

Review of routing protocol for low power and lossy network in the internet of things

Murtaja Ali Saare¹, Saima Anwar Lashari², Ayman Khalil³, Mahmood A. Al-Shareeda⁴, Selvakumar Manickam⁴

¹Department of Computer Technology Engineering, Shatt Al-Arab University College, Basrah, Iraq

²College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia

³School of business, Department of Information Technology Management, Lebanese American University (LAU), Beirut, Lebanon

⁴National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Penang, Malaysia

Article Info

Article history:

Received Apr 2, 2023

Revised Jul 7, 2023

Accepted Jul 20, 2023

Keywords:

Internet of things

Review of 6LoWPAN-RPL

RPL

RPL-IoT

RPL-IoT review

ABSTRACT

The growth of internet of things (IoT) devices and apps has caused disruptions in key sectors such as smart environment, healthcare, and mission-critical tool. Security of IoT devices, networks, and infrastructure is the biggest challenge. RPL, a routing protocol optimised for low-power and lossy networks, is applied by the IoT to offer seamless information transfer among the myriad of interconnected entities. So, the paper delves into the nuts and bolts of RPL, covering its protocol settings, trickle timer, and objective function, as well as the IoT's architecture and applications. This article also provides a framework for categorising past research on the effects of RPL-IoT on energy consumption, transportation, service quality, traffic congestion, and safety. The future of energy efficiency, congestion, objective function, mobility, stability, security, collaborative intrusion detection systems, active learning, and key management are all considered in this analysis.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Selvakumar Manickam

National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia

11800 USM, Penang, Malaysia

Email: selva@usm.my

1. INTRODUCTION

As its use in more and more fields rapidly grows, the internet of things (IoT) is now widely regarded as the most significant technological breakthrough of our time. The IoT is supposedly paving the way toward approving modernity by increasing the effectiveness and efficiency of the network through the reduction of wasted periods and operation automation and the introduction of smartness in things. As a result of advancements in technology, we now have the concept of “intelligent homes” [1], “intelligent cities” [2], “intelligent healthcare” [3], and even “wearable devices” [4]. In addition, it has had a major effect on resource conservation in the industrial and urban spheres [5], [6].

The IoT is often recognised as the most significant technological achievement of our time, and its use is fast expanding across a wide range of industries. According to proponents of IoT, it is this technology's ability to streamline processes, eliminate unnecessary steps, and infuse intelligence into everyday objects that will pave the road for widespread acceptance of modernity. There are now “intelligent homes” [1], “intelligent cities” [2], “intelligent healthcare” [3], and even “wearable devices” [4]. In addition, it has had a major effect on resource conservation in the industrial and urban spheres [5], [6].

IPv6 over low-power wireless personal area networks (6LoWPAN) [7] is a groundbreaking protocol that bridged the gap between internet protocol (IP) and low-power devices. It's an IP-based technology that may be used in low-power wireless personal area networks (LoWPANs) such wireless sensor networks (WSN) and incorporates both the IEEE 802.15.4 [8] and IPv6 [9] protocols. This extension allows for complete internet interaction within LoWPANs, allowing for new configuration options.

Routing protocol for low-power and lossy networks (RPL) is widely used in IoT networks. The internet engineering task force (IETF) [10] developed this protocol to address the dearth of a suitable alternative for use in low-power, resource-constrained, and lossy IoT devices. To perform routing functions, it employs the distance vector routing principle by forming a directed acyclic graph (DAG) or destination-oriented DAG (DODAG) [11]. Five primary control messages are recommended for use in establishing a communication network. DODAG information solicitation (DIS) are data inquiry, DODAG information objects (DIO) are data object, destination advertisement object (DAO) are acknowledgement, and consistency check (CC) are all part of the DODAG messages. Fixes for inconsistencies, broken links, and other problems are built into the protocol at both the local and global levels [12].

The rest of this paper is organized as follows. Section 2 describes the IoT in terms of architecture and application. Section 3 shows an overview of RPL with regards to protocol configuration, trickle timer, and objective function. Section 4 proposes a taxonomy of literature reviews for RPL-IoT. Section 5 discusses challenges and future directions. Lastly, section 6 concludes this review.

2. OVERVIEW OF INTERNET OF THINGS

2.1. Architectures of IoT

Several potential architectures that are conducive to the IoT have been proposed in the literature. Common architectures include middleware, service orientation, three-layer, and five-layer designs [13]. So far, no agreed-upon framework for the IoT exists in writing. Figure 1 shows that a three-layer design is the most frequently quoted IoT architecture [14]. Its increased popularity can be attributed to the fact that it is easy to use and represents IoT in an abstract way, both of which speed up the process of creating and releasing new applications. It consists of three distinct layers: the perceptual layer, the network layer, and the application layer. These tiers are underlined in the following steps.

- Perception layer: the perception layer helps keep the IoT three-tier architecture stable. The perception layer of an IoT system collects information about the surrounding environment. WSN technology allows us to expand our horizons. At this stage, the analogue input is converted to digital and the detected data is put to good use.
- Network layer: the network layer transfers sensory data to the perception and application layers safely. Wireless local-area network (WLAN), wireless personal area network (WPAN), LoWPAN, and global system for mobile communication (GSM) networking are used. It uses Bluetooth, long-term evolution (LTE), and near-field communication (NFC) transmission. It directs the IoT various sensors' data. IPv6 makes 6LoWPAN addresses unique.
- Application layer: the application layer offers IoT application consumers customizable services or a front end. It instantly sends network-processed data to users. Connects users to IoT services. Developers use IoT insights with the application layer. Uses include intelligent homes, electrical grids, industrial controls, surveillance systems, health-care controls, and logistics management [15]-[18].

2.2. Application of IoT

Although it would be impossible to provide a comprehensive list of all possible IoT applications, we can discuss some of the most popular ones to gain an understanding of the varying needs and design implications of this new field and the challenges that lie in its path to maturity. Some of the most common uses of IoT are depicted in Figure 2.

- Healthcare: the potential of the IoT and WSNs in health-care is limitless, and the projected benefits are countless, thus the idea has piqued the curiosity of many researchers. Care for the elderly, testing of vital signs, observation of the hospital environment, and detection of emergencies are all examples of healthcare applications [19]-[22].
- Smart environments: incorporating smart city, building, agricultural, and other applications. Because of the expansive nature of these applications, mobility, management, scalability, and low power consumption

are all must-haves. Privacy and security concerns may also be important in the context of smart building implementations [23]-[26].

