IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 27, 2020, accepted February 21, 2020, date of publication March 2, 2020, date of current version March 12, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2977476

Mitigation Mechanisms Against the DAO Attack on the Routing Protocol for Low Power and Lossy Networks (RPL)

ISAM WADHAJ, BARAQ GHALEB, (Student Member, IEEE), CRAIG THOMSON, AHMED AL-DUBAI, AND WILLIAM J. BUCHANAN

Institute for Informatics and Digital Innovations, Edinburgh Napier University, Edinburgh, EH10 5DT, U.K.

Corresponding author: Isam Wadhaj (i.wadhaj@napier.ac.uk)

This work was supported by Edinburgh Napier University.

ABSTRACT Destination Advertisement Objects (DAOs) are sent upward by RPL nodes toward the DODAG root, to build the downward routing paths carrying traffic from the root to its associated nodes. This routing mechanism can be exploited by a malicious node periodically transmitting a large volume of DAO messages towards its parent, which in turn will forward such messages to its own parent and so on, until they arrive at the Direction-Oriented Directed Acyclic Graph (DODAG) root. This ultimately results in a negative effect on network performance in terms of energy consumption, latency and reliability. The first objective of this paper is to evaluate the effect of such a DAO attack in the context of an RPL IoT network. In particular, identifying the particular performance metrics and network resources affected most greatly. The second objective is the proposal of mitigating security mechanisms in relation to DAO attacks and to evaluate their effectiveness. The simulation results have shown how the attack can damage the network performance by significantly increasing the DAO overhead and power consumption. It also demonstrated that the DAO attack affect the reliability of the downward traffic under specific conditions. The proposed mechanisms showed a good capacity in restoring the optimal performance of the network by up to 205%, 181%, 87% and 6%, in terms of overhead, latency, power consumption and packet delivery ratio respectively.

INDEX TERMS Internet of Things, low power and lossy networks, security in RPL, DAO attack.

I. INTRODUCTION

The Internet of Things (IoT) is a generic term used to describe network devices and things that are interconnected. This term often falls in the context of high-performance smartphones, tablet computers and small devices equipped with a tailored transmission technology as a basis for communication. The communication between said devices is subject to restrictions on the performance of nodes that have limited computing power and resources [1]. To cater for such limited resources, the Routing Over Low-power and Lossy Networks (RoLL) working group of the IETF investigated the capacity of common routing protocols to satisfy the routing requirements of the Low-power and Lossy Network (LLN). The group finally reached the conclusion that such can meet the special routing requirements of LLN, and, hence, introducing what they named as the Routing Protocol for Low power and Lossy Networks (RPL) [2], [3].The security features of RPL have been investigated extensively in research, indicating that there are some security issues that must be addressed to enable wider adoption of the protocol [4]–[14]. A vital security concern is the DAO (Destination Advertisement Object) attack. This attack functions with the adversary node regularly advertising false DAO messages to its parent nodes, leading to network resource exhaustion as the parent will attempt to update the routing table by flooding the network with the received DAO messages. Thus, the attack will lead to an increase on processing power required to complete the routing table update and the DAOs transmission to parent nodes. Another factor that increases the effectiveness of the attack is that in RPL under storing mode the transmission of DAO messages follows the upward direction towards the sink, and thus the scope of damage increases beyond area of the attacker node [3], [15]. These consequences downgrade the network performance with respect to routing overhead, power consumption, latency and PDR, which significantly shorten the network lifetime [16].

To address this issue, we extended our previous work in [17] in which we proposed a solution to mitigate the aforementioned attack. This work has been extended by first

The associate editor coordinating the review of this manuscript and approving it for publication was Haris Pervaiz.

introducing a new mitigation technique and evaluating their efficiency compared to the unsecured version of RPL as well as our previous solution. We have also evaluated both solutions under wider simulation environments and parameters. The obtained results have demonstrated that our proposed solutions are very effective in mitigating the DAO attack and can upgrade the network performance significantly with respect to power consumption, routing overhead and the packet delivery ratio.

