Journal of Engineering Science and Technology
Special Issue on Development of Sustainability Systems - III, 96 - 108

ROUTING PROTOCOL OF LOW-POWER AND LOSSY NETWORKS ENHANCEMENT FOR IOT UNDER BOTNET DISTRIBUTED DENIAL OF SERVICE CYBER ATTACKS

SHAYMA W. NOURILDEAN[1,*], SIDDEEQ Y. AMEEN[2]

[1]Communication Engineering Department, University of Technology, Iraq
[2]Cybersecurity Engineering Department, Duhok Polytechnic University, Duhok, Iraq
*Corresponding author: Shayma.w.nourildean@uotechnology.edu.iq

Abstract

Wireless Sensor Networks, as the elementary infrastructure of IoT, encounter significant challenges in terms of energy conservation and data reliability, as well as security against cyber-attacks. Thus, there is a need to ensure that the routing protocol, such as the Routing Protocol for Low-Power and Lossy Networks (RPL), can resist such cyber-attacks. The paper investigates the performance of the RPL routing protocol versus Ad-Hoc On-Demand Distance Vector (AODV) under Botnet Distributed Denial of Service (DDoS) attacks. NetSim simulation v14.2 is used for Quality of Service metrics analysis: throughput, delay, Bit Error Rate, and energy consumption with and without the attack. The findings indicate that DDoS attacks have degraded the performance of the network in all aspects except in the cases of RPL. Simulation results show that, under attack conditions, RPL maintains 15-25% higher throughput and 40% - 60% lower end-to-end delay compared to AODV. Bit Error Rate under RPL increases by only 40% - 60%, whereas AODV experiences more than a 150% increase. In addition, RPL demonstrates 20% - 30% lower energy consumption during attacks. These results confirm that RPL provides superior resilience, reliability, and energy efficiency under cyber-attack conditions, making it a suitable routing protocol for secure and resource-constrained IoT environments. However, the resource limitations of IoT devices in RPL networks exacerbate the problem, making them more susceptible to attacks and hindering the network's ability to scale effectively. Therefore, the paper suggests more research to enhance the RPL performance to reduce the DDoS attack intensity and scalability implications.

Keywords: AODV, Cyber-resilience, DDoS, Energy consumption, IoT, NetSim, RPL.

1. Introduction

The Internet of Things (IoT) interconnects things through the network of physical devices and sensors and wireless connectivity to perform intelligent data exchange and automation across a wide range of applications. The wireless sensor network (WSN) is an essential part of the Internet of Things (IoT). It links sensors, software, and technology over the Internet in order to communicate data with other systems and is referred to as the IoT [1]. The vast majority of network nodes for wireless sensor networks are low, battery -controlled equipment. For this reason, it is necessary to develop methods for collecting data that use low energy, while increasing the cost and networking life [2]. Self-organization and decentralization are two properties that define the nature of the Internet of Things network. These properties result in dynamic changes in the position of nodes. For this reason, it is very important for the successful transmission of routing data in the IoT [3, 4].

Applications based on IoT are the targets of cyber-kinetic attacks. Attacks of this kind harm not only human lives but also physical well-being and the natural environment [5]. Cybersecurity experts are employing AI to protect systems from cyberattacks. It is mostly employed for intrusion detection in cybersecurity by analysing traffic patterns to identify actions suggestive of an attack [6]. Security risks related to IoT are considered manageable with intrusion detection, a technique employed for over three decades. Intrusion detection technologies are a potential means to mitigate the impact of cyberattacks [4].

The Internet Engineering Task Force (IETF) developed the RPL routing protocol, which was then investigated for use with fixed IoT [7]. RPL is mainly designed for low electrical tools that use IPV6. It is supported by 6LOWPAN adaptation layers and is operated according to the IEEE 802.15.4 standard [8]. RPL is able to provide the necessary help to achieve the versatile requirements for a wide selection of IoT applications [9]. Most of the studies show that RPL is the superior routing protocol for the IoT as compared to other ad hoc protocols, such as the Ad hoc On-Demand Distance Vector Routing (AODV), in terms of quality of service metrics like throughput, delay, BER and energy consumption [10].

RPL's inherent design characteristics make it particularly susceptible to various DDoS attacks that can severely degrade network performance, which include:

Control Message Exploitation: Attackers can manipulate RPL's ICMPv6 control messages (DIO, DIS, DAO, DAO-ACK) to create network instability 6. For instance, Version Number attacks artificially increment the DODAG version, forcing unnecessary global repairs that consume resources [11].