- Transport: in several nations, important highways are already equipped with sensors that can detect when traffic volumes are excessive and take action to alleviate the resulting gridlock. For example, these sensors can tally the number of cars on the road, or they can identify the location of accidents and other crises [27]-[30].
- Industry: because of the widespread adoption of computers, factory automation, and other forms of mechanisation in recent decades, the industrial sector has emerged as one of the most significant technological catalysts [31]-[33].
- Military: because of the sensitive nature of the military environment, it can be difficult to gain physical access to nodes once they have been deployed. Batteries can't be easily replaced in dangerous environments or during battle, therefore energy consumption is a crucial measure to consider [34]-[37].

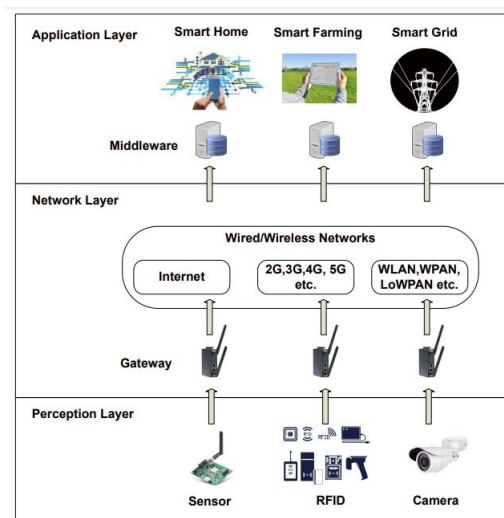


Figure 1. Three-layer architecture of IoT

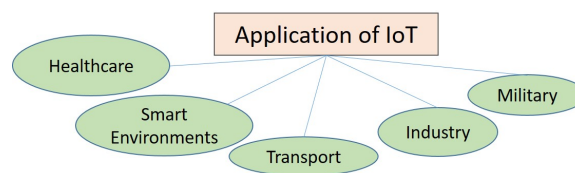


Figure 2. Application of IoT

3. DESCRIPTION OF RPL

3.1. Overview of RPL

RPL utilises the IEEE 802.15.4 standard and the 6LoWPAN adaptation layer to provide a long-distance vector protocol optimised for IPv6 low-power devices. Motivated by the desire to improve coordination between many nodes in a peer-to-peer or renewed star network [38]-[40], the routing over LLNs (RoLL) working group presented the routing requirements for low power and lossy networks (LLNs) in public, factoring in the disadvantage of powering, processing, and mind resources. With this protocol, the network's nodes are organised into a hierarchical structure with multiple intermediate nodes, allowing any node to broadcast information to its parent [41], [42], which will then forward it to the next higher level, ultimately reaching the gateway or sink node. Unicast messages can also be sent from the sink node to a specific peer in the source network [43]-[45].

3.2. Protocol configuration

When using RPL, a tree-like topology is produced (DAG). There is a ranking (Rank) system in place within the network, and as the teams branch out from the central node, the ranks of the individual nodes increase (DODAG) [46]-[48]. When resending data, the nodes prioritise the shortest path. With the help of RFC, ICMPv6 defines three control messages. The flow of RPL command messages is depicted in Figure 3.

- DIS (information request DODAG): similar to how router request messages are used to discover existing systems, DODAG can be used to inquire about nearby data.
- DIO (object of information of the DAG): transmission of DAG data in response to DIS messages; additionally utilized to update nodes' state about the network topology at regular intervals.
- DAO (object of update to the destination): teams send a message to the DODAG so that their "parent" nodes can see the latest changes to their information.

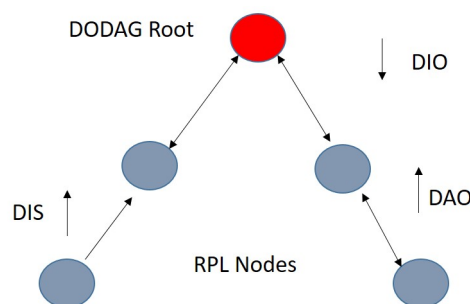


Figure 3. Control messages in RPL

3.3. Trickle timer

The exponentially growing interval used by the trickle timer [49]-[51] helps to reduce unnecessary control information. Since it was assumed that once connectivity was established, only a small number of DIO messages would be needed, the initial implementation of RPL made use of a trickle timer to store control messages only when they were actually needed by the network. RPL has two routing objective functions (OF) the hop count and the expected transmission count (ETX). In addition to these two OFs, RPL employs a trickle timer mechanism to regulate the rate at which command messages are sent. This trickle timer helps keep track of the messages sent by the sink when it tells the nodes "I am the sink".

3.4. Objective function

In order to determine which parent node is "better," RPL nodes utilise an OF that contains a set of criteria by which to compare them. The simplest and most basic objective function currently presented by the IETF is known as objective function zero (OF0) [52], [53], and it selects the device with the lower (better) rank based on a single metric: the node's rank relative to the root. The OF0 is intended to be a baseline from which more refined objective function implementations can be developed. The second is the container-based minimal rank with hysteresis objective function (MRHOF) [54], [55], which is likely the most widely used routing metric. By using a metric container, users can modify the metrics that are transmitted alongside DIO messages. ETX is the standard routing metric, however this enhancement enables the use of estimated energy expenditure as an alternative [56], [57].

4. TAXONOMY OF LITERATURE REVIEWS

This section shows the taxonomy of literature reviews. As shown in Figure 4, this review provides a taxonomy of literature reviews based on energy consumption, mobility, and quality of service (QoS), congestion, and security. The description and review of each type are provided as follows.

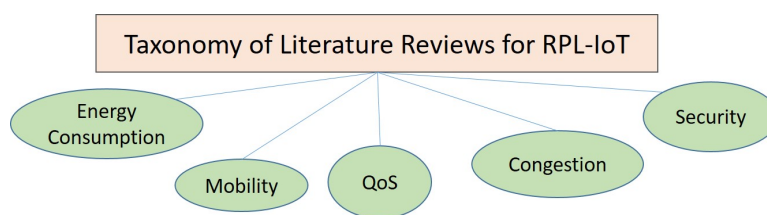


Figure 4. Taxonomy of literature reviews for RPL-IoT

4.1. Energy consumption

IEEE 802.15.4 and RPL were created with energy saving in mind because low power is such a significant issue for LLNs [58]. Many academics think about include energy usage as a routing parameter in the objective function when proposing enhancements to RPL. The original RPL standard ensures that nodes constructed to it can operate for years on a single battery charge [59], [60]. Using energy consumption as a parameter, a second study verifies these findings and adds that energy usage increases proportionally with network size and the number of nodes. The objective function (SEEOF) used by the authors of the study "Smart energy efficient objective function for smart metering and industrial applications" cites residual energy and predicted energy usage [61]. Like ants working together for the greater good of the colony, the collaborative approach chosen by the authors of [62] assumes that devices are autonomous decision-makers where the gain of each node is beneficial for the welfare of the network as a whole. Improved throughput and energy distribution among network nodes are reflected in the simulation findings as an improvement in lifetime. The authors of this work offer an radio duty cycle (RDC) based approach to estimating energy consumption as a means of improving energy distribution and boosting power density. Improved failure detection is one such solution that has been studied with the intention of increasing RPL's energy efficiency [63]. When deciding where to send traffic across a network, the routing and aggregation for minimum energy (RAME) technique takes into account data from the least power-hungry device [64].