The rest of the paper is structured as follows. Section II provides a brief overview of the security concepts of RPL.In Section III, the state of art is provided. An overview of the RPL protocol in storing mode is highlighted in Section IV. Section V presents an overview of the DAO attacks. Section VI presents detailed discussion of the proposed countermeasure to the attacks. Section VII evaluates the performance of a RPL network under DAO attack under various scenarios with respect to several metrics and through extensive simulation experiments.In section VIII the paper is concluded.

II. SECURITY CONCEPTS OF RPL

Vulnerable components in an LLN include the routing information that is exchanged and stored, as well as the available resources of the nodes and the processes running on them [17]. Routing information is exchanged in LLNs using wireless communication at the control layer and partially cached on the reprocessing nodes. The resources on the nodes consist of their computing power, available memory, available energy, and the bandwidth available to communicate with their neighbors. The routing processes of the node summarize services that generate and maintain routes in the topology. Among the potential attacks in the immediate area of the topology is the possibility to attack the RPL nodes from a distance through the Internet. This is made possible by the fact that RPL is designed for use on low-resource nodes, allowing communication and interaction with nodes from other IPv6-based networks [7], [8]. To protect against attacks, RPL defines optional cryptographic protections that enable secure communication using secret keys [18].

The type of RPL attacks can be categorized into two types of attacks:

1) Topology attacks: Attacks that can be used to manipulate the orientation of the paths of a DODAG (Direction-Oriented Directed Acyclic Graph). For this purpose, the attacker attempts to deform the DODAG in a targeted manner, so that the paths on which messages are exchanged are directed specifically into certain sections of the DODAG or the message exchange on the affected branches is disturbed. In the Storing Mode of Operation (MOP), the attacker can advertise paths to non-existent sub-DODAG nodes by tampering with DAOs, fictitious prefixes. The information about the advertised prefixes of the DAO propagates upward to the root of the DODAG. All parent nodes in the relevant branch enter the advertised prefixes in their routing tables, and potentially cannot enter and serve sub-DODAGs of other children. Nodes whose downward prefixes cannot be operated in the affected branch will only be able to advertise their prefixes in other branches if available. If the nodes migrate their paths to the alternate parent nodes, their downward routes are pushed out of the affected upward branch of the attacker, resulting in a degeneration of the original DODAG. If a child with its sub-DODAG incorrectly joins a parent node that cannot operate the sub-DODAG with messages in the direction of the child, the prefixes are not advertised upward and remain unknown on the downward path to the affected parent node [19], [20].
2) Resource Attack: Attacks that increase the energy consumption of RPL nodes. The attacker attempts to load a node with computationally intensive operations and frequently consumes its memory. The motivation behind the attacks is to weaken the performance of the entire topology and thereby disrupt the operation in the DODAG [21], [22].

III. RELATED WORK

The Rank authentication and Parent Failover techniques are two schemes described in [23] that provide a solution to Sinkhole attack. The first, relaies on the generation of one-way hashes (which are attached to DIO messages) to provide a mechanism for legitimate nodes to verify if another node on the path to the sink is advertising a fake rank. In the latter, a sink node uses an Unheard Nodes Set (UNS) field in the DIO message to advertise a child node that (based on pre-defined baseline) it is not sending enough traffic. When the advertised node receives the DIO message, it adds its parent node to a blacklist. It is noted that the hash calculation and verification process and the extra UNS field create additional energy consumption and traffic overhead which, however, do not degrade the network performance in a significant way. The two solutions together provide an efficient defence against sinkhole attacks, but this method is proven to not work against a combination of Sybil Attack and Sinkhole Attack and was not targeting the DAO attack.