Topology Disruption: DDoS attacks targeting RPL can increase end-to-end delay by over 90% while reducing throughput by similar margins, as demonstrated in NetSim v14.1 simulations 2. These attacks specifically exploit RPL's parent selection mechanism and rank properties.

Resource Depletion: The constrained nature of IoT devices (limited memory, processing power, and energy) makes them vulnerable to attacks that increase control traffic overhead by 200% or more [11]. Bit and piece DDoS attacks gradually overwhelm nodes by fragmenting malicious traffic.

Previous studies related to RPL-Based routing protocols are investigated as shown below.

Kharrufa et al. [8] provided an in-depth survey on RPL-based routing protocols for IoT applications, focusing on improvements to be made towards energy efficiency, reliability, mobility, congestion, and security. Their work systematically classified enhancements of RPL with respect to application domains and optimization goals and presented that the use of modified objective functions and adaptive control mechanisms can bring significant improvements on PDR, energy consumption, and end-to-end delay over standard RPL. Nevertheless, the majority of existing works considered only static or low mobility and experiment results were justified by small-scale simulations, leaving the high-speed mobility and heterogeneity traffic load not sufficiently addressed.

Darabkh et al. [11] provided a comprehensive and state-of-the-art survey of RPL over IoT via reviewing recent progress, simulation platforms, and performance improvements from 2010 to 2021. They showed that mobility-aware RPL variants and quality of service (QoS)-oriented objective functions can increase reliability and throughput by 20-30% with respect to RPL in constrained environments. However, the authors pointed out the remaining limitations for this approach, such as high control overhead, lack of responsiveness in dynamic topologies, and reduced validation under various mobility models and realistic traffic conditions , especially in comparative simulation scenarios.

Darabkh et al. [12] proposed a detailed survey of the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL), systematically addressing the protocol architecture, objective functions, routing metrics, as well as optimization in IoT contexts. Their work reviewed a substantial number of RPL-based approaches using qualitative comparison, where they paid special attention to metrics such as reliability, energy consumption efficiency, scalability, and resiliency. The authors found that a number of improved RPL versions result in significant enhancements in delivery rate (packet delivery ratio, PDR) and network lifetime, mainly due to energy awareness and mobility Awareness objectives functions. However, they noted that the majority of solutions were validated under static or low mobility conditions and that a significant part of the work was based on simulations only, which did not reflect real-world RPL performance, especially when there is high traffic.

Rani et al. [13] studied RPL-based routing protocols for the load balance in IoT networks and have a focus on Objective Functions like OF0 and MRHOF bases that work with hop count, ETX, RSSI or buffer occupancy. Their work analytically and experimentally demonstrated that the adoption of load-aware and traffic-aware objective functions can be beneficial in terms of PDR, energy efficiency, and network lifetime with respect to RPL in smart city as well as home automation settings. However, the authors point out that most of the considered approaches were validated in static or low-mobility scenarios without comprehensive mobility model availability and introduced new control overhead and computational complexity in a scalable and effective manner, especially for highly dynamic on-the-move MANET-IoT environments.

Important RPL routing attacks were the subject of complete experimental research by Alsukayati and Alreshoodi [9]. Research examined different types of attack methods used in the RPL network configuration of different sizes. In addition, the effectiveness of the total performance of the RPL network was taken into account in the study of various safety measures, as well as routing attacks.

They found a significant decline in the stability of their architecture, along with the quality of service (COOS) performance.

Liu et al. [14] examined the performance of RPL in large-scale IoT deployments with OMNeT++ based extensive simulations under various objective functions and routing metrics (such as hop count and ETX). In their work, ETX-based RPL provides a superior packet delivery ratio than hop-count routing but hop-count has a lower end-to-end delay; therefore, there is an inherent trade-off between performance. The authors also demonstrated that RPL scalability is possible up to a few hundred nodes if suitable trickle timer settings are employed. However, the work assumed static network topologies and does not account for node mobility or heterogeneous traffic loads, which reduces its applicability to dynamic MANET-IoT scenarios and motivates research under mobility-aware conditions.