4.2. Mobility

Many studies have been conducted on the topic of routing for mobile WSNs, with the most recent ones relying heavily on RPL [65], [66], the protocol that has become the de facto standard for the IoT [67]. The DAG-based multipath routing for mobile sensor networks (DMR) [68] uses a multipath method with redundant routes and a DODAG maintenance and repair technique; it was built with RPL with rank information and link quality identifier (LQI) as routing metrics. The authors of introduced a mobility support layer named MoMoRo to enable low-power WSN applications with human-scale mobility and low traffic. This layer includes a destination seeking technique by means of delivering adaptive flood messages to discover a missing node in the data collecting tree and permits nodes to send probes as soon as they become disconnected from their parent node. Gaddour *et al.* [69] introduced a corona mechanism with RPL (Co-RPL) based on the corona concept, which divides the system into circular coronas centred on the DODAG root and speeds up the process of nodes choosing a new parent without having to remodel the DODAG. Using this method, the nodes can make the necessary changes without disrupting the DODAG. Gara *et al.* [70] evaluates RPL for hybrid networks consisting of both mobile and static nodes, providing yet another improvement of RPL for medical and healthcare applications. Fotouhi *et al.* [71] developed a mobile version of RPL to accommodate mobility in IoT contexts. To facilitate quicker transitions between mobile nodes, this protocol extends the standard triceraddressing technique with four timers. Recent developments in mobility management have led to the development of the "Smarter-HOP" variation of mRPL. To ensure that nodes are aware of additional link metrics besides received signal strength indicator (RSSI), the target function is implemented into the parent selection method of this protocol, mRPL++ [72]. A robust routing method for WSNs with both stationary and mobile endpoints is presented in [73] in the form of Kalman positioning RPL (KP-RPL), a protocol based on RPL. For multihop routing in dynamic IoT services, Kharrufa *et al.* [74] created D-RPL to improve the capability of RPL in mobile systems with dynamic features. D-RPL makes use of some of mRPL's features, and it also has an adaptive timer that may be used as a reverse-trickle timer if movement is disabled.

4.3. Quality of service

Most IoT applications call for trustworthy data transmission, which can be achieved by decreasing the number of missed packets, maximising throughput, and minimising latency [75]. If you want to satisfy demanding QoS requirements, you need to enhance routing options, optimise data rates, and speed up topology repairs [76]. Dawans *et al.* [77] propose a reactive solution that makes use of the amount of received data packets rather than control messages to communicate updates on the link's quality. This technique adopts a similarly adaptive strategy to that proposed in [78], which suggests a cross-layer design to improve connection quality estimation in RPL; this permits secure data transmission while using less power and experiencing less delay than the original RPL. A method for identifying a root node failure is presented in [79]. Most writings take for granted that the sinknode is always strong, functional, and reliable. In order to improve routing precision, other research [80]-[82] have introduced multicast techniques. Several proposals have been made in these researches to control RPL multicast messages: stateless multicast RPL forwarding (SMRF), extended multicast RPL forwarding (ESMRF), and bidirectional multicast RPL forwarding. In order to reduce power consumption and expenses, the algorithm CooperativeRPL (C-RPL) [83] uses a cooperative technique for nodes with different sensing applications.

4.4. Congestion

The accumulation of data across successive hops causes bottlenecks at the node level, making congestion one of the primary issues with multi-hop routing [75], [84], [85]. Congestion in the wireless channel and the nodes' buffers is more likely to develop when a high number of nodes are transmitting data simultaneously [86]. Congestion has a major effect on energy consumption, dependability, and delay times [87]. Using RPL for routing and adjusting traffic according to RDC and buffer occupancy, Michopoulos *et al.* [88] established a duty cycle aware congestion control (DCCC6) for controlling traffic in 6LoWPAN networks. Castellani *et al.* [89] offered three congestion control schemes: griping, deaf, and fuse. Important factors in these implementations include queue length, buffer length, and the use of a hybrid method. For one problem with these systems, the lack of support for node priorities or application priorities, Al-Kashoash *et al.* [90] offered a game-theoretic framework for employing an adaptive transmission rate in sensor nodes. Using buffer occupancy as a measure, Hellaoui and Koudil [91] created a congestion control algorithm that can determine which channels are least impacted by congestion. The creators of use a queue utilisation strategy in which nodes share congestion details via DIO messages in order to achieve load balancing. A game-theoretic approach to the parent-child transition is proposed in [92]. Tang *et al.* [93] argue that there should be many routes for delivering data, with the best one being determined by objective function measurements. DIO data is used by the protocol to enable multi-path routing when congestion develops [94].

4.5. Security

For most IoT deployments, some measure of security is required based on factors such as the type of application, the location of deployment, and the significance of the data being provided [95]-[97]. IoT apps benefit from having trust, authenticity, authentication, availability, privacy, and integrity. An IETF standardisation proposal, RFC6553 [98], includes a cap on the number of tickle-resets that can be triggered in one hour. Mayzaud *et al.* [99] expand on this concept by suggesting an adaptive threshold that varies with the health of the network and the nature of the assault. The strategy has been shown to result in substantial improvements in energy efficiency. Blackhole and greyhole attacks, in which malevolent nodes surreptitiously drop off some of the datapackets, were proposed as a solution to this problem in a research published in [100]. Dvir *et al.* [101] presented a technique to use signed DIO messages to prevent bogus rank advertisements, which are used in sinkhole attacks in which a node falsely promotes itself with a high rank to attract data from surrounding nodes. Perrey *et al.* [102] also examined and refined the technique to make it more secure against spoofing and replay attacks. In this configuration, unlike sensor nodes, the agents' only job is to keep an eye on the network [103].

5. CHALLENGES AND FUTURE DIRECTIONS

The following sections will go into greater depth on the other central aspects of RPL, as well as their advantages, disadvantages, and future directions, as shown in Figure 5.

- Energy consumption: due of the restricted resources of the nodes, energy consumption is a crucial factor while developing an effective routing algorithm for an LLN. Therefore, studies aimed at bettering RPL

often centre on finding ways to reduce power consumption and extend the lifespan of networks. RPL was developed with the use of a trickle timer in mind, with the goal of lowering energy consumption.

