ARTIFICIAL INTELLIGENCE IN IDENTIFYING OR MITIGATING THREATS IN INTERNET OF THINGS NETWORKS

Mais A. Al-Sharqi [1]
[1] Bioinformatics Department
BioMedical Informatics College
University of Information Technology and Communications
Baghdad , Iraq
Thurajk@yahoo.com

Haitham S. Hasan[2]
2 Business Information Technology Department
Business Informatics College
University of Information Technology and Communications
Baghdad, Iraq
haitham@uoitc.edu.iq

Abstract- **The Internet of Things (IoT) is generally acknowledged as a dramatic change spearheaded by scientists and business executives. The IoT has the potential to improve our daily lives by connecting smart devices to the internet. Due to the limited resources and distant deployment of these IoT devices, securing them is a significant challenge today. This paper focuses primarily on mitigating threats and attacks on realistic artificial intelligence, such as network architecture for smart devices. The text on mitigating attacks in networks, especially those involving mobile nodes, is discussed. We develop and test a new countermeasure against all mitigated attack variants. The proposed approach combines node location and trust-based parent selection. The result demonstrates the viability of the suggested countermeasure. In addition, demonstrating the superiority of the suggested countermeasure involves considering the precision of detecting the attack and the delay in isolating the attacker. The proposed system is secure by assuming attackers have different identities in two places to ensure high security and reliability.**

Index Items: IoT, Routing Protocol, machine learning, artificial intelligence

I. INTRODUCTION

The Internet of Things (IoT) evolved from mobile ad hoc networks (MANETs) and wireless sensor networks (WSNs)(1,2). Artificial intelligence (AI) research has generated much interest and many studies (3,4). MANETs are networks of mobile devices that come together ad hoc (5), with no centralized management infrastructure. These networks self-organize and communicate to achieve their deployment goals (6). Because of their capacity to self-organize, these networks are sometimes called "Self-Organizing Networks". (SONs). The communication between nodes located close to one another in a MANET is given higher priority than other types of communication(7). It is usual practice for mobile nodes that make up ad hoc networks to cooperate to exchange data and disseminate information to other nodes in the network(1)(8).

The technology that powers the Internet of Things is astonishingly similar to the technology that powers these other sorts of technology (9). In order to connect a large number of IP-based devices, it makes use of a variety of cutting-edge technologies. It works toward the development of new protocols and guidelines. The growth of technology that allows items to be connected to the internet symbolizes a new wave of innovation that paves the way for a number of applications that may serve a range of purposes. This new generation of innovation opens the door to a whole new world of possibilities. The Internet of Things is expected to connect up to 75 billion devices by 2025, according to forecasts. (10), (11). The bulk of the components that go into making up the Internet of Things are made up of a wide variety of devices that are on the smaller side in terms of size (sensors and actuators). When referring to networks with low power and lossy qualities, the acronym LLNs is commonly used. There is a limit on the amount of memory, computing resources, and power that can be made available by LLN devices. This applies to both the devices and the network. These LLN networks are capable of controlling a wide variety of applications that are connected to the Internet of Things. Some examples of these applications include smart home systems, health care systems, agricultural systems, smart city systems, and industrial smart grid systems. Through the use of routing, it is now feasible to establish a network connection to a diverse selection of applications and to get data from sensor nodes. The retrieval of data from sensor nodes is another benefit

that may be gained via proper routing. As a direct result of this, routing has emerged as one of the most important engines that drives the myriad of applications that constitute the Internet of Things. The sole standard routing protocol that is presently available for usage with the Internet of Things is known as the Routing Protocol for Low-Power and Lossy Networks, or RPL for short (12). RPL cannot ensure safety against a wide range of routing attacks (13), (14), (15), (16) despite the fact that it has a multitude of unique properties (17–20). In spite of the fact that RPL is a routing protocol, this is the result. Additionally, the standard RPL programming language has a number of architectural flaws that make it susceptible to a wide range of different kinds of attacks (21), (22), (23). (21), (22), and (23) Sybil attacks, version number assaults, rank attacks, wormhole attacks, and sinkhole attacks are some of the types of attacks that fall under this category. All of these problems make it more challenging to offer crucial security services such as access control, confidentiality, and data integrity (24).

