M-SMDM: A model of security measures using Green Internet of Things with Cloud Integrated Data Management for Smart Cities

Amjad Rehman [a,*], Khalid Haseeb [b], Tanzila Saba [a], Hoshang Kolivand [c,d]

[a] *Artificial Intelligence & Data Analytics Lab (AIDA) CCIS Prince Sultan University, Riyadh, 11586, Saudi Arabia*
[b] *Computer Science Department, Islamia College Peshawar, Peshawar, Pakistan*
[c] *School of Computer Science and Mathematics, Liverpool John Moores University, Liverpool, UK*
[d] *School of Computing and Digital Technologies, Staffordshire University, Staffordshire, UK*

ABSTRACT

In recent years, the Green Internet of Things (G-IoT) has gained a lot of attention to developing energy-efficient communication systems. It consists of electronic devices and is integrated with numerous tight constraint sensors for observing the real world and provide communication services to end-users. However, optimal data collection and its management among the heterogeneous G-IoT objects are one of the main challenges. Many researchers are still proposing different solutions to cope with such problems and offering IoT-cloud paradigms for processing, storage, and scalability services. However, the data of smart cities is forwarded using the open-source IoT platform, and sensitive information may be compromised. Therefore, this research aims to propose a model of security measures using the Green Internet of Things with Cloud Integrated Data Management (M-SMDM) for Smart Cities. Firstly, it forms a long-run and energy-efficient connectivity using self-balancing trees and distributing load factors uniformly in green communication systems. Secondly, it addresses the problem of secret key distribution between peer nodes and attained trust for both partial and direct communication. In the end, it securing the transmission system from mobile gateways to application users against threats with improved overheads and data latency. The security analysis of the proposed M-SMDM model is done along with simulation-based experiments. The attained results disclose the importance of the proposed model in terms of network parameters compared to existing work.

1. Introduction

Many applications are based on G-IoT technology for observing the data of smart cities and facilitating the real world (Ram et al.,2019;Haseeb et al.,2020;Khasawneh et al.,2020;Li et al.,2018). It comprises many electronic devices, sensors, and actuators to communicate over the Internet and offer various services to academic and industrial applications. It is a network that connects the physical objects with the computing world and presents communication services at any time to connected IoT users. However, there are many communication and security related challenges in the development and management of green applications (Zeinab and Elmustafa,2017;Muhammad et al.,2019;Cui et al.,

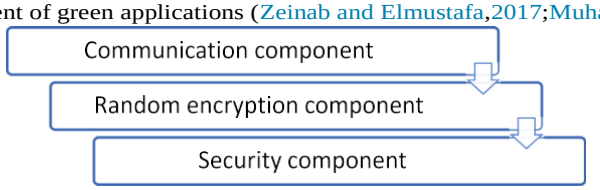

Fig. 1. Model of security measures for G-IoT system.

2018). Most of the important encounters need an optimal solution for the development of an energy-efficient paradigm with the semantically secure transmission in the presence of network abnormalities. Also, to enable G-IoT's persistent deployment, the application user's main demand is to maximize the power supply of the sensor nodes because they have very restricted constraints in terms of battery, memory, and storage attributes. Many researchers have recently given attention to facilitate real-time applications such as smart homes, industries, agriculture, e-health, sustainable cities, etc to cope with the tradeoff between communication systems and energy efficiency (Palmieri et al.,2015;Haseeb et al.,2019b,a; Maksimović and Omanović-Mikličanin,2017). These tiny and battery-powered G-IoT sensors are also operated over the Internet, which is unpredictable for secure and authentic communications. Many traditional cryptographic approaches (Bos et al.,2014;Brown,2009) have been utilized by Internet technologies to offer a method for sharing and joining the wireless medium. However, many restrictions are continuing to grow for application users with high computing cost for the implement of security solutions (Rani et al.,2019;Muthanna et al.,2019). For large-scale smart cities, the G-IoT are major components to gather real information and further forward cloud systems. The sensing systems in smart cities are distributed and exploit different scenarios for real-time events detection with various operations

management. Therefore, with various complications, secure end-to-end communication by mutual authentication is also a serious concern. However, due to smart cities' integrated existence with multiple technologies, developing an entirely optimized framework is an important and difficult task (Ouaddah et al.,2017;Kushwah et al.,2020;Hossain et al.,2018; Atlam et al.,2020). Moreover, according to users and environmental points of view, smart cities' communication systems must be secure. Such problems have forced network designers and developers to consider various scenarios for G-IoT-enabled smart cities in various conditions. The proposed solutions must require secure, authentic, and intelligent data management strategies in large-scale smart cities (Li et al.,2017;Zhang et al.,2020;Sharma and Kalra,2017). Therefore, this paper presents a model of security measures using G-IoT with cloud integration for smart cities, aiming to improve data management with a longer network lifetime and security. Although, introducing IoT-based electronic devices has provided a significant contribution to smart cities' operations and cope with remote monitoring of the physical conditions. However, such systems are operated on independent and unreliable nodes. Thus information about smart cities should be gathered on stable and reliable channels. Also, the observing field's real-time operations and confidential details of the electronic devices are transmitted to the cloud over the Internet. Thus security is another concern and must be considered in the development of any green IoT-based solution.

The proposed M-SMDM model includes the following contributions.

i. Firstly, point-to-point links are constructed using multiple AVL trees (Adel'son-Vel'skii and Landis,1962) and provide the G-IoT balance factor. Unlike some other solutions, it computes the nodes' priority function by minimizing the computing and complexity time for determining the shortest link for data routing. Such a solution leads to improve energy-saving and data delivery performance for large-scale smart cities.
ii. Also, it provides communication trust, such that directed or partially connected sensors securely distribute keys using random simulation. Moreover, unlike static keys, the proposed model produces keys using random simulation and valid only for a particular session. Later, the nodes need to negotiate with the updated keys for continuing their transmissions.
iii. Furthermore, it presents a security algorithm for data routing from middle-layer mobile gateways to cloud systems. The proposed solution reduces the key sizes than the existing solution for constraint-oriented networks with nominal overheads and transmission delay.
iv. The evaluation results have proven the proposed M-SMDM model's significant performance in terms of energy efficiency and provide security with lower routing cost than other schemes.

