Securing Low-Power Blockchain-Enabled IoT Devices Against Energy Depletion Attack

AMJAD ALSIRHANI, Jouf University, Sakaka Aljouf, Kingdom of Saudi Arabia and Faculty of Computer Science, Dalhousie University, Canada
MUHAMMAD ALI KHAN*, COMSATS University Islamabad, Lahore Campus, Pakistan
ABDULLAH ALOMARI, Albaha University, Kingdom of Saudi Arabia
SAUDA MARYAM, COMSATS University Islamabad, Lahore Campus, Pakistan
AIMAN YOUNAS, COMSATS University Islamabad, Lahore Campus, Pakistan
MUDDESAR IQBAL, London South Bank University, United Kingdom
MUHAMMAD HAMEED SIQQIDI, Jouf University, Kingdom of Saudi Arabia
AMJAD ALI, COMSATS University Islamabad, Lahore Campus, Pakistan

Blockchain-enabled Internet of Things (IoT) envisions a world with rapid development and implementations to change our everyday lives based on smart devices. These devices are attached to the internet that can communicate with each other without human interference. A well-known wireless network in blockchain-enabled IoT frameworks is the Low Power and Lossy Network (LLN) that uses a novel protocol known as Routing protocol for low power and lossy networks (RPL) to provide effective and energy-efficient routing. LLNs that run on RPL are inherently prone to multiple Denial of Service (DoS) attacks due to the low cost, shared medium and resource-constrained nature of blockchain-enabled IoT devices. A Spam DODAG Information Solicitation (DIS) attack is one of the novel attacks that drain the energy source of legitimate nodes and ends up causing the legitimate nodes to suffer from DoS. To address this problem, a mitigation scheme named DIS Spam Attack Mitigation (DISAM) is proposed. The proposed scheme effectively mitigates the effects of the Spam DIS attack on the network's performance. The experimental results show that DISAM detects and mitigates the attack quickly and efficiently.

CCS Concepts: • **Computer systems organization** → **Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability.

Additional Key Words and Phrases: Internet of Things, Block chain, Denial of Service, Battery Drainage Attack, DIS Attack

ACM Reference Format:
Amjad Alsirhani, Muhammad Ali Khan*, Abdullah Alomari, Sauda Maryam, Aiman Younas, Muddesar Iqbal, Muhammad Hameed Siqqidi, and Amjad Ali. 2022. Securing Low-Power Blockchain-Enabled IoT Devices Against Energy Depletion Attack. In . ACM, New York, NY, USA, 17 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

Blockchain-enabled Internet of Things (IoT) imagines a future in which billions of devices are connected to enable ubiquitous computing. The blockchain-enabled IoT integral part is to provide communication between low-power devices through the internet. The growth of wireless and embedded electronics results in smart devices with connectivity

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
© 2022 Association for Computing Machinery.
Manuscript submitted to ACM

and processing capacities ranging from sensor nodes to advanced household appliances and mobile devices. Throughout recent years several blockchain-enabled IoT technologies have grown, e.g., in industrial monitoring, medical services, smart grid, autonomous cars, smart manufacturing, and operations management [1]. For blockchain-enabled IoT services, the number of wirelessly accessible devices has been expected to increase to 50 billion at the end of 2020 and worldwide blockchain-enabled IoT revenue will also grow to $1.7 trillion by 2020 [2]. One of the basic components of blockchain-enabled IoT is low power and lossy networks. As part of the increasingly evolving blockchain-enabled IoT networks, low power and lossy networks play a noteworthy role in creating a ubiquitous computation consisting of constrained nodes with a restricted set of computation, bandwidth, and battery [3][4][5].

With the growing demand for resource-constrained nodes to be connected to the internet, the working group of Internet Engineering Task Force [6] has introduced a novel routing protocol defined as RPL [7]. Due to its ability to provide energy-efficient routing in low-power and lossy networks, RPL is used in a wide range of blockchain-enabled IoT implementations. [8, 9] RPL based networks are exposed to various threats that undermine the security and privacy of users due to the shared wireless medium, where an intruder can overhear, duplicate, corrupt or alter the data. With the lack of RPL routing protocol resources, physical security, and security specifications, RPL based low power lossy networks are prone to numerous Denial of Service attacks [10]. One of such damaging attacks is a destination-oriented directed acyclic graph (DODAG) Information Solicitation (DIS) flooding attack.

In this paper, we present and investigate a potential DoS attack, which is a Spam DIS attack, in RPL-based LLNs. In a Spam DIS attack, fraudulent node multicast a huge amount of fake DODAG Information Solicitation (DIS) requests with multiple fake identities to force the valid nodes to restart their trickle timer and distribute a high proportion of DODAG Information Object (DIO) messages. In RPL, DIS and DIO are control messages that are required to construct the routing topology. As a consequence, excessive receiving and broadcasting of control packets will exhaust the restricted energy resource of legitimate nodes and ultimately cause legitimate nodes to suffer from denial of service. The Spam DIS attack exploits predominantly the vulnerability of the DIO transmission mechanism in RPL by breaching an inherent premise, i.e., all valid nodes without hesitation and in a faithful manner transmits DIO messages when they receive a DIS message.

A large number of DIS and DIO control messages make the legitimate nodes suffer from denial of service and drain down the energy resource of legitimate nodes. It is difficult to differentiate legitimate DIS requests from requests that are part of a DIS attack because of their distributed nature and much harder to respond to when the attack is already underway. We investigate Spam DIS attack to minimize node energy consumption and improve DODAG 's security in RPL for a reliable and secure network. We propose DIS Spam Attack Mitigation (DISAM) Scheme to effectively detect and mitigate Spam DIS attacks. Our contribution is summarized below:

- We implement the original RPL and the RPL with the adversary. We present details on the implementation and evaluation of our novel countermeasure that we called DISAM.
- We compared DISAM and its efficiency to the original RPL in terms of energy consumption and detection rate metrics using comprehensive Contiki-Cooja experiments. The obtained results indicate that our solution effectively reduces the spam DIS attack effect and improves the energy consumption in the RPL LLN.

The rest of the paper is organized as follows. An overview of existing and relevant literature is provided in Section 2. Section 2 discusses the basic RPL operations and Spam DIS attack. Section 4 focuses on the adversarial model and the countermeasure proposed. Section 5 presents an overview of steps in detection and mitigation of spam DIS attack along with algorithms. Extensive simulation experiments are provided and analyzed in Section 6.

