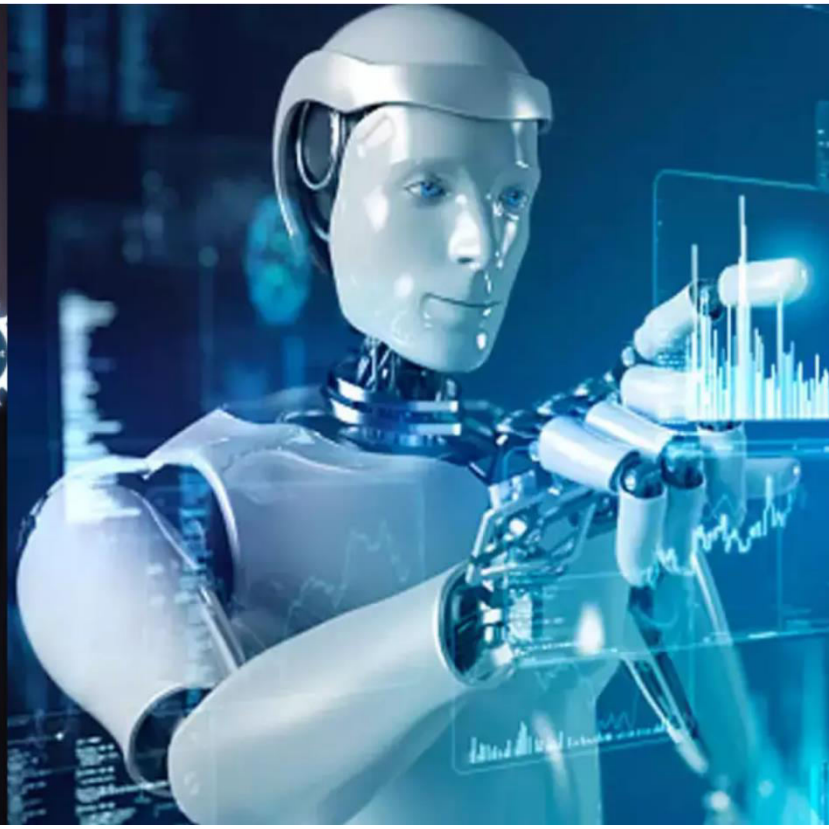
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 3, March 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403052|

An Examination of Black Hole Attacks in Internet of Things

Ms. C B Banupriya[1], Dr.S. Uma[2]

Ph.D. Research Scholar, Department of Computer Science, C.M.S College of Science and Commerce, Tamil Nadu, India[1]

Associate Professor, Department of Computer Science, Dr.N.G.P Arts and Science College, Tamil Nadu, India[2]

ABSTRACT: IOT described as Internet of things is a network which consist of physical objects and a compilation of sensors, software and other technologies meant for connecting and exchanging data with the systems on the internet or on the other devices. It is expected that the devices used in regular basis should be connected with the network. IPv6 header pressure technology, and accordingly, it is vulnerable to attack. The IOT is a collection of devices which are restricted in terms of memory and computational capability. To enhance this routing protocol for low power and lossy network is used which is distance vector routing protocol used for wireless networks. One of the problems faced by this RPL is Black hole attacks which affects the network traffic and indulge in loss of packet. The main aim of this paper were discussions on research of numerous attacks and current protection methods on the black hole attack. Discussions on various challenges and future of RPL security is also presented.

KEYWORDS: IPV6, RPL, IOT, 6LOWPAN

I.INTRODUCTION

The concept of the "Internet of things "is coined by Peter Lewis as" It is a collection of people, processes and technology with devices connected and sensors to which enables remote monitoring of devices, evaluation and manipulation of devices. To be in short" A period where things or objects are connected to the internet than people[26]. The engineering task force of the internet created RPL (Routing Protocol) for low power lossy networks. Moreover, IOT networks have asset limit and low throughput. The traffic are not determined just as far as a point-to-point network. RPL has grown in industry as well as academics due to its capacity to provide effective routing capability. However, rpl based networks are vulnerable to attacks because of their limited capabilities. Black hole attack is considered as one common type of arracks among all the attacks and pay way to all other attacks in network. It is an attack in which the rogue node loses all the packets which leads to energy loss. The assaults of black hole attacks lead to the topological separation for a subnet in a low power and lossy networks. 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 [1]. 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 to detected [2]. When a blackhole assault is deployed by spreading multiple nodes in a network, it will create the distributed denial of devices (DDoS) within the network [3]. 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 [4]. If the malicious node decreases its own packet sending behaviour to null, the packet latency and frequency may vary. This paper focuses on related literature discussions on blackhole attacks on IoT network, 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