A. Motivations and Contributions

The reasoning shown previously makes it clearly apparent that the topic of Internet of Things (IoT) security must be investigated in more detail in order to offer unique solutions. Furthermore, the solutions must be resource-efficient and capable of increasing communication dependability while working inside IoT networks with fewer resources available. Aside from that, there has been relatively little study on dealing with all three forms of Sybil attacks (SA), particularly on a realistic and popular routing protocol similar to RPL. There is a significant gap in this area's corpus of knowledge. This is one of the most critical constraints of the current state of the field. These are the types of compelling reasons that have encouraged us to commit our whole attention to achieving this goal.

As a consequence, we would want to suggest a novel decentralized countermeasure that might be utilized to guard against the assault that Sybil is waging. The suggested solution involves using a combination of techniques to effectively and promptly isolate the attacker node. This is achieved by utilizing the surveilling node, the nodes' spatial location, and a parent selection procedure that is based on trust values. This is done via the use of a hybrid technique. These three criteria are used to determine which nodes should be picked to serve as parents (s). In this regard, the following are the most significant contributions produced by our work:

We have developed a revolutionary architecture that is decentralized and resistant to all three forms of sybil assaults. When there is just one attacker node in the network, a Sybil attack known as SA-1 occurs; this sort of attack focuses on a particular section of the network. There are different types of Sybil attacks, including SA-2 and SA-3. SA-2 employs a multitude of mobile and dispersed attacker nodes within the network. RPL's multi-instance capability is now being investigated as part of continuing efforts to include the suggested decentralized countermeasure as an inherent component of the RPL protocol.

The distributed architecture has A basic sample applicable to every node and a monitor node explicitly designed for monitoring nodes. A minimal trust method is utilized in the process of choosing parents based on trust. Trace tables are considered a means of node monitoring, node information maintenance, and attacker node identification. These components are all linked and contribute to the distributed architecture. The utilization of two distinct instances is a crucial component of the proposed distributed architecture.

Moreover, the proposed defense entails the root or sink node in identifying and isolating the malicious attacker node more effectively than existing defenses. This is due to the suggested defense being founded on a different concept. This is because the sink/root node acts as a central destination for information (s). This, in turn, contributes to an increase in the effectiveness and precision of the recommended countermeasure that was offered.

Extensive simulations that take into account the architecture of a genuine, smart home are done to establish whether or not the suggested countermeasure is successful.

The study's findings suggest that the proposed solution outperforms the SecTrust (25) and LiDL (26) approaches presently in use in the firm.

II. RELATED WORK

RPL is a protocol that enables communication between small devices via multiple standardizations. It uses DODAG, a hierarchical virtual topology, and can organize nodes differently to facilitate communication on three levels.There are three communication levels: point-to-point, point-to-multipoint, and multipoint-to-multipoint. To differentiate DODAGs, use one of its three unique IDs found in the header. The DODAG ID, the Instance ID, and the DODAG version are the identifiers in question here. Although a node may serve several RPL instances, it can only actively participate in one of those instances at any one time. A single node might end up serving many RPL instances at the same time. DODAG roots can serve as a

portal or data sink., depending on their function, connecting to the internet for information transfer. Four unique control messages are utilized at various stages during the process of building and maintaining the RPL topology/ DODAG. These messages are used at different times. The DODAG Information Object, which is also referred to as DIO, is an object that is used in the process of communicating essential information about nodes. This information includes the node's rank, details about the DODAG being delivered, and metric values used to choose the best parent. Each node that is interested in taking part in the RPL protocol is required to have a neighbor table. A neighbor table is a database that stores information about the other nodes that are located in close proximity to the individual node. When choosing the ideal parent, the rank value of each item in the neighbor table is taken into consideration. Choose the best parent by assigning a rank value. Trickle algorithm (20) optimizes DIO messages for timely broadcast. Use DODAG Information Solicitation (DIS) to request information.This message is issued whenever a new node expresses an interest in joining an existing DODAG by indicating that it wants to become a member of the DODAG. When it gets a further DIS message, the node that has already been sent the DIS message will respond in the form of a DIO message. Therefore, in order to ensure the success of the process of forming a DODAG, it is necessary to make use of both of these different ways of communication. (iii) Once the DODAG creation process is complete and the best root is selected, the destination advertisement object (DAO) message is transmitted to the source node, which serves as the DAO message's intended recipient. This message contains information about the intended destination. (iv) RPL (Routing Protocol for Low-Power and Lossy Networks) possesses both storing and non-storing routing types. While in the storing mode, individual nodes maintain local copies of the routing table. Conversely, in the non-storing mode, the root/sink node keeps the routing information for the whole network. These modes work independently of each other. Enabling the DODAG Destination Advertisement Object Acknowledgment (DAO-Ack) allows for DAO packet acknowledgment. Users have access to both of these alternatives. Due to the fact that the RPL implementation particulars and its design principles are not within the purview of this particular piece of work, they have been omitted entirely. On the other hand, readers who are interested in getting a comprehensive comprehension of RPL may do so by reading (12) and (27). These two references are the best places to start.