Rakesh and Sultana [15] conducted a thorough review of the improved routing techniques of the RPL protocol in IoT networks, classifying the existing methods into peer-to-peer-based, multicast-based, mobility-supported, QoS-supported, energy-efficient routing approaches, as well as objective function-based improvements. They demonstrate that by using such techniques as energy-aware composite metrics, fuzzy-logic-based objective functions and mobility-assisted routing, the packet delivery ratio (PDR), delay, and network lifetime are remarkably enhanced with respect to standard RPL. However, the review points out some flaws, such as larger control overhead that results in higher memory requirements due to fuzzy systems and less applicability over high-mobility environments and a lack of validation against security threats like rank attacks. Furthermore, most of the surveyed solutions are based on altering control messages or complex approaches that decrease scalability and practical deployability in resource constraints IoT space.

It is clear from the related studies presented that RPL shows enhanced performance, but the previous studies did not investigate the effect of the RPL routing protocol on the IoT with a cyber-attack. Thus, with the increase of cyber-attacks such as DDOS, there is an importance to ensure that the RPL provides better safety and performance stability during cyber-attack situations and proves to be a more energy-capable and reliable routing protocol in the IoT-WSN environment.

The purpose of this research is to examine the RPL routing protocol for IoT networks under Botnet DDoS cyber-attacks, which degraded the throughput, latency, energy, and BER of the IoT networks. This study is examined using the NetSim v14.2 simulation program. The paper is organized as follows: Section 2 presents related work, including the studies within the field of RPL; Section 3 defines some theoretical concepts; Section 4 describes the research method, and the results are illustrated in Section 5; the conclusion is presented in Section 6.

2. Methods and Materials

2.1. IoT-wireless sensor network

The IoT is simply a link between humans and machines, in which humans issue orders and machines carry them out. The IoT refers to the integration and communication that occurs among intelligent objects (things). Through its domination, IoT enables the development of new technologies and applications. The data that is detected is transmitted from sensors to centralized databases, where

it is stored and made available to those who have the required access privileges. This is accomplished by connecting the sensors. WSN is the infrastructure that supports the IoT systems. It connects a wide variety of intelligent sensors and acts as the framework for the IoT-based systems that are all around us. The rapid proliferation of these electronic devices has given rise to major worries over the amount of energy that they use [2, 16].

WSNs are an important component of the IoT. It is comprised of a large number of sensor nodes which are equipped with communication, sensing, and computer technologies. Every node was able to detect the environment that an activity or item was in. Each sensor node either establishes a connection with its peers or transmits (receives) the data to or from a base station in order to collect the data that it has sensed. Base stations are used to establish connections between the sensor networks and other networks [17].

2.2. RPL routing protocols

Because of the IoT, it is now possible to connect smart devices that are embedded in a variety of items in a seamless manner. This makes it possible for these devices to be connected to any network, regardless of time or place. IoT networks are specified by decentralization and self- organization properties, so that the node's position changes dynamically. On account of this, routing in the Internet of Things is very necessary for the successful transfer of data. When it comes to routing in the Internet of Things network, the limited energy and processing capacity of the associated equipment cause significant obstacles to itself. Many different routing algorithms are clearly created for effective function in the Internet of Things network. These algorithms were designed to handle many challenges given by limited resources and circumstances in the environment [18, 19].

A large number of unit connections with limited resources in a Lossy Network LLN characterizes the IoT network. It is possible to establish a wireless data connection without reducing excessive expenses or with an excessive amount of energy consumption [9]. The IETF has recently adopted the IPv6 Routing Protocol (RPL) as a standard for LLNs. Throughout the entirety of the Internet community, this protocol has garnered nearly universal adoption [3].

RPL is a low -power routing protocol, mainly designed for low electric devices using IPV6. This technique is run according to the IEEE 802.15.4 standard, and the 6LOWPAN adaptation team supports it. In the context of nodes that have limited resources, the RPL protocol handles the path for data in an effective and optimal way. It provides a structure that ensures communication in both directions, as well as strength, reliability, flexibility, and scalability [8]. RPL takes an active approach to operations. The system makes it possible to communicate using multipoint-to-point, point-to-point and point-to-multipoint. Therefore, RPL provides significant help in fulfilling different types of IoT applications [9].

IoT is a relatively new technology that is already included in everyday life. Several research has been done on the RPL routing protocol. Abdel Hakeem et al. [20] proposed a realistic and false application of RPL behaviour. This application will meet the routing requirements of the WSN. Conclusions of Cooja implementation showed that many RPL nodes faced significant packet losses, networking congestion as a result of choosing trails with very incredible links.