2 RELATED WORK

This section classifies existing attacks and countermeasures of LLNs to explain how these attacks cannot resolve the spam DIS attack. In [11] heuristic-based detection technique to detect the malicious nodes to prevent suppression attacks in low-power lossy networks against Multicast Protocol, every node maintains the increment rate of a minimum sequence number in the Seed set and compares the recent increment of sequence numbers with the heuristically calculated threshold of sequence numbers. EYES [12] detects the forwarding misbehavior of multiple colluding malicious nodes in the energy harvesting networks. Each node checks the state (active and harvest) of the node and forwards the packet count to neighbor nodes to detect the malicious node.

In [13] CMD technique, the forwarding misbehavior of the preferred parent node is monitored, which observes the rate of packet loss and then compares the collected loss rate of packets with the observation result to detect the malicious node. A lightweight anti-jamming mechanism known as Dodge-Jam is proposed in [14] to investigate RPL reliability under external jamming attacks. It uses ACK channel hopping and multi-block data shifting with a small overhead to avoid stealthy jamming attacks. The exploration-based active detection (EBAD) scheme detects the routing misbehaviors in mobile ad hoc networks [15]. A source node broadcasts the router request packet with a fictitious destination node to attract potential malicious nodes. Then the digital signature techniques help to identify false information in the route reply packet. The camouflage-based active detection scheme proposed in [16] efficiently detects the forwarding misbehavior in Energy Harvesting Networks. Each node impersonates itself as an energy harvesting node and pretends not to overhear its neighboring nodes in any forwarding operations to detect malicious nodes.

Misbehavior aware detection scheme known as MAD is used to detect and prevent energy depletion attacks in RPL [17]. It maintains the count of several packets received from its neighboring nodes and compares that count with a dynamically computed threshold to detect malicious nodes in the network. In energy harvesting motivated networks, an acknowledgment-based countermeasure against stealthy collision intrusion is presented [19]. In wireless sensor networks, the identification of the selective forwarding attack is detected by using a single checkpoint supported approach combined with timeout and hop retransmission techniques with a random selection of a single checkpoint [20]. Dynamic Threshold Mechanism (DTM) scheme lowers the rate of discarding legitimate routes down the routing table by dynamically setting the threshold for every parent node.

Each node in the RPL network monitors its neighbor nodes and compares two consecutive DIS messages and its total count to a threshold value [21]. The initiators are blocked if their metrics exceed the threshold. Secure-RPL [22] uses the sender's IP address, previous DIS message receiving time, and the total number of DIS messages received since the last reset to mitigate the effect of DIS flooding attacks. It discards all DIS messages received before the expiry of RPL configured DIS interval from a particular neighbor. RPL-MRC [23] adapted RPL to reduce the response to multicast messages and readjusted trickle timer to address multicast DIS attacks in the RPL network. The authors in [24] examined the effects of DIS attack on DODAG construction and energy efficiency. They concluded with the simulation that the attack affects neighbor nodes more than the nodes at the extreme boundaries in terms of power consumption. A hybrid threshold-based IDS proposed in [25] uses DIS message sending rate and the packet interval to detect malicious RPL messages in the RPL-based IoT. The authors in [26] conducted extensive simulation experiments to evaluate the effects of a variety of battery drainage attacks against edge nodes in the IoT networks. They showed that the typical IoT devices' battery is certainly drained in 60 minutes even if they send a small number of packets. A hybrid placement strategy in [27] uses a blockchain, multi-agent, and deep learning algorithms to detect attacks from the IoT's transport layer.

Table 1. Summary of state-of-the-art methodologies against different problems

Methodology	DIS Requests	DAO Inconsistency	Forwarding Misbehavior	Route Manipulation	Multicasting Misbehavior	Packets Collision	Energy Consumption
HED [11]	×	×	×	×	✓	×	✓
EYES [12]	×	×	✓	×	×	✓	✓
CMD [13]	×	×	✓	×	×	×	✓
Dodge jam [14]	×	✓	×	×	×	×	✓
EBAD [15]	×	×	✓	✓	×	×	✓
CAM [16]	×	×	✓	×	×	×	✓
MAD [17]	×	×	✓	×	✓	×	✓
AAA [18]	×	×	✓	×	×	✓	✓
SCAD [15]	×	×	✓	×	✓	✓	✓
DTM [20]	×	✓	✓	✓	×	×	✓
[21]	✓	×	×	×	✓	×	✓
Secure-RPL [22]	✓	✓	×	×	✓	×	✓
RPL-MRC [23]	✓	✓	×	×	✓	×	✓
[24]	×	×	×	×	×	×	✓
[25]	×	×	×	×	×	×	✓
[26]	×	×	×	×	×	×	✓

Several solutions have assumed that the attack is triggered after the DODAG stability is reached; but it is possible with a zero-day attack before the DODAG formation. A threshold parameter to detect the DIS attack is used as a synthesis of security solutions by various state-of-the-art raise a question on how to set a threshold value for different topologies in dynamic networks? Some of the recent works only analyzed the forwarding misbehavior and route manipulation in a variety of network environments but did not focus on power consumption and control packets overhead. Moreover, most of these solutions do not consider RPL. We specifically addressed the DIS flooding in the RPL-based IoT environment and quantify the extent to which the DIS attack will affect battery consumption. Our proposed methodology does not require the formation of DODAG before the detection and mitigation of DIS attacks and can work during the DODAG formation. In addition, a trace table is maintained in a distributed architecture on all nodes. Table 1 presents a summary of proposed security solutions in the literature and demonstrates how it does not solve our problem.

3 THE RPL PROTOCOL AND SPAM DIS ATTACK

In this section we discuss the RPL protocol and spam DIS attack.

3.1 Overview of RPL Protocol

One of the most accepted routing protocols in terms of flexibility, proficient routing, and quality of service assistance in LLN's is RPL. It is a standardized network layer protocol introduced for LLN's. There are three types of topologies supported by RPL, labeled as a point to point, point to multipoint, and multipoint to point. RPL creates a simulated topological structure called DODAG is from LLN nodes. DODAG comprises three types of nodes labeled as router, host, and gateway, and it resembles a tree-like loop-free topology. Multiple RPL instances operate at the same time in a single blockchain-enabled IoT network, and there may be multiple DODAG's in a single RPL Instance. RPL instance-id

