A Root-based Defense Mechanism Against RPL Blackhole Attacks in Internet of Things Networks

Jun Jiang and Yuhong Liu and Behnam Dezfouli

Department of Computer Engineering
Santa Clara University
Santa Clara, CA, 95053
Emails:{ jun3525114@gmail.com, yhliu, bdezfouli}@scu.edu

***Abstract*—With the rapid development of the Internet of Things (IoT), various smart "things", such as home appliances, vehicles and mobile medical devices, connected through the Internet are increasingly adopted by consumers. Many of such connections are enabled by IoT routing protocol: IPv6 Routing Protocol for Low Power and Lossy Networks (RPL), which utilizes a variety of objective functions (OFs) and routing constraints to establish an optimal routing path for each network node. However, recent studies show that topology attacks, such as Blackhole attacks, have brought great security challenges to the secure routing in IoT networks. On the other hand, as most of the IoT edge devices are resource constrainted, they cannot afford intensive computations and communications required by conventional security solutions. Therefore, in this work, we propose a lightweight defense mechanism based on RPL routing protocol to detect Blackhole attacks and exclude the detected malicious nodes from the routing network. The results show that the proposed mechanism can effectively detect and defend against Blackhole attacks while causing limited energy consumption overhead.**

I. Introduction

Internet of Things (IoT) [1] allows vast amount of highly heterogeneous sensors/devices (i.e., edge nodes) to be closely sensing and monitoring the physical world and connecting to the Internet for communications. Due to its broad applications, IoT is experiencing explosive growth in recent years. It is estimated that by the year 2020, there will be about 30.7 billion connected sensors/devices. IoT has also been considered as the third wave of the information industry, which has turned the conventional "user-device" interactions into "device-device" interactions. Network standards and protocols that enable such massive communications among IoT devices have attracted wide attention recently.

As the existing Internet Protocol (IP) technology is complex and not suitable for low power and resource constrained Wireless Sensor Networks (WSN) [2], Internet Engineering Task Force (IETF) has designed lightweight IPv6 protocols based on the open source micro IP (uIP), which can run on low-power, resource constrained devices. IETF has completed the core standard specification, such as the Internet Protocol (IPv6) over Low-power Wireless Personal Area Networks (6LoWPAN) [3], and Routing Protocol for Low Power and Lossy Networks (RPL) [4], which have become the core of many other standards.

Specifically, RPL is a distance vector routing protocol based on IPv6. It establishes Destination Oriented Directed Acyclic Graphs (DODAG) by utilizing various objective functions (OFs), which identifies an optimal path to the destination by considering different routing costs and constraints. Each node in the DODAG except the root node selects a parent node as the default route based on the objective function.

Due to the increasing adoption of RPL, it has become a popular target for malicious attacks. One of such attacks is the Blackhole attack [5], in which one or more malicious nodes discard some or all the packets routed through them, resulting in interruptions of the normal traffic stream in the network. However, as most of IoT network nodes are resource constrained and cannot afford heavy computations and communications, conventional security solutions may not be directly applied in such scenario. There is an urgent need to investigate lightweight security solutions that ensure secure communications among IoT devices while taking energy efficiency into consideration.

Currently, there are mainly two types of non-cryptographic defense mechanisms against the Blackhole attack. The first one is to add a third-party IDS system to RPL network [6]. This approach detects the Blackhole attack by monitoring the traffic across the entire network. Nevertheless, this mechanism requires the involvement of a trusted third-party device. In addition, the IDS system's detection equipment needs to be placed in the central place to ensure coverage of the entire network, which may not be feasible in some scenarios. The second mechanism defends against the Blackhole attack through distributed monitoring manner [7]. Each node has to monitor its neighbors' traffic, detect malicious nodes through traffic analysis and report to the system. This method, however, leads to extra energy consumption at each individual node, which is critical for resource constrained IoT devices. In addition, it raises new challenges as how to ensure that each resource constrained node will reliably and honestly report its neighbors' behavior over a long period of time.