- Reliability: reliability in RPL is quantified by the percentage of transmitted data that never arrive and the average transmission delay among entities. Increased reliability often comes at the expense of more power being used for retransmissions or acknowledgments.
- Congestion: similarly to real-world examples, LLNs experience increased energy consumption, delay, and decreased reliability due to network congestion.
- Objective function: in RPL, the parent selection mechanism has the major drawback of always forwarding packets destined for the root through the same parent. As this type of forwarding only considers the shortest path, it can easily cause to energy outages or the demise of overburdened parent entities, which can cause disruptions in the network.
- Mobility: although RPL was not developed with mobile nodes in mind, such nodes may be required in some practical applications. RPL has limited adaptability to dynamic networks because, in its present form, it does not distinguish among non-mobile node and mobile node.
- Stability: both route stability and node stability are possible interpretations of the stability term when used in RPL contexts. Similarly to how long a given routing path remains functional, route stability is proportional to its overall robustness. Most research ignores mobility and instead focuses on node stability, or the time during which a child's preferred parents remain stable.
- Security: in accordance with RFC 6550, RPL supports three distinct security settings: an unprotected, pre-installed, and authenticated environment. As its name implies, the unsecured mode does not use encryption for its control messages.
- Collaborative intrusion detection system (IDS): these IDS rely on communication between sensor nodes and 6BR to quickly and accurately identify malicious activity. There aren't many studies in the literature that dig into the creation of collaborative IDS.
- Active learning: one of the major issues for ML-based IDS is a lack of data. Active learning, which optimises model learning during training, is a viable solution to this issue. There has been a recent uptick in interest in this topic from those working in the field of security. Additional research is required before this can be effectively used in the creation of IoT-based intrusion detection systems.
- Key management: in most IoT use cases, devices run in an unattended mode in an untrusted setting, making them vulnerable to attack. It's possible to view the pre-loaded security keys used in RPL's secure mode as a major security flaw due to their reliance on a single point of failure.

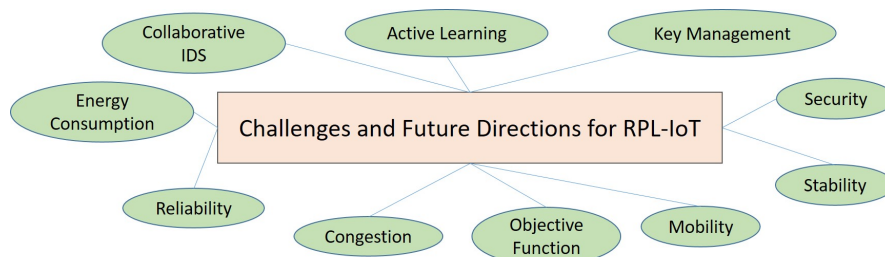


Figure 5. Challenges and future directions for RPL-IoT

6. CONCLUSION

The RPL-IoT is described in detail in this review. With regards to energy consumption, mobility, QoS, congestion, and security, this review also presents a taxonomy of literature reviews for RPL-IoT. Finally, this assessment touches on some of the difficulties and potential next steps. The proposed technique will be used to detect even more assaults from both types of RPL attacks in the future through the building of adversary models, simulation studies, dataset collection, and detection.

REFERENCES

- [1] Z. A. Almusaylim and N. Zaman, "A review on smart home present state and challenges: linked to context-awareness internet of things (IoT)," *Wireless Networks*, vol. 25, no. 6, pp. 3193–3204, Aug. 2019, doi: 10.1007/s11276-018-1712-5.
- [2] P. Chithaluru, F. Al-Turjman, M. Kumar, and T. Stephan, "I-AREOR: an energy-balanced clustering protocol for implementing green IoT in smart cities," *Sustainable Cities and Society*, vol. 61, p. 102254, Oct. 2020, doi: 10.1016/j.scs.2020.102254.
- [3] S. Selvaraj and S. Sundaravaradhan, "Challenges and opportunities in IoT healthcare systems: a systematic review," *SN Applied Sciences*, vol. 2, no. 1, p. 139, Jan. 2020, doi: 10.1007/s42452-019-1925-y.
- [4] S. J. Hussain, M. Irfan, N. Z. Jhanjhi, K. Hussain, and M. Humayun, "Performance enhancement in wireless body area networks with secure communication," *Wireless Personal Communications*, vol. 116, no. 1, pp. 1–22, Jan. 2021, doi: 10.1007/s11277-020-07702-7.
- [5] A. K. Sahu, S. Sharma, and D. Puthal, "Lightweight multi-party authentication and key agreement protocol in IoT-based e-healthcare service," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 17, no. 2s, pp. 1–20, Jun. 2021, doi: 10.1145/3398039.
- [6] M. M. Noor and W. H. Hassan, "Current research on internet of things (IoT) security: a survey," *Computer Networks*, vol. 148, pp. 283–294, Jan. 2019, doi: 10.1016/j.comnet.2018.11.025.
- [7] G. Mulligan, "The 6LoWPAN architecture," in *Proceedings of the 4th workshop on Embedded networked sensors*, Jun. 2007, pp. 78–82, doi: 10.1145/1278972.1278992.
- [8] L.-H. Yen and W.-T. Tsai, "The room shortage problem of tree-based ZigBee/IEEE 802.15.4 wireless networks," *Computer Communications*, vol. 33, no. 4, pp. 454–462, Mar. 2010, doi: 10.1016/j.comcom.2009.10.013.
- [9] N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over low-power wireless personal area networks (6LoWPANs): overview, assumptions, problem statement, and goals," Aug. 2007, doi: 10.17487/rfc4919.
- [10] O. Gaddour and A. Koubâa, "RPL in a nutshell: a survey," *Computer Networks*, vol. 56, no. 14, pp. 3163–3178, Sep. 2012, doi: 10.1016/j.comnet.2012.06.016.
- [11] M. A. Al-Shareeda, S. Manickam, M. A. Saare, and N. C. Arjuman, "Proposed security mechanism for preventing fake router advertisement attack in IPv6 link-local network," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 29, no. 1, pp. 518–526, Jan. 2022, doi: 10.11591/ijeecs.v29.i1.pp518-526.
- [12] A. Raoof, A. Matrawy, and C.-H. Lung, "Routing attacks and mitigation methods for RPL-based internet of things," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1582–1606, 2019, doi: 10.1109/COMST.2018.2885894.
- [13] P. Sethi and S. R. Sarangi, "Internet of things: architectures, protocols, and applications," *Journal of Electrical and Computer Engineering*, vol. 2017, pp. 1–25, 2017, doi: 10.1155/2017/9324035.
- [14] M. R. Abdmeziem, D. Tandjaoui, and I. Romdhani, "Architecting the internet of things: state of the art," in *Robots and Sensor Clouds. Studies in Systems, Decision and Control*, Cham: Springer, 2016, pp. 55–75.
- [15] L. Da Xu, W. He, and S. Li, "Internet of things in industries: a survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014, doi: 10.1109/TII.2014.2300753.
- [16] K. O. M. Salih, T. A. Rashid, D. Radovanovic, and N. Bacanin, "A comprehensive survey on the internet of things with the industrial marketplace," *Sensors*, vol. 22, no. 3, p. 730, Jan. 2022, doi: 10.3390/s22030730.
- [17] M. A. Al-Shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "Towards identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Access*, vol. 9, pp. 113226–113238, 2021, doi: 10.1109/ACCESS.2021.3104148.
- [18] L. Kong *et al.*, "Edge-computing-driven Internet of things: a survey," *ACM Computing Surveys*, vol. 55, no. 8, pp. 1–41, Aug. 2023, doi: 10.1145/3555308.
- [19] S. N. Sajedi, M. Maadani, and M. Nesari Moghadam, "F-LEACH: a fuzzy-based data aggregation scheme for healthcare IoT systems," *The Journal of Supercomputing*, vol. 78, no. 1, pp. 1030–1047, Jan. 2022, doi: 10.1007/s11227-021-03890-6.
- [20] A. H. Sodhro, A. I. Awad, J. Beek, and G. Nikolakopoulos, "Intelligent authentication of 5G healthcare devices: A survey," *Internet of Things*, vol. 20, p. 100610, Nov. 2022, doi: 10.1016/j.iot.2022.100610.
- [21] Y. Yang, H. Wang, R. Jiang, X. Guo, J. Cheng, and Y. Chen, "A review of IoT-enabled mobile healthcare: technologies, challenges, and future trends," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9478–9502, Jun. 2022, doi: 10.1109/JIOT.2022.3144400.
- [22] A. N. Bahache, N. Chikouche, and F. Mezrag, "Authentication schemes for healthcare applications using wireless medical sensor networks: a survey," *SN Computer Science*, vol. 3, no. 5, p. 382, Jul. 2022, doi: 10.1007/s42979-022-01300-z.
- [23] A. Souri, A. Hussien, M. Hoseyninezhad, and M. Norouzi, "A systematic review of IoT communication strategies for an efficient smart environment," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, Mar. 2022, doi: 10.1002/ett.3736.
- [24] H. Mori, J. Kundaliya, K. Naik, and M. Shah, "IoT technologies in smart environment: security issues and future enhancements," *Environmental Science and Pollution Research*, vol. 29, no. 32, pp. 47969–47987, Jul. 2022, doi: 10.1007/s11356-022-20132-1.
- [25] M. A. Al-Shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "SE-CPPA: a secure and efficient conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *Sensors*, vol. 21, no. 24, p. 8206, Dec. 2021, doi: 10.3390/s21248206.
- [26] M. V. Vinayak and T. Jarin, "An overview of security issues in internet of things based smart environments," *EAI Endorsed Transactions on Energy Web*, p. 170235, Jul. 2018, doi: 10.4108/eai.15-6-2021.170235.
- [27] P. Saraswathi and P. M. Rao, "Intelligent transport system using IoT-V2X: communication technologies, security issues, challenges and countermeasures," pp. 1–19, 2022, doi: 10.21203/rs.3.rs-1290602.
- [28] T. Garg and G. Kaur, "A systematic review on intelligent transport systems," *Journal of Computational and Cognitive Engineering*, Jun. 2022, doi: 10.47852/bonviewJCCE2202245.
- [29] M. A. Al-Shareeda, M. Anbar, S. Manickam, A. Khalil, and I. H. Hasbullah, "Security and privacy schemes in vehicular ad-hoc network with identity-based cryptography approach: a survey," *IEEE Access*, vol. 9, pp. 121522–121531, 2021, doi: 10.1109/ACCESS.2021.3109264.
- [30] S.-H. Chung, "Applications of smart technologies in logistics and transport: A review," *Transportation Research Part E: Logistics and Transportation Review*, vol. 153, p. 102455, Sep. 2021, doi: 10.1016/j.tre.2021.102455.




