Journal of Engineering Science and Technology
Special Issue on IAC2021, October (2021), 13 - 23

A TRUST-BASED APPROACH FOR DEFENCE AGAINST RPL RANK ATTACK FOR INTERNET OF THINGS

SYEDA M. MUZAMMAL, RAJA K. MURUGESAN*, N.Z. JHANJHI

School of Computer Science & Engineering, Taylor's University, Taylor's Lakeside Campus, No. 1 Jalan Taylor's, 47500, Subang Jaya, Selangor DE, Malaysia
*Corresponding Author: rajakumar.murugesan@taylors.edu.my

Abstract

The proliferation of Internet of Things (IoT) is inhabiting an important place in our daily lives. With the immense growth in the number of smart devices and applications, the increase in security risks and threats is inevitable. Among IoT layers, the network layer is critical from the security perspective. In addition, routing in IoT networks plays a vital part to establish the routes for data communication. IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) is the de facto routing protocol for most of the IoT applications. RPL is susceptible to a number of attacks based on its features and operations. Among these attacks, some are specific to RPL, and some are inherited from Wireless Sensor Networks (WSNs). RPL provides limited protection against routing attacks. Rank is an important property of RPL and an attack on it is severely disruptive to the network topology. For defence against RPL attacks, specifically the Rank attack, a trust-based security is a viable option as it incurs less overall cost. In this research, a trust-based solution, termed as SMTrust, is proposed for security against Rank attack in RPL by choosing the critical trust metrics. The mobility-based metrics are also included in trust evaluation for effective performance and operation of RPL in a mobile IoT environment. The weighted aggregation of the trust metrics for trust index evaluation establishes the trust relationship among network nodes. The proposed trust-based solution is embedded in the Objective Function (OF) of RPL. Simulation experiments indicate that the proposed SMTrustOF performs better than the standard RPL objective function, which is the Minimum Rank with Hysteresis Objective Function (MRHOF). The results analysis demonstrates the proposed security solution's efficacy in both static and mobile nodes in IoT.

Keywords: IoT, Routing, RPL, Security, Trust.

1. Introduction

Internet of Things (IoT) is referred to as a network of things. These things can be any physical objects that are connected to other devices and systems for data exchange over the Internet. IoT is taking place in daily chores of human lives via smart applications, for example, homes, cities, hospitals, retails, factories, transportation, and many more [1]. There have been predictions by researchers for the number of smart devices to reach up to billions. Li et al. [2], Cisco [3], and Statista Research Department [4] have predicted the exponential growth of IoT-connected devices in coming years. With the boost in smart and IoT-connected devices, the security concerns are escalating with the same pace. Recently, there have been reported several attacks which caused disruptions to the IoT-based networks and applications [5].

Security is an essential aspect which needs to be embedded in each layer of IoT architecture. Different researchers have categorized IoT architecture into three, four or five layers. A typical IoT architecture is composed of three layers [6]. These can be categorized as perception, network and application layers, as illustrated in Fig. 1. It also demonstrates the description of each layer from the security perspective. The application layer provides interface between user and IoT and employs several computing and data processing techniques to extract valuable information from data received from IoT devices. The transport or networking layer deals with the networking and routing operations for data communication among IoT devices. Whereas the sensing or perception layer consists of IoT devices and gateways for collecting the data or information. Other than these, there are cloud servers and storage devices that support IoT functionalities, which have their own security needs. The security of IoT system, mainly the protection of resource constrained IoT devices, network and routing operations, is very critical.

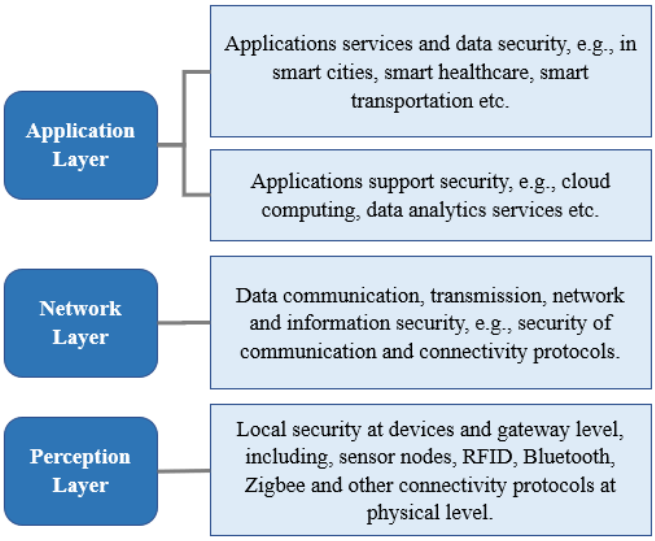

Fig. 1. Security perspective of IoT layers.

