International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7027
Article Received: 06 April 2023 Revised: 28 May 2023 Accepted: 09 June 2023

A Novel Detection Method for Grey Hole Attack in RPL

Atena Shiranzaei[1], Farhad Khoshbakht[2]
[1]Department of Computer Engineering (Khash),
University of Sistan and Baluchestan,
Zahedan, IRAN
ashiranzaei@eng.usb.ac.ir
[2]Department of Computer Science,
Jamia Millia Islamia University,
New Delhi-110025, INDIA
f.khoshbakht@gmail.com

Abstract— The Internet of Things (IoT) is a type of network that involves the Internet and things. This network consists of constrained devices that are connected through an IP protocol. In the IoT, a network with constrained devices is called 6LowPAN. RPL is a routing protocol to address the constraints and specific properties of these networks; though RPL puts the networks at risk through a large variety of attacks. The urgent need to develop secure routing solutions is required. In this paper, we investigated grey hole attacks and presented a detection method to identify and isolate the malicious node. The experiments show the proposed detection method improves PDR, Throughput and reduces PLR and E2ED in comparison with other scenarios.

Keywords- IoT; 6LowPAN; RPL; Grey Hole Attack; IoT Security; Selective Forwarding Attack.

I. INTRODUCTION

The IoT is a new paradigm growing in the context of the pervasive and global networks that provide a system to monitor and control the physical world via collecting, processing, and analyzing the data which has been generated by IoT sensor devices. Efforts to make a connection between the Internet and physical objects through IPv6 protocols [1] to form the IoT are underway. The IP connectivity in this type of network mainly relies on 6LowPAN [2] and Routing Protocol for Low-Power and Lossy Networks (RPL) [3]. 6LowPAN is a Wireless Sensor Network (WSN). This network uses IEEE 802.15.4 as a data link and physical layer protocol, and a compressed IPv6 protocol for networking.

RPL is a standardized routing protocol for IoT, which is fundamentally designed for low-power and lossy networks (LLN). This protocol makes a destination-oriented directed acyclic graph (DODAG) among the nodes in 6LowPAN. The DODAG is anchored at the border router network. Every node has to select the best parent to route the packets to the border router. In a DODAG, each node has a rank that shows the relative position of one node to other nodes. Ranks increase from the root of DODAG towards the nodes and decrease as they go up towards the DODAG root.

The IoT provides unique features, which makes vulnerabilities in the network so that it is essential to have some security approaches to protect against various attacks. The features that must be considered to have a secure network in IoT are [4] Availability, Authentication, Confidentiality, Integrity, non-repudiation, data freshness, robustness, and survivability. Availability is a process to provide network services to all nodes at all layers of a network when ensuring survivability. Survivability and robustness are like a guarantee that makes sure the network does not go down even when a collection of nodes is compromised because of security attacks. Confidentiality makes sure the information is not divulged by a wrong source. Integrity assures that the received data by the destination has not been changed. Non-repudiation includes a node as a source having the data sent until getting acknowledged receipt from a receiving node. The rest of this article is presented as follows: section 2 presented the related works. Section 3 gives preliminaries. Section 4 describes the proposed detection method. Section 5 presents the results and discussion. Finally, we presented the conclusion in section 6.

II. RELATED WORKS

In [5] the authors implemented a grey hole attack and presented an intrusion detection system based on heartbeat protocol. This protocol identifies that alive node and discovers node failure or jamming attack.

Authors in [6] have proposed a technique to mitigate blackhole attacks. The proposed technique is based on a global verification process related to local decisions constructed in an LLN with various nodes. In this technique, there is a local-decision making process made at the nodes. This process comprises the behavior of the node's neighbors to identify suspicious activity, then labels the nodes as suspicious or reliable nodes. Finally, the global verification recognizes whether there is a blackhole attack between the suspicious nodes.

Hung-Min Sun et al [7] have designed a multi-dataflow topology for wireless sensor networks to protect against grey hole attacks. There are no techniques to detect or mitigate grey hole attack. To provision of multi-dataflow paths will make in huge network overhead.

Shahid Raza et al [8] have presented an intrusion detection system for some attacks like grey hole attacks. This intrusion detection system uses a 6Mapper to reconstruct the RPL topology at the border router. This system can identify the attacker through 6Mapper. Although, if the intrusion node identifies the traffic used by 6Mapper, it performs as a normal node. Thus, the system cannot identify grey hole attack.