Fig.1demonstrates the operation phases of the proposed M-SMDM model. Further paper is organized in the following sections. Section2presents related work. In Section3, we present the detail of the proposed model with the network model and assumptions. Section4explains the results, discussion, and security analysis of the proposed model. Finally, the research work is concluded in Section5.

2. Related work

The rapid growth and communication applications, network, and smart devices make the IoT-based system interconnected in a smart city. However, IoT applications' perceived improvement has increased the risk of loss of privacy and authentication in many situations. That is why it identifies an obvious privacy-aware sharing requirement for IoT without compromising user privacy and conversation details. InPopescul and Genete(2016), the authors identified security issues in smart cities that are consist of many smart things, such as smart spaces, intelligent connectors, and intelligent citizens. Because the IoT systems are all connected, any threat traveling from one such system poses a threat to all of them. One possible concern may be the wider attack surface of IoT devices because of all the connected devices. The type of data in a smart city is most sensitive, so privacy and confidentiality are therefore required. These requirements can be filled by informing and educating citizens. Thus, the authors introduced privacy by design and privacy by default concepts and proposed to apply them in IoT and smart cities. They introduced a role-based access control system, which distinguishes managers' and visitors' positions subject to individuals accessing different resources within an organization. IoT nodes are given similar positions with various access privileges, such as reading, writing, and execution. This role-based access control scheme allows for a multitude of connections between access rights and nodes. InSinde et al.(2020), the authors introduce a model for wireless sensor networks (WSN) to stability period and energy consumption. It generates clusters by developing an Enhanced Low-Energy adaptive Clustering Hierarchy protocol (E-LEACH), which selects cluster heads and helper cluster heads based on parallel operating optimization and Discrete Particle Swarm Optimization techniques. The proposed solution also copes with the management of cluster size by either splitting or merging. Such actions decrease the ratio of unnecessary energy consumption for larger clusters size. Authors (Ilyas et al.,2020) proposed a trust-based energy-efficient IoT-based sensor network for improving throughput, network lifetime, and latency factors under the presence of malicious threats. It is a three-tier clustering technique with incorporated security methods to cope with network threats. The proposed solution is a centered-based clustering protocol. Also, hardware-based link quality estimators are included to evaluate the link measurement and to improve routing performance. InLi and Li(2018), the authors introduced an energy-balanced routing protocol (EBRP), which aims to construct the clusters using the K-means++ algorithm and perform the process for the selection of cluster heads based on the fuzzy logic system (FLS). Also, it proposed a genetic algorithm (GA) for obtaining fuzzy rules. The simulation-based experiments demonstrate the improved performance of EBRP as compared to other solutions. InKhan(2018), the authors suggested a lot of network attacks that compromise the IoT networks

and disturb their privacy. Also, the research community needs to develop a secure solution for IoT-based networks in smart cities. In the proposed work, a trust-based approach is developed and analyzed how it can be improved further for improving energy efficiency. In Priyadarshini and Sivakumar (2018), authors accomplished load balancing by using AVL tree rotation clustering. The network field is distributed into multiple clusters by using modified K-means clustering algorithm. Also, AVL-Tree rotation algorithm is exploited to determine the next round of cluster by using certain thresholds and values of residual energy. The proposed solution is also appropriate for both the sparse and dense topologies. Authors in Qin et al. (2015) proposed a new efficient key management scheme using Elliptic Curve Cryptography (ECC) and AVL tree for large-scale WSNs. The proposed solution makes use of the Elliptic Curve Paillier Encryption (ECPE) cryptography for network communication and AVL trees are used to store the neighbors' information such as ID and public key. Also, the keys are updated regularly and improves the security for the network structure.

It is seen from the study of the related work that IoT devices have a rapid use in the development of smart applications. However, G-IoT based solutions are remarkably demanded the better utilization of energy consumption in observing real-world communication. Also, due to the constraints of resources and their communication over the global network, arises high chances for data compromising and unauthorized access. Although, in recent decades, different solutions have been developed for G-IoT scenarios, however, they route the real-time information with an additional cost of computation and overlooked security issues. Moreover, it is seen that some solutions are proposed to tackle the security of constraint nodes but such schemes not able to optimize the delivery rate among partial and direct connected neighbors. It is also observed that some solutions are developed efficient mechanism with the collaboration of cloud network, however, they imposing high-security cost and communication complexity.

3. Proposed M-SMDM model

In this section, we discuss the architecture of the proposed work with its network model and assumptions.

3.1. Network model and assumptions

The proposed work structure consists of heterogeneous sensor nodes that are deployed randomly in the dimensional field. The nodes have limited transmission power and can adopt single and multi-hop data routing. If transmission power is less than the set distance threshold, the node adopts direct transmission. Otherwise, multi-hop forwarding is used. There are various gateway nodes are installed in the field to receiving the data from the IoT sensors and further routed towards the cloud. The gateway nodes have unique MAC identifiers with enough memory, computing power, and considered as trusted. Moreover, the gateway nodes are mobile and rotate at a fixed speed. The communication links are asymmetric and each node has a unique identifier *ID*. Each node maintains its routing table and is only updated when any changes occur around the neighborhood. This proposed work considers an energy model, as described in Heinzelman et al. (2000). The energy consumption on the transmission of single data bit l can be computed as given in Eq. (1).