In this work, we implement the Blackhole attack in RPL networks through Cooja, a sensor network simulator based on Contiki operating system. Furthermore, we propose a root-based defense mechanism against Blackhole attacks. In particular, we propose to have the root node actively track the

network packets and perform anomaly detection, so that other nodes will not spend extra energy for anomaly detection. In addition, by not involving third-party trusted devices, the proposed scheme can eliminate the additional risks introduced by third-party, and does not rely on specific network topologies. To our best knowledge, this is one of the first few studies that implement RPL Blackhole attacks and defenses in Cooja. The experiment results show that the proposed scheme can effectively detect and eliminate RPL Blackhole attacks while consuming only limited power.

II. Related work

A. RPL Security Attacks

RPL network faces various security risks from different aspects of wireless sensor networks. Common security attacks can be divided into three main parts [8]. The first type of attack is resource attacks, in which the attacker often misleads nodes to perform extensive unnecessary processes in a short time period. These processes can significantly consume nodes' limited resources and shorten their working life time. The second type of attack is traffic attack, in which attackers' goal is to manipulate the network traffic. For example, attackers can spread false information in the network, increase the entire network load and eavesdrop on conversations between nodes. The third type of attack is the network topology attack in which attackers mainly damage the security and stability of network by changing the network topology.

In RPL network topology attacks, Blackhole attack is the most serious type of attack in which the malicious node drops all or most of the packets it needs to forward [7], resulting in an isolation between a victim node and its parent. If the malicious node is in a very important position, it will bring catastrophic consequences to the network traffic.

B. RPL Security Solutions

When designing RPL protocol, IETF has defined several security mechanisms to ensure the basic security of RPL. For example, the RPL protocol internally integrates local and global repairing mechanisms, such as loop detection and avoidance [4]. In addition, two security functions are defined to provide confidentiality, integrity, delay protection, and replay protection for RPL message as additional options [9]. In reality, these basic repair mechanisms and security modules are far from adequate [7].

Many cryptographic based security mechanisms are proposed without considering energy efficiency. For example, public key infrastructure (PKI) can protect the communication between two terminals. However, when the number of devices in the network reaches a very high level, this technology will become very inefficient and energy-consuming. The authors in [10] use a hash function to encrypt messages, so that the transmission of data is protected. However, the use of cryptographic systems speeds up the consumption of node resources and increases the size of network packets. In addition, when one node moves from one network to another, the encryption information, such as key, needs to be updated.

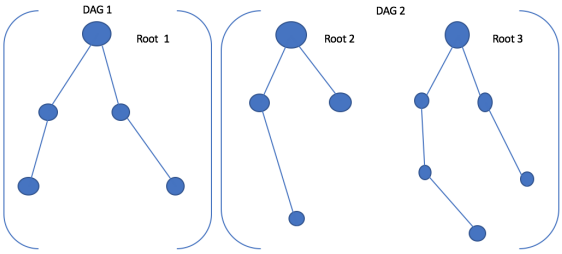


Fig. 1. RPL Topology

Some trust based non-cryptographic security mechanisms are then proposed. For example, the authors in [6] implement a third-party IDS system to monitor traffic across the network and detect malicious behavior. The involvement of third-party, however, introduces extra risks. In addition, the IDS system needs to be placed at the core of the network to ensure coverage of all nodes, which may not always be feasible as in reality, as the RPL network nodes are often deployed randomly in extreme environments. The authors in [7] propose a distributed trust-based mechanism to detect Blackhole attacks. Specifically, each node needs to monitor its neighbors' ratio of incoming traffic and forwarding traffic, and consider this ratio as a trust value in its objective function calculation. Only neighbors with high trust values will be later considered as potential parents to help with traffic forwarding. However, this method also has some limitations. For example, to obtain accurate estimation of its neighbors' traffic forwarding behavior, a network node, which was originally designed to save energy by entering sleeping mode, has to keep alive for a long time, resulting in significant increase of working time and energy consumption. More importantly, it raises new challenges as how to ensure that each resource constrained node can reliably and honestly report its neighbors' behavior in the long term.

To address these above mentioned challenges, in this work, we propose to have the root node in each DODAG monitor and detect abnormal traffic forwarding behaviors.