3. Method

The purpose of this study is to investigate the performance of an RPL-based IoT network with and without cyber-attacks. This study also aims to ensure that any user is able to use this IoT network, sustainable networks, in spite of any network threats or attacks. Therefore, this study examined the energy consumption, BER, throughput and latency metrics of RPL-based IoT network, comparing it with any other ad hoc network such as AODV. This is because the Botnet DDoS cyber-attack mitigates the traffic into the network, which causes a degradation in performance and reliability.

The research methodology is based on simulation research carried out with NetSim version 14.1 in a variety of modelled settings. Within the scope of this investigation, two scenarios were selected to investigate the impact of cyber assaults on IoT in terms of throughput and delay. The steps below show how these two scenarios were implemented with NetSim.

- In NetSim, click on New Simulation > Internet of Things
- Drop Nine sensors, one 6LOWPAN Gateway, Router and one Wired node (server)
- Set up eight different applications. Each application is transmitted from a sensor (1, 2, …, 9) to the server at a rate of 20 packets per second, with each packet having a size of fifty bytes.
- Configure the routing protocol to RPL and AODV in each sensor.
- Only path loss should be set as the channel characteristics for the wireless link. Log distance with a pathloss exponent of 4.5 is the formula for the pathloss model.
- All of the traffic coming from the sensors is directed through sensor 10, then it is sent to the gateway, and then sent to the server, as shown in Fig. 1.
- Add two malicious nodes and configure traffic from the malicious node to all sensors (1, 2,..., 9), as shown in Fig. 2. In this case, there is an exponential increase in the pace at which packets of size 10 bytes, which constitute a little attack data's quantity are sent out at a rate of 20 packets per second.
- Simulate for 1000 seconds, and the performance metrics acquired from sensors 1 through 8 were measured.

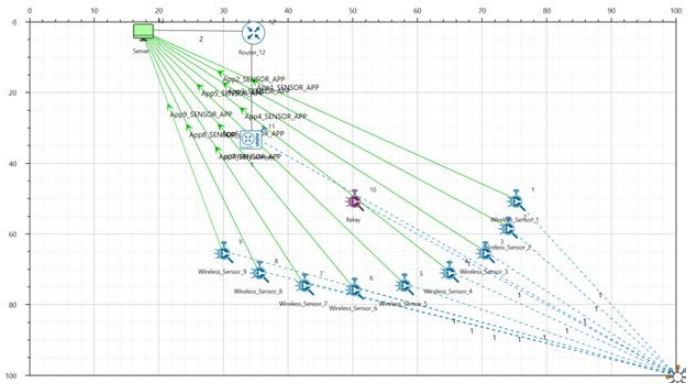

Fig. 1. IoT Network without a malicious node.

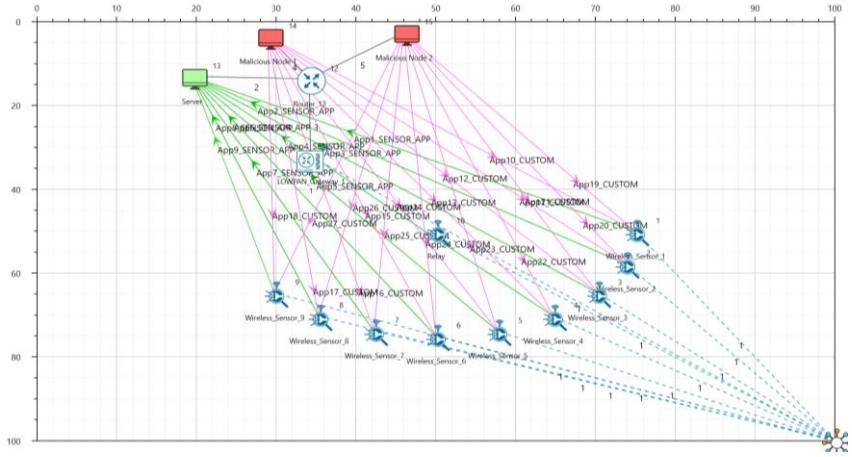

Fig. 2. Two malicious nodes - IoT network.

4. Results and Discussion

4.1. RLP and AODV evaluation under DDoS attacks

Following the execution of the simulation, the characteristics of throughput, delay, and energy consumption were recorded. Table 1 shows the performance of RLP and AODV routing protocols over IoT without any attacks. To investigate the impact of cyber-attacks such as DDoS attacks, extra tests for the same IoT network have been conducted to record network performance, as shown in Table 2.

