

Blackhole attacks in internet of things networks: a review

Noor Hisham Kamis¹, Warusia Yassin², Mohd Faizal Abdollah², Siti Fatimah Abdul Razak¹,
Sumendra Yogarayan¹

¹Faculty of Information Science and Technology, Multimedia University, Melaka, Malaysia

²Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia

Article Info

Article history:

Received Aug 16, 2022

Revised Nov 30, 2022

Accepted Jan 10, 2023

Keywords:

6LoWPAN

Blackhole

Internet of things

Routing protocol

Smart building automation

ABSTRACT

The internet of things (IoT) is one of data revolution area and is the following extraordinary mechanical jump after the internet. In terms of IoT, it is expected that electronic gadgets that are used on a regular basis would be connected to the current of the internet. IPv6 over low-power wireless personal area networks (6LoWPAN) is a one of IPv6 header pressure technology, and accordingly, it is vulnerable to attack. The IoT is a combination of devices with restricted resource assets like memory, battery power, and computational capability. To solve this, RPL or routing protocol for low power Lossy network is deploy by utilizing a distance vector scheme. One of denial of service (Dos) attack to RPL network is blackhole attack in which the assailant endeavors to become a parent by drawing in a critical volume of traffic to it and drop all packets. In this paper, we discuss research on numerous attacks and current protection methods, focusing on the blackhole attack. There is also discussion of challenge, open research issues and future perspectives in RPL security. Furthermore, research on blackhole attacks and specific detection technique proposed in the literature is also been presented.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Warusia Yassin

Faculty of Information and Communications Technology, University Teknikal Malaysia Melaka

Melaka, Malaysia

Email: s.m.warusia@utem.edu.my

1. INTRODUCTION

The internet of things (IoT) was authored, in the year 1999 and officially presented by the international telecommunication union (ITU) in year 2005 [1]. It is expected that IoT will grow to 75 billion in year 2025 [2]. The security worry for "Things" is caused by vulnerabilities acquainted due to negligent software design; this allow the access of malware to the device. low-power and lossy networks (LLNs) are form by massive quantity of embedded networking devices that share the same power, memory, and computational resources [3]. IoT are connected by embedded networking devices that have a predefined quantity of electricity, memory, and processing power. These are connected via a multiple type of interfaces and may be used for a multiple type of applications, including smart vehicle, health care, traffic monitoring and smart building [4]. The present routing methods in LLN are insufficient for dealing with the diverse communication in IoT. The internet engineering task force created the routing protocol (RPL) for LLNs also know as RPL to solved the LN's routing issues [5].

Moreover, IoT networks face critical asset limits (energy, memory, and registering), and their correspondence lines are intrinsically high-loss and low-throughput [6]. The traffic are not determined just as far as a point-to-point network. The gadgets regularly interface through highlight multipoint and multipoint-to-point protocol [7]. Current routing technique are insufficient to solve the needs of IoT communication.

Subsequently, a stack of standardised protocols created, with the IEEE 802.15.4 standard convention for the correspondence layers within WPANs, including 6LoWPAN, which characterise embodiment and header compression components for 802.15.4 and IPV6.

RPL has grown in popularity both in industry and academics [8] due to its capacity to provide effective routing among resource constraints IoT nodes and adaptability in adjusting to various quality of administration (QoS) support and network design [9]. RPL was planned to be a direct (yet useful) and utilitarian frameworks organization showing control of IoT networks which involves resource-constrained devices [5]. All these small intercommunicating gadgets are at present being utilized in an enormous display of IoT application organizations and used to complete any given task [10].

However, RPL-based networks are vulnerable to a massive security vulnerabilities due to their limited nature [11], [12]. The most dangerous attack in IoT implementation is the blackhole attack, which is regarded as one of the most dangerous and a point of entry for all other attacks [13]. Furthermore, it is also one of the lethal RPL attacks, initiated when a rogue node secretly loses all packets that it is intended to be transmitted [14], causing massive energy losses, congestion, and network overhead issues. RPL is also defenseless against blackhole assaults where the assaults can lead a topological separation for a sub network in a LLN. A pernicious inciting blackhole assault drops packet from node in its subtree which it ought to be process. Thus, the affected node actually segregates other nodes within the subtree from the remaining overall RPL traffic [7], [15].

A RPL-based network known as the 6LoWPAN network comprised of sensors and embedded devices that collect data and forward it to a root known as a IPv6 over low-power wireless personal area networks (6LoWPAN) border router (6LBR) for aggregation and processing [16]. Similar to other RPL-based networks, 6LoWPAN networks using the RPL protocol are also vulnerable to blackhole attacks which may involve a node or few cooperating nodes, making the attack more difficult to be detected [5]. When a blackhole assault is deployed by spreading multiple nodes in a network, it will create the distributed denial of services (DDoS) within the network [17]. Successfully concealed attacks may cause an attacked network to act very similarly to a healthy network and may disrupt communication and data flow between linked devices [18]. Increased delays in the delivery of the majority of packets to the sink, a decrease off overall packet delivery fraction, and increase of frequency of direction-oriented directed acyclic graph (DODAG) information object (DIO) messages exchanged between peers can all serve as primitive indicators, but do not constitute an exhaustive list of parameters sufficient to identify an attack. If the malicious node decreases its own packet sending behaviour to null, the packet latency and frequency of DIO messages may opera.

In this paper, related literature discussing blackhole attacks on IoT network are studied in terms of the experimental setup, limitations, detection and performance measures. This paper is organized in four main sections. Section 2 provides the preliminary studies which is IoT architecture, IPv6 over low-power wireless personal area networks (6LoWPAN), routing protocol for low-power and lossy networks (RPL), RPL based routing attack and blackhole attack. Section 3 discuss research that have been done related to blackhole attack in IoT network and section 4 concluded the paper

2. BACKGROUND

2.1. Internet of things (IoT) architecture

IoT allows immense quantity of extremely heterogeneous sensors or devices to be closely sensing the physical world and connect to the internet [19]. The architecture of IoT is composed of four main layers: the perception layer, the network layer, the support layer and the application layer [20], as shown in Table 1. IoT network layer stack is shown in Figure 1.