IoT layers are prone to several security attacks including attacks in data forwarding process, side-channel attack, replay attack, fake node or sybil attack,

denial of service, node capturing, and many more [7-12]. All layers in IoT architecture suffer from several attacks. Particularly network layer is exposed to several types of attacks including the routing attacks that are more disruptive to the IoT networks and applications. IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) is used for routing in majority of the IoT applications. RPL is prone to both RPL-specific attacks and the attacks inherited from Wireless Sensor Networks (WSNs) termed as WSN-inherited attacks.

Among other solutions for secure IoT networks, routing, and applications, a trust-based approach is feasible because it incurs less overall cost and is easily adaptable to IoT systems [13-17]. In this paper, we propose a trust-based routing security solution to defend Rank attack in RPL. The dynamicity of IoT network allows both mobile and static nodes. So, the trust-based and mobility-based metrics are chosen for trust evaluation via critical analysis of trust metrics in IoT [18]. The proposed solution is evaluated in comparison with the standard RPL objective function which is the Minimum Rank with Hysteresis Objective Function (MRHOF), for static as well as mobile scenarios via simulation experiments.

The main contributions of this research paper include firstly the analysis of trust-based approach to provide security for routing in IoT, particularly against Rank attack in RPL. Secondly, preliminary results are presented by evaluation the proposed approach via simulation experiments and compared with standard RPL objective function which is MRHOF. The paper is structured as follows: Section 2 explains the key related works of the problem area under consideration. Section 3 describes the methods and experimental setup. Section 4 presents the results, and Section 5 concludes the paper and presents future directions.

2. Related Work

Trust-based approach and trust modelling is a feasible method to countermeasure the security attacks in IoT networks. To make the system more reliable and trustworthy for users, trust modelling can be applied to the development of functional measures. Trust embedded in IoT networks and routing is significant for stability and security. This will enable the network maintenance, particularly with a rise and expansion of connected devices. In IoT networks and routing, trust-based approaches have not been thoroughly explored and pose a vital field of research, especially from the perspective of security. Additionally, the importance of trust models for IoT network and routing security, as explained by Muzammal et al. [18], indicates its implications.

2.1. Trust-based security solutions for RPL

Several trust-based security solutions for RPL have been proposed in existing literature. A trust-based mechanism for RPL security, SecTrust, is proposed [19]. It specifies its own OF to establish trust in RPL. The network efficiency and packet loss rate are evaluated considering the Sybil and Rank attacks. Similarly, a SecTrust revision is proposed to evaluate Blackhole attacks [20]. In addition, Airehrour et al. [21] and Hashemi et al. [22] proposed a trust model for IoT, using contextual knowledge, Quality of Service (QoS), and Quality of P2P Communication (QPC), for trust evaluation. The model is assessed for Sybil, Rank, and Blackhole attacks in RPL.

A cooperative and trust-aware routing protocol, MRTS, is proposed by Djedjig et al. [23]. Trust calculation in MRTS is done by adding ETX metric. Their

proposed approach is effective for packet delivery ratio (PDR), energy consumption, throughput, and node rank change. However, MRTS uses an IDS approach for attack detection and isolation, which is computationally expensive and requires a hardware security chip embedded in each node [24]. The existing approaches have a common research gap regarding the lack of consideration for mobility of nodes. Only Hashemi et al. [21] considered the mobility of nodes, but their evaluation is limited to sender nodes' mobility. Alsheshri and Hussain [25] presented a security protocol for trust management in IoT networks, but its focus is not on the routing attacks and nodes' mobility.

In Sakthivel and Chandrasekaran [26], a dummy packet is inserted in the network to mitigate the packet dropping attacks. The insertion of dummy packets creates high overhead, and this approach does not consider RPL-specific attacks. For attack detection and defence against malicious nodes, the trust-based approach is easily adaptable to IoT scenarios. It is also scalable at any node density level and can cope well with network size growth or shrinkage [27].