III. RPL Routing protocol

The IETF's Routing Over Low power and Lossy networks (ROLL) working group defines the Routing Protocol for LLN (RPL). In particular, each RPL network contains multiple RPL instances and each RPL instance may contain multiple DODAGs. In the DODAG, the root node can store and manage the DODAG information, such as the version number. A non-root node can join one RPL instance at a time, but can switch to other instances later. A DODAG is created by constructing a path between a leaf node and the root node. An example of DODAGs is shown in Fig.1. The links in Fig.1 show the "parent and child" relationship between two nodes.

A. RPL Control Message

There are four main types of control messages [4] in RPL:

1. DIO (DODAG Information Object): DIO message is sent by RPL nodes to advertise DODAG and its characteristics. DIO can be used for DODAG discovery, composition, and maintenance. Each node can modify part of the information received in the DIO, such as the rank value.

2. DIS (DODAG Information Solicitation): The DIS message is used to discover nearby DODAGs and to request DIO messages from nearby RPL nodes. It is similar to IPv6 route request message. When a node needs to join a DODAG or needs to change location, it sends DIS information.

3. DAO (Destination Advertisement Object): The DAO message is used to propagate the destination message upwards in the DODAG to fill the parent node's routing table. When a node receives a DIO message, it chooses to send a DAO confirmation message to its parent node.

4. DAO-ACK (Destination Advertisement Object Acknowledgement): Whenever a parent node receives DAO information from a child node, it sends a DAO-ACK message to the child node. This message is used by children nodes to confirm that the parent node has received its DAO information.

B. Topology Establishment

The whole DODAG construction can be divided into two parts: the construction of the upward-route and the construction of the downward-route.

As shown in Fig.2, the construction process of the upward-route starts from the root node. Root node broadcasts a DIO message carrying the information such as RPL instance ID, DODAG ID, rank, etc. After receiving the root's DIO message, NA selects the root as its parent and join the DODAG. NA then calculates the rank value according to its objective function, updates the received DIO packet, and broadcasts it. When NB receives NA's DIO packet, it selects NA as the parent node and joins the DODAG. Assume that after NB joins the DODAG, NC actively broadcasts a DIS message and seeks to join a DODAG. When receiving NC's DIS message, NB sends its DIO message to NC. NC can select NB as its parent and join the DODAG. At this moment, the entire DODAG upward route is established.

Downward routing is constructed using DAO packets. When receiving the root's DIO packet, NA returns a DAO packet to the root. When receiving NA's DAO message, the root adds the NA's information to the routing table and returns a DAO-ACK message. Similarly, when NB receives NA's DIO message, it sends DAO message to NA. NA processes the DAO packet and sends back a DAO packet to its parent node and a DAO-ACK message to NB. After receiving the DAO packet, the root adds NB's information to the routing table and returns a DAO-ACK message. Similarly, after each node processes the DAO information, it sends update information to its parent and returns a DAO-ACK message to its children nodes. Finally, the root node obtains all the information for the entire DODAG.

IV. Proposed Scheme

As mentioned earlier, Blackhole attacks can cause damages to the network, such as high packet loss, high latency and instability of the network. In addition, as RPL's global and local repair mechanisms will continue to work, normal nodes may be forced to deplete their own resources, leading to collapse of the entire network.

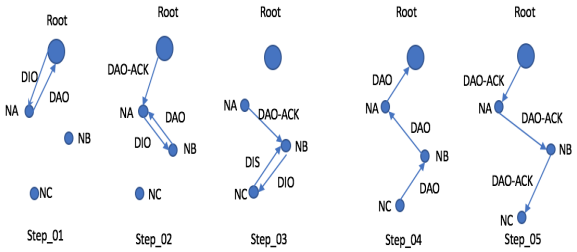


Fig. 2. Topology Establishment

In this work, we propose a root-based defense mechanism with the following goals. First of all, this mechanism should be lightweight and cannot over-consume the limited resources of the network node. Second, this mechanism should be effective in terms of detection rate. Third, it should have high portability and is easy to deploy.

A. Detection module

The purpose of the detection module is to detect the Blackhole attacks at the root end. First, we assume that each node's transmitted messages are protected by hash function, so that malicious nodes cannot change the contents of transmitted data. Second, the RPL network works in non-storing mode, indicating that non-root nodes do not have the ability to store information.