- [31] Z. Fatima *et al.*, "Production plant and warehouse automation with iot and industry 5.0," *Applied Sciences*, vol. 12, no. 4, p. 2053, Feb. 2022, doi: 10.3390/app12042053.
- [32] Y. Mashayekhy, A. Babaei, X.-M. Yuan, and A. Xue, "Impact of internet of things (IoT) on inventory management: a literature survey," *Logistics*, vol. 6, no. 2, p. 33, May 2022, doi: 10.3390/logistics6020033.
- [33] Y. Chen, Y. Lu, L. Bulysheva, and M. Y. Kataev, "Applications of blockchain in industry 4.0: a review," *Information Systems Frontiers*, Feb. 2022, doi: 10.1007/s10796-022-10248-7.
- [34] A. I. Sulyma and C. Henggeler, "Physical layer security for military iot links using MIMO-beamforming at 60 GHz," *Information*, vol. 13, no. 2, p. 100, Feb. 2022, doi: 10.3390/info13020100.
- [35] S. Apostolopoulos, "Internet of military things smart warrior," 2022.
- [36] M. M. Hamdi, A. S. Mustafa, H. F. Mahd, M. S. Abood, C. Kumar, and M. A. Al-shareeda, "Performance analysis of QoS in MANET based on IEEE 802.11b," in *2020 IEEE International Conference for Innovation in Technology (INOCON)*, Nov. 2020, pp. 1–5, doi: 10.1109/INOCON50539.2020.9298362.
- [37] A. Utsav, A. Abhishek, P. Suraj, and R. K. Badhai, "An IoT based UAV network for military applications," in *2021 Sixth International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Mar. 2021, pp. 122–125, doi: 10.1109/WiSPNET51692.2021.9419470.
- [38] A. Seyfollahi, M. Moodi, and A. Ghaffari, "MFO-RPL: a secure RPL-based routing protocol utilizing moth-flame optimizer for the IoT applications," *Computer Standards & Interfaces*, vol. 82, p. 103622, Aug. 2022, doi: 10.1016/j.csi.2022.103622.
- [39] M. A. Al-Shareeda and S. Manickam, "COVID-19 vehicle based on an efficient mutual authentication scheme for 5G-enabled vehicular fog computing," *International Journal of Environmental Research and Public Health*, vol. 19, no. 23, p. 15618, Nov. 2022, doi: 10.3390/ijerph192315618.
- [40] V. R. Rajasekar and S. Rajkumar, "A study on impact of DIS flooding attack on RPL-based 6LowPAN network," *Microprocessors and Microsystems*, vol. 94, p. 104675, Oct. 2022, doi: 10.1016/j.micpro.2022.104675.
- [41] S. Awiphan and S. Jathuphonserd, "Load-balanced structure for RPL-based routing in wireless sensor networks," in *2022 4th International Conference on Computer Communication and the Internet (ICCCI)*, Jul. 2022, pp. 122–126, doi: 10.1109/ICCCI55554.2022.9850237.
- [42] Z. Ghanbari, N. J. Navimipour, M. Hosseinzadeh, H. Shakeri, and A. Darwesh, "The applications of the routing protocol for low-power and lossy networks (RPL) on the internet of mobile things," *International Journal of Communication Systems*, vol. 35, no. 14, Sep. 2022, doi: 10.1002/dac.5253.
- [43] R.-G. Tsai, P.-H. Tsai, G.-R. Shih, and J. Tu, "RPL based emergency routing protocol for smart buildings," *IEEE Access*, vol. 10, pp. 18445–18455, 2022, doi: 10.1109/ACCESS.2022.3150928.
- [44] M. A. Al-shareeda *et al.*, "Proposed efficient conditional privacy-preserving authentication scheme for V2V and V2I communications based on elliptic curve cryptography in vehicular ad hoc networks," in *Advances in Cyber Security. ACeS 2020*, Singapore: Springer, 2021, pp. 588–603.
- [45] P. S. Nandhini, S. Kuppuswami, and S. Malliga, "Classification of intrusions in RPL-based IoT networks: a comparison," in *Mobile Computing and Sustainable Informatics*, S. Shakya, R. Bestak, R. Palanisamy, and K. A. Kamel, Eds. Singapore: Springer, 2022, pp. 849–862.
- [46] G. Sharma, J. Grover, and A. Verma, "Performance evaluation of mobile RPL-based IoT networks under version number attack," *Computer Communications*, vol. 197, pp. 12–22, Jan. 2023, doi: 10.1016/j.comcom.2022.10.014.
- [47] I. S. Alsukayti and A. Singh, "A lightweight scheme for mitigating RPL version number attacks in IoT networks," *IEEE Access*, vol. 10, pp. 111115–111133, 2022, doi: 10.1109/ACCESS.2022.3215460.
- [48] D. Arshad, M. Asim, M. Tariq, T. Baker, H. Tawfik, and D. Al-Jumeily OBE, "THC-RPL: a lightweight trust-enabled routing in RPL-based IoT networks against sybil attack," *PLOS ONE*, vol. 17, no. 7, p. e0271277, Jul. 2022, doi: 10.1371/journal.pone.0271277.
- [49] P. Levis, T. Clausen, J. Hui, O. Gnawali, and J. Ko, "The trickle algorithm," Mar. 2011. doi: 10.17487/rfc6206.
- [50] Z. G. Al-Mekhlafi *et al.*, "Chebyshev polynomial-based fog computing scheme supporting pseudonym revocation for 5G-enabled vehicular networks," *Electronics*, vol. 12, no. 4, p. 872, Feb. 2023, doi: 10.3390/electronics12040872.
- [51] S.-T. Liu and S.-D. Wang, "Improved trickle algorithm toward low power and better route for the RPL routing protocol," *IEEE Access*, vol. 10, pp. 83322–83335, 2022, doi: 10.1109/ACCESS.2022.3196693.
- [52] L. Al-Qaisi, S. Hassan, and N. H. B. Zakaria, "Secure routing protocol for low power and lossy networks against rank attack: a systematic review," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 5, 2022, doi: 10.14569/IJACSA.2022.0130539.
- [53] P. Thubert, Ed., "Objective function zero for the routing protocol for low-power and lossy networks (RPL)," Mar. 2012. doi: 10.17487/rfc6552.
- [54] I. Zaatouri, N. Alyaoui, A. B. Guiloufi, F. Sailhan, and A. Kachouri, "Design and performance analysis of objective functions for RPL routing protocol," *Wireless Personal Communications*, vol. 124, no. 3, pp. 2677–2697, Jun. 2022, doi: 10.1007/s11277-022-09484-6.
- [55] T. W. Ching, A. H. M. Aman, W. M. H. Azamuddin, H. Sallehuddin, and Z. S. Attarbashi, "Performance analysis of internet of things routing protocol for low power and lossy networks (RPL): energy, overhead and packet delivery," in *2021 3rd International Cyber Resilience Conference (CRC)*, Jan. 2021, pp. 1–6, doi: 10.1109/CRC50527.2021.9392475.
- [56] N. S. Abu Ennab, M. B. Yassein, and O. AlZoubi, "Performance analysis of RPL objective functions in a medium spars network," in *2022 13th International Conference on Information and Communication Systems (ICICS)*, Jun. 2022, pp. 100–103, doi: 10.1109/ICICS55353.2022.9811137.
- [57] Z. G. Al-Mekhlafi, M. A. Al-Shareeda, S. Manickam, B. A. Mohammed, and A. Qtaish, "Lattice-based lightweight quantum resistant scheme in 5G-enabled vehicular networks," *Mathematics*, vol. 11, no. 2, p. 399, Jan. 2023, doi: 10.3390/math11020399.
- [58] A. J. H. Witwit and A. K. Idrees, "Energy-efficient load-balanced RPL routing protocol for internet of things (IoTs) networks," *International Journal of Internet Technology and Secured Transactions*, vol. 1, no. 1, p. 1, 2020, doi: 10.1504/IJITST.2020.10030144.