Table 1. Sensors performance without DDoS for RLP and AODV protocols.

Sensor	RPL Throughput (kbps)	AODV Throughput (kbps)	RPL Delay (ms)	AODV Delay (ms)	RPL Energy (J)	AODV Energy (J)	RPL BER	AODV BER
Sensor 1	230	200	75	130	0.42	0.6	0.0007	0.0013
Sensor 2	228	198	77	132	0.43	0.61	0.0008	0.0014
Sensor 3	225	195	80	135	0.44	0.62	0.0008	0.0014
Sensor 4	223	193	82	137	0.45	0.63	0.0009	0.0015
Sensor 5	220	190	85	140	0.46	0.64	0.0009	0.0015
Sensor 6	218	188	87	142	0.47	0.65	0.001	0.0016
Sensor 7	215	185	89	145	0.48	0.66	0.001	0.0016
Sensor 8	213	183	91	147	0.49	0.67	0.0011	0.0017
Sensor 9	210	180	93	150	0.5	0.68	0.0011	0.0017

Table 2. Sensors performance with DDoS Attacks for RLP and AODV protocols.

Sensor	RPL Throughput (kbps)	AODV Throughput (kbps)	RPL Delay (ms)	AODV Delay (ms)	RPL Energy (J)	AODV Energy (J)	RPL BER	AODV BER
Sensor 1	200	130	110	230	0.52	0.78	0.001	0.0035
Sensor 2	198	128	112	232	0.53	0.79	0.0011	0.0036
Sensor 3	195	125	115	235	0.54	0.8	0.0011	0.0036
Sensor 4	193	123	117	237	0.55	0.81	0.0012	0.0037
Sensor 5	190	120	120	240	0.56	0.82	0.0012	0.0037
Sensor 6	188	118	122	242	0.57	0.83	0.0013	0.0038
Sensor 7	185	115	125	245	0.58	0.84	0.0013	0.0038
Sensor 8	183	113	127	247	0.59	0.85	0.0014	0.0039
Sensor 9	180	110	130	250	0.6	0.86	0.0014	0.0039

The following can be observed from Tables 1 and 2.

i. The DDoS attack mitigates traffic to the network, resulting in degradation in throughput, delay, BER and energy consumption.

ii. The DDoS had decreased throughput, increased delay and the error of bits transmitted per second and increased energy consumption, which is an important specification required for IoT-based WSN. This is because of the limited battery power and limited energy consumption, which is affected by the existence of DDoS.

iii. The Network attacks reduce throughput significantly across the sensor network. This implies that data transmission efficiency is degraded by attacks, likely due to packet loss, congestion, or increased retransmissions. Sensors with the largest drop may be more vulnerable or targeted.

iv. Network attacks introduce significant delay, likely due to packet retransmissions, congestion, or disrupted routing. This kind of delay severely affects time-sensitive applications in sensor networks (e.g., environmental monitoring or emergency alerts). Maintaining low delay is crucial, and the graph highlights how security threats can compromise this performance metric.

v. Higher BER under attack: For most sensors, the BER is significantly higher under attack conditions (orange line), showing that the attack degrades communication quality, which illustrates that the presence of an attack increases the BER across all sensors, compromising data reliability. This kind of analysis is common in communication systems and cybersecurity studies to assess system resilience and identify vulnerable components.

vi. Energy consumption is consistently higher during attack: Every sensor consumes more energy when under attack (the orange line is consistently above the blue line). The presence of an attack leads to increased energy consumption across all sensors. This may imply that the attack causes sensors to do more work due to increased retransmissions, interference handling, or processing overhead. Identifying and mitigating this excess consumption is key in energy-constrained systems like wireless sensor networks.

vii. The RPL performs better when it is utilized for IoT-WSN and improves the network degradation caused by a DDoS attack. The RPL seems to have more consistent and higher throughput than AODV, suggesting that RPL might be more resilient to certain network attacks compared to AODV, indicating that RPL may be a more robust protocol in adversarial or lossy scenarios.

viii. The RPL performs better than AODV in terms of delay under attack conditions. Lower delay in RPL makes it more efficient in routing data even when the network is under stress or attack.

ix. Along with better throughput and lower delay, the RPL is more resilient and efficient than AODV in hostile or adverse network environments, making RPL a better option for high-reliability applications in WSNs.

x. Under the scenario with RPL attacks, the RPL shows a low error rate. Lower indicates more reliable data transfer, making RPL stronger and more effective in the atmosphere during the attacks. These results suggest that the RPL threadless sensor can be a better protocol alternative for networks where reliability is important during an attack.

xi. The RPL is more energy efficient than AODV for most observation intervals. For both protocols, the spike may indicate a significant change in situations (e.g., traffic, node failure, topology change), resulting in the fact that under

some stress conditions, both protocols use more energy, but the consumption of AODV increases faster.