The trust models proposed for routing security in IoT, in the current literature, require further work on some features, such as consideration of IoT nodes mobility, heterogeneity in IoT environments, adaptability to IoT networks and routing, and consideration of RPL-specific attacks. Hence, it can be figured out that the existing trust-based approaches for RPL security are not adequate from the perspective of the mobile nodes in IoT. In proposed SMTrust, which is a trust-based security solution, the trust is computed considering the appropriate trust metrics including the mobility-based metrics for trustee nodes. This will facilitate the trust relationship between the nodes based on their mobility scenarios as well. Moreover, our proposed solution is evaluated in static as well mobile nodes scenarios for performance. It is different from the related methods basically for considering mobility-based metrics for trust computation, evaluation in dynamic scenarios, and enhanced performance for static and mobile IoT environments.

3. Methods and Experimental Setup

In SMTrust-based secure routing protocol, a node's reliability is determined by direct and indirect trust recommendation. The proposed solution's distinctiveness is that suitable metrics regarding mobility of nodes are considered for trust evaluation to adapt to a mobile IoT environment. The diagrammatic model and workflow of SMTrust is based on the concepts detailed in [28, 29]. The main components include trust metrics computation, trust index calculation, trust rating, trust value update, attacks detection, malicious nodes isolation, trust decay and maintenance. Figure 2 depicts the flowchart of SMTrust.

The process flow of SMTrust starts with the initialization of RPL routing operation, and goes on for trust computation, trust value update, attacks detection, and finally the processing of trusted nodes for routing. The process further goes on to update the trust value based on certain criteria. A trust-based security solution is adaptable for detecting and preventing malicious nodes in a variety of attacks. Furthermore, it is scalable at any node density and can handle network size expansion and contraction well [27]. Additionally, the appropriate trust metrics and mobility-based trust metrics in a trust-based security solution are effective and adaptable to dynamic and mobile IoT environments.

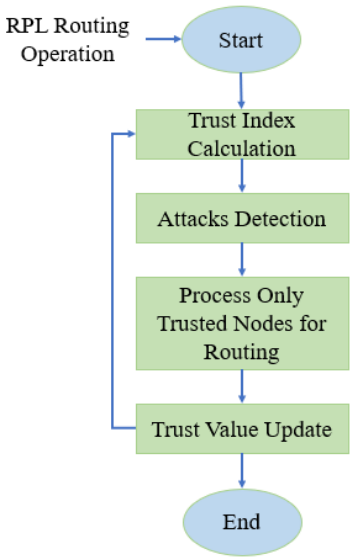

Fig. 2. Flowchart of SMTrust process.

3.1. Trust metrics and trust index calculation

For the proposed SMTrust-based security solution, six trust metrics are selected, which include the historical observations, energy level, success rate, link stability, mobility, and trust recommendation. Success rate is determined by the ratio of the number of packets forwarded to the packets received by the node. Energy level is the remaining energy of the node. Historical observation is quantified by the recent trust value calculated for the node.

Link stability is determined by the Received Signal Strength Indicator (RSSI) value. Mobility is the distance which the node has moved from its previously noted position. Recommended trust is the feedback from the one-hop neighbours. The above trust metrics are aggregated to calculate the trust index of the trustee node. The computed trust index is then ranked using the fuzzy-based assessment to determine the trustworthiness of the node based on a threshold value.

3.2. Rank attack detection

The actual rank of an attacker node is changed in a Rank attack. This is to advertise better rank in the network to attract the traffic. The overhearing and monitoring of neighbouring nodes is employed in SMTrust for the Rank attack detection. When a DIO message is received by a node from a neighbouring node, it checks for its rank and DIO_seq. A fake DIO is detected if the new DIO_seq is less than or equal to the current DIO_seq. Therefore, a Rank attacker node is identified.

The concept of Rank attack detection is adopted from [19, 30], according to the definition and working of the Rank attack. The attack detection mechanism in SMTrustOF will check the validity of the potential parents unless it finds a trustworthy preferred parent. Hence, only the trustworthy nodes will be forwarded for routing decisions in the network.