In [9], Mehetre et al proposed a secure routing algorithm. This algorithm includes a two-stage security model, and a twin assurance method to protect the information packets in a wireless sensor network by choosing a node. The methods depend on Active Trust to secure such attacks like a grey hole attack through the routing. Thus, the proposed algorithm identifies the trusted path and create the safe routing.

The authors in [10] proposed a routing algorithm based on the delivery of forged packets to enhance the detection rate and remove the malicious node. In the presented algorithm, the malicious node was recognized via sending forged RREQ and RREP packets, the nodes were deleted from the routing tables. The proposed approach was able to recognize the secure route detecting the malicious nodes.

Authors in [11] presented the JDICA method to assess blackhole attack. This method detected the attack by checking the physiological information gathered from biomedical sensors. According to the behaviors of the nodes, attacks were detected. The results show JDICA approach detects blackhole attack with extreme accuracy and isolate the malicious node in the network. Moreover, it improves PDR and reduces the delay.

III. PRELIMINARIES

A. 6LowPAN

The IEEE 802.15.4 protocol is used as the PHY at the MAC layer protocol on a smart object network. Although, the Wireless Personal Area Network (WPAN) does not support IPv6 over IEEE 802.15.4. To overcome this limitation, the Internet Engineering Task Force (IETF) created the 6LowPAN standard [2]. This standard supports IPv6 over IEEE 802.15.4 LowPAN networks. In the fact, 6LowPAN integrates wireless sensor networks (WSN) and IP-based infrastructures by defining the way IPv6 packets should be transmitted in such constrained networks like 802.15.4 networks. For getting this purpose, the 6LowPAN standard has provided the mechanism which is header compression, such as next header compression for the IPv6 extension headers, the IP header compression for the IPv6 header, also the user datagram protocol header. The Maximum Transmission Unit (MTU) of the link layer in 6LoWPAN is 127 bytes, which is the most limitation as implementing the standard IPv6 headers over the low-power Wireless Personal Area Networks (LoWPAN) would result in a small payload for higher layer protocols. Due to this problem, 6LoWPAN can fragment and reassemble a datagram. This type of network is connected to the Internet through a gateway which is known as 6LoWPAN Border Router (6BR). This router is analogous to a WSN sink. The 6BR is responsible to execute compression, decompression, fragmentation, and assembly of the IPv6 datagram. Fig. 1 shows the architecture of the 6LoWPAN.

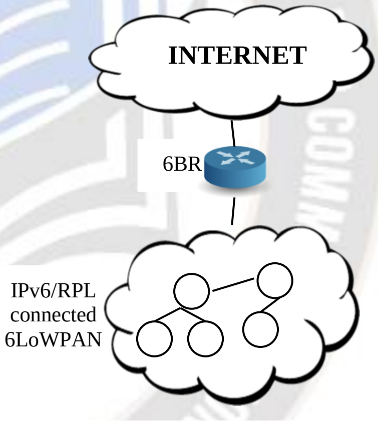

Figure 1. The Architecture of the 6LoWPAN Network

B. RPL

RPL is a standardized routing protocol for IoT and is mainly designed for 6LoWPAN [3]. RPL is placed at the network layer to make the appropriate routes and distribute the information of the route to other nodes. This routing protocol is a Distance Vector IPv6 routing protocol for LLNs, so the route information of the network is organized as a collection of DODAG. Each DODAG roughly includes a sink node and sensor nodes. In the RPL, the route selection depends on two things, the DODAG link, and the information cost.

The procedure of a routing topology is that each node selects the parent which has the best path toward the sink. There are three types of control messages in RPL. These messages are used for forming and managing the routing of information over the network. The messages are [12]:

- *DODAG information object (DIO):* DIO utilizes and updates the topology of a network.
- *DODAG Advertisement Object (DAO):* DAO broadcasts and advertises the information of the destination upward to update the route of the network.
- *DODAG Information Solicitation (DIS):* DIS is sent when a new node demands to join the network and waits for the topology information.

C. Grey Hole Attack

The first persons who described the grey hole attack are Karlof and Wanger [13]. This attack is also known as the Selective Forwarding Attack. In a grey hole attack, the affected nodes throw or selectively forward some packets which have been sent by a specific node or a group of nodes. This makes DoS attack. It might even happen to the route of some messages. grey hole attack can acknowledge the reception of data that is not transmitted by a malicious node. The worst case of this attack occurs until the compromised node blocks all packets, such as in a blackhole attack. The combination of this attack with another attack causes severer consequences. Delays in passing the packets and making confusion in the route of information are other variances of grey hole attacks.