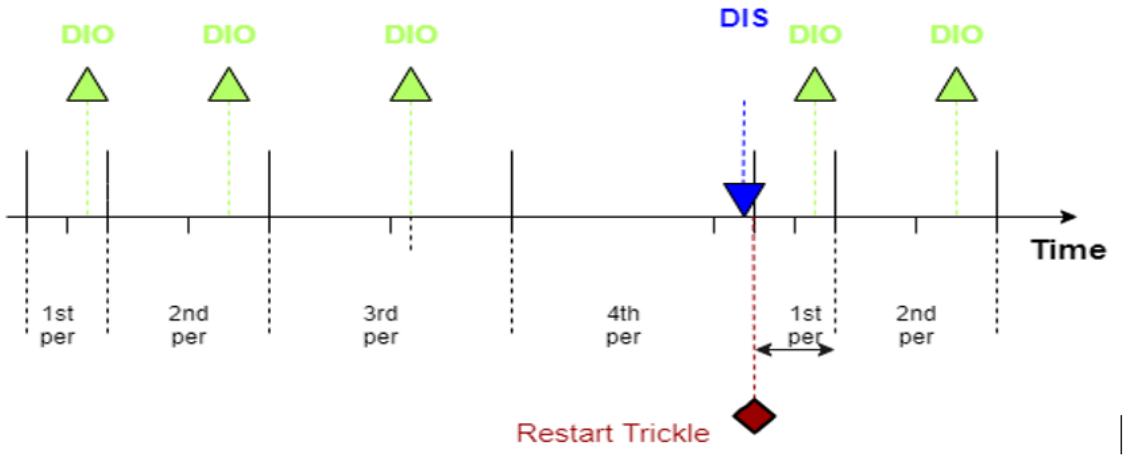

Fig. 1. Working of Trickle Algorithm

identifies RPL instance while DODAG id has a unique ipv6 address used to identify DODAG. RPL uses an adaptable mechanism called "Trickle Timer" to lessen the energy consumption of the network and to limit the control traffic.

There are four forms of control messages named, DODAG information object (DIO), DODAG information solicitation (DIS), Destination Advertisement Object (DAO), and DAO Acknowledgment (DAO-ACK) used by RPL for formation and preservation of DODAG [21]. A DIO message is methodically sent by the DODAG root, which is responsible for the advertising node's ranks. Whenever a node sends a DIO message, it advertises its assistance to its neighbors on their route to the DODAG root. The neighbor node can select a sender node as a preferred parent node in the DODAG. When the receiving node sends its own DIO, its neighbor can do the same as well, and so on. The trickle timer assists as a node's scheduler for DIO messages. Figure 1 shows that at the beginning of each cycle, the node sets the timer to the second half of the cycle by a random time and increase its time period if no DIS request is received. If the DIO messages are issued in the present cycle and do not exceed the threshold, the node transmits a DIO message to its neighbor. After this short cycle, the frequency of DIO messages gradually decreases and stays low as long as the network is secure [21].

DIO messages are requested from the DODAG node using DIS control messages. Nodes that are latest or existing use DIS to seek a nearby DODAG [21]. These are transmitted repeatedly by a node until it joins DODAG. As a result, there is a quick change in the network at the cost of control traffic. Trickle timer resets when a node receives a DIS message so that a DIO response can be sent back by the node rapidly [27]. Descending route information in the ascending direction along the DODAG using DAO messages [28]. DAO is unicast to choose parent in storage mode, and it is unicast to the root in DODAG [30]. DAO messages broadcast overturn route information and report the nodes visited along the ascending route. An overall descending path between the DODAG root and the node is acclaimed when the DODAG root receives the DAO messages [29]. DAO-ACK is a unicast packet delivered by the DAO parent or DODAG root to the source of the DAO message for acknowledgment as a response. Figure 2 shows how the exchange of control messages establishes the RPL network.

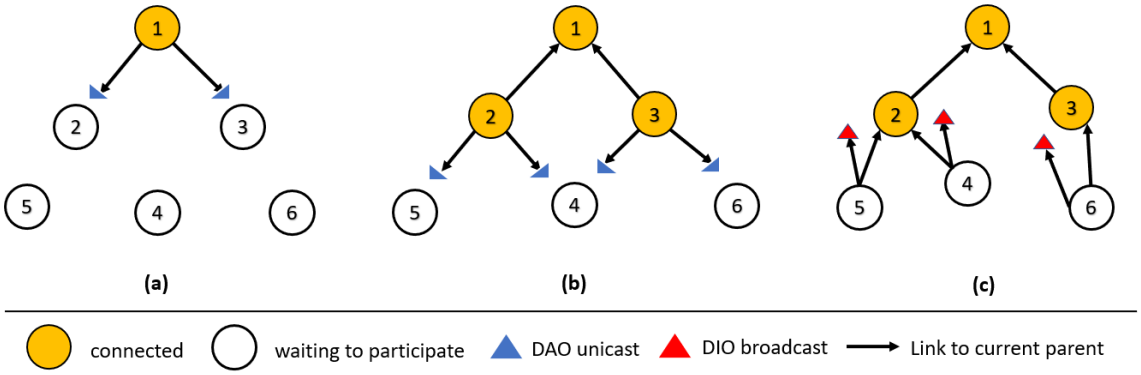

Fig. 2. Exchange of control messages to construct the topology using RPL a) Router node begins the propagation with DIO messages; b) establishes the connection and forward the information downwards; c) establishes the connection and send DAO message upwards

3.2 SPAM DIS Attack

The core concept of spam DIS attack is that the fraudulent node multicasts DIS messages in large proportion with multiple fake identities. These randomly generated fake identities do not exist in the network. The valid nodes consider them as new identities and restart the Trickle algorithm and distribute a large number of DIO messages in the network, which rapidly drains the energy supply of valid nodes and eventually makes them unable to communicate.

When the fraudulent node multicasts DIS requests with fake identity to nearby nodes, the neighboring nodes restart the Trickle algorithm from the minimum period tmin and send a DIO message with current network information at a random time in the second half of tmin. This repeated resetting of the trickle timer increases the control messages sent by the nodes. The control packet overhead increases, therefore, resulting in an unstable network. This sudden increase in control messages increases the total network power usage and decreases the overall life of the network. Figure 5 shows a DODAG, where a node Va is a malicious node that sends DIS messages with fake identities to valid nodes. The legitimate nodes start their trickle algorithm and flood the network with DIO messages after receiving multiple DIS requests from a malicious node. All the nodes in the network restart their trickle algorithm repeatedly and distribute many DIO messages in the network when the fraudulent node multicasts frequent DIS requests at a steady rate with fake identities to the neighboring nodes. Figure 3 shows that the malicious node Va multicasts multiple DIS requests with fake identities to the nodes v6, v7, and v8. The nodes that repeatedly receive multiple DIS requests restarts their Trickle algorithm from tmin and then transmits the DIO messages, which cause victim nodes to shorten the time interval of consecutive DIO messages due to a large number of received DIS requests and transmitted DIO messages will exhaust energy supply and communication throughput, and eventually causing the valid node v2 to drain its energy and suffer from denial of service.

4 THE PROPOSED DISAM SCHEME

We propose a DIS Spam Attack Mitigation (DISAM) scheme to detect Spam DIS attacks in RPL blockchain-enabled IoT and take sufficient measures against it. The DISAM algorithm follows the distributed architecture and runs on every node in the RPL network.