$$E_{Tr}(k, a) = l(E_e + E_{fs} * D^{\beta}), if\, a \leq d_t \tag{1}$$

where,
E_e is dissipated energy of transmitter
E_{fs} is an amplifier unit
a is a distance value
β is an exponent of the propagation unit, and its value is (2, 4), if $\beta = 2$, it is free space otherwise explains the multi-path model.
and
d_t is distance threshold,
$E_{Rx}(l)$ defines the energy consumption in the reception of the during the reception of l data bits, as shown in Eq. (2).

$$E_{Rx}(l) = E_e . l \tag{2}$$

3.2. Model architecture

This section presents the architecture of the proposed model and its working mechanism is depicted in Fig. 2. In the beginning, the gateway nodes construct map tables $T(ID, p)$ that contains the identity *ID* and position p information of the IoT sensors that fall into their transmission range. Before initiating the communication system, IoT sensors must need to register with their closest gateway nodes. The gateway nodes produce encryption keys for their nearer sensors based on the Lehmer random number generator (Payne et al., 1969), also called Lehmer Method. This method generates a set of pseudo-random numbers in a precise series, as given in Eq. (3).

$$K_{i+1} = aK_i \bmod m \tag{3}$$

where,

k is the sequence of keys based on pseudo-random numbers, m is the modulus and must be > 0, and K_0 is the initial value, termed as a seed value. Afterward, the gateway nodes digitally signed the generated secret keys using their private keys P and send them towards appropriate sensor nodes. The generated secret keys are only valid for the specific session, and after its expiry, the source node has to negotiate with the gateway for obtaining the other one. Also, gateways create an entry against each node in the map table regarding the assigned secret key. Upon receiving the secret keys, each node verifies its authenticity using the gateway node's public key.

Afterward, the proposed M-SMDM model organized the IoT sensors in AVL trees based on the priority. The priority depends on the energy and cumulative distance factors. The gateways nodes are placed on the root of AVL trees, while the nodes whose priority threshold is below a certain level are placed on the left sub-trees, and those whose priority level is higher than a certain threshold are placed in the right sub-trees. The nodes' energy is denoted by E_i and can be computed as e_i/E, where e_i is residual energy and E is the collective energy of $T_x + R_x$. Let us us consider that d_i is the distance of the node from the mobile gateway and D is the distance of the mobile gateway from the cloud server, the distance factor D_t can be computed as d_i/D. Thus the priority of the sensor node can be determined as given in Eq.(4).

$$N_i = E_i + D_t \in T_h, \tag{4}$$

where,

T_h is a threshold and its value ranges from 0 to 1. After the formulation of AVL trees, sensor nodes forward the gathered data by governing the following rules.

i. If the sensor node s_i is closest to the gateway node, it simply performs encryption function as given in Eq.(5).

$$E(d_i) = d_i \oplus K_i || ID_{si} \tag{5}$$

where,
ID_{s_i} is a unique identity of sensor node s_i
d_i is gathered data
$\oplus$ is the XoR'd function
K_i is a secret key between a sensor node s_i and mobile gateway

ii. However, if the gateway node is partially connected to a sensor node s_i, and direct transmission cannot be applied, then the multi-hop paradigm is adopted as given in Eq.(6).

$$E(d_{i+1}) = [E(d_i) + (d_{i+1} \oplus K_{i+1})] || ID_{si+1} \tag{6}$$

where,
d_{i+1} is the next data block
K_{i+1} is a next-level secret key

Upon receiving the encrypted blocks to the gateway, it verifies the identity nodes using the map table. If it matches, the gateway node performs further processing for routing the gathered data towards the cloud server. Otherwise, it considers the data as malicious and ignores it.

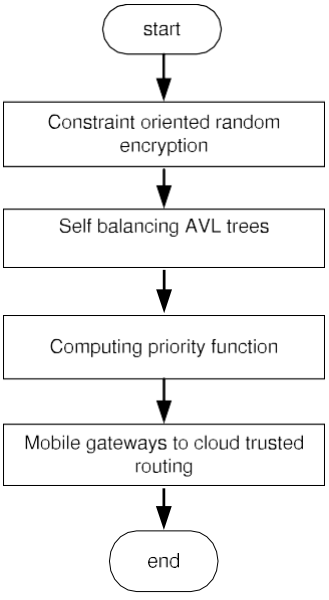

Fig. 2. Working mechanism of M-SMDM model.

The proposed M-SMDM model exploits cloud servers integrated with mobile gateways for data management and

decreases communication time on the IoT sensors. The collected data security is achieved between gateways and cloud paradigms using the Diffie–Hellman algorithm (Diffie and Hellman,1976). It aims to share the smaller-sized, robust and stronger secret key using public–private keys pair with decrease memory overheads. Also, it improves the communication performances in terms of network threats and appropriate for constraints nodes. To accomplish this, four parameters are used i.e. p (prime number), g (the primitive root of p), and both are considered public keys. However, c and d are assumed as private keys. The mobile gateway M_gw and cloud server C_sr uses these parameters. It generates a piece of key information. Later they exchange the generated information with each other as given in Eqs.(7)and(8).

$$x = g^c \bmod p \tag{7}$$

$$y = g^d \bmod p \tag{8}$$

Afterward, based on the obtain public information x and y, symmetric keys are generated for the mobile gateway k_g and cloud server k_c as given inEqs.(9)and(10).

$$k_g = y^a \bmod p \tag{9}$$

$$k_c = x^b \bmod p \tag{10}$$

Accordingly to mathematical computing $k_g = k_c$. Now, both M_gw and C_sr have the same secret keys. The encryption of the data block M from M_gw to the cloud server C_sr is denoted by C along with the MAC_{id}, an encrypted value with the private key P. Such encrypted MAC_{id} value is included in the block to verify the identity of M, as given in Eq.(11).

$$E = C + P^e.MAC_{id} \tag{11}$$

The C_{sr} decrypts the encrypted block using the public key of mobile gateway R to verify the MAC_{id}. Later, it uses the same secret key to recover the actual sensors' data denoted by C', as given in Eq.(12).

$$D = R^d.MAC_{id} + C' \tag{12}$$

The pseudocode of the proposed model is given as follows.