All messages generated by nodes will be forwarded through the root. Therefore, we propose to introduce a sequence number in each node's message, so that the root node can keep track of the messages coming in and going out of each node. Specifically, we use the first byte in the data payload as a sequence number. Each time when a node needs to send data through the root, its sequence number will be recorded by the root. At the non-root node side, each time it sends out one message, the sequence number will be increased by one. At the root side, a counter variable (C_i) is defined to record the number of packets sent out by node i and successfully received by the root node. As a result, the packet loss rate L_i can be calculated as follows.

$$L_i = \frac{S_i - C_i}{S_i} \tag{1}$$

where S_i indicates the sequence number embedded in node i's message. The root node will identify the nodes with low packet delivery ratios as malicious nodes, and broadcast the detection results to the entire network. It is worth noting that because of the instability of the RPL network, the packet loss rate of each node may fluctuate over time. To minimize false alarms, we use the average value of packet loss rate.

TABLE I
CONTIKI SIMULATION PARAMETERS

Simulation Parameters	
Platform	Contiki 3.0
Mote Type	Z-mote
Simulation time	1440 seconds
Total nodes	15
Root node	1
Blackhole Malicious Nodes	2
Legitimate nodes	12
Network Layer Protocol	IP
Transport Layer Protocol	UDP
Routing Protocol	RPL
Link Layer Protocol	ContikiMAC

B. Report module

When the root node detects a Blackhole node, it starts broadcasting this message to the network. Because the RPL network has a very strict hierarchical relationship, general message types, such as UDP, can only be received by children nodes if the parent node forwards it. If the parent node is a Blackhole node, its children nodes will not be able to receive the anomaly report messages sent by the root node. Therefore, we propose to use the ICMP6 control messages to broadcast the anomaly detection results as the non-root node can get the ICMP6 messages forwarded not only by its parent but also by its neighbors. In particular, we propose to use the first byte in the payload of ICMP6 control messages to represent the ID of the Blackhole node.

C. Isolation module

When a non-root node in the network receives this ICMP6 control message, it checks whether the reported Blackhole node is its parent nodes. If yes, this node will delete the parent node from its parent list, reselect its preferred parent node and broadcast this ICMP6 control message to its neighbors. If not, the node broadcasts this ICMP6 control message to its neighbors directly. Through this process, the Blackhole node is isolated by its children.

V. EXPERIMENT

A. Experiment Setup

In this work, we choose Contiki operating system. In Contiki, the system has two objective functions, including Objective Function zero (OF0) and Minimum Rank with Hysteresis Objective Function (MRHOF), which prioritizes potential parent nodes according to their ranks, and their Expected Transmission Count (ETX) values, respectively. In this work, we adopt the latter one as our objective function. The simulation parameters are shown in TABLE I.

The deployment of RPL network nodes is shown in Fig.3. In particular, node 1 is the root node. Node 14 and node 15 are Blackhole malicious nodes. The rest of nodes are legitimate nodes. In the network topology establishment process, the nodes are randomly deployed. In Cooja, it takes about 10 seconds to set up the entire RPL network.

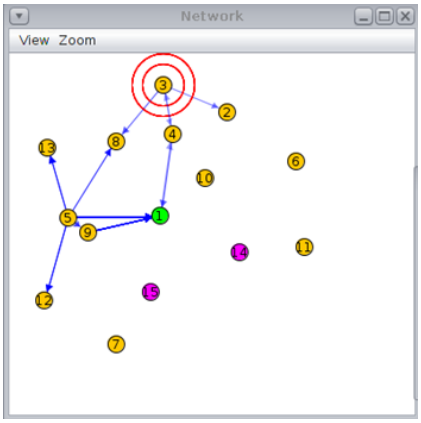


Fig. 3. Network Nodes Deployment

For RPL network, the packet delivery ratio is determined by many factors [11] [12], such as frequency of application messages, DIO minimum interval and Duty-Cycling interval. In the experiment, we can control these factors to maintain the legitimate node's packet delivery ratio as 99% in Cooja simulator and set the packet loss rate detection threshold as 6% [13].

