Blackhole Attack Detection and Countermeasure Solution in RPL

Fatiè Daoud Idriss Siéba, Hamadoun Tall, Amado Illy, and Tiguiane Yélémou(✉)

Université Nazi BONI, Bobo-Dioulasso, Burkina Faso
tyelemou@gmail.com

Abstract. The Routing Protocol for Low-power and lossy networks (RPL) is proposed by the Routing Over Low-power and Lossy Networks (ROLL) team to meet the routing requirements of the Internet of Things. Since its introduction into our daily lives, the Internet of Things (IoT) has led to a considerable increase in the number of devices used for this purpose. Unfortunately, this increase has been accompanied by the emergence of a number of attacks affecting this equipment and network operation. The RPL protocol, for example, is subject to a blackhole attack aimed at isolating part of the network. Effective solutions are struggling to emerge due to the resource constraints of the connected objects used in these networks. In this paper, we present a lightweight and effective method for detecting blackhole attacks by the victim node itself, and propose countermeasures.

Keywords: blackhole attack · RPL

1 Introduction

The quick development of communication technologies and microelectronics has led to the emergence of miniature devices capable of communicating without a wired link. Most of these devices are characterised by their small size and limited resources (CPU, on-board power, memory). As a result, these nodes cannot support traditional routing protocols. This is why the Routing Over Low-power and Lossy Networks (ROLL) team of the Internet Engineering Task Force (IETF) proposed the Routing Protocol for Low-power and lossy networks (RPL) in March 2012 through RFC 6550 [1]. RPL allows nodes far from the sink to use intermediate nodes to transmit their data.

In its description, RPL has numerous security mechanisms that enable it to effectively face to external attacks. Unfortunately, most of these mechanisms are not sufficiently specified and therefore not implemented. This makes the protocol vulnerable to both internal and external attacks. The blackhole attack is one of the attacks to which this protocol is exposed. In this attack, a malicious node acting as an intermediary rejects messages sent to the sink node. This means that

A. Sere et al. (Eds.): AFRICOMM 2023, LNICST 587, pp. 288–295, 2025.
https://doi.org/10.1007/978-3-031-81570-6_19

packets coming from the downstream part of the sink and using this malicious node cannot reach the sink. This creates an isolation of this part of the network.

In this paper, we propose a mechanism for detecting this malicious behaviour by the victim node itself and an approach for thwarting the attack. Our approach does not involve any nodes other than the victim nodes. It is therefore less complex than most approaches involving additional nodes or the use of specific messages. The rest of our paper is organised as follows. In Sect. 2, we present a brief state of the art on RPL security. Our contribution is presented in Sect. 3. In Sect. 4, we conclude with some perspectives.

2 Related Works

RPL is a distance vector and source routing protocol. It is the preferred routing protocol for low-resource equipment. Because of the limited resources (CPU, on-board energy, memory) of sensor nodes, it is difficult to implement traditional security mechanisms in these networks. As a result, this protocol is vulnerable to a number of attacks. The authors of [2–4] propose a classification of these attacks as follows: resource attacks, topology attacks and traffic attacks. Figure 1 summarises these categories and the attacks belonging to them. as well as the attacks belonging to these categories.

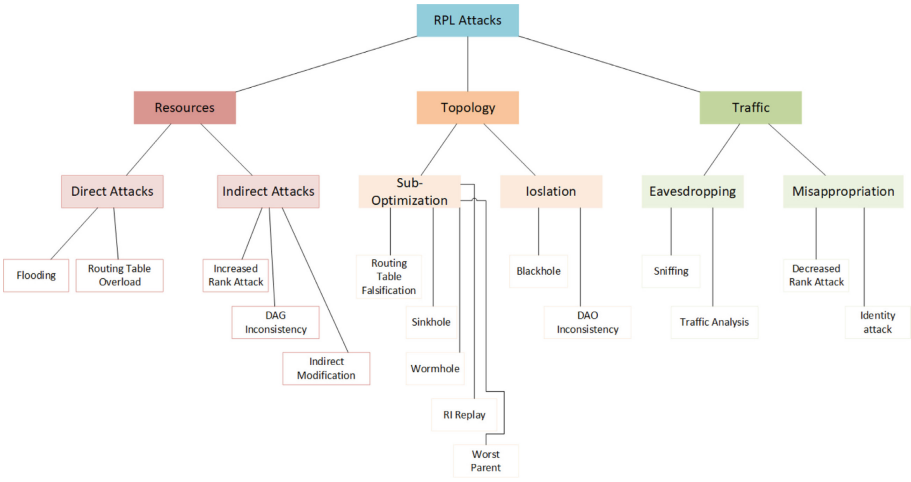

Fig. 1. Taxonomy of attacks against RPL networks [2].