The authors in [24] investigated the consequences of a Blockhole attack in RPL topology highlighting different factors which indicates the network could be under a this attack: rate of DIO messages, packet delivery ratio and packet loss. They also proposed a defence system which is based on a per-node trust mechanism based on the forwarding behaviour of neighbours node in the network. The Trust value depends on the positive feedback awareness among the nodes and the trust evaluation analysis. It is a fairly complicated method which will create overhead and require additional computational power, but results from the paper prove it to be effective.

In [6] the authors proposed a solution for the detection and isolation of a malicious node that is attempting a Decreased Rank attack. The Version Number and Rank Authentication (VeRA) system prevents the attacking nodes of obtaining false rank values through crafted advertisement, by implementing a one-way hash chain method in the RPL protocol and making sure that rank advertisements in the topology are from legitimate nodes; this will prevent compromised nodes from publishing an illegitimate decreased Rank to its neighbours. The system is developed upon three building blocks a Hash Function, MAC (message authentication) and a Digital Signature function. The system is also proven to be effective against the Version Attack, but it will inevitably create traffic overhead and requires more computational operation, hence degrades the overall networks performances.

The authors in [14] proposed several countermeasures against DIO suppression attack that are more protocol oriented, appending a Message Integrity Code (MIC) to the messages as RPL specification can be effective in preventing the DIO suppression attack. Another proposed solution is to enable MAC-layer encryption to make it impossible for the attacking node to distinguish DIO messages from other messages. The latter solution will creates network traffic overhead and will need more computational power.

A solution proposed to mitigate the Selective forwarding attack in [7] is to create alternative path in the RPL topology that are dynamically selected by nodes. The solution seems feasible if we assume that there may be multiple nodes in the DODAG with a similar link quality. However, this type of traffic control will inevitably create some overhead in the network. Another solution is to use encryption mechanism to make the malicious node not distinguish different type of traffic and therefore either forward or drop all traffic.

In [25] the authors presented different solutions to detect and mitigate a wormhole attack. One approach is to give geographical information to the nodes and, therefore, to the neighbourhood. Another solution is to use separate link layer keys for different portion of the network, resulting in the impossibility for two nodes in different segments to communicate between each other. A more complicated approach is to use a Merkel Tree Authentication schema for the construction of the topology. Basically, this approach makes use of nodes IDs and public key for Hash calculation. The topology construction starts from the leaf rather than from the sink and a parent is identified by its children. The nodes authentication starts from the root and if any nodes fails to authenticate, the children discard the node as parent.

Reference [26] states that no solution has been specifically designed for HELLO Flooding attack. It shows through a simulation how the attach will be removed in a reasonable amount of time by the RPL Global and Local repair mechanism.

In [27] the author proposed a dynamic threshold mechanism to mitiagte DAO inconsistency attack, named DTM. With this mechanism, parent nodes could dynamically regulate the threshold of receiving forwarding error packets within a period. Beside this, RPL includes an optional mechanism that can be used to repair DAO inconsistencies called DAO inconsistency loop recovery.

IV. RPL ROUTING PROTOCOL OVERVIEW

The RPL routing protocol provides the primary communication pattern for multi-hop communication in LLNs. In addition to the multipoint-to-point (MP2P) communication, RPL also allows point-to-point (P2P) communication between two nodes within the topology, as well as a point-to-multipoint (P2MP) communication in which, the root node simultaneously transmits packets to several node in the topology. RPL uses Directed Acyclic Graphs (DAGs) to construct its physical topology, where each DAG is rooted at a single destination known as a Destination-Oriented DAG (DODAG) [3], [4].

A node sends DIO control messages to advertise its position in the DODAG and inform the neighbor node in its environment whether it is available as a default next-hop node. The DIO contains the necessary information that allows a node to join the DODAG as a participant [3]–[5]. In addition, it can determine the preference for a particular parent node, which it uses as the preferred node to communicate upwards towards root [3]. If the DIO sender is selected as the new preferred parent node, the receiver node will first add the sender address to the parent list then calculates its own rank in the DODAG, using the information from the DIO and the OF. It then set up a default route towards its preferred parent and update the DIO message with the new rank. The updated DIO message is then multicasted to the neighboring nodes to repeat the said operation [3], [4].