16. $S_{i+1} \leftarrow E(d_{i+1}) = [E(d_i) + (d_{i+1} \oplus K_{i+1})] \| ID_{si+1}$
17. $M\_gw, C_{sr} \leftarrow y^a \bmod p = x^b \bmod p$
18. $E(M\_gw) \leftarrow C + P^e.MAC_{id}$
19. $D(C\_sr) \leftarrow R^a.MAC_{id} + C'$
20. **end procedure**

4. Experiments

This section presents the following sub-sections to discuss the simulation environment, discussion on results with security analysis.

4.1. Simulation setup

In this section, the proposed M-SMDM model is evaluated against existing work in terms of the number of nodes and data sizes. The IoT sensors are deployed randomly in the range of 100 to 300. The number of gateway nodes is set to 5

Table 1
Simulation parameters.

Parameter	Value/Range
Deployment	Random
Sensor nodes	100–300
Network attackers	10
Initial energy	1j–3j
Transmission radius	15 m
Gateway nodes	5
Speed of gateway	3 m/s
Cloud server	1
Simulation interval	1000 s
Data size	1000 bits

which is movable at the speed of 3 m/s. The simulation-based experiments are done in a discrete-event network simulator (NS-3) (Liu et al.,2016;Paliwal and Taterh,2018) for packet loss rate, network throughput, energy consumption, end-to-end delay, and computational overhead. Each node has an initial energy level from 1j to 3j. The experiments are done for

the interval of 1000 s. The data block size is fixed to 1000 bits and each node has a transmission radius is set to 15 m. The default range of the simulation parameters used in the proposed work is listed inTable1.

4.2. Security analysis

In WSN-based applications, due to restricted constraint on sensor node, data security is one of the significant importance. Most of the solutions proposed routing decisions, however, they overlooked network threats and malicious activities in data transmission for smart cities. Such solutions do not consider the interaction of malicious or faulty nodes in the observing field, resulting in increasing packet loss rate and compromised data security. In the proposed work, before initiating the routing process, the sensor nodes must register with their closest gateway to achieving data privacy and authentication. Initially, the gateway nodes use the multiplicative Congruential method to generate random keys and distribute them among register nodes. Also, the identity of register sensor nodes is store in the map table for data authentication. Moreover, public–private keys are used to verify the authenticity of gateway nodes to IoT-based sensors. If IoT sensor is directly connected with the gateway, then data encryption is done using the shared secret key. However, if there is partial connectivity towards the gateway, then data privacy and integrity are obtained using the shared secret keys

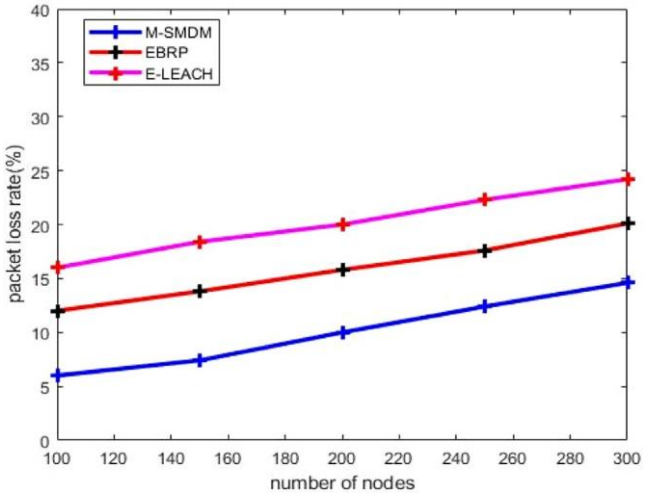

Fig. 3. Packet loss rate and number of nodes.

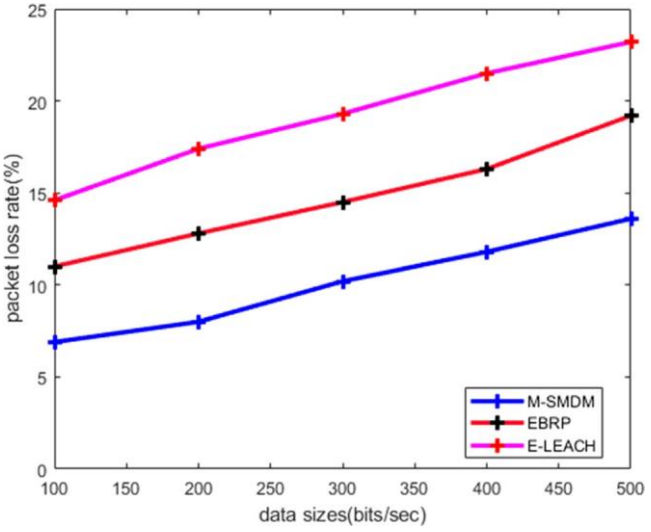

Fig. 4. Packet loss rate and data sizes.

in a multi-hop pattern. Accordingly, the XoR'd operation based on generated keys and sensors' data offers encrypted hash blocks, which can be forwarded either directly or through multi-hop paradigms. The hash blocks cope to retain the data integrity against abnormal activities. Unlike RSA, the proposed M-SMDM model uses the Diffie–Hellman algorithm, which aims to share stronger and smaller-sized keys using public–private key pairs and minimize the computation overheads

between gateway nodes and cloud server. Moreover, the identity of the gateway node is proven on a cloud server using encrypted MAC_{id}.