B. Results Analysis

In our simulation, we let the Blackhole nodes start working at the 10^{th} minute after the network established. In Fig.4, the root node detects the Blackhole node in the 14^{th} minute and reports Blackhole node information in Cooja Mote output window, including the sequence number, packet loss rate and source ID. In addition, the root node adds the Blackhole node's ID to the payload buffer of the ICMP6 control message, and then broadcasts it.

In [14], the repair mechanism of the RPL network largely depends on DIO messages. This means that the delay of the network repairing process depends on the frequency of DIO messages. If the Blackhole node starts working right after the root node sending out a DIO message, it can remain unidentified and continue damaging the network for a long time. For example, in Contiki system, the default value of maximum DIO sending interval is 1048.576 seconds. With the proposed scheme, the isolation of Blackhole nodes is no longer dependent on DIO messages. When the root detects the Blackhole node, the network will start the repairing process immediately, which can significantly shorten the working time of the Blackhole nodes.

In Fig.5, before detection, the original preferred parents of node 7 and node 11 were Blackhole nodes 15 and 14, repectively. When node 7 and node 11 receive the detection reports sent by the root node, they start the isolation process. They first extract the Blackhole node information from the ICMP6 control message, remove the Blackhole node form their parent lists and pick their new preferred parents. As shown in Fig.5, node 11 picks node 6 as its new preferred

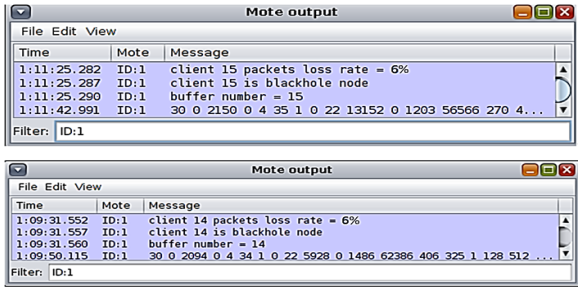


Fig. 4. Detection of RPL Blackhole Malicious Node

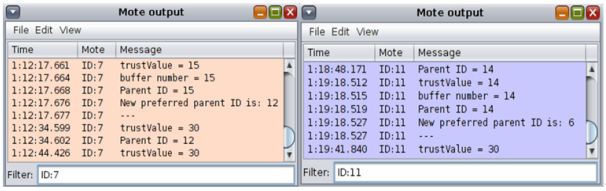


Fig. 5. Isolation of Blackhole node

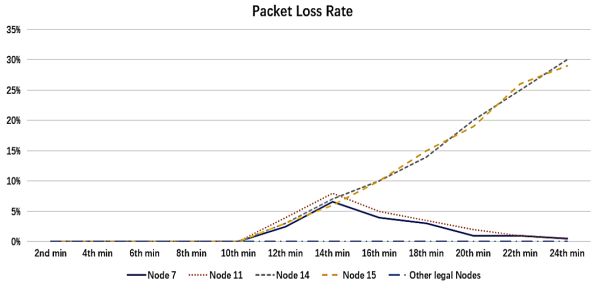
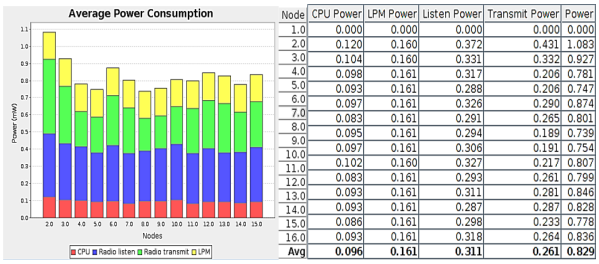
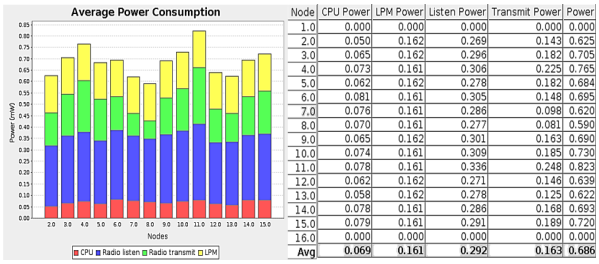