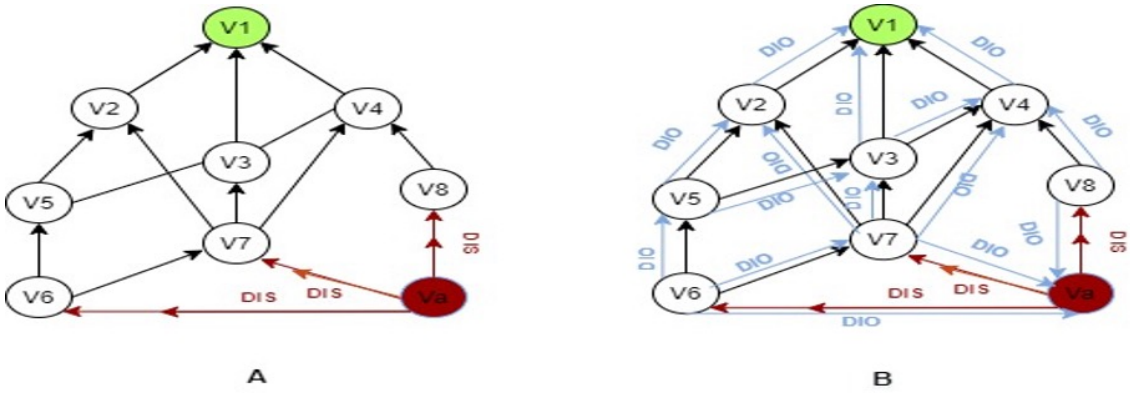

Fig. 3. In A part, a malicious node Va (in red) multicast DIS requests with fake identities to adjacent node and In B part, on receiving DIS requests the valid nodes flood the network with DIO messages

4.1 Adversary Model

In the RPL, we consider a low-power lossy network where one root of DODAG communicates with a set of constrained nodes through lossy connections. A unique ID identifies each node in the RPL network. In this paper, we consider one DODAG structure rooted in a DODAG root. An adversary can target and manipulate a legitimate node, gain access to confidential data like encryption keys, and reprogram it for malicious behavior.

The compromised node creates fictitious identities by changing the outgoing address in its packet. The legitimate nodes present in the network consider it a new node that wishes to join the network. The victim nodes accept the incoming DIS request of a new node and generate excessive DIO packets in the whole network to construct a link with the new node in the existing network. But at the same time, the malicious node starts injecting the packets multiple times with the new fake identities in the network. Every time the victim nodes receive a DIS packet, it will assume that new nodes want to be part of the network. So, the legitimate nodes will start generating DIO packets to establish links with these nodes resulting in the battery consumption of the nodes as the malicious node remains part of the network.

4.2 DIS Attack (DISA) Detection

We have proposed a detection technique to detect the Spam DIS Attack (DISA). DISA detection technique records every incoming DIS request from the new nodes that wish to be part of the network. It maintains a neighbor table for every new incoming neighboring node. The neighbor table stores the node ID and information of DIS and DAO packets received from the new node and keeps a record of new entries in that table until it reaches a threshold value. Whenever an existing network receives a DIS request, the detection process will start. A legitimate node starts maintaining the table upon receiving DIS requests. It will store the node ID, DIS, and DAO of that incoming packet. Figure 5 shows that the valid node always sends the DAO request after sending the DIS request if it joins the network. The table will store the entry of all new neighboring nodes until the DAO is not received to check the validity of new nodes. The table deletes the entry of the nodes whose record satisfies the normal working of the network. But, if the legitimate node does not receive the DAO packet in return for the DIS packet, then the record remains incomplete, and the table stores the information of that node permanently.

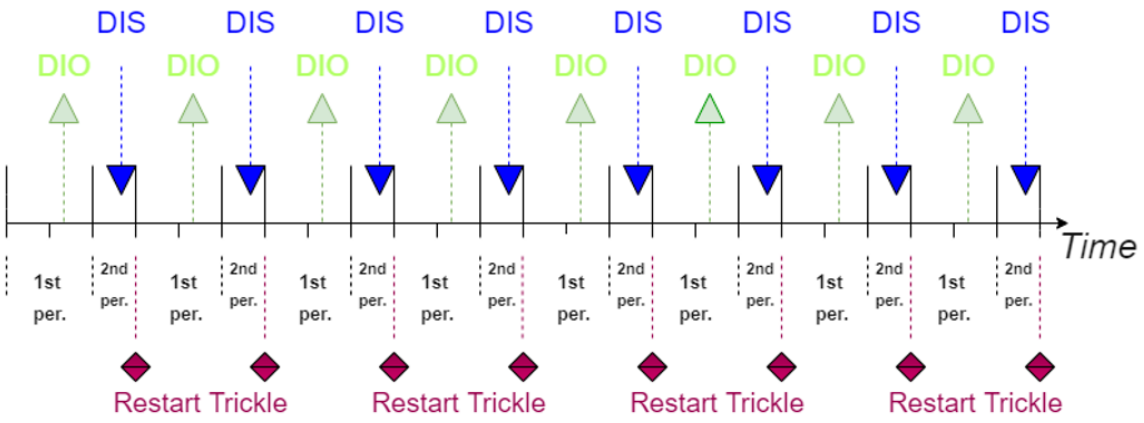

Fig. 4. The legitimate node v6, v7 and v8 repeatedly restarts its trickle algorithm after receiving multiple DIS requests

When a threshold value reaches, the legitimate node detects a fake node in that vicinity that sends multiple fake DIS requests with fictitious identities. So, it will start the mitigation process to secure the network by saving the energy of the nodes. Figure 6 shows that the malicious node Va sends a DIS request to its neighboring node. It sends another DIS request by changing its identity as b, and it sends multiple requests every time by changing its address in the DIS packets as c, d, e, f, etc., at the same time, the legitimate nodes will maintain the table and keep the check of DAO received from these nodes.

4.3 DIS Attack Mitigation (DISAM) Scheme

We propose a countermeasure that we called the DIS attack mitigation (DISAM). DISAM saves the energy consumption of the nodes by maintaining a threshold value to prevent the Spam DIS attack. The legitimate leaf nodes use the threshold value to secure the network by discarding the malicious DIS packet at their end. It saves the network from generating excessive DIO in reply to DIS requests from fake identities. This process saves energy by controlling the rate of new generating packets. Once the time of DISAM has elapsed, the network will return to its normal state. If the attack remains in the network, then DISAM will again start its process. The network will continue to go back and forth between the mitigating and normal states until the attack vanishes entirely from the LLN network. Figure 6 shows how does the network discards the upcoming DIS requests.