4.3. Results

4.4. Discussion

Figs.3and4depict the performance of the proposed M-SMDM model is compared to existing work in terms of packet loss rate under varying numbers of nodes. It is observed that by increasing the number of nodes from 100 to 300, and data sizes from 100 to 500 bits, the packet loss rate ratio also increases. However, the proposed M-SMDM model significantly decreases the packet drop ratio by an average of 33% and 34% in the comparison of EBRP and E-LEACH. It is due to the incorporation of security management using lightweight multiplicative congruential cryptographic algorithms and securely distribute the keys among IoT sensors. Such proposed solution intelligently identified the malicious nodes and

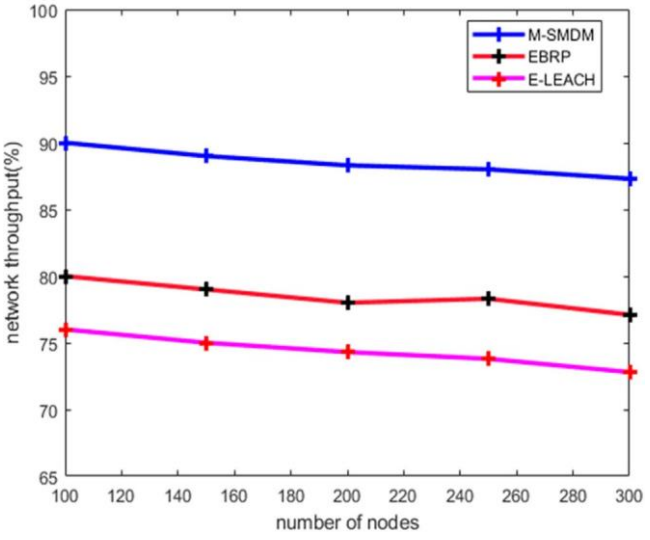

Fig. 5. Network throughput and number of nodes.

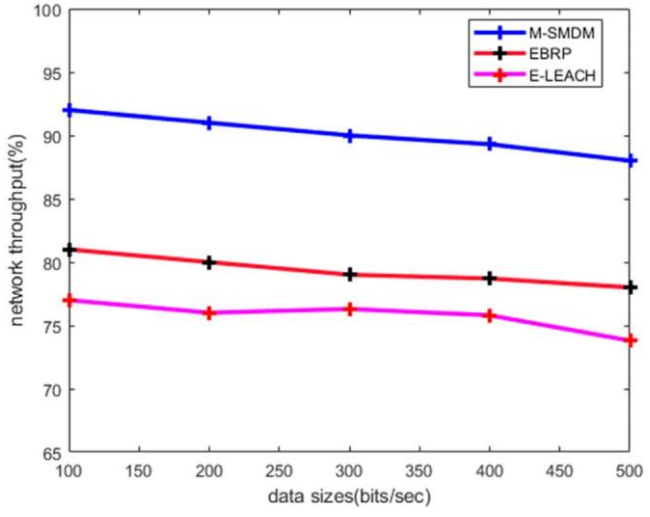

Fig. 6. Network throughput and data sizes.

avoid their practice for packet drop and involvement in transmission routes. Based on the simulation experiments, it is seen that the existing solution is increasing the packet loss rate as the number of nodes is increasing because they ignore security measurements. It also balances the load factor among neighbors using the AVL tree and generates the most energy-efficient and shortest communication route. The results have proven the saving in packet loss ratio, which shows the M-SMDM model's efficacy for data forwarding in a large-scale observing field.Figs.5and6illustrate the

performance of the proposed M-SMDM model in terms of network throughput compared to EBRP and E-LEACH. It is seen from the experiments that the M-SMDM model increases the measurement of network throughput by an average of 17% and 16% than other solutions. The network throughput is a key parameter for the analysis of any routing protocol, its performance decreases in congested and heavy network traffic. The M-SMDM model improves the network throughput because it utilized the self-balancing tree for data collection and transmission. The AVL trees are based on the priority function, which comprises energy and cumulative distance parameters. Also, it adopts the mobile gateway nodes, which explicitly increases the availability of the channel dynamically with IoT sensors and improves data delivery performance. Moreover, the M-SMDM model offers a secure transmission system under malicious threats and tackles such attacks efficiently with nominal computing resources of IoT sensors. As a result, it decreases the chances for exposed attacks for re-directing sensors' data and decreases route damages and dis-connectivity. Furthermore, it uses both direct and partial data delivery paths and optimizes the transferring time between connected nodes and the real world. Figs. 7 and 8 illustrate the evaluation of the proposed M-SMDM model in terms of energy consumption than other solutions. It is revealed from the

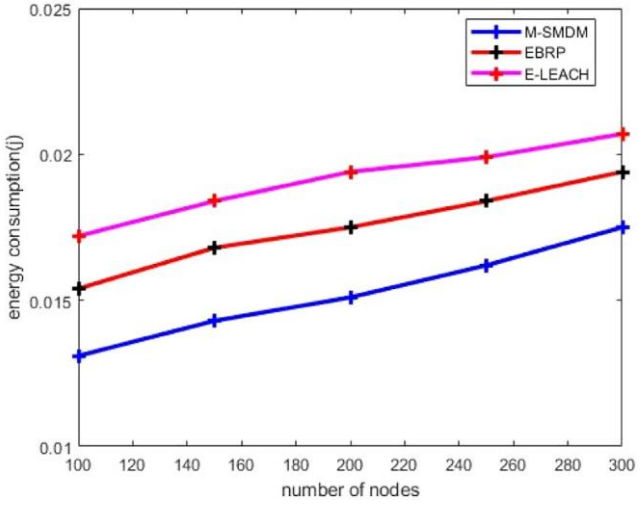

Fig. 7. Energy consumption and number of nodes.