Fig. 6. Packet Loss Rate



Node	CPU Power	LPM Power	Listen Power	Transmit Power	Power
1.0	0.000	0.000	0.000	0.000	0.000
2.0	0.120	0.160	0.372	0.431	1.083
3.0	0.104	0.160	0.331	0.332	0.927
4.0	0.098	0.161	0.317	0.206	0.781
5.0	0.093	0.161	0.288	0.206	0.747
6.0	0.097	0.161	0.326	0.290	0.874
7.0	0.083	0.161	0.291	0.265	0.801
8.0	0.095	0.161	0.294	0.189	0.739
9.0	0.097	0.161	0.306	0.191	0.754
10.0	0.102	0.160	0.327	0.217	0.807
11.0	0.083	0.161	0.293	0.261	0.799
12.0	0.093	0.161	0.311	0.281	0.846
13.0	0.093	0.161	0.287	0.287	0.828
14.0	0.086	0.161	0.298	0.233	0.778
15.0	0.093	0.161	0.318	0.264	0.836
16.0	**0.096**	**0.161**	**0.311**	**0.261**	**0.829**
Avg					

Fig. 7. Energy Consumption of RPL Network with Root-based Defense Mechanism



Node	CPU Power	LPM Power	Listen Power	Transmit Power	Power
1.0	0.000	0.000	0.000	0.000	0.000
2.0	0.050	0.162	0.269	0.143	0.625
3.0	0.065	0.162	0.296	0.182	0.705
4.0	0.073	0.161	0.306	0.225	0.765
5.0	0.062	0.162	0.278	0.182	0.684
6.0	0.081	0.161	0.305	0.148	0.695
7.0	0.076	0.161	0.286	0.098	0.620
8.0	0.070	0.161	0.277	0.081	0.590
9.0	0.065	0.162	0.301	0.163	0.690
10.0	0.074	0.161	0.309	0.185	0.730
11.0	0.078	0.161	0.336	0.248	0.823
12.0	0.062	0.162	0.271	0.146	0.639
13.0	0.058	0.162	0.278	0.125	0.622
14.0	0.078	0.161	0.286	0.168	0.693
15.0	0.079	0.161	0.291	0.189	0.720
16.0	0.000	0.000	0.000	0.000	0.000
Avg	**0.069**	**0.161**	**0.292**	**0.163**	**0.686**

Fig. 8. Energy Consumption of RPL Network without Root-based Defense Mechanism

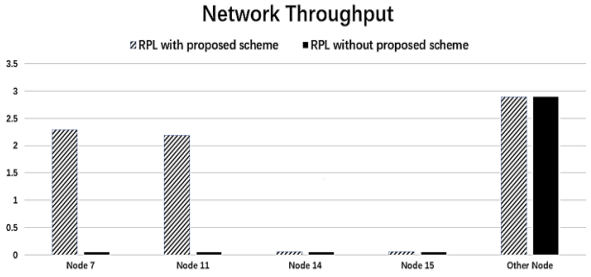


Fig. 9. Comparison of Network Throughput between Root-based RPL and RPL without Root-based Mechanism

parent. Node 7 picks node 12 as its new preferred parent. The isolation process takes only a few seconds, which is much faster than that of [14].

Fig.6 shows the packet loss rate over time for each node. In our simulation, the Blackhole nodes start working at the 10^{th} minute. We can observe that the packet loss rates at node 7, node 11, node 14 and node 15 start to increase from the 10^{th} minute. Around the 13.5^{th} minute, our defense mechanism starts to work. The packet loss rates of node 7 and 11 begin to drop at about the 14^{th} minute. At the Blackhole nodes 14 and 15, packet loss rates continue increasing since they keep blocking all the traffic. The results show that our defense mechanism can effectively eliminate the damage caused by Blackhole nodes in the network.

Fig.7 and Fig.8 show the energy consumption of the RPL network with and without the proposed scheme, respectively. Each bar in the figure represents the average power consumption of each node. The different colors in each bar show the distribution of energy consumption for each node to perform different functions. By comparing the two figures, we can find that the proposed scheme does not significant increase the energy consumption of the network.