Table 1. IoT architecture

Layer	Technology
Application Layer	Smart House Application, Mobile Application
Support Layer	Data Analytics, Data Storage, Cloud Computing
Network Layer	Internet, Mobile Network, 2G/3G/4G Communication Network
Perception Layer	Wireless Sensor, GPS, RFID Reader

LoWPAN use IPv6 to comply the 127 bytes of frame size for low power sensor device [21]. The distribution of IPV6 packet is supported at data link later while fragmentation is done at the adaptation layer. Fragmentation overlapping and duplication can happen due to lack of authentication in 6LoWPAN. 6LoWPAN is standardized for the IPv6 adaptation layer, which contains data client and cross-layer which realize the usage if IPV6 addressing protocolover LLNs [7].

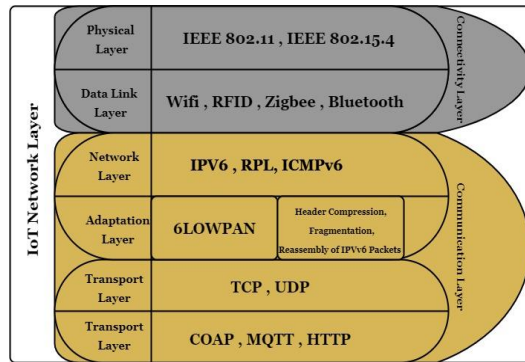


Figure 1. IoT network layer stack

Because of IoT characteristics like significant packet loss, resource constraints and slow network speed, cutting-edge routings like Adhoc open shortest path first (OSPF) are unsuitable for LLNs. To address this issue, an assortment of protocols has been devised. IEEE 802.15.4 PHY/MAC for the physical and data link layers, 6LoWPAN, RPL, and application layer constrained application protocol are among these conventions. The essential user datagram protocol layer is utilized for transport. RPL was standardized as RFC 6550 by IETF routing over low power and lossy networks (ROLL) group in year 2015 [5], [22].

2.2. IPv6 over low-power wireless personal area networks (6LoWPAN)

There are numerous communication protocols available for long and short range IoT connectivity, including 6LoWPAN, Wi-Fi, NB-IoT, WiMax, LTE-M, radio frequency identification (RFID), and Bluetooth [23]. 6LoWPAN protocol is a short-range protocol, low power and optimized for personal area networks (PAN) and it utilizes the idea of encapsulation technique and IPv6 header which is suitable for IoT devices [9]. 6LoWPAN advocates the inclusion of an adaptor layer in between the network and data connection levels in the IP stack. 6LoWPAN supports IPv6 packet fragmentation and defragmentation within IEEE 802.15.4 frames, enabling IPv6 header compression. In 6LoWPAN, packet transfer from a source node to a recipient node is depending on a wireless mesh network [24]. Contributions from the 6LoWPAN facilitated the establishment of an IP-based network of tiny devices and, as a result, the improvement of IoT applications. By specifying the routing of IPv6 packets in limited networks, 6LoWPAN facilitates the integration of IP-based infrastructures with WSNs. RPL is created as part of 6LoWPAN in order to efficiently manage the network layer activities during Internet connectivity.

2.3. Routing protocol for low-power and lossy networks (RPL)

LLNs have a critical limitation with the accessibility of assets at a node. They have restricted handling and memory capacities, and are controlled by batteries or a charging device. These nodes are associated through lossy associations that can keep up with their state at low data rates. In contrast with other routing protocols (e.g., Ad Hoc on-demand distance vector (AODV) and dynamic source routing (DSR)), RPL might give a quicker reaction time because of the route being accessible upon demand (e.g., continuously steering through the parent node). The results uncover that most of reactive routing protocols (for instance, AODV and DSR) experience the ill effects of unreasonably unique node versatility because of their low course intermingling and correspondence throughput. With RPL, it can moderately effectively adjust the rate at which a parent node is refreshed in light of the dynamism of the network [14].

The RPL topology, which is designed for use in distance vector routing, is built of one or more DODAGs that are each rooted at a DODAG root [25]. Each RPL network is composed of several RPL instances, each of which may include a DODAG [26]. The DODAG's root node may store and manage data, for example the version number. It frequently serves as an IPv6 border router (BR) and merges LLNs to another network or Internet from which instructions may be obtained or data gathered and processed. DODAG information object (DIO), DODAG information solicitation (DIS) and destination advertisement object (DAO) are types of control messages used in RPL [27]. Nodes function through RPL in positions, each containing an optimization objective that holds on the objective of the application, later functioning as the objective function (OF) [28], [29]. DIO's main function is to broadcast messages and involve in topology change [30].

Moreover, in RPL, every node selects a parent node based on a set of criteria, and this chosen parent acts as the node's gateway. A non-root node may join only one RPL instance, but may switch to another afterwards. Assuming a node decides to communicate a packet for which it doesn't have a routing table entry, it basically advances it to a favored parent who has a way to the objective or to its own parent for additional

transmission until the packet arrives at the last objective in the tree [31]. RPL sees way determination as significant and consequently applies an assortment of measurements to achieve this goal. Each node in the DODAG works out its position comparable to the DODAG root hub's (sink) position and the places of the other nodes. A node's position diminishes as it moves toward the DODAG root, however, increments as it approaches the leaf nodes. Storing and non-storing mode are supported in the RPL network and in source directing, data of objective is kept in each packet. This needs the DODAG root to keep a data set of data about each organization node. In non-storing mode away mode, in network routing table is remain to identify the destination of packet send by RPL nodes.

Ns has a critical limitation with accessibility of assets at node .They have restricted handling and memory capacities, and are controlled by batteries or a searching device.These nodes are associated through lossy associations that can keep up with their state at low data rates [32]. It is every now and again unreliable because to the variable packet delivery speeds. In contrasted with other routing protocol (e.g., AODV and DSR), RPL might give a quicker reaction time because of the route being accessible upon demand (e.g., continuously steering through the parent node). The results uncover that most of reactive routing protocol (for instance, AODV and DSR) experience the ill effects of unreasonably unique node versatility because of their low course intermingling and correspondence throughput. With RPL, it can alter it moderately effectively to adjust the rate at which parent node is refreshed in light of the dynamism of the network [14].