- [59] M. Durvy *et al.*, “Making sensor networks IPv6 ready,” in *Proceedings of the 6th ACM conference on Embedded network sensor systems*, Nov. 2008, pp. 421–422, doi: 10.1145/1460412.1460483.
- [60] N. Tsiftes, J. Eriksson, and A. Dunkels, “Low-power wireless IPv6 routing with ContikiRPL,” in *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks*, Apr. 2010, pp. 406–407, doi: 10.1145/1791212.1791277.
- [61] N. M. Shakya, M. Mani, and N. Crespi, “SEEOF: smart energy efficient objective function: adapting RPL objective function to enable an IPv6 meshed topology solution for battery operated smart meters,” in *2017 Global Internet of Things Summit (GloTS)*, Jun. 2017, pp. 1–6, doi: 10.1109/GIOTS.2017.8016252.
- [62] B. Mohamed and F. Mohamed, “QoS routing rpl for low power and lossy networks,” *International Journal of Distributed Sensor Networks*, vol. 11, no. 11, p. 971545, Nov. 2015, doi: 10.1155/2015/971545.
- [63] N. Khelifi, S. Oteafy, H. Hassanein, and H. Youssef, “Proactive maintenance in RPL for 6LowPAN,” in *2015 International Wireless Communications and Mobile Computing Conference (IWCMC)*, Aug. 2015, pp. 993–999, doi: 10.1109/IWCMC.2015.7289218.
- [64] A. Riker, M. Curado, and E. Monteiro, “Neutral operation of the minimum energy node in energy-harvesting environments,” in *2017 IEEE Symposium on Computers and Communications (ISCC)*, Jul. 2017, pp. 477–482, doi: 10.1109/ISCC.2017.8024574.
- [65] A. Vaezian and Y. Darmani, “MSE-RPL: mobility support enhancement in RPL for IoT mobile applications,” *IEEE Access*, vol. 10, pp. 80816–80832, 2022, doi: 10.1109/ACCESS.2022.3194273.
- [66] S. M. Muzammal, R. K. Murugesan, N. Z. Jhanjhi, M. Humayun, A. O. Ibrahim, and A. Abdelmaboud, “A trust-based model for secure routing against RPL Attacks in internet of things,” *Sensors*, vol. 22, no. 18, p. 7052, Sep. 2022, doi: 10.3390/s22187052.
- [67] M. R. Palattella *et al.*, “Standardized protocol stack for the internet of (important) things,” *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 1389–1406, 2013, doi: 10.1109/SURV.2012.111412.00158.
- [68] K.-S. Hong and L. Choi, “DAG-based multipath routing for mobile sensor networks,” in *ICTC 2011*, Sep. 2011, pp. 261–266, doi: 10.1109/ICTC.2011.6082593.
- [69] O. Gaddour, A. Koubâa, and M. Abid, “Quality-of-service aware routing for static and mobile IPv6-based low-power and lossy sensor networks using RPL,” *Ad Hoc Networks*, vol. 33, pp. 233–256, Oct. 2015, doi: 10.1016/j.adhoc.2015.05.009.
- [70] F. Gara, L. Ben Saad, R. Ben Ayed, and B. Tourancheau, “RPL protocol adapted for healthcare and medical applications,” in *2015 International Wireless Communications and Mobile Computing Conference (IWCMC)*, Aug. 2015, pp. 690–695, doi: 10.1109/IWCMC.2015.7289167.
- [71] H. Fotouhi, D. Moreira, and M. Alves, “mRPL: boosting mobility in the internet of things,” *Ad Hoc Networks*, vol. 26, pp. 17–35, Mar. 2015, doi: 10.1016/j.adhoc.2014.10.009.
- [72] M. C. R. Anand and M. P. Tahiliani, “mRPL++: smarter-HOP for optimizing mobility in RPL,” in *2016 IEEE Region 10 Symposium (TENSYMP)*, May 2016, pp. 36–41, doi: 10.1109/TENCONSpring.2016.7519374.
- [73] M. Barcelo, A. Correa, J. L. Vicario, A. Morell, and X. Vilajosana, “Addressing mobility in RPL with position assisted metrics,” *IEEE Sensors Journal*, vol. 16, no. 7, pp. 2151–2161, Apr. 2016, doi: 10.1109/JSEN.2015.2500916.
- [74] H. Kharrufa, H. Al-Kashoash, Y. Al-Nidawi, M. Q. Mosquera, and A. H. Kemp, “Dynamic RPL for multi-hop routing in IoT applications,” in *2017 13th Annual Conference on Wireless On-demand Network Systems and Services (WONS)*, Feb. 2017, pp. 100–103, doi: 10.1109/WONS.2017.7888753.
- [75] F. Kaviani and M. Soltanaghvaei, “CQARPL: congestion and QoS-aware RPL for IoT applications under heavy traffic,” *The Journal of Supercomputing*, vol. 78, no. 14, pp. 16136–16166, Sep. 2022, doi: 10.1007/s11227-022-04488-2.
- [76] Y. Chen, J. P. Chanet, and K. M. Hou, “RPL routing protocol a case study: precision agriculture,” *First China-France Workshop on Future Computing Technology (CF-WoFUCT 2012)*, p. 6, 2012.
- [77] S. Dawal, S. Duquennoy, and O. Bonaventure, “On link estimation in dense RPL deployments,” in *37th Annual IEEE Conference on Local Computer Networks – Workshops*, Oct. 2012, pp. 952–955, doi: 10.1109/LCNW.2012.6424087.
- [78] E. Ancillotti, R. Bruno, and M. Conti, “Reliable data delivery with the IETF routing protocol for low-power and lossy networks,” *IEEE Transactions on Industrial Informatics*, vol. 10, no. 3, pp. 1864–1877, Aug. 2014, doi: 10.1109/TII.2014.2332117.
- [79] K. Iwanicki, “RNFD: routing-layer detection of DODAG (Root) node failures in low-power wireless networks,” in *2016 15th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, Apr. 2016, pp. 1–12, doi: 10.1109/IPSN.2016.7460720.
- [80] G. Oikonomou, I. Phillips, and T. Tryfonas, “IPv6 multicast forwarding in RPL-based wireless sensor networks,” *Wireless Personal Communications*, vol. 73, no. 3, pp. 1089–1116, Dec. 2013, doi: 10.1007/s11277-013-1250-5.
- [81] K. Q. A. Fadeel and K. E. Sayed, “ESMRF: enhanced stateless multicast RPL forwarding for IPv6-based low-power and lossy networks,” in *Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems*, May 2015, pp. 19–24, doi: 10.1145/2753476.2753479.
- [82] G. G. Lorente, B. Lemmens, M. Carlier, A. Braeken, and K. Steenhaut, “BMRF: bidirectional multicast RPL forwarding,” *Ad Hoc Networks*, vol. 54, pp. 69–84, Jan. 2017, doi: 10.1016/j.adhoc.2016.10.004.
- [83] M. Barcelo, A. Correa, J. Lopez Vicario, and A. Morell, “Cooperative interaction among multiple RPL instances in wireless sensor networks,” *Computer Communications*, vol. 81, pp. 61–71, May 2016, doi: 10.1016/j.comcom.2015.12.008.
- [84] S. A. Rashid *et al.*, “Congestion aware genetic Q-learning based RPL routing protocol for vehicle ad-hoc networks,” in *2022 5th International Conference on Engineering Technology and its Applications (IICETA)*, May 2022, pp. 464–469, doi: 10.1109/IICETA54559.2022.9888583.
- [85] A. Maheshwari, R. K. Yadav, and P. Nath, “Data congestion control using offloading in IoT network,” *Wireless Personal Communications*, vol. 125, no. 3, pp. 2147–2166, Aug. 2022, doi: 10.1007/s11277-022-09649-3.
- [86] H. A. A. Al-Kashoash, F. Hassen, H. Kharrufa, and A. H. Kemp, “Analytical modelling of congestion for 6LoWPAN networks,” *ICT Express*, vol. 4, no. 4, pp. 209–215, Dec. 2018, doi: 10.1016/j.icte.2017.11.001.
- [87] H. A. A. Al-Kashoash, H. Kharrufa, Y. Al-Nidawi, and A. H. Kemp, “Congestion control in wireless sensor and 6LoWPAN networks: toward the Internet of Things,” *Wireless Networks*, vol. 25, no. 8, pp. 4493–4522, Nov. 2019, doi: 10.1007/s11276-018-1743-y.
- [88] V. Michopoulos, L. Guan, G. Oikonomou, and I. Phillips, “DCC6: duty cycle-aware congestion control for 6LoWPAN networks,” in *2012 IEEE International Conference on Pervasive Computing and Communications Workshops*, Mar. 2012, pp. 278–283, doi: 10.1109/PerComW.2012.6197495.