Fig.9 shows a comparison on the node throughput with and without the proposed scheme. We can observe that the proposed scheme greatly improves the network's throughput. When the Blackhole nodes 14 and 15 begin to attack, the throughput of node 7 and node 11 will drop to zero if the proposed scheme is absent. With the proposed scheme, all the nodes, except the two Blackhole nodes 14 and 15, will yield high overall throughputs. This also means that no node in the network will select the Blackhole nodes as its parent later.

VI. Conclusion

As RPL networks become more prevalent, its security issues also attract more attention. Blackhole attack as a topology attack can significantly drop the network's performance. The

development of an effective and lightweight security solution to secure IoT routing is critical. In this work, we propose a root-based defense scheme against Blackhole attacks. It detects the Blackhole malicious nodes by implementing a packet loss detection algorithm at the root node, which broadcasts the Blackhole node information to the entire network. Non-root nodes use the Blackhole node information to isolate the malicious nodes. Simulations based on Cooja have been performed. Experiment results have shown that the proposed scheme achieves fast detection and isolation of the Blackhole nodes while causing limited energy overhead. To the best of our knowledge, this is one of the very few works that implement Blackhole attacks and its defense schemes in Cooja and perform energy analysis.

As one of the first few studies on Blackhole attacks in RPL, in this work, we mainly focus on the straightforward Blackhole attacks, where malicious nodes simply block the traffic. In the future research, Blackhole nodes with more diverse behaviors will be investigated and implemented. We will examine how the variation of legitimate and malicious nodes affect the performance of the proposed scheme. More advanced defense solutions, such as the detection accuracy by adaptively setting the threshold, that detect malicious nodes by analyzing their history behavior will be further explored.

REFERENCES

[1] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future generation computer systems,* Volume 29, Number 7, Pages 1645-1660, September, 2013

[2] Bruno Marques, Manuel Ricardo, "Energy-efficient node selection in application-driven WSN," *Wireless Networks,* Volume 23, Number 3, Pages 889-918, 2017

[3] A. Le, J. Loo, A. Lasebae, M. Aiash, and Y. Luo, "6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach," *International Journal of Communication Systems,* Volume 25, Number 9, Pages 1189-1212, 2012

[4] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, et al, "RPL: IPv6 routing protocol for low-power and lossy networks," Available:https://tools.ietf.org/html/rfc6550, 2012.

[5] Karishma Chugh, Aboubaker Lasebae, Jonathan Loo, "Case study of a black hole attack on LoWPAN-RPL," *Proc. of the Sixth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), Rome, Italy (August 2012),* Pages 157-162, 2012

[6] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad hoc networks,* Volume 11, Number 8, Pages 2661-2674, 2013

[7] David Airehrour, Jairo Gutierrez and Sayan Kumar Ray, "Securing RPL routing protocol from blackhole attacks using a trust-based mechanism," *Telecommunication Networks and Applications Conference (ITNAC), 2016 26th Internationa,* Pages 115-120, 2016

[8] Antha Mayzaud, Rmi Badonnel, Isabelle Chrisment, "A Taxonomy of Attacks in RPL-based Internet of Things," *International Journal of Network Security,* Volume 18, Number 3, Pages 459-473, 2016

[9] R. K. Alexander, M. Richardson, T. Tsao, V. Daza, A. Lozano, and M. Dohler, "A security threat analysis for the routing protocol for low-power and lossy networks (rpls)," IETF Internet Draft (draft-ietf-roll-security-threats-06), 2015

[10] K. Weekly and K. Pister, "Evaluating sinkhole defense techniques in RPL networks," *Network Protocols (ICNP), 2012 20th IEEE International Conference on,* Pages 1-6, 2012

[11] H. Ali, "A performance evaluation of rpl in contik," SICS Swedish Institute of Computer Science, 2012

[12] Daniel Benson, "A Performance Study of RPL with Trickle Algorithm Variants," Worcester Polytechnic Institute, 2016

[13] Mansfield, K.C., Antonakos, J.L, "Computer Networking for LANS to WANS: Hardware," *Software, and Security, Course Technology, Cengage Learning, Boston,* 2010

[14] A. Brandt, E. Baccelli, R. Cragie, P. van der Stok, "Applicability Statement: The Use of the Routing Protocol for Low-Power and Lossy Networks (RPL) Protocol Suite in Home Automation and Building Control," *Consultant,* 2016