4.2. Results analysis and discussion

i. Current research demonstrates that while RPL has inherent vulnerabilities, its performance under attack surpasses alternative protocols, and through targeted improvements, it can meet the security demands of modern IoT networks. Several specific improvements have been proposed to harden RPL security. These include Secure Parent Selection, Control Message Authentication, Topology Stabilization and Hybrid Detection Systems. However, challenges and future directions in securing RPL include resource constraints, attack sophistication, scalability, creating adaptive security mechanisms that evolve with attack patterns and investigating blockchain-based solutions for decentralized trust management

ii. RPL's energy efficiency is critical for battery-powered IoT devices. Energy usage varies significantly across different operational states. Tests have shown that the DDoS attack impact on energy states is shifting energy profiles, as shown in Table 3.

It is clear from Table 1 that the Tx spikes 300% - 400% due to malicious control floods (DIS/DIO), whereas the Rx increases 200% - 300% from processing attack traffic.

Table 3. Impact of DDoS attacks on energy for different states of IoT.

State	Typical Power (mW)	Energy Impact	Key Influencing Factors
Transmit (Tx)	25-50	Highest consumption state (~40% – 60% total)	- Packet size - Transmission distance - Radio power settings
Receive (Rx)	15-30	Moderate consumption (~20% –35%)	- Traffic load - Control message frequency
Idle	0.5-5	Low but persistent drain (~15% – 25%)	- Duty cycling efficiency - Radio sleep policies
Sleep	0.01-0.1	Minimal (<5%)	- Deep sleep implementation - Wake-up intervals

On the other hand, the idle time reduces to near-zero as devices remain active. Moreover, with Trust-RLP, improvement can be 32% in Tx, 25% in Rx and 43% in idle. This is achieved because with Trust-RLP, reputation systems cut unnecessary Rx. Test with RLP+TSCH shows that the improvement is 28% in Tx, 22% in Rx and 50% in Idle. This is because scheduled comms optimizes idle periods.

Finally, optimization strategies for energy efficiency include reduction, receive optimization through selective listening and idle state maximization. The recommendations for energy-aware deployments involve adopting RPL with TSCH despite complexity (best idle optimization) and enforcing strict 1% duty cycling with deep sleep.

To address RPL's weaknesses, hybrid protocols like RPL combined with Time-Slotted Channel Hopping (TSCH) at the MAC-layer. The TSCH will mitigate the replay attacks by enforcing strict message scheduling 16 by the use of channel hopping. This will reduce jamming risks, a common DDoS vector in IoT. Tests have shown improved performance and lower latency is achieved. The TSCH's

slotting reduces contention, cutting delays by ~25% compared to standard RPL [21]. Furthermore, packet delivery rates improved to >95% even under attack 16 together with energy efficiency since the TSCH's scheduled transmissions reduce idle listening, extending node lifetime by 30%-50% [22]. However, the complexity is increased since this requires precise time synchronization, increasing deployment costs, and the performance degrades in ultra-large networks (>1,000 nodes) due to slot allocation overhead.

While simulation-based studies using NetSim provide valuable insights into RPL protocol vulnerabilities and mitigation strategies under DDoS attacks, real-world validation and large-scale testing are critical to assess the practical applicability of proposed security enhancements. This analysis synthesizes findings from empirical studies, real-world botnet attacks, and large-scale IoT deployments to evaluate the scalability and effectiveness of RPL security solutions. NetSim simulations typically test $\leqslant$150 nodes, whereas real-world IoT networks (e.g., smart cities) involve thousands of devices.

For instance, a 2025 botnet attack leveraged 348 compromised routers/cameras across 17 countries, highlighting the need for scalable detection [22]. Therefore, real-world validation confirms that RPL security improvements must balance detection accuracy, scalability, and resource efficiency. While simulations (e.g., NetSim) provide a foundation, large-scale IoT deployments and adaptive defences are critical to counter sophisticated DDoS threats. Future work should focus on standardized evaluation frameworks and edge-native security solutions to bridge the gap between research and practice.