In this paper, we are going to look at topology attacks. The aim of topology attacks is to affect the transmissions of certain network nodes. They can be divided into sub-optimisation attacks and isolation attacks. Sub-optimisation attacks concern the construction of the network and directly affect the network topology. The network does not converge optimally and the nodes do not use

the best paths for their transmissions. Most of these attacks involve communicating incorrect control messages or inducing a node to choose a non-optimal parent. A malicious node may also delay the transmission of data messages to the destination. Path reversal is also used for espionage purposes.

Isolation attacks aim to prevent a node from transmitting its packets to a destination. They consist of retaining all or part of the victim's packets. These attacks can take place during topology construction by withholding control messages [5,6] or during the data transmission phase by simply deleting packets received from nodes downstream of the sink. Several authors have carried out work to counter these attacks. Verma et. Al [7] propose Ensemble Learning based Network Intrusion Detection System (ELNIDS). ELNIDS is an IDS based on artificial intelligence. This IDS uses learning to combat sinkhole, blackhole, selective forwarding, sybil, clone-ID, flooding and local repair attacks. The IDS uses the following modules: the sniffer, the sensor events/traffic repository, the feature extraction module, the analysis engine, the signature database and the alarm/attack notification manager. Although the test results highlight its performance, this evaluation was carried out on matlab and concerns only the overall binders.

Self-Organizing Map IDS for RPL Protocol Attacks was proposed in [8]. The solution uses artificial intelligence and more specifically Self-Organizing Maps (SOM), which was proposed by T. Kohenen. This method provides a simplified representation of a high-resolution map based on self-learning [8]. Various modules are used to produce this map. The IDS detects flooding, sinkhole and DODAG version number attacks. It all starts with data from various simulations in real-life situations. This data is provided as input to a module called 'aggregator'. This module takes six (06) parameters: message type (DIO/DIS/DAO), source IP address, destination IP address, current DODAG version value, current source node rank and Unix timestamp [8]. This input will give six (06) output parameters: the ratio of DIS messages, the ratio of DIO messages, the ratio of DAO messages, the ratio of version number changes, the ratio of rank changes and the energy consumption at the destination node. The ratios are calculated on the basis of the different messages having a common destination during a given period [8]. The output data is then passed on to a normalization module called the 'nomalizer', which is responsible for normalizing the data. After normalization, the data is then passed to the trainer module to build the maps. The downside of their assessment is the lack of data on the time taken to detect the attack, as well as the false positive and false negative rates.

Hybrid of Anomaly-Based and Specification-Based IDS for IoTs Using Unsupervised OPF Based on MapReduce Approach was proposed in [9]. This solution counters selective forwarding, sinkhole and wormhole attacks by combining an Anomaly Agent-Based IDS (AA-IDS) and several Specification Agent-Based IDSs (SA-IDSs) [10]. SA-IDSs are implemented at router node level, while AA-IDS is implemented at root node level. The role of SA-IDSs is to collect traffic information and help unmask malicious nodes. Once the data has been collected, it is transmitted to the root node. The root node is responsible for distributing

the received data using an algorithm called Optimum-Path Forest without assistance. This algorithm groups the data into clusters, enabling the root node to perform anomaly detection. To classify nodes as malicious or not, the root node relies on the analyses of the AA-IDS and SA-IDSs. The IDS can be extended to cover attacks such as the Blackhole and decrease rank attacks. The downside of this solution is the high energy consumption of the router nodes and the root node, due to the tasks they perform.

Game Theory IDS was proposed in [11]. This IDS has a decentralized localization and combines signature-based detection with anomaly-based detection. Signature-based detection is used to detect known attacks on the RPL protocol, while anomaly-based detection is used to detect unknown attacks. In order to detect attacks, the system initializes a game between the two (02) IDSs and the attackers using Nash Equilibrium Game Theory. Nash Equilibrium is used in this solution to determine a state of equilibrium. This state of equilibrium enables the system to activate the anomaly detection technique to identify new attack signatures [11]. With the combination of these two (02) IDS types, the solution can counter flooding, sinkhole, blackhole, sybil and wormhole attacks.

In [12], Ribera et al. propose a solution for detecting blackhole and greyhole attacks using the heartbeat protocol. Their solution is based on the lightweight heartbeat protocol (LHP) proposed by Wallgren et al. in [13]. The solution in [13] is based on sending ICMPv6 ECHO messages at regular time intervals and waiting for a response from the receiving node. Any absence of response indicates a blackhole attack. Ribera et al. propose a solution with the same operating principle as LHP, the only difference being that messages are based on the User Datagram Protocol (UDP). According to the authors, this change enables a shorter detection time. Evaluation of their solution against normal operation shows only a 0.23% increase in CPU usage, 0.01% in TX transmission rate, and 0.06% in RX reception rate.