- [89] A. P. Castellani, M. Rossi, and M. Zorzi, "Back pressure congestion control for CoAP/6LoWPAN networks," *Ad Hoc Networks*, vol. 18, pp. 71–84, Jul. 2014, doi: 10.1016/j.adhoc.2013.02.007.
- [90] H. A. A. Al-Kashoash, M. Hafeez, and A. H. Kemp, "Congestion control for 6LoWPAN networks: a game theoretic framework," *IEEE Internet of Things Journal*, vol. 4, no. 3, pp. 760–771, Jun. 2017, doi: 10.1109/JIOT.2017.2666269.
- [91] H. Hellaoui and M. Koudil, "Bird flocking congestion control for CoAP/RPL/6LoWPAN networks," in *Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems*, May 2015, pp. 25–30, doi: 10.1145/2753476.2753480.
- [92] C. Ma, J.-P. Sheu, and C.-X. Hsu, "A game theory based congestion control protocol for wireless personal area networks," *Journal of Sensors*, vol. 2016, pp. 1–13, 2016, doi: 10.1155/2016/6168535.
- [93] W. Tang, X. Ma, J. Huang, and J. Wei, "Toward improved RPL: a congestion avoidance multipath routing protocol with time factor for wireless sensor networks," *Journal of Sensors*, vol. 2016, pp. 1–11, 2016, doi: 10.1155/2016/8128651.
- [94] M. A. Lodhi, A. Rehman, M. M. Khan, and F. B. Hussain, "Multiple path RPL for low power lossy networks," in *2015 IEEE Asia Pacific Conference on Wireless and Mobile (APWiMob)*, Aug. 2015, pp. 279–284, doi: 10.1109/APWiMob.2015.7374975.
- [95] M. Pishdar, Y. Seifi, M. Nasiri, and M. Bag-Mohammadi, "PCC-RPL: an efficient trust-based security extension for RPL," *Information Security Journal: A Global Perspective*, vol. 31, no. 2, pp. 168–178, Mar. 2022, doi: 10.1080/19393555.2021.1887413.
- [96] A. D. K. Marapatla and E. Ilavarasan, "Security attacks and its countermeasures in RPL," in *Smart and Sustainable Technologies: Rural and Tribal Development Using IoT and Cloud Computing. Advances in Sustainability Science and Technology*, Singapore: Springer, 2022, pp. 9–28.
- [97] C. Dogan, S. Yilmaz, and S. Sen, "Analysis of RPL objective functions with security perspective," in *Proceedings of the 11th International Conference on Sensor Networks*, 2022, pp. 71–80, doi: 10.5220/0011011900003118.
- [98] J. Hui, "The routing protocol for low-power and lossy networks (RPL) option for carrying RPL information in data-plane datagrams," Mar. 2012. doi: 10.17487/rfc6553.
- [99] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schönwälder, "Mitigation of topological inconsistency attacks in RPL-based low-power lossy networks," *International Journal of Network Management*, vol. 25, no. 5, pp. 320–339, Sep. 2015, doi: 10.1002/nem.1898.
- [100] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: real-time intrusion detection in the internet of things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2661–2674, Nov. 2013, doi: 10.1016/j.adhoc.2013.04.014.
- [101] A. Dvir, T. Holczer, and L. Buttyan, "VeRA - version number and rank authentication in RPL," in *2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems*, Oct. 2011, pp. 709–714, doi: 10.1109/MASS.2011.76.
- [102] H. Perrey, M. Landsmann, O. Ugus, T. C. Schmidt, and M. Wählisch, "TRAIL: topology authentication in RPL," Dec. 2013, [Online]. Available: <http://arxiv.org/abs/1312.0984>.
- [103] A. Mayzaud, R. Badonnel, and I. Chrisment, "A distributed monitoring strategy for detecting version number attacks in RPL-based networks," *IEEE Transactions on Network and Service Management*, vol. 14, no. 2, pp. 472–486, Jun. 2017, doi: 10.1109/TNSM.2017.2705290.