4.3.1 Maintaining Trace Table. The nodes start maintaining the table whenever they receive a DIS request from any node with different addresses. The table stores node ID, DIS, and DAO. The node ID will store the address of a node that has received the DIS request. DIS check verifies the DIS request from the node ID, and DAO check verifies the DAO request from that node ID. The entries that satisfy the normal working of the network will be removed i.e., the exchange of three control messages (DIO, DAO, and DAO-ACK) after receiving DIS creates a permanent network connection with that node. So, when the entry satisfies the check of DIS and DAO messages received from the same node, it passes the normal working of the RPL. It will only store entries that do not generate DAO message that defies standard RPL operation. Table 2 presents few entries of the malicious node and shows the DIS request from a, b, c, d, e is received but DAO is not received. The DISA neighbor table keeps entering the new nodes until it reaches the threshold value.

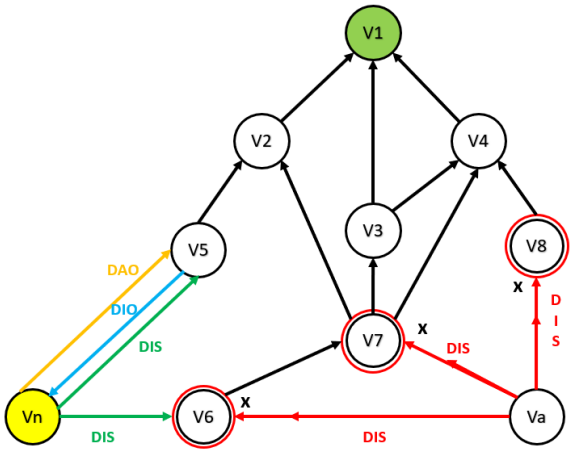

Fig. 5. This displays the exchange of control messages of non-malicious node

4.3.2 Detection of Attack. In this step, the victim nodes check the count of records with DIS requests received and no DAO received. If the count of such entries in the table exceeds our given threshold value, then this means spam DIS requests are coming into our network. We detect an attack and apply a mitigation scheme to reserve the resources of the sensor nodes.

4.3.3 Mitigating the Attack. After detecting the attack, the victim node/nodes will discard the DIS request that enters the network for a predefined period. Once the time of mitigation has expired, then the network is in its normal state.

5 PERFORMANCE ANALYSIS

5.1 Simulation Platform

We implement and evaluate our methodology by extensive simulation experiments on the COOJA Simulator of Contiki-NG running on Linux 18.12 (64 bit). The operating system used for memory, network constrained, and low-power blockchain-enabled IoT is Contiki-NG programmed in C language. This platform provides flexible simulation for the sensor networks and facilitates the effective implementation of new incoming protocols. Contiki-NG implements RPL-lite, the default protocol of IEEE. Contiki-NG contains two implementations of the RPL protocol, RPL lite and RPL classic. RPL lite contains a non-storing mode of operation of nodes and removes the complexity of handling multiple DODAGs and instances. The non-storing mode uses less power and memory in which only the DODAG root makes the routing table, and all other nodes do not have to make the routing table for the downward routes. It uses MRHOF, an

Table 2. DIS and DAO counter difference

Node ID	DIS check	DAO check
V_a	✓	×
V_b	✓	×
V_c	✓	×
V_d	✓	×

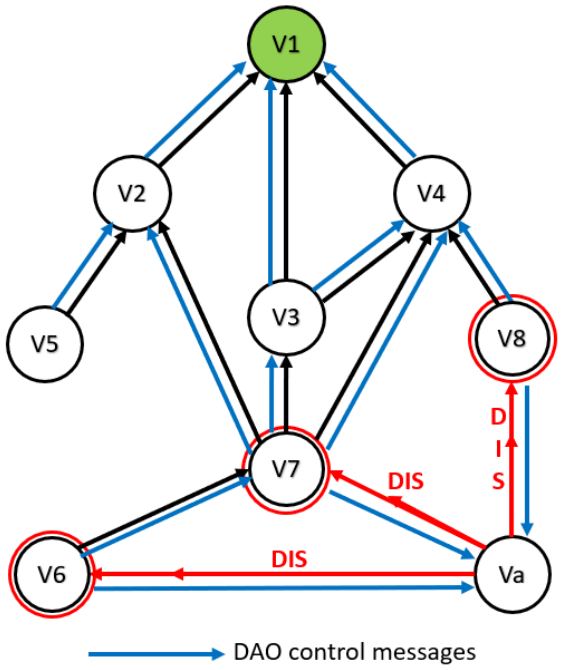

Fig. 6. Malicious node sends DIS request by changing the address of its outgoing packets

objective function that calculates the rank to make the topology. COOJA is used in our case to test the code for the emulation of resource-constrained devices and the communication with the realistic protocol before emulating it on real hardware. Table 3 shows the simulation parameters.

5.2 Network Model

The network configuration contains 30 nodes uniformly distributed with one DODAG root in a 100 x100m square area. The communication transmission range and the interference range are set to 30m. There is one DODAG root node in the network, which is node 1, and a total of three malicious nodes, which are randomly distributed in the network and marked as node 6, node 11, and node 20. All other nodes are client nodes as described in the network diagram. The packet rate of spam DIS injection is set to 0.1-5pkt/sec. We have used the lowest rate of 0.1pkt/sec to test the low data rate conditions of the attack and implemented methodology, and DISAM beats every data rate of the attack whether it is too low or high. Total simulation time is 600 seconds with a 5-time repetition to obtain steady performance results. The threshold value set for making the neighbor table is 3, and the other threshold set for the mitigation time is 30 seconds. Figure 7 shows the network configuration.

5.3 Energy Calculation Parameter Description

Energy consumption is directly proportional to the number of transmission energy. The transmission process consumes the maximum amount of energy consumes in sensor networks. The processing energy or the receiving energy is very minimal as compared to the energy consumed during transmission. So, we can approximate the energy consumed in the

Algorithm 1: Spam DIS Attack Detection and Mitigation Algorithm

```
input : node id N_id, packet type P_t, control message P_kt, DIS or DAO type T, sender id S_id, check packets C_pkt,
        trace table Table, detection function Detect(.), and mitigation function Mitigate(.);
// Step 1: Maintaining Table
if P_kt → DIS then
    Table = [S_id, true, false]
    C_pkt → DAO
    if Table = [S_id, true, true] then
        do nothing
    else
        // Step 2: Detection
        Function Detect():
            if Table = [S_id, true, false] ≥ threshold then
                discard irrelevant DIS requests
                // Step 3: Mitigation
                Function Mitigate():
                    discard incoming DIS requests for t30
                    if P_kt = DIS then
                        go to step 1
                    end
                End Function
            else
                do nothing
            end
        End Function
    end
else
    go to step 1
end
output : Spam DIS Attack Mitigation after Detection
```

network by counting the number of packets transmits in the normal state, attacking state, and the state when DISAM is applied. The DISAM reduces the number of DIO control packets in the network. Key parameters including the injection rate of the DIS message and the number of malicious nodes are changed to measure the energy consumption using the DIO control packet. Blockchain-enabled IoT devices are power constrained. Therefore, in this paper, we measure the performance in terms of energy consumption by changing key simulation parameters, including spam DIS message injection rate and the number of the malicious node. Power consumption is the average power consumed by all the nodes in the network during the simulation. Power consumption for each node is measured by adding up the energy consumed on CPU ON (listening state), LPM (low power idle state), RX (radio listen state), and TX (radio transmit state). Packet injection rate is set to 0.1, 0.2, 0.3, 0.4, and 0.5 pkt/sec to emulate low data rate and high data rate scenarios. The number of malicious nodes varies from 1-3.