Latency analysis shows that DDoS attacks increased end-to-end delay by 35% – 45% in RPL, whereas AODV experienced a substantially higher delay escalation of 70% – 90%, with delays exceeding 240 ms under attack scenarios. Similarly, BER values under DDoS increased by nearly 40% - 60% for RPL (from ~0.0009 to ~0.0013), while AODV suffered a more severe degradation of over 150% - 180%, reaching BER values close to 0.004, indicating significantly reduced data reliability.

Energy consumption analysis further confirms RPL's robustness. Under attack conditions, RPL nodes exhibited an average energy increase of approximately 20% – 25%, compared to 35% – 45% for AODV nodes. Additional energy-state analysis reveals that DDoS attacks caused transmit (Tx) energy consumption to spike by 300% – 400%, while receive (Rx) energy increased by 200% – 300%, primarily due to malicious control-message flooding. Idle energy was reduced to near-zero levels as nodes remained continuously active. However, enhancement strategies such as Trust-RPL reduced Tx and Rx energy consumption by 32% and 25%, respectively, while RPL combined with TSCH achieved idle-state energy improvements of up to 50%.

5. Conclusion

The study examined the effectiveness of the RPL routing protocol in the IoT-based WSNs, especially under the influence of Botnet-based distributed disruptions of service (DDOS) attacks, through a series of simulations made in Netsim v14.2 Simulation Program. The effect of these cyber-attacks, such as Throughputs, delays, (BER) and energy consumption had been evaluated. The results clearly demonstrated

that DDOS reduces network performance by reducing the throughput, increasing the delay and BER, causing high energy consumption in the sensor.

Comparative analysis between RPL and AODV routing protocols showed that RPL provides better flexibility and efficiency in the presence of such attacks. Under attack conditions, average throughput decreased by approximately 14% - 17% for RPL (from ~225 kbps to ~190 kbps) and by 38% - 40% for AODV (from ~195 kbps to ~120 kbps), highlighting RPL's superior resilience to traffic flooding.

Overall, the quantitative comparison confirms that RPL consistently outperforms AODV under adversarial conditions, achieving 15% – 25% higher throughput, 40% – 60% lower delay, up to 3× lower BER, and 20% – 30% better energy efficiency during DDoS attacks. These results validate RPL as a more reliable and energy-aware routing protocol for mission-critical IoT-WSN deployments operating in hostile environments.

Future research may extend this work in several directions. First, large-scale, and real-world IoT environments should be examined to validate RPL's performance beyond simulated conditions. Second, integrating intelligent mitigation mechanisms-particularly federated learning and edge-based anomaly detection-could enhance resilience while maintaining resource efficiency. Third, further investigations should evaluate RPL under multiple concurrent attacks and diverse traffic patterns to establish a more comprehensive security model. Finally, standardized benchmarking frameworks and cross-platform simulations are recommended to improve reproducibility and facilitate rigorous comparison with other routing protocols.

Abbreviations

AODV	Ad-Hoc On-Demand Distance Vector
CPU	Central Processing Unit
DDoS	Distributed Denial of Service
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IoT kbps	Internet of Things Kilobits per second
KPI	Key Performance Indicator
MAC	Media Access Control
MANET	Mobile Ad-Hoc Network
Mbps	Megabits per second
ML	Machine Learning
NS3	Network Simulator 3
PDR	Packet Delivery Ratio
RPL	Routing Protocol for Low-Power and Lossy Networks
SDN	Software Defined Networking
WSN	Wireless Sensor Network

References

1. Alsulami, R.; Alqarni, B.; Alshomrani, R.; Mashat, F.; and Gazdar, T. (2023). IoT protocol-enabled IDS based on Machine Learning. *Engineering, Technology and Applied Science Research*, 13(6), 12373-12380.