III. PROPOSED COUNTERMEASURE

The proposed countermeasure is a decentralized surveillance infrastructure that is one-of-a-kind. This design examines the parallel operation of many RPL instances. Not only is a decentralized technique for network topology monitoring very effective, but it also reduces the stress placed on the sink/root node. In addition, the hybrid technique underlying the suggested countermeasure combines the monitoring node, the nodes' spatial locations, and a parent selection procedure based on trust values to ensure the attacker node is isolated precisely and in a timely manner. This strategy presupposes that an adversary node with the same ID cannot exist in many geographical locations at once.

A.Architecture and Constituents of Distributed Monitoring

In the next part, we will discuss the many operational ideas and components that constitute the architecture. These will be divided into several categories. The recommended countermeasure, in particular, consists of the components that will be discussed in further detail in the paragraphs that follow. The first thing that we do is investigate whether or not the decentralized architecture that we have presented can be implemented into the RPL protocol that is currently in place. If this is feasible, then we will go on to the next step. Next, we will discuss the novel and lightweight trust computation that has been developed for the trust-based parent selection process that serves as a protective mechanism against attacker nodes. This computation has been designed for the trust-based parent selection process. The trust-based parent selection method has just been updated to include the addition of this computation. The next step is to determine which node in the network was responsible for the attack by examining the "Trace Tables" that monitoring nodes use to store information regarding other network nodes and find out who was behind the assault. Trace Tables are a method of storing information about network nodes that is used by monitoring nodes (s). Figure 1 clearly illustrates the multiple instances necessary to implement the proposed decentralized architecture. We can see the instances of both the monitoring nodes and all nodes in the topology, providing a comprehensive view of the system.

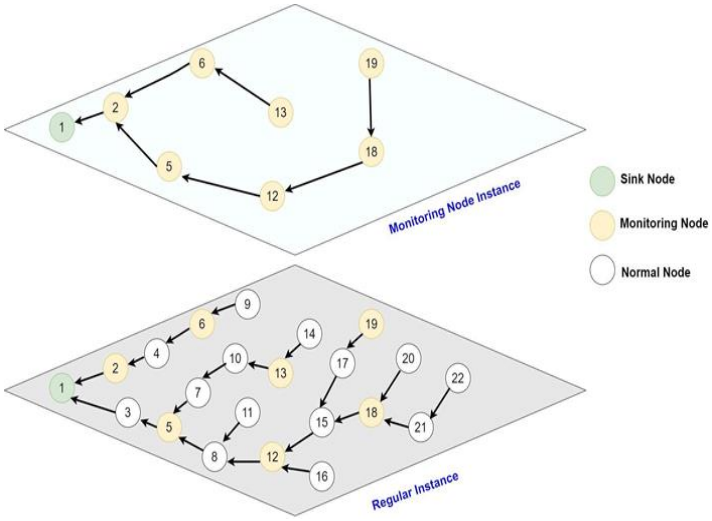

Fig.1. Distributed Monitoring Architecture for RPL.

B. Implanting Distributed Monitoring Architecture in RPL:

The architecture that has been presented has monitoring nodes that have already been established in the network. These monitoring nodes are in charge of lightening the burden that is placed on the sik or root node, as well as simplifying the process of discovering and isolating the attacker node in the smallest amount of time that is practically possible (s). In order for us to be able to do this, we investigate the multi-instance capacity that the RPL protocol has. The RPL requires that the monitoring nodes have a connection to an additional instance of the program. In addition to the regular instance, sometimes frequently referred to as InstanceS, there is another instance known as InstanceQ.