3.3. Trust value update

Once the trust index is calculated, it is not static and rather keeps on updating considering two conditions, periodic and reactive monitoring. In SMTrust, a trickle timer algorithm for sending DIO messages in RPL is adopted for periodic update of the trust value. Whereas for reactive trust update, the monitoring process is initiated considering the changes in the behaviour of the node, for example, change of rank without changing the DIO-seq, thus causing a Rank attack.

3.4. Experimental setup

For experiments and evaluation, we used ContikiOS/Cooja simulator. Contiki is an open-source, wireless sensor network operating system. ContikiRPL implementation is according to the specification of RPL in RFC 6550 [31]. SMTrust-based security solution is embedded in the objective function of RPL, as part of the routing operation. The experiments are carried out with thirty nodes in the RPL network, including three attacker nodes and one sink node. The performance of SMTrustOF is analysed in three different scenarios, including Scenario I with static nodes, Scenario II with mobile sender nodes, and Scenario III with mobile senders and sink node. The performance parameters and comparison of results and analysis is described in next section.

4. Results Analysis

The proposed SMTrust-based secure routing protocol is evaluated by replicating static as well as mobile IoT environments. The performance parameters include the topology stability, packet loss rate, and throughput. A comparison of results is done with standard RPL objective function, which is MRHOF.

4.1. Topology stability

In RPL routing, a change in the node rank typically indicate the re-alignment of a child node to another preferred parent node. According to the rank computation in RPL, a child node's rank is always greater than the parent node rank to maintain a loop-free topology. When the rank of the parent node or the child node changes, it ensures that the rules of RPL routing are followed, hence the child node tends to select a new parent.

The network topology in RPL is said to be stable if there is minimal frequency of nodes rank changes. Figure 3 demonstrates the comparison of average results for the topology stability under Rank attacks for SMTrustOF and MRHOF. The results indicate that the frequency of nodes rank changes for SMTrustOF are 54, 56.7, and 71.3 in Scenario I, II, and III, respectively, which is much less as compared to MRHOF which are 287, 352, and 576.

Under Rank attack, the frequency of nodes rank changes is high due to the activities of malicious nodes. For example, in a Rank attack when a malicious nodes keep advertising a lower Rank to its neighbours, the neighbours will tend to select a better parent, and hence keep on re-aligning themselves according to the fake rank information in topology. Due to frequent changing of nodes rank, the topology is considered to be unstable and more vulnerable to attacks.

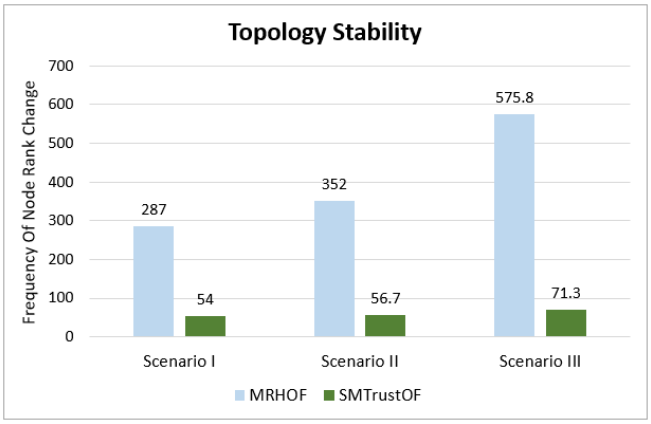

Fig. 3. Results comparison of topology stability.

4.2. Packet loss rate

With regards to the network performance measurement, the packet loss is determined by the number of packets which failed to transmit from one destination to another. The packet loss rate is the percentage of lost packets in the routing operation. For evaluation of SMTrust, the packet loss rate is determined which ultimately indicates the loss of data and the effect on packet delivery in the network. For this research, the overall packet loss rate in the network is examined.

Figure 4 illustrates the comparison of average packet loss rate under three scenarios. As compared to MRHOF, SMTrust has much reduced packet loss rate of 15.5%, 10.7%, and 22.9%, in Scenario I, II, and III, respectively, under Rank attack. Whereas MRHOF shows a packet loss rate of 67.2%, 72.7%, and 76.2%, in Scenario I, II, and III, respectively. The difference of packet loss rate of MRHOF and SMTrustOF is because in standard RPL implementation, there is no mechanism to analyse the integrity of Rank advertisement in the network. The successful packet delivery will be affected under the Rank attack in network with fake rank and articulated route information advertised in the network. The high the packet loss rate, the higher will be the impact of attacks in the network.