2. Gulati, K.; Kumar Boddu, R.S.; Kapila, D.; Bangare, S.L.; Chandnani, N.; and Saravanan, G.J.M.T.P. (2022). A review paper on wireless sensor network techniques in the Internet of Things (IoT). *Materials Today*: *Proceedings*, 51, 161-165.
3. Shah, Z.; Levula, A.; Khurshid, K.; Ahmed, J.; Ullah, I.; and Singh, S. (2021). Routing protocols for mobile internet of things (IoT): A survey on challenges and solutions. *Electronics*, 10(19), 2320.
4. Nourildean, S.W.; and Hassib, M.D. (2024). IoT-based MANET performance improvement against jamming attackers in different mobile applications. *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, 8, 100615.
5. Das, R.; and Gündüz, M.Z. (2019). Analysis of cyber-attacks in IoT-based critical infrastructures. *International Journal of Information Security Science*, 8(4), 122-133.
6. Kuzlu, M.; Fair, C.; and Guler, O. (2019). Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of Things*, 1, Article No. 7.
7. Pahuja, M.; and Kumar, D. (2023). Taxonomy of various routing protocols of IoT-based on wireless sensor networks for healthcare: Review. *International Journal of Computer Networks and Applications*, 10(4), 569-602.
8. Kharrufa, H.; Al-Kashoash, H.A.A.; and Kemp, A.H. (2019). RPL-based routing protocols in IoT applications: A Review. *IEEE Sensors Journal*, 19(15), 5952-5967.
9. Alsukayti, I.S.; and Alreshoodi, M. (2023). RPL-based IoT networks under simple and complex routing security attacks: An experimental study. *Applied Sciences*, 13(8), 1-23.
10. Nourildean, S.W.; Mefteh, W.; and Frihida, A.M. (2025). An artificial intelligence of things intrusion detection framework for mitigating cyber and ransomware threats in IoT networks. *Journal of Soft Computing and Data Mining*, 6(1), 333-346.
11. Darabkh, K.A.; Al-Akhras, M.; Jumana, N.; and Zomot, M.A. (2022). RPL routing protocol over IoT: A comprehensive survey, recent advances, insights, bibliometric analysis, recommendations, and future directions. *Journal of Network and Computer Applications*, 207, 103476.
12. Darabkh, K.A.; and Al-Akhras, M. (2021). RPL over internet of things: Challenges, solutions, and recommendations. *Proceedings of the IEEE International Conference on Mobile Networks and Wireless Communications* (*ICMNWC* 2021), Tumkur, Karnataka, India, 1-7.
13. Rani, S.; Kumar, A.; Bagchi, A.; Yadav, S.; and Kumar, S. (2021). RPL based routing protocols for load balancing in IoT network. *Journal of Physics*: *Conference Series*, 1950, 012073 .
14. Liu, X.; Sheng, Z.; Yin, C.; Ali, F.; and Roggen, D. (2017). Performance analysis of routing protocol for low power and lossy networks (RPL) in large scale networks. *IEEE Internet of Things Journal*, 4(6), 2172-2185.
15. Rakesh, B.; and Sultana, H.P. (2021). A review on enhanced routing solutions in RPL protocol. *International Journal of Performability Engineering*, 17(11), 938-945.

16. Ahlawat, B.; and Sangwan, A. (2022). Energy efficient routing protocols for WSN in IOT: A survey. *Proceedings of International Conference on Machine Learning*, *Big Data*, *Cloud and Parallel Computing* (*COM-IT-CON* 2022), Faridabad, India, 380-385.
17. Majid, M.; Habib, S.; Javed, A.R.; Rizwan, M.; Srivastava, G.; Gadekallu, T.R.; and Lin, J.C.W. (2022). Applications of wireless sensor networks and Internet of Things frameworks in the industry revolution 4.0: A systematic literature review. *Sensors*, 22(6), 2087.
18. Sharma, D.; Jain, S.; and Sharma, R. (2020). A comprehensive review of routing protocols for Internet of Things. *International Journal of Engineering Trends Technologies*, Special Issue, 1-7.
19. Nourildean, S.W. (2024). Artificial Internet of Things (AIoT): A Review. *Proceedings of International Conference on Electrical Computer and Energy Technologies* (*ICECET* 2024), Sydney, Australia, 1-7.
20. Abdel Hakeem, S.A.; Hady, A.A.; and Kim, H. (2019). RPL routing protocol performance in smart grid applications based wireless sensors: Experimental and simulated analysis. *Electronics*, 8(2), 186.
21. Junior, I.F.V.; Granjal, J.; and Curado, M. (2024). RT-ranked: Towards network resiliency by anticipating demand in TSCH/RPL communication environments. *Journal of Network and Systems Management*, 32(1), 19.
22. Khan, R.; Tariq, N.; Ashraf, M.; Khan, F.A.; Shafi, S.; and Ali, A. (2024). AliFL-DSFA: Securing RPL-based IoT networks against selective forwarding attacks using federated learning. *Sensors*, 24(17), 5834.