The RPL topology, which is designed for use in distance vector routing, is built of one or more DODAG that are each rooted at DODAG root [25]. It frequently serves as an IPv6 border router (BR) and merge LLN to the another network or Internet from which instructions may be obtained or data gathered processed. DODAG information object (DIO), DODAG information solicitation (DIS) and destination advertisement object (DAO) are type of control message used in RPL [27]. Nodes function through RPL in-positions, each contain of an optimization objective that hold on the objective of the application, later function as the objective function (OF) [28], [29]. DIO main function to broadcast message and involve in topology change [30].

Each RPL network is composed of several RPL instances, each of which may include a DODAG [26]. The DODAG's root node may store and manage data, example the version number. In RPL, every node selects a parent node based on a set of criteria, and this chosen parent acts as the node's gateway. A non-root node may join only one RPL instance, but may switch to another afterwards. Assuming a node decides to communicate a packet for which it doesn't have a routing table entry, it basically advances it to a favored parent who has a way to the objective or to its own parent for additional transmission until the packet arrives at the last objective in the tree [31]. RPL sees way determination as significant and consequently applies an assortment of measurements to achieve this goal. Each node in the DODAG works out its position comparable to the DODAG root hub's (sink) position and the places of the other nodes. A node's position diminishes as it moves toward the DODAG root, however, increments as it approaches the leaf nodes. Storing and non-storing mode are supported in the RPL network and in source directing, data of objective is kept in each packet. This needs the DODAG root to keep a data set of data about each organization node. In non-storing mode away mode, in network routing table is remain to identify the destination of packet send by RPL nodes.

2.4. Routing protocol for low-power and lossy networks (RPL) based routing attack

RPL has a few self-healing mechanisms and security protections in its standard version to ensure optimal network operation. Confidentiality and integrity of data are built-in components of the protection system [28]. In authenticated mode, they enter the network only as leaves before they get a second key from an authority before serving as routers. In the pre-installed modes ,with pre-shared keys the nodes will join the network. In unsecured mode makes use of link elements to safeguard exchanges [28].

The ROLL gives a comprehensive understanding of the RPL's security features [33]. These security assaults are classed using the security model's confidentiality, integrity, authentication, and availability criteria (C.I.A.A). Due to the complexity of RPL security, existing wired security techniques like as firewalls are inapplicable, and hence its nodes lack well-defined boundaries. Due to the lack of centralised management and node collaboration, cryptographic procedures cannot be employed to safeguard RPL routing's security. Additionally, because the nodes' equipment are not tamper-resistant, it easy to be expose and compromise the node encryption. Therefore, because of the alteration of their source code, the tested nodes will downgrade the output of the RPL network [34]. Figure 2 which is based on study by [35] categorised security attacks related to RPL as follows: i) attack on network resource, ii) attack on network topology, and iii) attack on network traffic.

RPL attacks also target network topology. It may be classified into two broad categories: suboptimization and isolation [36], [37]. In the instance of sub-optimization attacks, the attackers strive to degrade network efficiency by failing to generate the optimal pathways. Selective Forwarding attack, sinkhole attack, neighbour attack, wormhole attack, routing information reply attack, and worst parent attack are all currently undergoing sub optimization [38]. Additionally, topology attacks enable the isolation of a node or a

group of nodes, preventing it from contacting to their parents or the root. In the sub-optimization attack category, attackers attempt to degrade network efficiency by failing to generate optimum pathways.