5.4 Simulation Results and Analysis

Figure 8 shows the energy consumption against the packet injection rate. The packet injection rate in the network is measured in terms of the number of broadcasts and received DIO messages by changing key parameters. The spam DIS injection rate and the number of malicious nodes in the network are changed to measure the energy consumption in the network. The original RPL and the RPL with adversary show the different energy consumption rates. It indicates

Table 3. Simulation Parameters

Parameter Names	Values
Simulation Area	100 ×100m
Number of Nodes	30
Simulation Time	6000 sec
Mote Type	Cooja Mote
Mac/Adaptive Layer	IEEE 802.15.4/6/6LowPAN
Radio Model	CC2420
Transmission Range	30m
Interference Range	35m
Routing Protocol	RPL
Mode of Operation	Non-Storing Mode
Rank Metric	MRHOF
Packets Send Interval	0.1-0.2-0.3-0.4-0.5 (pkt/sec)
Node Distribution	Uniform Distribution
Malicious Nodes	6, 11, 20
DISA Neighbor Table Threshold	1
Mitigation Time Threshold	30sec

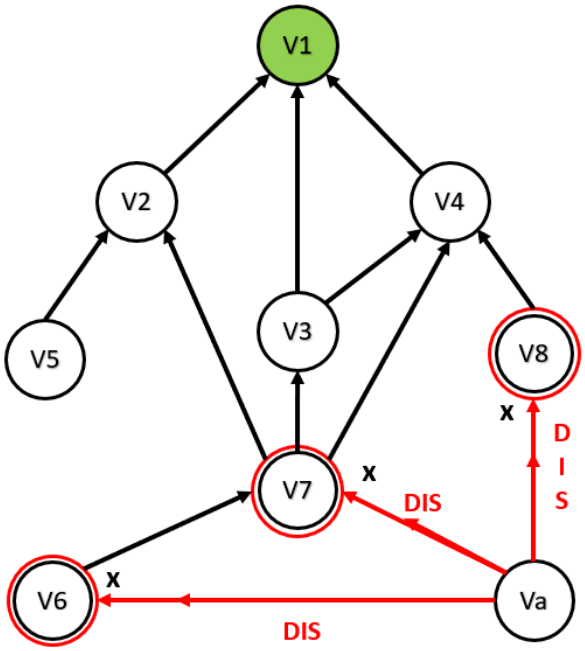

Fig. 7. Valid nodes discard the upcoming DIS requests

that energy consumption is directly proportional to the number of malicious nodes and their packet injection rate in the network. Because more malicious nodes exist in the network, therefore, the number of DIS messages increases. The malicious node broadcasts DIS messages by frequently changes its identity to probe for DIO messages. Although the

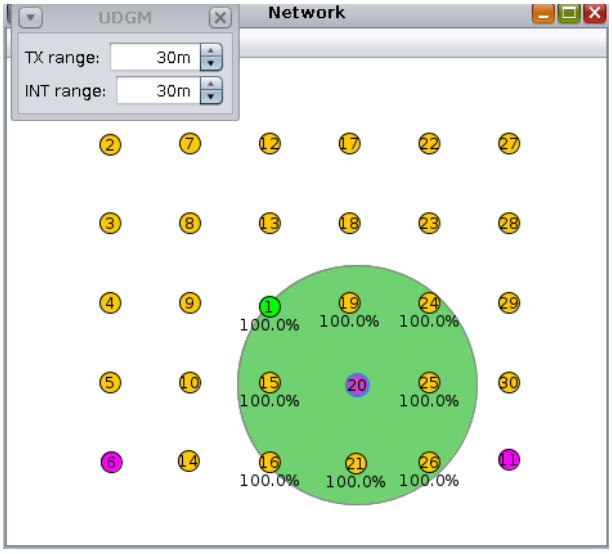

Fig. 8. Network Model

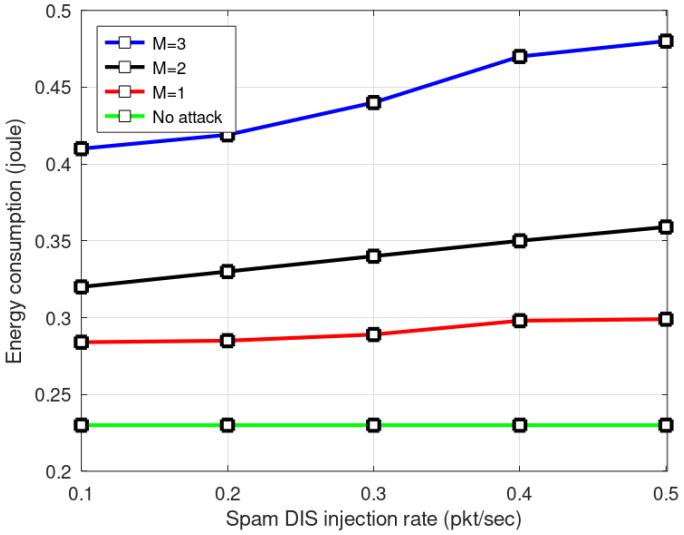

Fig. 9. Energy Consumption against Packet Injection Rate

Trickle timer reduces the redundant DIO messages in the network, the increased spam DIS injection rate restarts the trickle timer again, and again and the DIO messages increase significantly. Thus, energy consumption increases.

Figure 9 shows the energy consumption against elapsed simulation time by varying the DIS injection rate and the number of malicious nodes. The RPL with and without adversary indicates that energy consumption increases as time increase. The malicious nodes quickly increase energy consumption by generating spam DIS requests in the network.