II. IOT ARCHITECTURE

IOT allows large quantity of extremely immense sensors or devices to be closely sensing the physical world and connect to the internet [5]. The architecture of IoT consist of four main layers: the perception layer, the network layer, the support layer and the application layer [6], as shown in Table 1.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403052|

Table1: Iot Architecture

Layer	Technology
Application Layer	Smart home application, Mobile Application
Support Layer	DataStorage, Cloud Computing
Network Layer	Internet, Mobile network
Perception Layer	GPS,Wireless Sensors

Ipv6 packets are distributed at the data link layer while fragmentation is done at the adaptation layer. Authentication is not supported by the 6LowPAN.Adaptation layer contains data client and cross layer which helps to identify usage of IPV6 over Low power lossy networks**.**

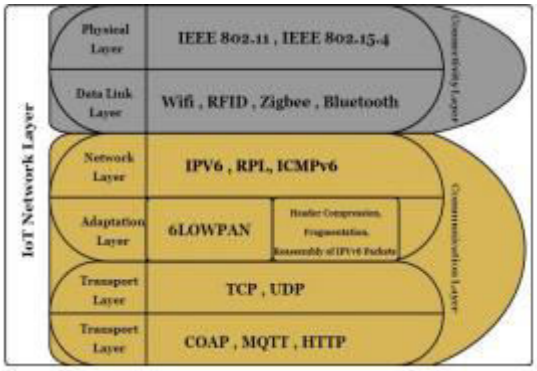


Figure 1:IOT network layer stack[6]

IoT characteristics such as packet loss, resource constraints and slow network speed, OSPF are unsuitable for LLNs. To address this issue, an assortment of protocols has been devised.6LoWPAN, RPL are among these conventions. Transport is done by user datagram protocol.

A. Ipv6 over Low-Power Wireless Personal Area Networks (6lowpan)

There are enormous 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 [7]. 6LoWPan protocol is a short-range protocol, low power and optimize used for personal area networks (PAN) Encapsulation technique is utilized and uses IPv6 header for IoT devices [8]. 6LoWPAN suggested the inclusion of an adaptation layer in between the network and data connection levels in the IP stack.6LoWPAN uses wireless mess network for transmission of packet from source to destination. It helps in the improvements of IoT Applications. During Internet Connectivity RPL is created to efficiently manage the activities of network layer.

B.Routing Protocol For Low-Power And Lossy Networks (RPL)

It is abbreviated as Routing Protocol for Low Power and Lossy Networks for different traffic networks. It is a routing protocol which is used by wireless networks. It holds communication of both one to one and many to many communications. It creates a destination oriented direct acyclic graph (DODAG) which has both root node and sink node. The objective function used here defines the method that finds the best optimized route among the sensor devices.

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 [9]. 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 [10]. Nodes function through RPL in-positions, each contain of an optimization

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403052|

objective that hold on the objective of the application, later function as the objective function (OF) [11]. DIO main function to broadcast message and involve in topology change [12].

C. Attacks Based On RPL

RPL lacks lot of security features which make them more prone to attacks, hence the existing technique such as firewall cannot be applied and it leads to lack of boundaries. It does not have central management and does not support node collaboration. Hence cryptographic methods are not supported .The source code can be easily altered which leads to the degradation in output. Security attacks on RPL related to the study[13] are as follows.(i)attack on network source (ii) attack on network topology (iii)attack on network traffic .Network topology is also affected by RPL .It may be classified into two types: suboptimization and isolation[13].In case of suboptimization the attackers degrade the efficiency of network which result in providing failure pathway .In case of isolation the child or sub node is prevented from contacting the root or parent node.