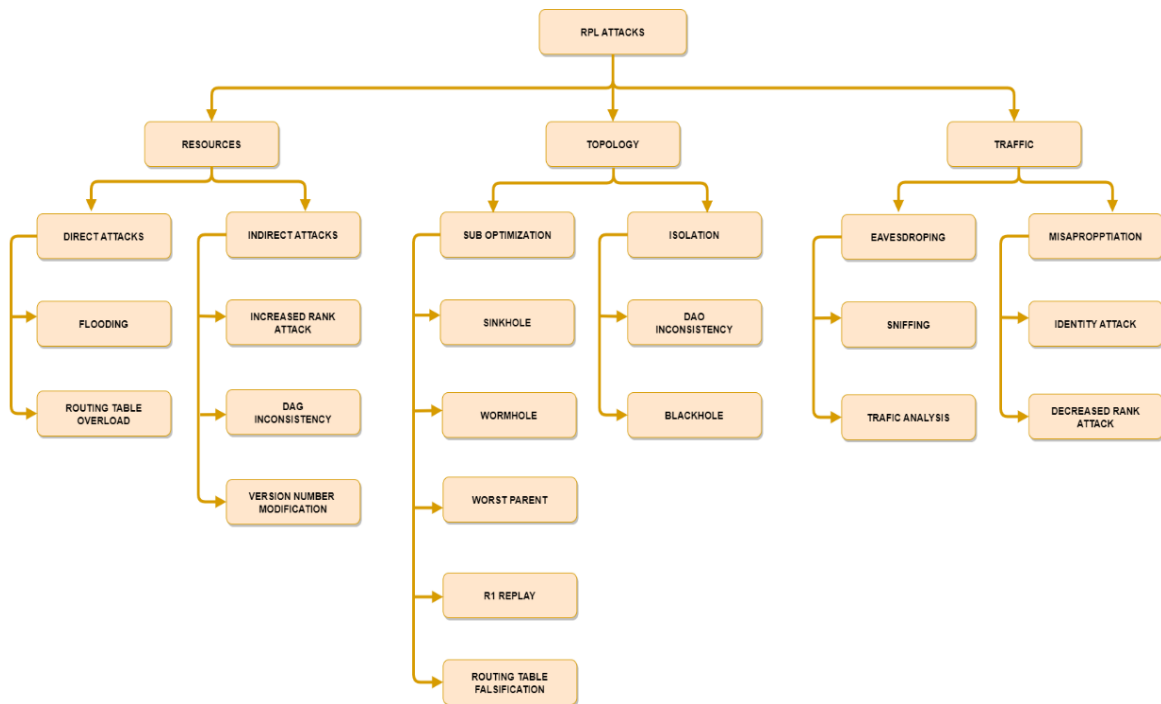


Figure 2. RPL attacks in IoT

2.5. Blackhole attack

Blackhole attacks carry out malicious actions such as creating a high rate of packet loss, packet overhead and depleting the IoT nodes' limited resources [13]. The stability of RPL network will be affected due to changes of node ranks and increase of network latency due to blackhole attack by the malicious node. Furthermore, the nodes' rankings are recalculated as a result of the rank change. The rank change triggers RPL's self-healing method for removing local routing loops. When the frequency of blackhole assaults rises, the local repair turn to ineffective, forcing DODAG root to initiate global repair. RPL network become unstable due to frequent change by the repair message [39]. Due to the protocol's dynamic nature by listening for manipulating request packets by an attacker. This is performed by sending back forged traffic with information about the destination's shortest path. As a result, a link is formed among the source node and blackhole node. In general the blackhole node controls every packet on that path [18]. Due to blackhole attack, retransmission rate is increase by child node and lead to DoS attack [40].

A blackhole assault or attack occurs when a hostile node secretly drops all packets that it is intended to send [8], [41]. It can result in severe traffic loss, loss of resource energy, and even end-to-end packet delay problems in a RPL network [42]. Each RPL node has an vertical default route point at root that includes list of preferred parents [43]. If a node start to send message to BR, the message is first sent through the node's parent. A rogue node presents itself as the best path throughout this procedure [44]. Nodes choose the rouge node as their preferred parent and begin forwarding data packets to it; the rogue node then exclude any data packets intended for the root in a discrete manner. This is called as single blackhole assault or attack.

Blackhole assault's primary purpose is to launch an internal denial of service attack against the child nodes by removing any information received from the other nodes. A malicious node that launches this attack is like a blackhole that absorbs everything and it also does not generate messages [45]. This behaviour, if done at the correct time and place will isolate other nodes in the downward route from the attacker node from the rest of the network [19]. It is worth noting that a node rank change in RPL routing indicates a calculation and arrangement of a child-node to new parent. A malicious node promoting themselves to nearest nodes as shortest routes with an apperance to influence other nodes in RPL while dropping the packets [39]. This fake routing table information reduces the authenticity of routing information in networks, affecting system efficiency and overall performance [46]. There are two sorts of blackhole assaults: single and colluding blackhole attacks which is have shown a great impact on IoT network topology [47], [48].

3. DISCUSSION

IoT is a rapidly growing area of research that linked the data analytics capabilities to strong merchandise, industrial, utility parts, and sensors over the Internet. To reform day-to-day work, play, and life, the IoT tries in creating a connected intelligent world. IoT gadgets incorporate various objects through the association of applications alongside remote empowering technologies [49]. Small sensor nodes are utilised to power batteries, compute, and solve equations. These devices are incapable of being encrypted using normal encryption techniques. Due to the tools' inherent nature and dependency on wireless media, they are liable to a number of attacks, for instance the blackhole attack. By accessing the network, hackers may simply attack these nodes. An advance research has been done as such far, yet more proficient work will be expected to forestall sensor networks from such attacks [13].

For instance, an intrusion detection named SVELTE [50] that concentrated on routing risks such as sinkholes, selective forwarding, and data that has been altered or fabricated has been suggested. SVELTE utilises end-to-end message security methods such as and datagram transport layer security and internet protocol (IP) Security. It adopts a hybrid, centralised and distributed method, with modules located in both border router and resource-constrained nodes. It is made up of three fundamental components, i.e., entry module, intrusion detection module and mini firewall module. 6LoWPAN mapper (6Mapper), collect and reconstructs data on the RPL network in the border router [50]. The intrusion detection module investigates the planned data and identifies intrusion. The mini firewall is expected to free nodes stress by separating undesired traffic before it enters the resource-constrained network. However, the results shows that a number of normal nodes was mistakenly identified as an attacking node which led to a high false alarm rate [51].

Ahmed and Ko [14], it takes a different strategy, identifying questionable nodes by studying the activity of neighbouring nodes to verify the suspected node is indeed a blackhole. Single and colluding blackhole attacks are mitigated by boosting the rate of malicious node detection and its associated packet delivery rate (PDR). The approach is composed of two steps. The first step refers to global verification process where a local decision made by a node that watches the behaviour of its neighbours. If a rogue node is detected, decision on whether it is a blackhole node or not is decided by the root. This strategy is claimed to be highly successful. However, when each node monitors the behaviour of its neighbours, the volume of memory overflow increased in these constrained devices. Moreover, since the root node is the one making the final decision, possibility of single point of failures will increase (if compromised) [14]. This is crucial since majority of the IoT devices have memory and processor limitations. Memory and processing power are scarce resources that are used to store routing information and queue data packets for transmission.

Djedjig *et al.* [52] is using a modified objective function dubbed the trust objective function. They create a separate hardware chip, named trusted platform module (TPM) which stores the MRTS or Metric-based RPL trustworthiness scheme used to calculate trust values. Additionally, the data are utilised to determine the presence of blackhole nodes. This approach demonstrates how to secure RPL networks regardless of the services supplied by trusted devices [52]. MRTS is a cooperative mechanism that enforce RPL node estimates information of its nearby nodes using both direct and indirect suggestions. One downside of MRTS is that it determines the ideal path for traffic routing only based on node metrics. If nodes are not self-centered, the fundamental standard for determining the parent will be energy. As a result, certain nodes near the chosen trustworthy path will use high usage of energy than others, that lead tp an unequal distribution of energy consumption. Additionally, because MRTS disregards connection data, it degrades packet delivery ratio. The researchers proposed many methods for determining the dependability of a route, including the projected number of retransmissions (ETX), the link quality level (LQL) and received signal strength (RSS).

Based on RPL network, [39] has established a trust value on IoT node which used to quantify trust while include determined trust values for routing purpose. This combines the required information to make the best routing choice while exclude rogue nodes. Additionally, this value determines the effective feedback based on the following two assumptions; i) a node runs in a promiscuous mode, letting it to listen in on the transmissions of neighbouring packets and ii) because each blackhole attacking node would eventually discard all route packets, successful feedback between nodes will necessarily reflect any node's blackhole character. To increase the RPL's isolation from blackhole attacks, the trust-based method is merged into a new protocol.