C. Computation of Trust:

One could conceptualize the trust value of a node as a form of "soft security" wherein connections with malicious nodes are fortified based on their interactions with other nodes. This makes it possible to identify potentially dangerous nodes on the network and remove them from the system. We choose a straightforward binary trust model rather than a more complex probabilistic trust model since this allows us to reduce the amount of work that has to be done at the node level and, as a direct result of this, the amount of energy that needs to be spent. The trust rating may be anything from 0 to 1, with 1 denoting a node that is highly trustworthy and 0 denoting a node that is very untrustworthy. The number 1 stands for a trust-weighting factor that may have any value between 0 and 1, and the answer to the equation that determines trustworthiness is 1. In the event that anything positive or trustworthy takes place in the world, the trust-weight component will most likely increase. In the case that a trustworthy occurrence has taken place, the degree of confidence that should be assigned to it may be calculated using the following formula:

$$T\ V\ ID = T\ V\ ID + \omega 1 \quad (1)$$

As an alternative, if there has been anything unfavorable or upsetting that has happened, then the value of the trust will fall in accordance with equation 2. The weight factor 2, which may be anything at all, can have any value between 0 and 1. Any number between 0 and 1 can be set to it. In the case that anything negative does occur, the following equation may be used to assess the level of trust:

$$T\ V\ ID = T\ V\ ID \times \omega 2 \quad (2)$$

Note that the monitoring node is to blame for the occurrence of the malicious event because it used a response packet Rpkt that was precisely crafted and is the response to the inquiry packet Qpkt that was submitted by any ordinary node. This means that the monitoring node is to blame for the fact that the malicious event occurred. It is indispensable to keep this in mind since doing so will make the process of implementation a great deal simpler and more streamlined. As soon as it is determined that a node poses a danger to the network, the trust value that is associated with that node is set to 0. After that, we take advantage of this decreased trust value to isolate the attacker node by choosing trustworthy parents based on the trustworthiness of the nodes they came from. This is done by lowering the trust value of the nodes that they come from.

IV. RESULTS

The findings that we have obtained for each of the parameters that were assessed, as well as an interpretation of those results, are discussed in this section. In addition, we will share some background information about how we arrived at these findings. In order for us to arrive at these conclusions, we used the RPL-UDP gather view program as well as the contiki-os editor. These two projects were of great assistance in many ways. We used Contiki OS, a portable and open-source operating system for IoT devices, and Cooja simulator to simulate hardware implementation. Cooja used MSPSim to emulate the microcontroller architecture and MSP430F1611 microcontroller used in Tmote Sky node. RPL packet modification was done using

protothreads, the default programming language for Contiki OS. The Cooja mobility plugin was used for node mobility. Tmote Sky sensor was used to sense light, temperature, and humidity, and it's standardized with IEEE 802.15.4 - CSMA and Contiki MAC. As shown in Table 1

TABLE 1: SIMULATION PARAMETERS

Parameters	Value
Simulator	Cooja
Operating System	Contiki V 2.7
Node Type	Tmote Sky
Number of Nodes	35 (Including 1 sink / root and Monitoring Nodes)
Radio Medium	Unit Disk Graph Medium (UGDM): Distance Loss
PHY and MAC Layer	IEEE 802.15.4 with CSMA and ContikiMAC
ESMRF	Contiki V 2.7 Default
Transmission Range	50 Meters
Simulation Duration	20 Minutes
Number of Simulations	3

The simulator is put to use in order to generate and evaluate all of the test traffic that is used for the purposes of conducting experiments. The goal of this test traffic is to test various things. Three minutes after the beginning of the simulation, according to the attack model that has been presented, the adversary nodes will be activated. By this time, the topology of the network will have reached a stable state. After the structure of the network has achieved a steady state, this step is carried out. First, the performance of the given approach in relation to the vital parameters is examined. Then, the SecTrust and the LiDL are utilized to figure out whether or not the suggested technique is correct. The amount of accuracy that the SA-1 attack detection system has may be observed, which can be found here. When it comes to defense against assaults of the SA-1 kind, LiDL and the solution that was described work noticeably better than SecTrust does.

The strategy that was proposed maintains an accuracy rate that is really close to that which would be regarded as ideal. Increasing the accuracy of the identification of the node that is being attacked is possible in a number of different ways, one of which is by making use of the geographical position of the node that is being attacked. The ability of the SA-2 assault type to deliver perfect accuracy in battle. An increase in the proportion of Sybil identities results in an approximate 8 percent decrease in the rate of precision of SecTrust. However, as the ratio of Sybil identities increases, the accuracy rate of LiDL decreases by around 4 percent. The strategy that was recommended, on the other hand, maintains an accuracy rate that is really near to one hundred percent. The nodes that are responsible for the attack are identified by using location data in conjunction with parental information from the past. This is done so that the degree of accuracy that was first achieved can continue to be maintained.