III.BLACKHOLE ATTACKS

Blackhole attacks performs malicious actions such as creating packet loss, packet overhead and wasting the IoT nodes' limited resources [13]. The malicious node of black hole attack decreases the stability of RPL by making changes in the rank of nodes and increase in network latency. 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 [13]. Due to the protocol's dynamic nature by listening for manipulating request packets by an attacker. This is performed by sending back forced information about the destination's shortest path. As a result, a link is formed among the source node and blackhole node. Due to blackhole attack, retransmission rate is increase by child node and lead to DoS attack [14]. A blackhole assault or attack occurs when a hostile node secretly drops all packets that it is initiated to send [14]. It can result in severe traffic loss, loss of resource energy, and packet delay problems in a RPL network [15]. Each RPL node has an vertical default route point at root that includes list of preferred parents [16]. 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 [17]. Nodes choose the rouge node as their preferred parent and begin forwarding data packets to it; the rogue node then separate 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 [18]. 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 [5]. A malicious node promoting themselves to nearest nodes as shortest routes with an apperance to influence other nodes in RPL while dropping the packets [19]. This fake routing table information reduces the authenticity of routing information in networks affecting system efficiency and overall performance [20]. There are two sorts of blackhole assaults: single and colluding blackhole attacks which provides a vast change in network topology.

IV.DISCUSSION

IoT is a rapid growing technology in today's world.To change day-to-day work, the IoT tries to create an intelligent world. IoT gadgets incorporate various objects through the association of applications alongside remote empowering technologies [20]. Small sensor nodes are utilised to power batteries, compute, and solve equations. Due to the tools' nature and dependency on wireless media, they are subjected to a number of attacks, for example the blackhole attack. By accessing the network, hackers may simply attack these nodes. Advance research has been done as such far, yet more proficient work will be expected to forestall sensor networks from such attacks [13].

Ahmed and Ko [21], uses questioning node to neighbouring node to verify whether it is a blackhole. Single and colluding blackhole attacks are harmed by increasing the rate of malicious node detection and packet delivery ratio. The approach is composed of two steps. The first step refers to global verification process where a node watches the behaviour of the neighbouring node. If a malicious node is detected, decision on whether it is a blackhole node or

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403052|

not is decided by the root. This strategy is tend to be successful by the overflow of memory increases which becomes the crucial part of IoT network which has certain limitations on its memory[14].

Djedjig *et al*. [22] used a different objective function called dubbed the trust objective function. They create a seperate hardware chip, named trusted platform module (TPM) which stores the trustworthiness of the nodes In addition the data in that are checked to notify the presence of blackhole nodes. This approach demonstrates how to secure RPL networks regardless of the services supplied by trusted devices [22]. If nodes are self centred the trustworthy nodes uses more energy which in turn decreases the efficiency of the network. The researchers proposed various methods to determine node dependability. Based on RPL network, [19] has proposed 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 which eliminates false nodes. A new protocol has been proposed to reduce the blackhole attack.

A paper proposing a root-based protection to protect from blackhole attacks [23]. It differentiates malicious node by introducing a group misfortune identification method on the root node, which distributes data about the suspected node to the entire network. This method works as follows the root node distributes information about suspicious node, the neighbouring Nonpromoted detection and isolation of a blackhole nodes with incurring a minimal energy cost.

In a study [23] introduced a novel detection approach for blackhole and grey hole assaults based on an existing lightweight heartbeat protocol (LHP). The approach provides two parts: detection stage: during the discovery process, it is positioned at the root node and network node's IP and detection stage: every k seconds, the detection phase is started, looking for a probable blackhole attack by referring the predefined threshold. The counter will be reset if a node is defined as false node. It will resend UDP queries to each node.

Table 2 Blackhole Attack Detection

S.no	Source	objectives	Limitation	Performance Measures
1	Raza et al.[25]	Realtime intrusion detection in internet of	High false positive rate,timing difference in rank estimation	Overhead, detection rate,Power Consumption
2	Ahmed and Ko[21]	Neighbour node behaviour based on	Single and colluding black hole attack Memory wastage	Packet delivery rate,True positive rate False positive rate End to end delay
3	Djedjig et al.[22]	Metric based RPL trustworthy Scheme	Addon trusted platform chip More expenses on network	Average PDR,Average Throughput
4	Airehrour et al.[19]	Trust based Mechanism	Involves every node for detection,Uses the value of packet	Average Throughput,Packet loss rate
5	Jiang et al.[23]	Root based mechanism	Uses single blackhole detection	Loss of packet,Energy Consumption
6	Ribera et al.[24]	Heartbeat based detection	Single black hole detection ,Increase in cpu usage	Rate of transmission

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403052|

V. CONCLUSION

Blackhole attack is described as denial of service attacks within RPL network. An active area of DODAG, the attacker aims to become a root and makes a larger traffic to it and absorbs all the traffic and packets. It is also called 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 are some limitations such as 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 this , a blackhole attack in RPL network is a kind of attack, which is very difficult to detect and defend. When the attak happens the entire performance of network will be affected. The situation is worst when colluding blackhole attacker nodes are present in the RPL network. This requires a deeper study on blackhole detection that can detect single and and colluding blackhole in RPL networks.