However, in this approach, the detection and verification processes will involve nodes in the RPL network [39]. Additionally, each node's energy level is not measured in this investigation. Strainer-based intrusion detection of blackholes in 6LoWPAN for the internet of things (SIEWE) created in [5], demonstrated a simple method for detecting and mitigating single blackholes. The suggested technique begins by constructing a list of suspects depending on behavior of nodes and network operation, suspicious node are confirmed by referring to their neighbouring nodes' behaviour. The last phase, the BR node will take care of the malicious node's global omission. To remove the node from the network, the strategy applies a blacklist mechanism. It is divided into two modules: a local one installed on each node and a global one deployed on each border router (BR). The conventional RPL protocol is compared to a suggested method that utilises the

PDR statistic in the research. The PDR value is the ratio of packets produced by network sensor nodes to packets received by the BR.

A paper proposing a root-based protection to protect from blackhole attacks [53]. It distinguishes malicious node by introducing a bundle misfortune identification method on the root node, which distributes data about the suspected node to the entire network. This method assessing the typical bundle misfortune rate, it mitigates misleading cautions then non-root node segregate malicious node by using their insight about blackhole node [53]. The proposed technique was found to have a prompt detection and isolation of a blackhole nodes with incurring a minimal energy cost. According to the research, this is one of the rare works in Cooja that incorporates blackhole assaults and their defensive tactics, as well as energy analysis [54]. Further developed defense arrangements, for example, identifying malicious nodes by dissecting their set of history, might be important to further develop framework execution. The research provides a detail security solution to solve blackhole issue [53].

In a study [55] introduced a novel detection approach for blackhole and greyhole assaults based on an existing lightweight heartbeat protocol (LHP). The approach provided clearly comprises of two parts: i) detection stage: during the discovery process, it is positioned at the root node and network node's IP and ii) detection stage: every k seconds, the detection phase is started, looking for a probable blackhole assault by referring the counter to a predetermined threshold. The counter will be reset if a node is defined as malicious. It will resend UDP queries to each node.

CPU and memory use, as well as transmission and reception rates (TX and RX) are used to evaluate detection approaches [55]. This experiment demonstrated an increase in all factors mentioned. Table 2 summarises the preceding discussion.

Table 2. Blackhole attack detection

Source	Country	Objectives	Experimental Setup	Limitation	Performance Measures
Raza <i>et al.</i> [50]	Sweden	SVELTE: Real-time intrusion detection in the Internet of Things	Contiki's network simulator Cooja	1. Placement of IDS in network 2. Timing irregularity in rank estimations 3. Incorrect topology creation at 6BR 4. High false positive rate (FPR).	1. Overhead at node-level and network level 2. Detection rate 3. Power Consumption
Ahmed and Ko [14]	Korea	Mitigation technique based on neighbourhood node behaviour	Contiki's network simulator Cooja	1. Single & colluding blackhole detection 2. Each node notices the way of behaving of its neighbors which builds the memory over-burden in these compelled devices	1.False Positive Rate 2.True Positive Rate 3.Packet Delivery Rate 4.End to End Delay
Djedjig <i>et al.</i> [52]	Algeria	Metric-based RPL Trustworthiness Scheme (MRTS)	Contiki's network simulator Cooja	1. Add on Trusted Platform Module chip 2. Additional expense for IoT network and perhaps infeasible for some IoT applications.	1. Average Packet Delivery Ratio 2. Average Throughput
Airehrour <i>et al.</i> [39]	New Zealand	Trust-based mechanism	Contiki's network simulator Cooja	1. Implementation it will involve every node for detection and verification process 2. Uses only packet forwarding value to calculate trust.	1. Average Throughput 2. Packet Loss Rate
Patel and Jiwala [5]	India	SIEWE (Strainer based Intrusion Detection of Blackhole in 6LoWPAN for the Internet of Things)	Contiki's network simulator Cooja	1.Single blackhole detection	1. Packet Delivery Ratio (PDR) metric
Jiang <i>et al.</i> [53]	United State of America	Root-based Defence Mechanism Against RPL Blackhole Attacks	Contiki's network simulator Cooja	1. Single blackhole detection	1. Packet Loss Rate 2.Energy Compsution 3. Network Throughput
Ribera <i>et al.</i> [55]	United Kingdom	Heartbeat-Based Detection	Contiki's network simulator Cooja	1. Single blackhole detection only 2. Increase in CPU usage, memory usage, TX and RX	1. Transmmission Rate 2. Reception Rate

4. CONCLUSION

6LoWPAN empowers devices with serious asset imperatives to interface with IPv6 organizations. To control the whole organization, RPL makes an upgraded destination-centered guided acyclic graph (DODAG) in view of the border router (BR). Blackhole attack or assault is defined as denial of service attacks within RPL network. An active area of DODAG, the attacker attempts to become a parent and draws a larger traffic to it and absorbs all the traffic and packets. The blackhole attack avoids the receipt of packets at BR. Blackhole attack influences the network's packet distribution ratio and ultimately compromises the overall network's reliability. The attack prevents packets from being received at the BR, degrades the network's packet distribution ratio, and eventually jeopardises the network's reliability. Blackhole attack known as single blackhole attack happens when an attacker node acts as a single node. When one attacker node work together with another malicious node to misguide the remaining nodes more efficiently, this is described as a colluding blackhole attack. Based on study on blackhole detection method, there is limitation in the technique for example false positive rate (FPR), increase of processing power bandwidth consumption and memory usage. There is also lack of detection methods related to colluding blackhole attack. To conclude, a blackhole attack in RPL network is a kind of denial of service attack, which is very difficult to detect and defend. When a and such blackhole attack happens, the entire performance of the network will be affected. The situation can be worst if multiple or colluding blackhole attacker nodes are present in the RPL network. This requires further study on blackhole detection that can detect single and and colluding blackhole in RPL networks.