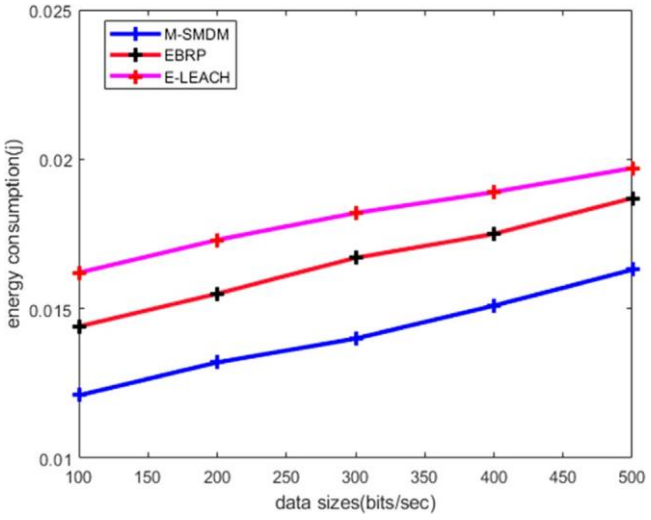

Fig. 8. Energy consumption and data sizes.

experiments that the M-SMDM model significantly improves the energy consumption by an average of 13% and 15% than EBRP and E-LEACH due to dynamic factors. The M-SMDM model operates in different phases and each phase notices the constraint resources of the sensor nodes. Instead of determining the next-hop in an entire field, the M-SMDM model uses AVL trees to balance the load factor among nodes and decreases unnecessary energy consumption. The data routing is also based on the priority function, which utilized energy, cumulative distance from the node to the gateway node, and from the gateway node to the cloud server. This gives the least overheads in finding the appropriate route for the transmission of observed data with minor re-transmissions. Figs. 9 and 10 show the proposed model's analysis of the existing solution

in terms of end-to-end delay under a varying number of nodes. The delay performance metrics are also a key feature for evaluating the performance of the data transmission system. If the delay value is high, then any routing solution lacks route creditability and dependability. It is noticed that with increasing the number of nodes, the ratio of end-to-end delay is also increasing. However, the results have proven that the M-SMDM model decreases the latency rate by an average of 27% and 26% over the insecure medium due to the secure algorithm's consideration and optimizes the construction of self-balancing trees. Also, the AVL based heuristic tree reduces the time complexity in determining the reliable path and distribute the energy load uniformly. Moreover, the gateway nodes in the M-SMDM model operate in dual-mode and decreasing the delay factor, one with observing field and the other with cloud paradigm.Figs.11and12demonstrate the performance of the M-SMDM model with other solutions for computational overhead. The computational overhead is also an important factor for constraint-oriented networks, especially in constraint-oriented IoT networks, which comprise

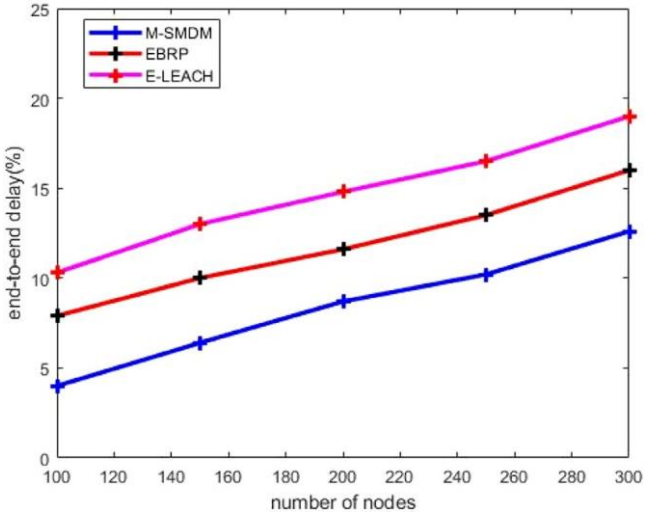

Fig. 9. End-to-end delay and number of nodes.

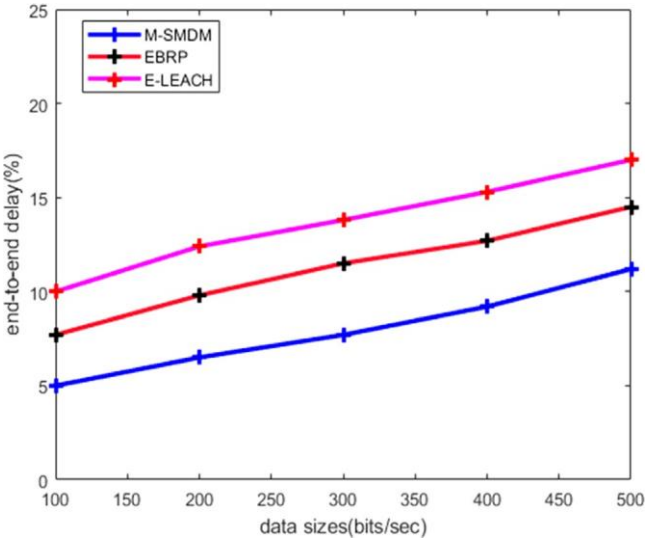

Fig. 10. End-to-end delay and data sizes.

battery power electronic devices. It is observed from the simulation experiments that as the number of nodes increases, the ratio of computational overheads also increasing. However, based on the result's analysis, it is proven that the M-SMDM model decreases the computational overhead than EBRP and E-LEACH solutions by an average of 29% and 27%. It is because instead of transmitting the sensors' data directly to cloud servers, the M-SMDM modeled mobile gateways as intermediate devices. Also, the nodes in the same transmission ranges are operated by a single gateway node. Thus their supervision is manageable for the large-scale region with minimal computing power. Unlike EBRP and E-LEACH, the M-SMDM model increases the ratio of route maintenance by integrating the security mechanisms and avoid the chances of external attacks for misusing the resources for data re-routing and route rediscoveries.