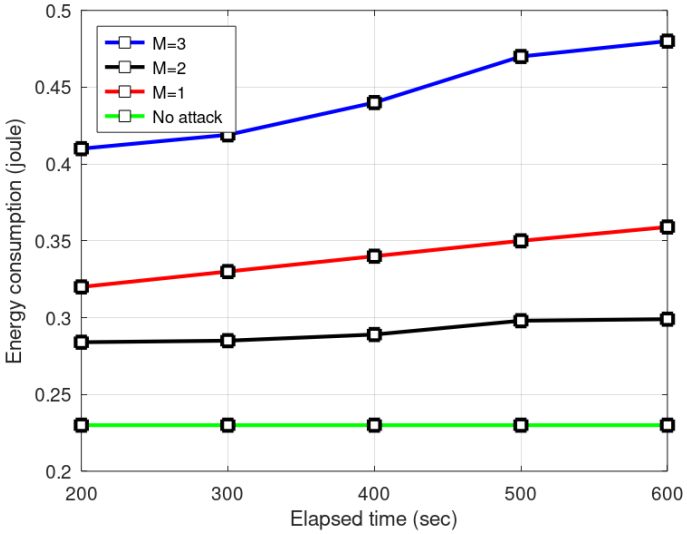

Fig. 10. Energy Consumption against Elapsed Time

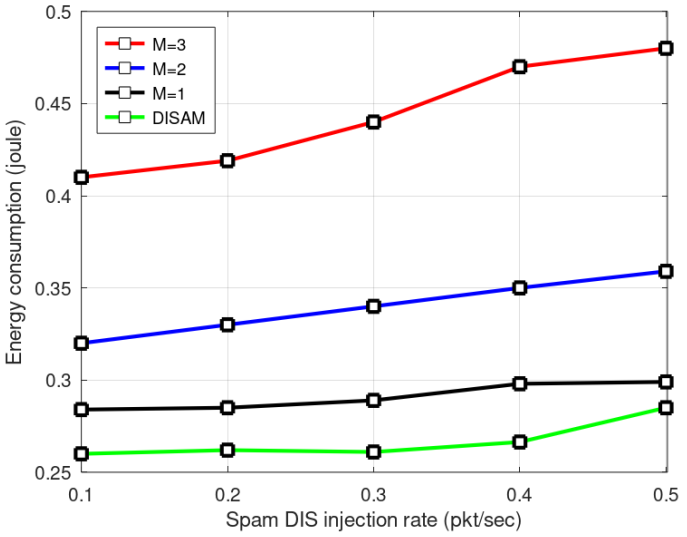

Fig. 11. Performance Evaluation with Attack and DISAM

As the multiple spam DIS requests with different fictitious identities increase as time passes, it restarts the trickle timer again and again in the network and generates an increased number of DIO packets. Hence energy consumption in the network increases because of increased DIO packets in the network.

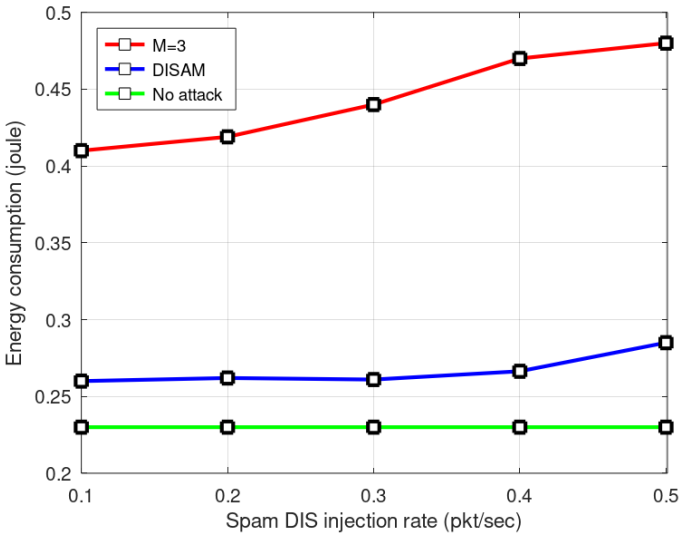

Fig. 12. Performance Evaluation of DISAM against Packet Inject Rate

Figure 10 shows the comparison between the DIS attack and the DISAM technique. The energy consumption against the packet injection rate is measured. The graph indicates that as the packet injection rate of malicious nodes increases in the network, the energy consumption increases. But, with DISAM technique shows the lower energy consumption in the network as compared to the RPL in an adversary state. The DISAM technique reduces the number of malicious DIO packets in the network and thus mitigates the attack at a constant rate. The DISAM technique is independent of the DISA injection rate and reduces the attack at a constant rate.

In figure 11, we measure the detection rate of the proposed DISAM technique against energy consumption and compare the energy consumption between attack state, no attack state, and the state when DISAM is applied. The graph indicates the greater energy consumption in case of attack and the lowest energy consumption when no adversary is present. It shows more change in energy consumption between normal states and the attack state. Furthermore, it presents a slight change in energy consumption between the normal state and the state when the DISAM technique is applied. It shows the DISAM's effectiveness in bringing back the adverse network to the normal state and increasing the network performance.

It can be seen from the graph that how the DISAM technique has worked with the lowest and highest packet injection rate. When the DISA injection rate is low enough i.e., 0.1pkt/sec the DISAM detects and mitigate it at a constant rate, and when the spam DIS injection rate is high enough i.e., 0.5, the mitigation scheme has not been affected by this too and works consistently in all the conditions that show that it is independent of the spam DIS injection rate. Hence, the energy consumption of the nodes does not increase as the packet rate increases under the DISAM technique.

6 CONCLUSION

A spam DIS attack is one of the energy depletions attacks in which a malicious node generates multiple fictitious identities and sends a DIS request to increase the transmission process in the network and thus depletes the battery of

the nodes. In this paper, we have implemented the spam DIS attack and proposed its detection and mitigation scheme. We compare energy consumption in an original RPL, DIS attack, and under the DISAM states. Simulation results show that the attacking state consumes more energy than the normal state, and under DISAM, slightly more energy is consumed. Moreover, the DISAM technique detects and mitigates the attack independent of malicious nodes and spam DIS injection rate. We aim to extend our work on the DIS plus DAO attack and its detection and mitigation scheme in future work.

REFERENCES

[1] Pallavi Sethi and Smruti R. Sarangi. 2017. Internet of Things: Architectures, Protocols, and Applications. Journal of Electrical and Computer Engineering, Vol. 2017. Article 9324035. 2017, 25 pages. https://doi.org/10.1155/2017/9324035.

[2] Ibrar Yaqoob, Ejaz Ahmed, Ibrahim Abaker Targio Hashem, Abdelmuttlib Ibrahim Abdalla Ahmed, Abdullah Gani, Muhammad Imran, and Mohsen Guizani. 2017. Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges. In IEEE Wireless Communications, Vol. 24. Issue 3. 22 June 2017, 10-16. doi: 10.1109/MWC.2017.1600421.