IV. PROPOSED WORK

In this part, we described our proposed detection method to discover and isolate grey hole attacks. This method uses Lightweight Heartbeat Protocol [14] with UDP-based heartbeat and ICMPv6 messages. We decided to use UDP messages because they would be most probably dropped by the malicious node affected by a grey hole attack. To achieve the best performance, IPsec and ESP are enabled as well so the malicious node is unable to individualize between ICMPv6 traffic and normal traffic as they are encrypted. This method includes two phases: the detection phase and the isolation phase. The first phase identifies the malicious node. The second phase isolates the malicious node. These phases are as follows:

Phase 1: The method sends a UDP request to all the nodes available in the network every 15 seconds and increases the counter of each node (C_i) by 1. While it receives the UDP reply, the counter of the node will be set to 0. If the period of a UDP reply expires, it compares C_i with the trust threshold (C_{th}), if C_i is more than C_{th}, the method identifies the attack, updates the blacklist, and notifies the children by ICMPv6 message. Additionally, the root broadcast the blacklist over the network to inform all the nodes. The pseudo-code is given in Algorithm 1.

Algorithm 1: Detection of a malicious node

```
Send UDP request to all the nodes
Foreach node ∈ list.node do
    $C_i$=Ci+1;
While (received UDP reply) do
    $C_i$=0
While (time period expires) do
If ($C_i$>$C_{th}$) then
    Raise alarm for attack
    Blacklist.add(node.currentparent)
    Broadcast(blacklist)
    Preferred Parent=RplSelectParent(dag)
    Notify all the nodes
```

Phase 2: After attack identification, the affected nodes will be notified and re-select a parent. Moreover, every node in the network checks the blacklist before selecting the best parent as the next route to avoid choosing a malicious node. The pseudo-code is given in Algorithm 2.

Algorithm 2: Isolation the attacker

```
If (blacklist not empty) then
    While (choosing the best parent) do
        If (blacklist not empty && Parent[id]==Blacklist[id]) do
            Remove Parentid
            PreferredParent=RplSelectParent(dag)
```

V. RESULTS AND DISCUSSION

A. Simulation Setup

In this section, the proposed method was designed and implemented in the Cooja simulator [15], which is a network software of Contiki [16]. In this simulation, one hundred nodes are randomly deployed, including a root node, 79 legitimate non-root nodes, and 20 malicious nodes. MRHOF is used as the objective function. The simulation parameters are illustrated in Table 1.

TABLE I. SIMULATION PARAMETERS IN THE NETWORK

S.N	Parameters	Value
1	Operating System	Contiki-NG
2	Routing protocol	RPL
3	Network size	600×200 m^2
4	Type of motes	Z1
5	Number of nodes	100
6	TX/RX ratio	100 × 100 m
7	Type of attack	Grey Hole Attack
8	Simulation time	30 m

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7027
***Article Received**: 06 April 2023 **Revised:** 28 May 2023 **Accepted:** 09 June 2023*

To evaluate the proposed method, the authors compared the performance of the proposed method with normal network scenario and grey hole attack scenarios.

B. Performance Evaluation

In this part, the following metrics were used to analyze the performance of the proposed method.

Packet Delivery Ratio (PDR): PDR is one of the important parameters to analyze the performance of the proposed methods in any network. PDR can be obtained from the total number of packets received by the destination to the total number of packets sent by the sources. The equation (1) of the PDR is shown below.

$$\text{PDR}=\frac{\sum_{i=1}^{n} ReceivedPackets}{\sum_{i=1}^{n} SentPackets}*100 \qquad (1)$$

N stands for the total amount of nodes.

Packet Loss Ratio (PLR): PLR is the total number of packets that has not been received by the destination to the total number of packets sent by the source. Equation (2) shows the PLR.

$$\text{PLR}=\frac{SentPackets - ReceivedPackets}{SentPackets} * 100 \qquad (2)$$

Throughput: Throughput is the total number of bits transferred successfully from one place to another place in bps, Mbps, or Gbps. Equation (3) shows the Throughput.

$$\text{Throughput}=\text{Pkt}_s*\frac{ReceivedPackets - NotReceivedPackets}{SentPackets} \qquad (3)$$

End-to-End Delay (E2ED): E2ED is the time spent to route a packet from a source to a destination. Equation (4) illustrates E2ED.

$$\text{E2ED}=\frac{1}{n}\sum_{i=1}^{n}(ReceivedTime - SentTime)*1000(\text{ms}) \qquad (4)$$

C. Packet Delivery Ratio analysis

The packet Delivery Ratio (PDR) is the packet received ratio at the destination to packets sent by the source node. As it is shown in Fig. 2, the PDR under a normal network, under a grey hole attack and under the proposed method are 0.8, 0.2 ad 0.6, respectively. As the result, the proposed method improves the PDR as compared to the case of grey hole attacks.

