu M, Ma Y, Song L, Liu C. Understanding the game behavior with sentiment and unequal status in cooperation network. Knowledge-Based Systems 2021; 212:106588. https://doi.org/10.1016/j.knosys.2020.106588.
[62] Ioannou CA, Romero J. A generalized approach to belief learning in repeated games. Games and Economic Behavior 2014; 87:178–203. https://doi.org/10.1016/j.geb.2014.05.007.
[63] Dahiya A, Gupta BB. A reputation score policy and Bayesian game theory based incentivized mechanism for DDoS attacks mitigation and cyber defense. Future Generation Computer Systems 2021; 117:193–204. https://doi.org/10.1016/j.future.2020.11.027.
[64] Kang X, Wu Y. Incentive Mechanism Design for Heterogeneous Peer-to-Peer Networks?: A Stackelberg Game Approach. IEEE Transactions on Mobile Computing 2015; 14:1018–1030.
[65] Chen S, Wang G, Jia W. Cluster-group based trusted computing for mobile social networks using implicit social behavioral graph. Future Generation Computer Systems 2016; 55:391–400. https://doi.org/10.1016/j.future.2014.06.005.
[66] Nohuddin PNE, Coenen F, Christley R, Setzkorn C, Patel Y, Williams S. Finding "interesting" trends in social networks using frequent pattern mining and self organizing maps. Knowledge-Based Systems 2012; 29:104–113. https://doi.org/10.1016/j.knosys.2011.07.003.
[67] Duan Z, Sun X, Zhao S, Chen J, Zhang Y, Tang J. Hierarchical community structure preserving approach for network embedding. Information Sciences 2021; 546:1084–1096. https://doi.org/10.1016/j.ins.2020.09.053.
[68] Mohaisen A, Tran H, Chandra A, Kim Y. Trustworthy distributed computing on social networks. IEEE Transactions on Services Computing 2014; 7:333–345. https://doi.org/10.1109/TSC.2013.56.
[69] Abbass H, Greenwood G, Petraki E. The N-Player Trust Game and its Replicator Dynamics. IEEE Transactions on Evolutionary Computation 2016; 20:470–474. https://doi.org/10.1109/TEVC.2015.2484840.
[70] Chaal M, Bandaa OAV, Glomsrud JA, Basnet S and Kujala P. A framework to model the STPA hierarchical control structure of an autonomous ship. Safety Science 2020; 132: 104939.
[71] Jiang S, He D, Rao J. A prediction-based link availability estimation for routing metrics in MANETs. IEEE/ACM Transactions on Networking 2005; 13:1302–1312. https://doi.org/10.1109/TNET.2005.860094.
[72] Machado C, Westphall CM. Blockchain incentivized data forwarding in MANETs: Strategies and challenges. Ad Hoc Networks 2021; 110. https://doi.org/10.1016/j.adhoc.2020.102321.
[73] Chancay-García L, Hernández-Orallo E, Manzoni P, Vegni AM, Loscrí V, Cano JC, Calafate C. Optimising message broadcasting in opportunistic networks. Computer Communications 2020; 157:162–178. https://doi.org/10.1016/j.comcom.2020.04.031.

Appendix 1.

List of acronyms.

Abbreviation	Definition	Remark
MASS	Maritime Autonomous Surface Ship	
BoT	Belief of Trust	
MUNIN	Maritime Unmanned Navigation through Intelligence in Networks	

AAWA	Advanced Autonomous Waterborne Applications	
SVAN	Safer Vessel with Autonomous Navigation	
UAV	Unmanned Aerial Vehicle	
CPS	Cyber Physical System	
VHF	Very High Frequency	The dominant voice/data communications utilize frequency within this spectrum for maritime usage.
P2P	Peer-to-Peer	
IMO	International Maritime Organization	
CA	Certificate Authority	A commercial body or non-commercial organization that issues identification certificates endorsing its trust.
PKI	Public Key Infrastructure	
AIS	Automatic Identification System	
AL	Autonomy Level	
DTL	Direct Trust Length	
GFT	Gossip Forwarding Table	
RTCN	Relationship Trees of Certificate Nodes	
ITTC	Inherent Train of Trusted CA	
NCC	Nearest Common CA	
PriBoT	Prior Belief of Trust	
CG	Credence Giver	
CR	Credence Recipient	
TCP	Trust Contact Point	
ID	Identity	
MMSI	Maritime Mobile Service Identity	
ARPA	Automatic Radar Plotting Aid	
IP	Internet Protocol	The fundamental network-layer protocol that governs the data transmission in the Internet.
MAC	Media Access Control	
QoS	Quality of Service	Some quantitative characteristics to indicate the performance of data transfer across a network.
ITU	International Telecommunication Union	
ISP	Internet Service Provider	Equivalently called *carrier* in the literature.
INMARSAT		The name of a company that is the major provider of global mobile satellite communications.
VDES	VHF Data Exchange System	
ASM	Application Specific Message	
VDE-TER	VHF Data Exchange -Terrestrial	
VDE-SAT	VHF Data Exchange-Satellite	
VANET	Vehicular Ad Hoc Network	