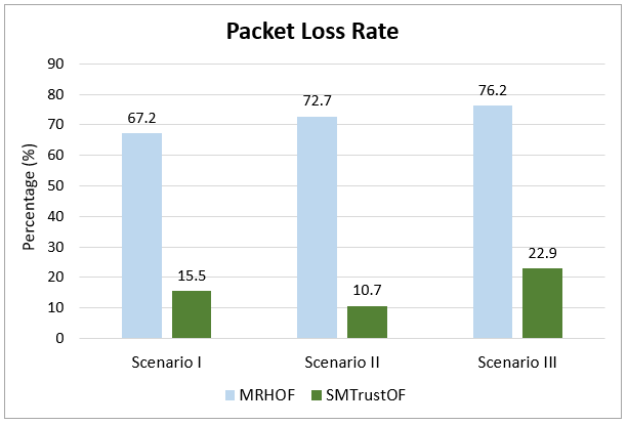

Fig. 4. Results comparison of average packet loss rate.

4.3. Throughput

Throughput is an essential parameter to examine the performance of a network or routing protocol. The throughput measurement is a well-known parameter for network performance analysis and is based on the amount of data successfully transferred from the source to the destination in a network within a given timeframe. In order to determine the performance of RPL, measuring throughput is an important parameter. It basically indicates amount of data successfully reach the destination. For this thesis, throughput is measured in kilo-bits-per-second (kbps).

Figure 5 shows the comparison of SMTrustOF and MRHOF for average throughput values in kbps, under Rank attack, in static and mobile scenarios. The throughput of MRHOF stays much lower, such as, 1.53, 1.48, and 1.29 kbps as compared to SMTrustOF, such as, 5.13, 5.37, and 4.40 kbps, for static scenario, sender nodes mobility scenario, and sink node mobility scenario, respectively. Under the Rank attack, the throughput significantly decreases due to the data loss and malicious activities of attacking nodes in the network.

The results comparison and graphical illustrations indicate that overall SMTrust-based objective function performs better than MRHOF. The difference in performance is due to the fact that in MHROF, there is no security mechanism for communication among nodes. Whereas, in SMTrustOF, a trust relationship is established between nodes for constructing a trustworthy network topology. In addition, the choice of trust-based metrics plays a critical role in a trust-based solution, especially for IoT routing and networks security. Moreover, though the network performance is decreased to some extent with mobility of nodes in the network, especially with the mobility of sink node, still SMTrustOF is minimally affected. Because SMTrustOF attempts to consider the trust-based parent selection for route selection, and the trust-based metrics also include the mobility-based metrics for trust formation in the network.

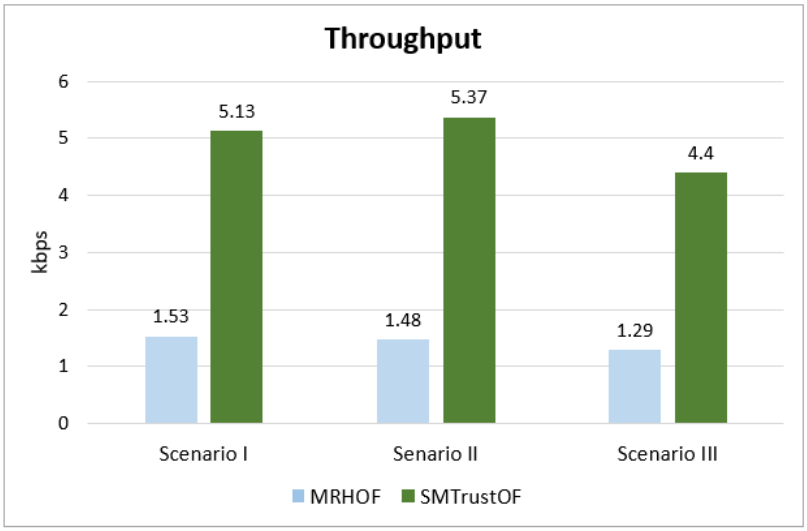

Fig. 5. Results comparison of average throughput.