In [14], Lightweight Trust-Aware RPL is proposed by D. Airehrour et al. to combat blackhole and selective forwarding attacks. When these attacks are carried out, malicious nodes have a higher packet loss rate than normal nodes. Thus, the solution makes it possible to determine the reliability of nodes through trust values based on this characteristic of the attacks. The system works on the basis of the Minimum Rank with Hysteresis Objective Function (MRHOF). This function selects paths with low metrics, using hysteresis. Hysteresis will reduce the rate of disconnections due to small metric changes. Lightweight Trust-Aware RPL can detect complex blackhole attacks and control the frequency of rank changes. As a result, throughput and packet loss can be improved. Nevertheless, the solution has two drawbacks: high power consumption due to promiscuous mode, and unintentional packet rejection by some nodes due to errors that could be assimilated to a blackhole attack [14].

In [15], IOULIANOU et al. offer an intrusion detection system called Security Framework for RPL-Based IoT Networks (SRF-IoT) to combat blackhole and rank attacks. In its implementation, two networks are created. The first is a monitoring network featuring the SFR-IDS, and the second is the supervised

network. The solution is based on the success rate of messages sent by each node, through a sniffing of packets sent across the network and other metrics that the SRF-IDS provides to the various nodes within its reach. This task is performed by the SRF-IDS to optimize the energy consumption of the network nodes being monitored. These metrics (node ip address, verified IP flag and number of packets sent) are sent to the nodes to enable them to choose the best parent by calculating a confidence value. Nodes with a value below a certain threshold are blacklisted. Although the solution is effective in detecting and isolating malicious nodes, it does entail the creation of large storage tables for neighborhood entries.

3 Our Solution

In this section, we present our approach to dealing with the blackhole attack. First, we present our mechanisms for detecting the attack. Then we propose a countermeasure solution. Unlike the majority of existing approaches, our approach uses only victim nodes with traditional RPL mechanisms for both detecting the attack and resolving it.

Principle of the Blackhole Attack Detection Solution. The solution we propose enables a malicious node to be detected in an RCSF using the various child nodes. In normal operation, a parent node receives messages from its child nodes and forwards them to the sink. In normal operation, some messages may not be transmitted for various reasons (poor quality radio links, a node that is far away and therefore unreachable, sabotage by a malicious parent node, etc.). The blackhole attack on the RPL protocol consists of a malicious parent node not retransmitting messages received from its children to the sink. Our solution enables a child to know whether or not its message is being retransmitted to the sink by its parent node. To this end, each node must operate in promiscuous mode and have two (02) counters: C1 and C2. Counters C1 and C2 are used respectively to count the number of messages sent by the node and the number of these messages retransmitted by its parent. The promiscuous mode in our situation allows the node to detect messages that are retransmitted by the parent node to the next node towards the sink. The malicious parent node in charge of sending their messages to the sink silently rejects them. Each node increments its C1 counter each time a data packet is sent. After sending, it listens to its parent. The data messages sent by the latter are intercepted and processed to determine whether the source address is its own. A comparison function is implemented to perform this task. Once the address has been obtained, the node compares this value with its own address. If the source address of the intercepted message is not its own, the message is simply dropped. If the source address is that of the node which sent the message, C2 is incremented. From the C1 and C2 counters, it will then be able to determine the rate of packets retransmitted to the sink with a ratio of C2/C1. To take into account the different causes of packet loss, the retransmission rate threshold for determining the malicious node is set at

50%. The choice of this threshold value is justified by the operating mode of the blackhole attack as well as other retransmission problems that may intervene. Taking these parameters into account, the child node can formally identify a malicious parent node.

Description of the Principle of the Detection Solution. Our proposed solution to the blackhole attack is based on the statistical results generated by the nodes through the C1 and C2 counters. This solution will allow a child node that detects that its parent is malicious to initiate a search procedure for a new parent. In addition to these counters, we are implementing a blacklist on each node to store the address of the malicious parent. Using the statistics provided by C1 and C2, when a child node determines that its parent is malicious, the first step is to activate the blacklisting function for the malicious parent's address. Once this has been done, the second step is to initiate a procedure to choose the new best parent. For this choice, the node will choose the second best parent that it has stored in its neighbourhood table. This operation will save resources compared to a global repair procedure. Once the new parent has been chosen, communications resume and the nodes in the subnetwork concerned reset their counters without removing the malicious parent from the blacklist cache. Our solution works as shown in the flowchart in Algorithms 1 and 2.