5. Conclusion

This paper presents a security measures model for the green Internet of Things with cloud-integrated data management in smart cities to attain energy efficiency and secure communication. The proposed M-SMDM model increases G-IoT systems' efficiency in terms of network lifetime and data delivery performance. Unlike most of the existing work, it avoids the additional load on IoT sensors and minimizes the communication time in computing the routing decision based on AVL trees. Also, it offers the trust mechanism based on a cryptography algorithm to generate secret keys using

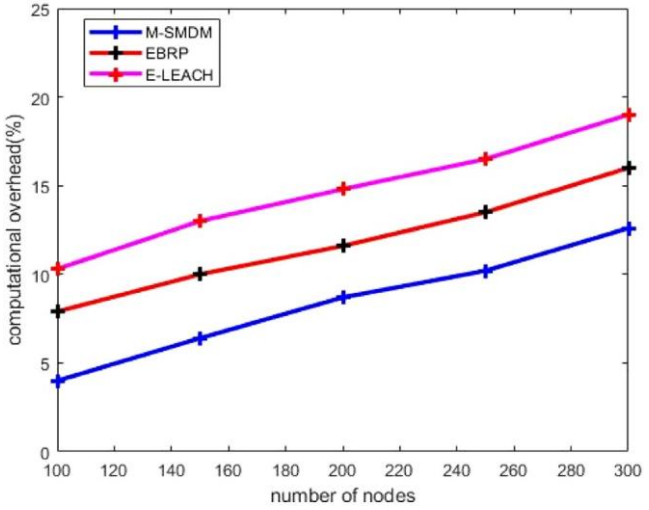

Fig. 11. Computational overhead and number of nodes.

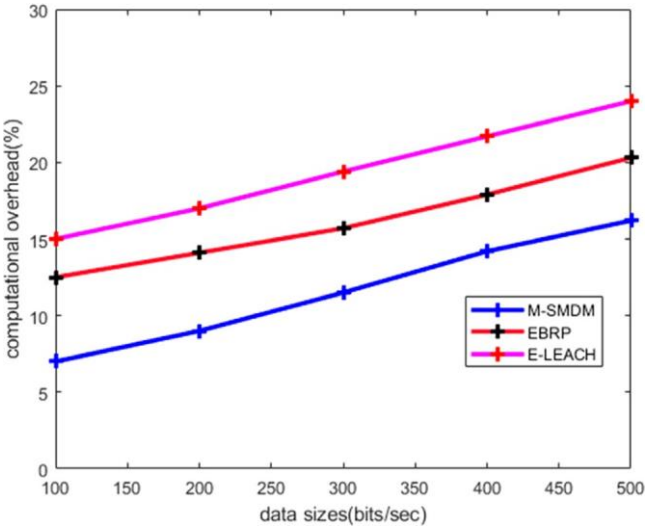

Fig. 12. Computational overhead and data sizes.

random simulation for each session and securely distribute among peer sensors. The integration of the mobile gateways explicitly increases the deployed G-IoT sensors' connectivity ratio with cloud servers with minimal routing overheads. Moreover, the lightweight XoR'd function imposes the least computing power of battery-powered sensors with ease of data management. Furthermore, by utilizing the cryptograph based algorithm, the proposed model securely established nodes' session using public–private keys between mobile gateways and the cloud system. Such adopted strategy in the proposed M-SMDM model maintains the data confidentiality and authentication of communicating objects. However, the proposed M-SMDM model still needs improvement to deal with the bulk of traffic in computing the priority conditions. Also, the security algorithm can be extended to analyze the paradigm of IoT and smart cities against distributed denial of services. Thus, in the future, we aim to introduce a machine learning-based technique to make the model more intelligent and train it for security analysis under real-time data collections.

CRediT authorship contribution statement

Amjad Rehman: Conceptualization, Methodology, Writing – original draft. **Khalid Haseeb:** Experiments, Methodology, Validation, Writing – review & editing. **Tanzila Saba:** Investigation, Formal analysis, Resources, Writing – review & editing. **Hoshang Kolivand:** Software, Validation, Visualization, Formal analysis.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This work was supported by the Artificial Intelligence & Data Analytics Lab (AIDA), CCIS, Prince Sultan University, Riyadh, Saudi Arabia.