5. Conclusion and Future Work

IoT is flourishing in our daily lives to facilitate the execution of daily tasks from routine chores to large-scale sectors. The wide-scale adoption of IoT paradigm relies on its privacy and security aspects. Routing and networks are among the key components of IoT ecosystem. Routing in majority of the IoT applications is performed using RPL, and RPL is susceptible to several disrupting attacks, specifically the high-impact attacks based on its features, functionalities or properties. Rank attack is among such attacks which severely disrupt the network topology. In this research study, a trust-based solution is proposed for defence against RPL Rank attack. The trust-metrics are critically chosen for trust index evaluation, including the mobility-based metrics, that helps in adapting the proposed solution to mobile IoT environments. The simulation experiments and analysis indicate that the proposed solution, SMTrust, provides enhanced network performance under Rank attacks as compared to MRHOF, in static as well as mobile scenarios.

In the future work of this research, the proposed secure routing solution will be evaluated for increased number of nodes and improved for additional parameters, such as, power consumption, delay, etc. SMTrust will be enhanced for defence against other attacks, to provide a holistic security approach.

References

1. Muzammal, S.M.; Shah, M.A.; Khattak, H.A.; Jabbar, S.; Ahmed, G.; Khalid, S.; Hussain, S.; and Han, K. (2018). Counter measuring conceivable security threats on smart healthcare devices. *IEEE Access*, 6, 20722-20733.
2. Li, A.; Liu, W.; Zhang, S.; and Xie, M. (2020). Fast multicast with adjusting transmission power and active slots in software define IoT. *IEEE Access*, 8, 226352-226369.
3. Cisco. (2020). Internet of things – CISCO. Retrieved June 27, 2021, from https://www.cisco.com/c/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.html.
4. Statista Research Department. (2020). Number of connected devices worldwide 2030 – Statista. Retrieved May 26, 2020, from https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/.
5. Ferrante, A.J. (2017). Battening down for the rising tide of IoT risks. *ISSA Journal*, 15(8), 20-24.
6. Ray, P.P. (2018). A survey on internet of things architectures. *Journal of King Saud University - Computer and Information Sciences*, 30(3), 291-319.
7. El-hajj, M.; Fadlallah, A.; Chamoun, M.; and Serhrouchni, A. (2019). A survey of internet of things (IoT) authentication schemes. *Sensors*, 19(5), , 1141.
8. Airehrour, D.; Gutierrez, J.; and Ray, S.K. (2016). A lightweight trust design for IoT routing. *Proceedings of the IEEE 14th International Conference on Dependable, Autonomic and Secure Computing, 14th International Conference on Pervasive Intelligence and Computing, 2nd International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)*. Auckland, New Zealand, 552-557.