[3] Ali Kadhum Idrees, Karine Deschinkel, Michel Salomon, and Raphael Couturier. 2017. Multiround Distributed Lifetime Coverage Optimization protocol in wireless sensor networks. The Journal of supercomputing. 74. December 2017. 1949–1972. https://doi.org/10.1007/s11227-017-2203-7.

[4] Ali Kadhum Idrees, Karine Deschinkel, Michel Salomon, and Raphael Couturier. 2016. Perimeter-based coverage optimization to improve lifetime in wireless sensor networks. Engineering Optimization, March 2016. 48:11, 1951-1972. doi: 10.1080/0305215X.2016.1145015.

[5] Ali Kadhum Idrees, Karine Deschinkel, Michel Salomon, and Raphael Couturier. 2015. Distributed lifetime coverage optimization protocol in wireless sensor networks. The Journal of supercomputing.71, November 2015. 4578–4593. https://doi.org/10.1007/s11227-015-1558-x.

[6] Mark Needleman. 2000. The internet engineering task force. Serials Review 26, Issue 1.2000. 69-72.

[7] Tim Winter, Pascal Thubert, Anders Brandt, Jonathan W. Hui, Richard Kelsey, Philip Levis, Kris Pister, Rene Struik, Jean-Philippe Vasseur, and Roger K. Alexander. 2012. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. rfc 6550. 2012. 1-157.

[8] Patrick Olivier Kamgueu, Emmanuel Nataf, and Thomas Djotio Ndie. 2018. Survey on RPL enhancements: a focus on topology, security and mobility. Computer Communications. 120. 2018. 10-21.

[9] Harith Kharrufa, Hayder AA Al-Kashoash, and Andrew H. Kemp. 2019. RPL-based routing protocols in IoT applications: A Review. IEEE Sensors Journal. Vol 19. Issue 15. 2019. 5952-5967.

[10] Arsalan Mosenia and Niraj K. Jha. 2016. A comprehensive study of security of internet-of-things. IEEE Transactions on emerging topics in computing. Vol 5. Issue 4. 2016. 586-602.

[11] Cong Pu, Xitong Zhou, and Sunho Lim. 2018. Mitigating suppression attack in multicast protocol for low power and lossy networks. In 2018 IEEE 43rd Conference on Local Computer Networks (LCN). 2018. 251-254.

[12] Cong Pu, Sunho Lim, Byungkwan Jung, and Jinseok Chae. 2018. EYES: Mitigating forwarding misbehavior in energy harvesting motivated networks. Computer Communications 124. 2018. 17-30.

[13] Cong Pu and Salam Hajjar. 2018. Mitigating forwarding misbehaviors in RPL-based low power and lossy networks. In 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC). 2018. pp. 1-6.

[14] Jeongyoon Heo, Jung-Jun Kim, Saewoong Bahk, and Jeongyeup Paek. 2017. Dodge-jam: Anti-jamming technique for low-power and lossy wireless networks. In 2017 14th Annual IEEE International Conference on Sensing, Communication,

and Networking (SECON).2017. 1-9.
[15] Cong Pu, Sunho Lim, Jinseok Chae, and Byungkwan Jung. 2019. Active detection in mitigating routing misbehavior for MANETs. Wireless Networks 25, Issue 4. 2019. 1669-1683.
[16] Cong Pu and Sunho Lim. 2015. Spy vs. spy: Camouflage-based active detection in energy harvesting motivated networks. In MILCOM 2015-2015 IEEE Military Communications Conference. 2015. 903-908.
[17] Cong Pu and Bryan Groves. 2019. Energy depletion attack in low power and lossy networks: Analysis and defenses. In 2019 2nd International Conference on Data Intelligence and Security (ICDIS). 2019. 14-21.
[18] Cong Pu, Sunho Lim, Byungkwan Jung, and Manki Min. 2017. Mitigating stealthy collision attack in energy harvesting motivated networks. In MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM). 2017. 539-544.
[19] Cong Pu and S. Lim. 2018. A Light-Weight Countermeasure to Forwarding Misbehavior in Wireless Sensor Networks: Design, Analysis, and Evaluation. IEEE Systems Journal. Vol. 12. Issue. 1. 2018. 834–842.
[20] Cong Pu. 2018. Mitigating DAO inconsistency attack in RPL-based low power and lossy networks. In 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC). 2018. 570-574.
[21] Ge Guo. 2021. A Lightweight Countermeasure to DIS Attack in RPL Routing Protocol. 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC). 2021. 0753-0758.
[22] Abhishek Verma and Virender Ranga.2020. Mitigation of DIS flooding attacks in RPL-based 6LoWPAN networks. Transactions on emerging telecommunications technologies 31, Issue 2. 2020. e3802.
[23] Faiza Medjek, Djamel Tandjaoui, Nabil Djedjig, and Imed Romdhani. 2021. Multicast DIS attack mitigation in RPL-based IoT-LLNs. Journal of Information Security and Applications 61. 2021. 102939.
[24] Saurabh Sharma and Vinod Kumar Verma. 2021. Security explorations for routing attacks in low power networks on internet of things. The Journal of Supercomputing 77, Issue 5. 2021. 4778-4812.
[25] Philokypros P Ioulianou and Vassilios G. Vassilakis. 2019. Denial-of-Service Attacks and Countermeasures in the RPL-Based Internet of Things.In CyberICPS/SECPRE-/SPOSE/ADIoT@ ESORICS. 2019. 374-390.
[26] Ryan Smith, Daniel Palin, Philokypros P. Ioulianou, Vassilios G. Vassilakis, and Siamak F. Shahandashti. 2020. Battery draining attacks against edge computing nodes in IoT networks. Cyber-Physical Systems 6, Issue 2. 2020. 96-116.
[27] Chao Liang, Bharanidharan Shanmugam, Sami Azam, Asif Karim, Ashraful Islam, Mazdak Zamani, Sanaz Kavianpour, and Norbik Bashah Idris. 2020. Intrusion detection system for the internet of things based on blockchain and multi-agent systems. Electronics 9, Issue 7. 2020. 1120.
[28] Habib M Ammari. 2019. Mission-Oriented Sensor Networks and Systems: Art and Science. Studies in Systems, Decision and Control. 2019.
[29] Cong Pu. 2019. Spam DIS attack against routing protocol in the Internet of Things. In 2019 International Conference on Computing, Networking and Communications (ICNC). 2019. 73-77.
[30] Aashima Bisen and Jimmy Matthew. 2018. Performance Evaluation of RPL Routing Protocol for Low Power Lossy Networks for IoT Environment. In 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET). 2018. 1-8.