ACKNOWLEDGEMENTS

The authors would like to thank everyone who has contributed to this research, either directly or indirectly. The authors would also like to thank the anonymous reviewers for their insightful feedback.

REFERENCES




- [1] T. A. Ahanger and A. Aljumah, "Internet of things: a comprehensive study of security issues and defense mechanisms," *IEEE Access*, vol. 7, pp. 11020–11028, 2019, doi: 10.1109/ACCESS.2018.2876939.
- [2] I. Butun, P. Osterberg, and H. Song, "Security of the internet of things: vulnerabilities, attacks, and countermeasures," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 1, pp. 616–644, 2020, doi: 10.1109/COMST.2019.2953364.
- [3] S. Naveen, "Study of IoT understanding IoT architecture, applications, issues and challenges," *International Journal of Advanced Networking & Applications (IJANA)*, pp. 477–482, 2016.
- [4] M. Abdullahi *et al.*, "Detecting cybersecurity attacks in internet of things using artificial intelligence methods: a systematic literature review," *Electronics (Switzerland)*, vol. 11, no. 2, 2022, doi: 10.3390/electronics11020198.
- [5] H. B. Patel and D. C. Jinwala, "Blackhole detection in 6LoWPAN based internet of things: an anomaly based approach," in *TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON)*, Oct. 2019, vol. 2019-October, pp. 947–954, doi: 10.1109/TENCON.2019.8929491.
- [6] S. Dange and M. Chatterjee, "IoT botnet: the largest threat to the IoT network," *Advances in Intelligent Systems and Computing*, vol. 1049, pp. 137–157, 2020, doi: 10.1007/978-981-15-0132-6_10.
- [7] W. Kassab and K. A. Darabkh, "A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations," *Journal of Network and Computer Applications*, vol. 163, p. 102663, Aug. 2020, doi: 10.1016/j.jnca.2020.102663.
- [8] A. Sanila, B. Mahapatra, and A. K. Turuk, "Performance evaluation of RPL protocol in a 6LoWPAN based smart home environment," in *2020 International Conference on Computer Science, Engineering and Applications (ICCSEA)*, Mar. 2020, pp. 1–6, doi: 10.1109/ICCSEA49143.2020.9132942.
- [9] A. Verma and V. Ranga, "Security of RPL Based 6LoWPAN Networks in the internet of things: a review," *IEEE Sensors Journal*, vol. 20, no. 11, pp. 5666–5690, 2020, doi: 10.1109/JSEN.2020.2973677.
- [10] K. Kaur and V. Gandhi, "Internet of things: a study on protocols, security challenges and healthcare applications," in *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, Apr. 2022, pp. 1206–1210, doi: 10.1109/ICACITE53722.2022.9823422.
- [11] Y. Benslimane and K. B. Ahmed, "Efficient end-to-end secure key management protocol for internet of things," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7, no. 6, p. 3622–3631, Dec. 2017, doi: 10.11591/ijece.v7i6.pp3622-3631.
- [12] J. Karande and S. Joshi, "DEDA: An algorithm for early detection of topology attacks in the internet of things," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 2, p. 1761, Apr. 2021, doi: 10.11591/ijece.v11i2.pp1761-1770.
- [13] S. Ali, M. A. Khan, J. Ahmad, A. W. Malik, and A. Ur Rehman, "Detection and prevention of black hole attacks in IoT and WSN," *2018 3rd International Conference on Fog and Mobile Edge Computing, FMEC 2018*, pp. 217–226, 2018, doi: 10.1109/FMEC.2018.8364068.
- [14] F. Ahmed and Y.-B. Ko, "Mitigation of black hole attacks in routing protocol for low power and lossy networks," *Security and Communication Networks*, vol. 9, no. 18, pp. 5143–5154, Dec. 2016, doi: 10.1002/sec.1684.
- [15] K. Avila, D. Jabba, and J. Gomez, "A nonlinear robust sliding mode controller with auxiliary dynamic system for the hovering flight of a tilt tri-rotor UAV," *Applied Sciences (Switzerland)*, vol. 10, no. 18, p. 6472, Sep. 2020, doi: 10.3390/APP10186472.
- [16] P. Suganya and P. R. Pradeep, "LNR-PP: Leaf node count and RSSI based parent prediction scheme to support QoS in presence of mobility in 6LoWPAN," *Computer Communications*, vol. 150, pp. 472–487, 2020, doi: 10.1016/j.comcom.2019.12.012.
- [17] R. Sahay, G. Geethakumari, B. Mitra, and V. Thejas, "Exponential smoothing based approach for detection of blackhole attacks in IoT," in *International Symposium on Advanced Networks and Telecommunication Systems, ANTS*, Dec. 2018, vol. 2018-December, pp. 1–6, doi: 10.1109/ANTS.2018.8710073.