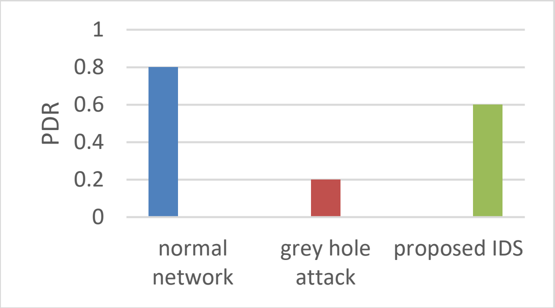

Figure 2. Comparison of PDR

D. Packet Loss Ratio analysis

PLR is the number of lost packets per unit of time. Fig. 3 shows the result of PLR under a normal network, under grey hole attack and the proposed method are 0.004, 0.014, 0.008, respectively. Hence, the proposed method reduces PLR in pps (packet per second) as compared to the case of grey hole attack scenarios.

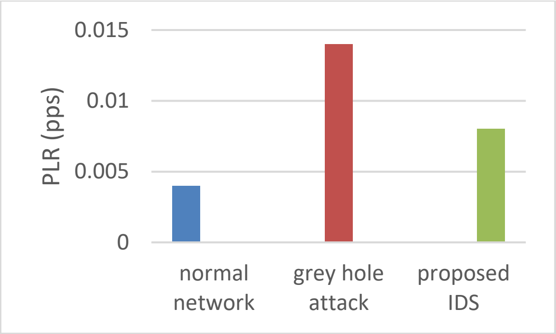

Figure 3. Comparison of PLR

E. Throughput analysis

Throughput is formulated as the number of bits sent per unit of time. Fig. 4 Displays the results of throughput under a normal network, under grey hole attack, and the proposed methods are 11.9, 2, and 10.1. It is observed that throughput is improved under the proposed method as compared to the case of grey hole attack scenarios.

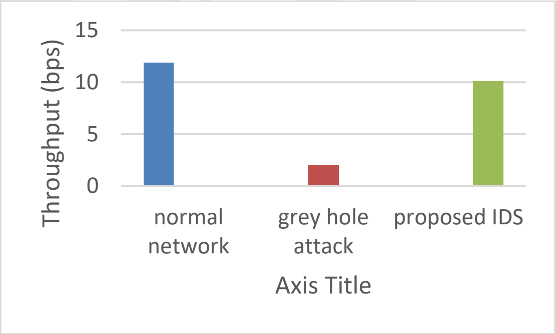

Figure 4. Comparison of Throughput

F. End-to-End Delay Analysis

The E2ED is the average time spent in delivering packets from source to destination. Fig. 5 Represents the E2ED in seconds under a normal network, under a grey hole attack, and under proposed methods are 0.7, 0.8, and 0.74. Therefore, the E2ED is reduced as compared to the case of a grey hole attack.

DOI: https://doi.org/10.17762/ijritcc.v11i7s.7027
***Article Received**: 06 April 2023 **Revised:** 28 May 2023 **Accepted:** 09 June 2023*

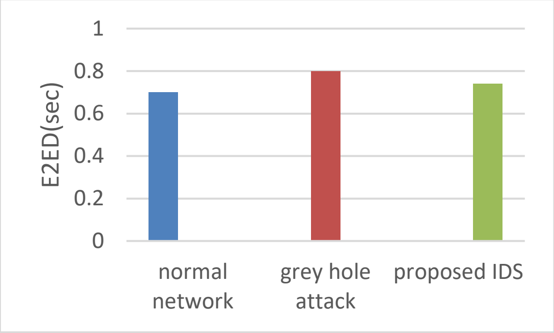

Figure 5. Comparison of E2ED

G. *Detection Rate and False Positive Rate Analysis*

Other essential metrics to evaluate the performance are Detection Rate (DR) and False Positive Rate (FPR). DR is the number of recognized attackers to the total number, and its equation is as below.

$$DR=TP/TP+FN * 100 \qquad (5)$$

TP (True Positive) is the number of attackers truly detected. FN (False Negative) is the total number of not detected malicious nodes.