9. Tawalbeh, L.A.; and Somani, T.F. (2016). More secure internet of things using robust encryption algorithms against side channel attacks. *Proceedings of the IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*. Agadir, Morocco, 1-6.
10. Na, S.J.; Hwang, D.Y.; Shin, W.S.; and Kim, K.-H. (2017). Scenario and countermeasure for replay attack using join request messages in LoRaWAN. *Proceedings of the International Conference on Information Networking (ICOIN)*. Da Nang, Vietnam, 718-720.
11. Evangelista, D.; Mezghani, F.; Nogueira, M.; and Santos, A. (2016). Evaluation of sybil attack detection approaches in the internet of things content dissemination. *2016 Wireless Days (WD)*, 1-6.
12. Anirudh, M.; Thileeban, S.A.; and Nallathambi, D.J. (2017). Use of honeypots for mitigating DoS attacks targeted on IoT networks. *Proceedings of the International Conference on Computer, Communication and Signal Processing (ICCCSP)*. Chennai, India, 1-4.
13. Muzammal, S.M.; Shah, M.A.; Zhang, S.-J.; and Yang, H.-J. (2016). Conceivable security risks and authentication techniques for smart devices: A comparative evaluation of security practices. *International Journal of Automation and Comput*ing, 13(4), 350-363.
14. Zahra, F.-T.; Jhanjhi, N.Z.; Brohi, S.N.; and Malik, N.A. (2019). Proposing a rank and wormhole attack detection framework using machine learning. *Proceedings of the 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics*. Karachi, Pakistan, 1-9.
15. Almusaylim, Z.A.; Alhumam, A.; and Jhanjhi, N.Z. (2020). Proposing a secure RPL based internet of things routing protocol: A review. *Ad Hoc Networks*, 101.
16. Muzammal, S.M.; and Murugesan, R.K. (2018). A study on leveraging blockchain technology for IoT security enhancement. *Proceedings of the 2018 4th International Conference on Advances in Computing, Communication and Automation*. Subang Jaya, Malaysia, 1-6.
17. Hassan, T.; Asim, M.; Baker, T.; Hassan, J.; and Tariq, N. (2021). CTrust-RPL: A control layer-based trust mechanism for supporting secure routing in routing protocol for low power and lossy network-based internet of things applications. *Transactions on Emerging Telecommunications Technol*ogies, 32(3).
18. Muzammal, S.M.; Murugesan, R.K.; and Jhanjhi, N.Z. (2020). A comprehensive review on secure routing in internet of things: Mitigation methods and trust-based approaches. *IEEE Internet Things Journal*, 8(6), 4186-4210.
19. Airehrour, D.; Gutierrez, J.A.; and Ray, S.K. (2018). SecTrust-RPL: A secure trust-aware RPL routing protocol for internet of things. *Future Generation Computer Systems*, 93, 860-876.
20. Airehrour, D.; Gutierrez, J.; and Ray, S.K. (2018). A trust-based defence scheme for mitigating blackhole and selective forwarding attacks in the RPL routing protocol. *Journal of Telecommunications and the Digital Econ*omy, 6(1), 41-59.
21. Hashemi, S.Y.; and Aliee, F.S. (2019). Dynamic and comprehensive trust model for IoT and its integration into RPL. *The Journal of Supercomputing*, 75(7), 3555-3584.

22. Hashemi, S.Y.; and Aliee, F.S. (2020). Fuzzy, dynamic and trust-based routing protocol for IoT. *Journal of Network and Systems Management*, 28(4), 1248-1278.
23. Djedjig, N.; Tandjaoui, D.; Medjek, F.; and Romdhani, I. (2020). Trust-aware and cooperative routing protocol for IoT security. *Journal of Information Security and Applications*, 52.
24. Djedjig, N.; Tandjaoui, D.; Medjek, F.; and Romdhani, I. (2017). New trust metric for the RPL routing protocol. *Proceedings of the 8th International Conference on Information and Communication Systems*. Irbid, Jordan, 328-335.
25. Alshehri, M.D.; and Hussain, F.K. (2018). A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT). *Computing*, 101(7), 791-818.
26. Sakthivel, T.; and Chandrasekaran, R.M. (2018). A dummy packet-based hybrid security framework for mitigating routing misbehavior in multi-hop wireless networks. *Wireless Personal Communications*, 101(3), 1581-1618.
27. Khanna, N.; and Sachdeva, M. (2019). Study of trust-based mechanism and its component model in MANET: current research state, issues, and future recommendation. *International Journal of Communication Systems*, 32(12).
28. Muzammal, S.M., Murugesan, R.K., Jhanjhi, N.Z.; and Jung, L.T. (2020). SMTrust: Proposing trust-based secure routing protocol for RPL attacks for IoT applications. *Proceedings of the 2020 International Conference on Computational Intelligence (ICCI)*. Bandar Seri Iskandar, Malaysia, 305-310.
29. Muzammal, S.M.; Murugesan, R.K.; and Jhanjhi, N.Z. (2021). Introducing mobility metrics in trust-based security of routing protocol for internet of things. *Proceedings of the 2021 National Computing Colleges Conference*. Taif, Saudi Arabia, 1-5.
30. Le, A.; Loo, J.; Chai, K.K.; and Aiash, M. (2016). A specification-based IDS for detecting attacks on RPL-based network topology. *Information*, 7(2).
31. Winter, T.; Thubert, P.; Brandt, A.; Hui, J.; Kelsey, R.; Levis, P.; Pister, K.; Struik, R.; Vasseur, J.P.; and Alexander, R. (2012). RFC 6550 - RPL: IPv6 routing protocol for low-power and lossy networks. Retrieved October 30, 2020, from https://tools.ietf.org/html/rfc6550.