Algorithm 1. Malicious node detection

Require: $C1 = 0, C2 = 0, R = 0, i = 0$
  while $i < 11$ **do**
    if $next_hop! = NULL$ **then**
      node.child.sendto(next_hop)
      ++C1
      $listento(next\_hop)$
      if transfered_source_address=node.child.address **then**
        $++C2$
      end if
      $++i$
    end if
  end while
  $R = C2/C1$
  if $R < 0.5$ **then**
    print ("malicious node")
  end if

4 Conclusion

Threats to WSNs are on the increase. The nodes involved in these networks are highly vulnerable. Their low capacity (CPU, memory, on-board energy) makes it difficult to apply traditional security mechanisms. This paper highlights a number of attacks on RPL. We are particularly interested in the blackhole attack.

Algorithm 2. Blacklisting and new parent selection

```
if R < 0.5 then
   printf ("malicious node")
end if
blacklist(next_hop.id)
init_DIS_send
if parent.id = next_hop.id then
   reject(next_hop.id)
else
   select(parent.id)
end if
sent_DAO_send(parent.id)
```

This attack consists of a parent node preventing its child nodes from transmitting data to the sink. A number of solutions have been proposed to deal with this attack. Most of these solutions use IDS or cryptographic protocols. Due to the nature and complexity of some of these solutions, expected performance is mixed. Our contribution to securing RPL covers two aspects (detection and countermeasure). Detection is achieved through simple calculations based on a system of two counters and a ratio to determine a malicious parent. Countermeasure uses a blacklist and a mechanism to search for a new parent when the malicious parent is detected. The countermeasure principle uses RPL's own new parent search mechanism. This limits the additional resource-intensive operations required to counter the blackhole attack. For future work, we are planning real-life tests to confirm the performance of our approaches.

References

1. Brandt, A.,et al.: RFC 6550: RPL: IPv6 routing protocol for low-power and lossy networks (2012)
2. Almusaylim, Z.A., Alhumam, A., Jhanjhi, N.Z.: Proposing a secure RPL based internet of things routing protocol: a review. Ad Hoc Netw. **101**, 102096 (2020)
3. Boudouaia, M.A., Ali-Pacha, A., Abouaissa, A., Lorenz, P.: Security against rank attack in RPL protocols. IEEE Netw. **34**(4), 133–139 (2020)
4. Kamble, A., Malemath, V.S., Patil, D.: Security attacks and secure routing protocols in RPL-based internet of things: survey. In: 2017 International Conference on Emerging Trends & Innovation in ICT (ICEI), pp. 33–39. IEEE (2017)
5. Sokat, B.: Blackhole attacks in IoT networks. Ph.D. thesis, Izmir Institute of Technology (Turkey) (2020)
6. Mayzaud, A.: Monitoring and Security for the RPL-based Internet of Things. Ph.D. thesis, Université de Lorraine (2016)
7. Verma, A., Ranga, V.: ELNIDS: ensemble learning based network intrusion detection system for RPL based internet of things. In: 2019 4th International conference on Internet of Things: Smart innovation and usages (IoT-SIU), pp. 1–6. IEEE (2019)

8. Kfoury, E., Saab, J., Younes, P., Achkar, R.: A self organizing map intrusion detection system for RPL protocol attacks. Int. J. Interdiscipl. Telecommun. Netw. (IJITN) **11**(1), 30–43 (2019)
9. Bostani, H., Sheikhan, M.: Hybrid of anomaly-based and specification-based ids for internet of things using unsupervised OPF based on MapReduce approach. Comput. Commun. **98**, 52–71 (2017)
10. Simoglou, G., Violettas, G., Petridou, S., Mamatas, L.: Intrusion detection systems for RPL security: a comparative analysis. Comput. Secur. **104**, 102219 (2021)
11. Sedjelmaci, H., Senouci, S.M., Taleb, T.: An accurate security game for low-resource IoT devices. IEEE Trans. Veh. Technol. **66**(10), 9381–9393 (2017)
12. Ribera, E.G., Alvarez, B.M., Samuel, C., Ioulianou, P.P., Vassilakis, V.G.: 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), pp. 1–6. IEEE (2020)
13. Wallgren, L., Raza, S., Voigt, T.: Routing attacks and countermeasures in the RPL-based internet of things. Int. J. Distrib. Sens. Netw. **9**(8), 794326 (2013)
14. Airehrour, D., Gutierrez, J., Ray, S.K.: A trust-aware RPL routing protocol to detect blackhole and selective forwarding attacks. J. Telecommun. Digital Econ. **5**(1), 50–69 (2017)
15. Ioulianou, P.P., Vassilakis, V.G., Shahandashti, S.F.: A trust-based intrusion detection system for RPL networks: detecting a combination of rank and blackhole attacks. J. Cybersecur. Priv. **2**(1), 124–153 (2022)