FPR is the number of nodes falsely identified as attacker nodes. Equation (6) calculated FPR:

$$FPR=FP/TN+FP *100 \qquad (6)$$

Where FP (False Positive) is the number of normal nodes falsely detected as a malicious node. TN (True Negative) is the number of normal nodes identified as normal nodes. The result shows in a total of 20 attackers and 79 normal nodes. DR and FPR are 85% and 6%.

VI. CONCLUSION

The goal of this paper was to introduce a grey hole attack and implement a security approach to detect and isolate the grey hole attack in RPL. Here, we developed a detection method consisting of two stages: Detection of attacks and isolation of malicious nodes. At first, for detecting the attack, UDP requests were broadcasted, and beyond investigated UDP threshold with UDP responses. Later, if the malicious node exists, the notification and isolation were done. After performance evaluation, the proposed method achieves 0.6 PDR and 10.1 Throughput which improves the performance as compared with the grey hole attack scenario. The method achieves 0.008 PLR and 0.74 which is reduced as compared with the grey hole attack scenario. Furthermore, it reaches an 85% detection rate and 6% FPR. Therefore, it proved that the detection method was efficient to detect and isolate grey hole attacks in RPL.

REFERENCES

[1] A. Shiranzaei and R. Z. & Khan, "Internet protocol versions—A review," in In 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), 2015.

[2] J. Hui and P. Thubert, Compression format for IPv6 datagrams over IEEE 802.15. 4-based networks (No. rfc6282), 2011.

[3] J. Jiang and Y. Liu, "Secure IoT routing: Selective forwarding attacks and trust-based defenses in RPL network," arXiv, 2022.

[4] A. Shiranzaei and R. Z. Khan, "IPv6 Security Issues – A Systematic Review," in In 50th Golden Jubilee Annual Convention On Digital Life, 2015.

[5] M. Marjanović, A. Antonić and I. P. Žarko, "Edge computing architecture for mobile crowdsensing," Ieee access, 2018.

[6] K. K. R. Choo, O. F. Rana and M. Rajarajan, "Cloud security engineering: Theory, practice and future research," IEEE Transactions on Cloud Computing, 2017.

[7] Dr. V. Arthi. (2020). A Novel Channel Estimation Technique in MIMO-OFDM Mobile Communication Systems. International Journal of New Practices in Management and Engineering, 9(02), 08 - 14. https://doi.org/10.17762/ijnpme.v9i02.84

[8] C. Wang, G. Liu, H. Huang, W. Feng, K. Peng and L. Wang, "MIASec: Enabling data indistinguishability against membership inference attacks in MLaaS," IEEE Transactions on Sustainable Computing, vol. 5, no. 3, pp. 365-376, 2019.

[9] 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, 2013.

[10] D. C. Mehetre, S. E. Roslin and S. J. Wagh, "Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust," Cluster Computing, vol. 22, pp. 1313-1328, 2019.

[11] T. Delkesh and M. A. Jabraeil Jamali, "EAODV: Detection and removal of multiple black hole attacks through sending forged packets in MANETs," Journal of Ambient Intelligence and Humanized Computing, vol. 10, pp. 1897-1914, 2019.

[12] Martin, S., Wood, T., Hernandez, M., González, F., & Rodríguez, D. Machine Learning for Personalized Advertising and Recommendation. Kuwait Journal of Machine Learning, 1(4). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/156

[13] A. J. C. Sunder and A. Shanmugam, "Jensen–Shannon divergence based independent component analysis to detect and prevent black hole attacks in healthcare WSN," Wireless Personal Communications, vol. 107, pp. 1607-1623, 2019.

[14] M. A. Boudouaia, A. Abouaissa, A. Ali-Pacha, A. Benayache and P. Lorenz, "RPL rank based-attack mitigation scheme in IoT environment," International Journal of Communication Systems, vol. 34, no. 13, 2021.

[15] S. Singh and H. S. Saini, "Learning-based security technique for selective forwarding attack in clustered WSN," Wireless Personal Communications, vol. 118, no. 1, pp. 789-814, 2021.

[16] 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 . In 2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), 2020.

[17] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne and T. Voigt, "Cross-level sensor network simulation with cooja," in In Proceedings. 2006 31st IEEE conference on local computer networks , 2006.

[18] G. Oikonomou, S. Duquennoy, A. Elsts, J. Eriksson, Y. Tanaka and N. Tsiftes, "The Contiki-NG open source operating system for next generation IoT devices," SoftwareX, 2022.