BIOGRAPHIES OF AUTHORS






Murtaja Ali Saare    is an assistant professor at the Department of Computer Technology Engineering, Shatt Al-Arab University College, Iraq. He received his master's degree in information technology at Universiti Utara Malaysia (UUM), in 2017. He completed his Ph.D. at School of Computing, Sintok, UUM, Kedah, Malaysia, in 2021. His research interest includes aging and cognition, e-health, and human-centered computing. He has published his research work in reputable indexed journal. He can be contacted at email: mmurtaja88@gmail.com and murtaja.a.sari@sauc.edu.iq.






Saima Anwar Lashari    is currently working as assistant professor at Saudi Electronic University, Saudi Arabia. She received bachelor's degree (Hons.) in computer science from University of Engineering and Technology (UET), Lahore, Pakistan, in 2004, later, she obtained her M.Sc. and Ph.D. degrees in information technology from Universiti Tun Hussein Onn Malaysia (UTHM), Malaysia, in 2012 and 2016, respectively. Her research interests include machine learning, deep learning, pattern recognition, and image processing. She has published a number of publications in reputed journals. She can be contacted at email: s.lashari@seu.edu.sa.






Ayman Khalil    received his M.E. in networking and telecommunications from the Lebanese University/Saint Joseph University, Beirut, Lebanon in 2007, and his Ph.D. in telecommunications from the National Institute of Applied Sciences (INSA), Rennes, France in 2010. During its Ph.D. he was with the Electronics and Telecommunications Institute of Rennes (IETR), where he worked on the optimization of high data rate WPAN systems. He has been involved in several European projects including OMEGA where he worked for three years in developing solutions and protocols for next generation home networks. His main research interests lie in next generation wireless systems, heterogeneous networks, network coding, and AI-based optimization solutions. He has been involved in supervising Ph.D. students in Lebanon and France. He can be contacted at email: ayman.khalil23@gmail.com.



Mahmood A. Al-Shareeda    obtained his Ph.D. in advanced computer network from University Sains Malaysia (USM). He is currently a postdoctoral fellowship at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His current research interests include network monitoring, internet of things (IoT), vehicular ad hoc network (VANET) security, and IPv6 security. He can be contacted at email: alshareeda022@usm.my.



Selvakumar Manickam    is currently working as an associate professor at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His research interests include cybersecurity, internet of things, industry 4.0, and machine learning. He has authored and co-authored more than 160 articles in journals, conference proceedings, and book reviews and graduated 13 Ph.Ds. He has 10 years of industrial experience prior to joining academia. He is a member of technical forums at national and international levels. He also has experience building IoT, embedded, server, mobile, and web-based applications. He can be contacted at email: selva@usm.my.