- [18] A. Zrelli, C. Nakkach, and T. Ezzedine, "Cyber-security for IoT Applications based on ANN algorithm," in *2022 International Symposium on Networks, Computers and Communications, ISNCC 2022*, Jul. 2022, pp. 1–5, doi: 10.1109/ISNCC55209.2022.9851715.
- [19] M. Conti, P. Kaliyar, and C. Lal, "A robust multicast communication protocol for low power and lossy networks," *Journal of Network and Computer Applications*, vol. 164, p. 102675, Aug. 2020, doi: 10.1016/j.jnca.2020.102675.
- [20] B. Mostefa and G. Abdelkader, "A study of the security problems of wireless sensor networks into the context of the internet of things," in *Proceedings of the 2nd International Symposium on Computer Science and Intelligent Control*, Sep. 2018, pp. 1–6, doi: 10.1145/3284557.3284699.
- [21] S. M. Muzammal, R. K. Murugesan, and N. Z. Jhanjhi, "A comprehensive review on secure routing in internet of things: mitigation methods and trust-based approaches," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4186–4210, Mar. 2021, doi: 10.1109/JIOT.2020.3031162.
- [22] A. E. Hassani, A. Sahel, A. Badri, and E. M. Ilham, "Multi-constraints based RPL objective function with adaptive stability for high traffic IoT applications," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 22, no. 1, p. 407, Apr. 2021, doi: 10.11591/ijeecs.v22.i1.pp407-418.
- [23] T. Ladd and O. Groth, "The internet of things," *Economist (United Kingdom)*, vol. 411, no. 8964, pp. 376–380, 2015.
- [24] N. H. M. Yusoff, N. A. Zakaria, and A. H. Rosli, "Design and implementation of 6LoWPAN application: A performance assessment analysis," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 8, pp. 262–269, 2020, doi: 10.14569/IJACSA.2020.0110834.
- [25] M. Zhao, I. W.-H. Ho, and P. H. J. Chong, "An energy-efficient region-based RPL routing protocol for low-power and lossy networks," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 1319–1333, Dec. 2016, doi: 10.1109/JIOT.2016.2593438.
- [26] P. S. Nandhini and B. M. Mehtre, "Intrusion detection system based RPL attack detection techniques and countermeasures in IoT: a comparison," in *2019 International Conference on Communication and Electronics Systems (ICCES)*, Jul. 2019, pp. 666–672, doi: 10.1109/ICCES45898.2019.9002088.
- [27] N. H. M. Yusoff, N. A. Zakaria, A. Sikora, and J. Sebastian E., "6LoWPAN protocol in fixed environment: a performance assessment analysis," in *2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Sep. 2019, vol. 2, pp. 1142–1147, doi: 10.1109/IDAACS.2019.8924283.
- [28] P. O. Kamgueu, E. Nataf, and T. D. Ndie, "Survey on RPL enhancements: A focus on topology, security and mobility," *Computer Communications*, vol. 120, pp. 10–21, May 2018, doi: 10.1016/j.comcom.2018.02.011.
- [29] P. Satanasawapak and C. Khunboa, "The improvement of node mobility in RPL to increase transmission efficiency," *International Journal of Electrical and Computer Engineering*, vol. 9, no. 5, pp. 4238–4249, Oct. 2019, doi: 10.11591/ijece.v9i5.pp4238-4249.
- [30] A. Dhingra and V. Sindhu, "A study of RPL attacks and defense mechanisms in the internet of things network," in *2022 International Conference on Computing, Communication, Security and Intelligent Systems (IC3SIS)*, Jun. 2022, pp. 1–6, doi: 10.1109/IC3SIS4991.2022.9885473.
- [31] I. S. Alsukayti, "The support of multipath routing in IPv6-based internet of things," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 2, p. 2208, Apr. 2020, doi: 10.11591/ijece.v10i2.pp2208-2220.
- [32] H. Lamaazi and N. Benamar, "A comprehensive survey on enhancements and limitations of the RPL protocol: A focus on the objective function," *Ad Hoc Networks*, vol. 96, p. 102001, Jan. 2020, doi: 10.1016/j.adhoc.2019.102001.
- [33] J. V. V. Sobral, J. J. P. C. Rodrigues, R. A. L. Rabêlo, J. Al-Muhtadi, and V. Korotaev, "Routing protocols for low power and lossy networks in internet of things applications," *Sensors (Switzerland)*, vol. 19, no. 9, 2019, doi: 10.3390/s19092144.
- [34] Z. A. Almusaylim, A. Alhumam, and N. Z. Jhanjhi, "Proposing a secure RPL based internet of things routing protocol: a review," *Ad Hoc Networks*, vol. 101, 2020, doi: 10.1016/j.adhoc.2020.102096.
- [35] I. Dhyani, N. Goel, G. Sharma, and B. Mallick, "A reliable tactic for detecting black hole attack in vehicular Ad Hoc networks," in *Advances in Intelligent Systems and Computing*, vol. 553, 2017, pp. 333–343.
- [36] D. Sharma, I. Mishra, and S. Jain, "Impact factor: 4.295 A detailed classification of routing attacks against RPL in internet of things," *International Journal of Advance Research*, vol. 3, pp. 692–703, 2017, [Online]. Available: www.ijarlit.com.
- [37] A. Mayzaud, R. Badonnel, and I. Chrismet, "A taxonomy of attacks in RPL-based internet of things," *International Journal of Network Security*, vol. 18, no. 3, pp. 459–473, 2016.
- [38] S. R. Boualam, M. Ouaisa, M. Ouaisa, and A. Ezzouhairi, "Secure and efficient routing protocol for low-power and lossy networks for IoT networks," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 27, no. 1, p. 478, Jul. 2022, doi: 10.11591/ijeecs.v27.i1.pp478-487.
- [39] D. Airehrour, J. Gutierrez, and S. K. Ray, "Securing RPL routing protocol from blackhole attacks using a trust-based mechanism," in *2016 26th International Telecommunication Networks and Applications Conference (ITNAC)*, Dec. 2016, pp. 115–120, doi: 10.1109/ATNAC.2016.7878793.
- [40] P. P. Ioulianou, V. G. Vassilakis, and S. F. Shahandashti, "ML-based detection of rank and blackhole attacks in RPL networks," in *2022 13th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)*, Jul. 2022, pp. 338–343, doi: 10.1109/CSNDSP54353.2022.9908049.
- [41] A. Le, J. Loo, A. Lasebae, A. Vinel, Y. Chen, and M. Chai, "The impact of rank attack on network topology of routing protocol for low-power and lossy networks," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3685–3692, Oct. 2013, doi: 10.1109/JSEN.2013.2266399.
- [42] P. Dewal, G. S. Narula, V. Jain, and A. Baliyan, "Security attacks in wireless sensor networks: A survey," in *Advances in Intelligent Systems and Computing*, vol. 729, 2018, pp. 47–58.
- [43] S. R. Taghanaki, K. Jamshidi, and A. Bohloli, "DEEM: A decentralized and energy efficient method for detecting sinkhole attacks on the internet of things," *2019 9th International Conference on Computer and Knowledge Engineering, ICCKE 2019*, pp. 325–330, 2019, doi: 10.1109/ICCKE48569.2019.8965177.
- [44] V. Dani, "iBADS: An improved black-hole attack detection system using trust based weighted method," *Journal of Information Assurance & Security*, vol. 17, no. 3, pp. 91–99, 2022.
- [45] A. Mathur, T. Newe, and M. Rao, "Defence against black hole and selective forwarding attacks for medical WSNs in the IoT," *Sensors*, vol. 16, no. 1, p. 118, Jan. 2016, doi: 10.3390/s16010118.
- [46] S. Kaushik, K. Tripathi, R. Gupta, and P. Mahajan, "Performance analysis of AODV and SAODV routing protocol using SVM against black hole attack," in *2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM)*, Feb. 2022, pp. 455–459, doi: 10.1109/ICIPTM54933.2022.9754166.
- [47] L. A. K. Al Dulaimi, R. B. Ahmad, N. Yaakob, M. H. Yusoff, and M. Elshaikh, "Black hole attack behavioral analysis general network scalability," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 13, no. 2, p. 677, Feb. 2019, doi: 10.11591/ijeecs.v13.i2.pp677-682.