REFERENCES

[1] 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,”, vol. 150, pp. 472–487, 202

[2]Noor Hisan kamis,warusia Yassin”black hole attack in internet of things networks -A review” Indonesian Journal of Electrical Engineering and Computer Science Vol. 30, No. 2, May 2023, pp. 1080~1090 ISSN: 2502-4752, DOI: 10.11591/ijeecs.v30.i2.pp1080-10

[3] R. Sahay, G. Geethakumari, B. Mitra, and V. Thejas, “Exponential smoothing based approach for detection of blackhole attacks in IoT,” in Dec. 2018, vol. 2018-December, pp. 1–6, doi: 10.1109/ANTS.2018.8710073. ∟ ISSN: 2502-4752

[4] A. Zrelli, C. Nakkach, and T. Ezzedine, “Cyber-security for IoT Applications based on ANN algorithm,” in *2022 ISNCC 2022*, Jul. 2022, pp. 1–5, doi: 10.1109/ISNCC55209.2022.9851715.

[5] 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.

[6] B. Mostefa and G. Abdelkader, “A study of the security problems of wireless sensor networks into the context of the internet ofthings,” in Sep. 2018, pp. 1–6, doi: 10.1145/3284557.3284699.

[7] T. Ladd and O. Groth, “The internet of things,” *Economist (United Kingdom)*, vol. 411, no. 8964, pp. 376–380, 2015.

[8] 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.

[9] N. H. M. Yusoff, N. A. Zakaria, A. Sikora, and J. Sebastian E., “6LoWPAN protocol in fixed environment: a performance assessment analysis,” in *2019*, doi: 10.1109/IDAACS.2019.8924283.

[10] 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.

[11] A. Dhingra and V. Sindhu, “A study of RPL attacks and defense mechanisms in the internet of things network,” in *2022 (IC3SIS)*, Jun. 2022, pp. 1–6, doi: 10.1109/IC3SIS54991.2022.9885473

[12] J. Karande and S. Joshi, “DEDA: An algorithm for early detection of topology attacks in the internet of things,” *(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, FMEC 2018*, pp. 217–226, 2018, doi: 10.1109/FMEC.2018.836406

[14] P. P. Ioulianou, V. G. Vassilakis, and S. F. Shahandashti, “ML-based detection of rank and blackhole attacks in RPL networks,” in *2022*

[15] 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.

[16] S. R. Taghanaki, K. Jamshidi, and A. Bohlooli, “DEEM: A decentralized and energy efficient method for detecting sinkhole attacks on the internet of things,”, *ICCKE 2019*, pp. 325–330, 2019, doi: 10.1109/ICCKE48569.2019.8965177.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403052|

[17] 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.
[18] A. Mathur, T. Newe, and M. Rao, "Defence against black hole and selective forwarding attacks for medical WSNs in the*Computers and Communications*, vol. 2016-February, pp. 962–967, 2016, doi: 10.1109/ISCC.2015.7405638.
[19] D. Airehrour, J. Gutierrez, and S. K. Ray, "Securing RPL routing protocol from blackhole attacks using a trust-based mechanism," in *2016 (ITNAC)*, Dec. 2016,pp. 115–120, doi: 10.1109/ATNAC.2016.787879
[20] 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 (ICIPTM)*, Feb. 2022, pp. 455–459, doi: 10.1109/ICIPTM54933.2022.9754166.
[21] 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.
[22] N. Djedjig, D. Tandjaoui, and F. Medjek, "Trust-based RPL for the internet of things," *Proceedings - IEEE Symposium on on Computers and Communications*, vol. 2016-February, pp. 962–967, 2016, doi: 10.1109/ISCC.2015.7405638.
[23] 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:
[24] 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 *(CSNDSP)*, Jul. 2020, pp. 1–6, doi: 10.1109/CSNDSP49049.2020.9249519
[25] 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

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details