References

Adel'son-Vel'skii, G.M., Landis, E.M., 1962. An algorithm for organization of information. Doklady Akademii Nauk. Russian Academy of Sciences.
Atlam, H.F., Alenezi, A., Alassafi, M.O., Alshdadi, A.A., Wills, G.B., 2020. Security, cybercrime and digital forensics for IoT. In: Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm. Springer, pp. 551–577.
Bos, J.W., Halderman, J.A., Heninger, N., Moore, J., Naehrig, M., 2014. Elliptic curve cryptography in practice. In: International Conference on Financial Cryptography and Data Security. Springer.
Brown, D., 2009. Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography, Vol. 1. Released Standard Version.
Cui, L., Xie, G., Qu, Y., Gao, L., Yang, Y., 2018. Security and privacy in smart cities: Challenges and opportunities. IEEE Access 6, 46134–46145.
Diffie, W., Hellman, M., 1976. New directions in cryptography. IEEE Trans. Inform. Theory 22 (6), 644âĂŞ654.
Haseeb, K., Islam, N., Almogren, A., Din, I.U., 2019a. Intrusion prevention framework for secure routing in WSN-based mobile Internet of Things. IEEE Access 7, 185496-185505.
Haseeb, K., Islam, N., Saba, T., Rehman, A., Mehmood, Z., 2019b. LSDAR: A light-weight structure based data aggregation routing protocol with secure internet of things integrated next-generation sensor networks. Sustainable Cities Soc. 101995.
Haseeb, K., Lee, S., Jeon, G., 2020. EBDS: An energy-efficient big data-based secure framework using Internet of Things for green environment. Environ. Technol. Innov. 101129.
Heinzelman, W.R., Chandrakasan, A., Balakrishnan, H., 2000. Energy-efficient communication protocol for wireless microsensor networks. In: System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference. IEEE.
Hossain, M., Islam, S.R., Ali, F., Kwak, K.-S., Hasan, R., 2018. An internet of things-based health prescription assistant and its security system design. Future Gener. Comput. Syst. 82, 422–439.
Ilyas, M., Ullah, Z., Khan, F.A., Chaudary, M.H., Malik, M.S.A., Zaheer, Z., Durrani, H.U.R., 2020. Trust-based energy-efficient routing protocol for internet of things–based sensor networks. Int. J. Distrib. Sens. Netw. 16 (10), 1550147720964358.
Khan, Z.A., 2018. Using energy-efficient trust management to protect IoT networks for smart cities. Sustainable Cities Soc. 40, 1–15.
Khasawneh, A.M., Kaiwartya, O., Lloret, J., Abuaddous, H.Y., Abualigah, L., Shinwan, M.A., Al-Khasawneh, M.A., Mahmoud, M., Kharel, R., 2020. Green communication for underwater wireless sensor networks: Triangle metric based multi-layered routing protocol. Sensors 20 (24), 7278.
Kushwah, R., Batra, P.K., Jain, A., 2020. Internet of things architectural elements, challenges and future directions. In: 2020 6th International Conference on Signal Processing and Communication (ICSC). IEEE.
Li, L., Li, D., 2018. An energy-balanced routing protocol for a wireless sensor network. J. Sensors 2018.
Li, Z., Liu, Y., Liu, A., Wang, S., Liu, H., 2018. Minimizing convergecast time and energy consumption in green Internet of Things. IEEE Trans. Emerg. Top. Comput..
Li, W., Song, H., Zeng, F., 2017. Policy-based secure and trustworthy sensing for internet of things in smart cities. IEEE Internet Things J. 5 (2), 716–723.
Liu, W., Wang, X., Zhang, W., Yang, L., Peng, C., 2016. Coordinative simulation with SUMO and NS3 for vehicular ad hoc networks. In: 2016 22nd Asia-Pacific Conference on Communications (APCC). IEEE.
Maksimović, M., Omanović-Mikličanin, E., 2017. Green internet of things and green nanotechnology role in realizing smart and sustainable agriculture. In: VIII International Scientific Agriculture Symposium AGROSYM 2017.
Muhammad, K., Lloret, J., Baik, S.W., 2019. Intelligent and energy-efficient data prioritization in green smart cities: Current challenges and future directions. IEEE Commun. Mag. 57 (2), 60–65.
Muthanna, A., Ateya, A.A., Khakimov, A., Gudkova, I., Abuarqoub, A., Samouylov, K., Koucheryavy, A., 2019. Secure and reliable IoT networks using fog computing with software-defined networking and blockchain. J. Sens. Actuator Netw. 8 (1), 15.
Ouaddah, A., Abou Elkalam, A., Ouahman, A.A., 2017. Towards a novel privacy-preserving access control model based on blockchain technology in IoT. In: Europe and MENA Cooperation Advances in Information and Communication Technologies. Springer, pp. 523–533.
Paliwal, G., Taterh, S., 2018. Impact of dense network in MANET routing protocols AODV and DSDV comparative analysis through NS3. In: Soft Computing: Theories and Applications. Springer, pp. 327–335.
Palmieri, F., Ricciardi, S., Fiore, U., Ficco, M., Castiglione, A., 2015. Energy-oriented denial of service attacks: an emerging menace for large cloud infrastructures. J. Supercomput. 71 (5), 1620–1641.
Payne, W., Rabung, J.R., Bogyo, T., 1969. Coding the Lehmer pseudo-random number generator. Commun. ACM 12 (2), 85–86.
Popescul, D., Genete, L.-D., 2016. Data security in smart cities: challenges and solutions. Inf. Econ. 20 (1).
Priyadarshini, R.R., Sivakumar, N., 2018. Cluster head selection based on minimum connected dominating set and bi-partite inspired methodology for energy conservation in WSNs. J. King Saud Univ.-Comput. Inf. Sci..
Qin, Z., Zhang, X., Feng, K., Zhang, Q., Huang, J., 2015. An efficient key management scheme based on ECC and AVL tree for large scale wireless sensor networks. Int. J. Distrib. Sens. Netw. 11 (9), 691498.
Ram, M., Kumar, S., Kumar, V., Sikandar, A., Kharel, R., 2019. Enabling green wireless sensor networks: Energy efficient T-MAC using Markov chain based optimization. Electronics 8 (5), 534.
Rani, R., Kumar, S., Dohare, U., 2019. Trust evaluation for light weight security in sensor enabled internet of things: game theory oriented approach. IEEE Internet Things J. 6 (5), 8421–8432.
Sharma, G., Kalra, S., 2017. A secure remote user authentication scheme for smart cities e-governance applications. J. Reliab. Intell. Environ. 3 (3), 177–

188.
Sinde, R., Begum, F., Njau, K., Kaijage, S., 2020. Lifetime improved WSN using enhanced-LEACH and angle sector-based energy-aware TDMA scheduling. Cogent Eng. 7 (1).
Zeinab, K.A.M., Elmustafa, S.A.A., 2017. Internet of things applications, challenges and related future technologies. World Sci. News 2 (67), 126–148.
Zhang, H., Babar, M., Tariq, M.U., Jan, M.A., Menon, V.G., Li, X., 2020. SafeCity: Toward safe and secured data management design for IoT-enabled smart city planning. IEEE Access 8, 145256-145267.