- [48] R. Ramachandran and M. Arun, "Sensitivity based optimal real power rescheduling for congestion management using black hole algorithm," *Australian Journal of Basic and Applied Sciences*, vol. 10, no. October, pp. 183–193, 2016.
- [49] Y. Bin Zikria, M. K. Afzal, F. Ishmanov, S. W. Kim, and H. Yu, "A survey on routing protocols supported by the Contiki Internet of things operating system," *Future Generation Computer Systems*, vol. 82, pp. 200–219, May 2018, doi: 10.1016/j.future.2017.12.045.
- [50] 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.
- [51] C. Panos, C. Ntantogian, S. Malliaros, and C. Xenakis, "Analyzing, quantifying, and detecting the blackhole attack in infrastructure-less networks," *Computer Networks*, vol. 113, pp. 94–110, Feb. 2017, doi: 10.1016/j.comnet.2016.12.006.
- [52] N. Djedjig, D. Tandjaoui, and F. Medjek, "Trust-based RPL for the internet of things," *Proceedings - IEEE Symposium on Computers and Communications*, vol. 2016-February, pp. 962–967, 2016, doi: 10.1109/ISCC.2015.7405638.
- [53] J. Jiang, Y. Liu, and B. Dezfouli, "A root-based defense mechanism against RPL blackhole attacks in internet of things networks," in *2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, Nov. 2018, pp. 1194–1199, doi: 10.23919/APSIPA.2018.8659504.
- [54] V. R. J. Manne and S. Sreekanth, "Detection and mitigation of RPL routing attacks in internet of things," in *2022 9th International Conference on Computing for Sustainable Global Development (INDIACom)*, Mar. 2022, pp. 481–485, doi: 10.23919/INDIACom54597.2022.9763140.
- [55] E. G. Ribera, B. M. Alvarez, C. Samuel, P. P. Ioulianou, and V. G. Vassilakis, "Heartbeat-based detection of blackhole and greyhole attacks in RPL networks," in *2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)*, Jul. 2020, pp. 1–6, doi: 10.1109/CSNDSP49049.2020.9249519.

BIOGRAPHIES OF AUTHORS






Ts. Noor Hisham Kamis    has been a Specialist 1 in the Faculty of Information Science and Technology at Multimedia University (MMU), Melaka, Malaysia, since 2016. He graduated from Universiti Teknologi Malaysia (UTM) with Bachelor's Degree Science Computer (Computer System) in 2002 and a Master's Degree Master in Computer Science (Internetworking Technology) from Universiti Teknikal Malaysia Melaka (UTEM) in 2012. He is currently pursuing his Doctor of Philosophy (PhD) in Information Technology at Universiti Teknikal Malaysia, Melaka (UTEM). His research interest includes the internet of things, cloud computing, computer security and server administration. He can be contacted at email: noorhisham.kamis@mmu.edu.my.







Dr. Warusia Yassin    is a senior lecturer in Department of Computer Systems and Communication at the Faculty of Information Technology and Communication, Universiti Teknikal Malaysia Melaka (UTeM). He is a member of information security, digital forensic and computer networking (INSFORNET) research group. He completes his Bachelor Degree in Computer Science (2008), Master of Science (2011) and PhD (2015) at Universiti Putra Malaysia (UPM). His research interests include security in computing, machine learning and cloud computing. He can be contacted at email: s.m.warusia@utem.edu.my.







Assoc. Prof. Dr. Mohd Faizal Abdollah    has been currently working as a Associate Professor under Department of Computer and Communication System, Faculty of Information and Communication Technology, University Technical Malaysia Melaka (UTeM). He received his first degree and Master degree from University Utara Malaysia and University Kebangsaan Malaysia. Dr Mohd Faizal obtained his Phd from University Technical Malaysia Melaka in Computer and Network Security. Previously, he worked as a MIS Executive at EON Berhad, Selangor and as a System Engineer at Multimedia University, Melaka for six years. His interest is mainly in network and wireless technology, network management and network and wireless security. He can be contacted at email: faizalabdollah@utem.edu.my.



Ts. Dr. Siti Fatimah Abdul Razak     has been a Lecturer at the Faculty of Information Science and Technology, Multimedia University, since 2005. She graduated from Multimedia University (MMU) with a Doctor of Philosophy (PhD) in Information Technology in 2018 and a Master of Information Technology (Science and System Management) in 2004. She is also an active member of the Centre for Intelligent Cloud Computing. Her research interest includes vehicle safety applications, the internet of things, rule mining, information systems development, and educational technology. She can be contacted at email: fatimah.razak@mmu.edu.my.



Sumendra Yogarayan     is currently a Lecturer in the Faculty of Information Science and Technology, Multimedia University (MMU), Melaka, Malaysia. He is an active member of the Centre for Intelligent Cloud Computing (CICC), Multimedia University (MMU). He graduated from Multimedia University (MMU) with a Master of Science (Information Technology) in 2019 and a Bachelor of Information Technology (Security Technology) in 2015. He is currently pursuing his Doctor of Philosophy (PhD) in Information Technology at Multimedia University (MMU). His research interest includes intelligent transportation systems, vehicular ad hoc networks, wireless communication and mesh networks. He can be contacted at email: sumendra@mmu.edu.my.