While it comes to the amount of precision that can be reached when recognizing SA-2 assaults, both the Local Trace Tables and the Global Trace Tables have a significant impact on the level of accuracy that can be accomplished. The results obtained after examining them with respect to the SA-3 type may be seen here. The approach that was provided yields an accuracy rate of around 93 percent when mobile attacker nodes are taken into consideration. Following the successful completion of this objective, LiDL (89 percent) and SecTrust, in the specified sequence, come in second and third, respectively (79 percent). Trace Tables are updated incorrectly and sluggishly as a result of the nomadic nature of the attacker nodes. This contributes to a reduction in the detection accuracy of the method that was presented. This is due to the transient nature of the nodes that are launching the assault. When considering mobile attacker nodes, the proposed method demonstrates a significantly higher accuracy rate of approximately 93%. This performance is surpassed only by LiDL (82%) and SecTrust (71%). These findings suggest that the proposed method may prove to be a highly effective solution for detecting and mitigating threats posed by mobile attacker

nodes as shown in Figure 2

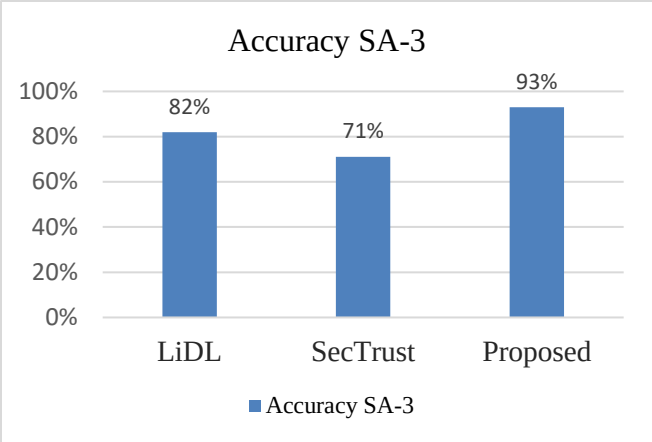

Fig. 2. Accuracy SA-3

V. Conclusion

We have conceived of a one-of-a-kind decentralized countermeasure and conducted research on it in order to lessen the impact of the attack. The proposed methodology has been subjected to rigorous testing employing the Contiki 2.7 operating system and the Cooja simulator.

One of the unique techniques that we have recommended and examined takes use of the multi-instance capabilities that are offered by the RPL protocol. This is one of the novel strategies that we have suggested and evaluated. In addition to this, we make use of monitoring nodes that have been specifically configured to locate the node that is being used dishonestly for its operation. This is made possible by the use of monitoring nodes (s). Because it focuses solely on these monitoring nodes, the recommended mitigation strategy may be able to successfully isolate the attacker node in a significantly shorter amount of time when compared to the other possibilities that have been considered in the past. This is because it is designed to target only these monitoring nodes. In addition to this, we have given some attention to the optimal placement of the monitoring nodes from the perspective of maximizing the advantages obtained. One of the things that we investigated was a simulation study that we carried out on the topology of an application for a smart home. In order to conduct an investigation into and validate the proposed procedure, the operating system Contiki 2.7 was used. We investigate the suggested plan of action by referring to essential aspects of the network, such as the precision of attack detection, the average packet delivery ratio (APDR), the average power consumption (APC), and the control message overhead (CMC). The LiDL and SecTrust tactics that are now being employed are inferior to the countermeasure that has been offered because they better take into account all of the necessary factors. The countermeasure that has been recommended.

REFERENCES

1. Agrawal R, Faujdar N, Romero CAT, Sharma O, Abdulsahib GM, Khalaf OI, et al. Classification and comparison of ad hoc networks: A review. Vol. 24, Egyptian Informatics Journal. Elsevier B.V.; 2023. p. 1–25.
2. T. Watteyne M. G. Richichi and M. Dohler AM. From MANET to IETF roll standardization: A paradigm shift in WSN routing protocols. IEEE Communications Surveys & Tutorials. 2010;13(4):688–707.
3. Hasan H AKS. Fingerprint image enhancement and recognition algorithms: a survey. Neural Comput Appl. 2013;23:606–1608.
4. Al-Sharqi HSHA. Hand vein recognition with rotation feature matching based on fuzzy algorithm. International Journal of Nonlinear Analysis and Applications. 2021;
5. Ramteke AOB and PL. Manet: history, challenges and applications. International Journal of Application or Innovation in Engineering & Management (IJAIEM). 2013;2(9):249–251–249–251.
6. Tabatabaei S. Introducing a new routing method in the MANET using the symbionts search algorithm. PLoS One. 2023 Aug 1;18(8 August).
7. Jansi KR, Arulprakash M. Decentralized and collaborative approach to mobile crowdsensing by implementing continuous feedback between the nodes. Egyptian Informatics Journal. 2023 Mar 1;24(1):95–105.
8. Sengan S, Khalaf OI, Koteswara Rao GR, Sharma DK, Amarendra K, Hamad AA. Security-aware routing on wireless communication for e-health records monitoring using machine learning. International Journal of Reliable and Quality E-Healthcare. 2022 Jul 1;11(3).
9. D. Airehrour, J. Gutierrez and SKR. Secure routing for internet of things: A survey. Journal of Network and Computer Applications. 2016;66:198–213.
10. Internet of things (iot) - the future of iot miniguide:

The burgeoning iot market continues. 2019; Available from: https://www.cisco.com/c/en/us/solutions/internet-of-things/future-of-iot.html

11. MacGillivray MS and C. The growth in connected iot devices is expected to generate 79.4 zb of data in 2025, according to a new idc forecast. 2019;
12. T. Winter Ed (Cisco S, P. Thubert Ed (Cisco S, Designs) AB (Sigma, Corporation) JH (Arch R, Corporation) RK (Ember, University) PL (Stanford, et al. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks Abstract Low-Power. Internet Engineering Task Force (IETF). 2010;6550:1689–99.
13. A. Raoof, A. Matrawy and CHL. Routing attacks and mitigation methods for rpl-based internet of things. IEEE Communications Surveys & Tutorials. 2018;21(2):1582–606.
14. Hwang YH. Iot security & privacy: threats and challenges. In: Proceedings of the 1stACM workshop on IoT privacy, trust, and security. 2015. p. 1–1.
15. Rao LP and UP. Internet of things—architecture, applications, security and other major challenges. In: 3rd International Conference on Computing for Sustainable Global Development (INDIACom). INDIA: IEEE; 2016. p. 1201–6.
16. H. Kharrufa, H. A. Al-Kashoash and AHK. Rpl-based routing protocols in iot applications: A review. IEEE Sens J. 2019;19(15):5952–67.
17. MacGillivray MS and C. The growth in connected iot devices is expected to generate 79.4 zb of data in 2025, according to a new idc forecast. 2019;
18. T. Winter Ed (Cisco S, P. Thubert Ed (Cisco S, Designs) AB (Sigma, Corporation) JH (Arch R, Corporation) RK (Ember, University) PL (Stanford, et al. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks Abstract Low-Power. Internet Engineering Task Force (IETF). 2010;6550:1689–99.
19. A. Raoof and C.-H. Lung AM. Routing attacks and mitigation methods for rpl-based internet of things. IEEE Communications Surveys & Tutorials. 2018;21(2):1582–606.
20. Hwang YH. Iot security & privacy: threats and challenges. In: Proceedings of the 1stACM workshop on IoT privacy, trust, and security. 2015. p. 1.
21. B. Ghaleb, A. Al-Dubai, E. Ekonomou, M. Qasem, I. Romdhani and LM. Addressing the dao insider attack in rpl's internet of things networks. IEEE Communications Letters. 2018;23(1):68–71.
22. Y. Tahir, S. Yang and JM. Brpl: Backpressure rpl for high-throughput and mobile iots. IEEE Trans Mob Comput. 2017;17(1):29–43.
23. Chavan PP and G. A survey: Attacks on rpl and 6lowpan in iot. In: International conference on pervasive computing (ICPC). IEEE; 2015. p. 1–6.
24. A. Le, J. Loo, Y. Luo and AL. The impacts of internal threats towards routing protocol for low power and lossy network performance. In: Symposium on Computers and Communications (ISCC). IEEE; 2013. p. 000789–94.
25. D. Airehrour, J. A. Gutierrez and SKR. Sectrust-rpl: A secure trust-aware rpl routing protocol for internet of things. Future Generation Computer Systems. 2019;93:860–76.
26. P. Kaliyar, W. B. Jaballah, M. Conti and CL. Lidl: Localization with early detection of sybil and wormhole attacks in iot networks. Comput Secur. 2020;101849.
27. H.-S. Kim, J. Ko, D. E. Culler and JP. Challenging the ipv6 routing protocol for low-power and lossy networks (rpl): A survey. IEEE Communications Surveys & Tutorials. 2017;19(4):2502–25.