In RPL DAO control messages are used to build routes in the downward direction. DAOs propagate upwards in the direction of the root node and include information on the branches of a node in the downward direction. They allow you to build routes from a node to the leaf nodes of the topology. DAO control messages are sent when a DIO is received to advertise which nodes the sender of a DIO can reach downward. A node slightly delays the sending of DAO control messages. This allows the node to consolidate information from one-way DAOs of the downward branches before forwarding the information in DAOs to its parent node. Receiving a DAO can optionally be confirmed by a DAO ACK control message [3].

In the non-storing MOP, each node enters its prefix and that of its parent node into the RPL Target option of a DAO and sends it directly to the root of the DODAG. The DAO is forwarded from each node unchanged to its parent node until it arrives at the root. This allows the root to learn all nodes, as well as their parent-child relationships, and generate source routes for the downward communication with them. If the attacker can successfully uncover the root's routing table by advertising fictitious prefixes, it can then block the prefixes throughout the DODAG [3], [4].In the Storing MOP, node sends such a manipulated DAO to their parents' nodes. Then the parent advertise the manipulated entered relationship between the reachable prefixes further in their upward paths. If a message is now sent to one of the prefixes, through the deception the message will change direction when forwarded to the destination prefix and thus be forwarded inconsistently. The nodes directly involved in the forwarding detect a local inconsistency that reset their trickle-timer and initiate a local repair operation [3], [4].

V. THE DAO ATTACK

DAO messages are used in RPL networks to create the routing paths that will carry the downward traffic from the DODAG root to the respective nodes. The specification of RPL does not define how often and/or when such messages are to be transferred. Therefore, different implementations of the protocol may opt to propagate DAOs messages differently. For example, the implantation of RPL in [15] have chosen to transmit DAOs periodically with a pre-specified interval while they have been propagated in the Contiki RPL implementation [28] based on the timing of DIO messages. In Contiki RPL, a child node will usually send a DAO to its preferred parent in three occasions: 1) after receiving a DIO from its own parent; 2) when changing the preferred parent; and 3) in the detection of some specific errors. A critical issue here is that a DAO sent by a child node will lead to the transmission of several DAOs equivalent to the number of parents up to the DODAG root. A malicious node may exploit this case to drain the network resources by judiciously and repeatedly transmitting DAO messages to its parent node. One approach to perform this attack is by replaying a DAO sent by a legitimate node by an outsider malicious attacker [14]. RPL's security services deployed by layers underneath such as the cryptographic challenge-response handshake and link layer encryption can be used to mitigate this attack [14]. However, an insider attacker can easily bypass such security mechanisms triggering the need for more efficient solutions [14].

VI. PROPOSED SOLUTION

In order to address the DAO insider attack in RPL, two mitigation mechanisms have been proposed, named SecRPL1 and SecRPL2. These schemes need to be activated at the beginning of the network operations. In SecRPL1, we restrict the number of forwarded DAOs per child. This is achieved by having each parent node count the number of DAOs received from each child node in the parent sub-DODAG. Then the parent node will stop forwarding the child's DAOs when their number exceeds a pre-specified threshold. Hence, during a specific time slot, a node will forward up any received DAO initiated by a specific child until it reaches a pre-specified limit. When reaching that limit, no further DAOs from that child will be forwarded until the end of that time slot. The start and the end of time slot is controlled by the Trickle timer of DIO messages. In other words, the length of each time slot is equivalent to the length of DIO current interval.

To guarantee that no DAOs will be discarded due to the time factor, we reset the DAO counter at every DIO interval specifically, at the time a parent sends out a DIO message.

In the second scheme (SecRPL2), we restrict the entire number of forwarded DAOs by a specific node regardless of the child node who initiated the DAO. Hence, during a specific time slot, a node will forward up any received DAO until it reaches a pre-specified limit (*DAO_FORWARD_MAX*). When reaching that limit, no further DAOs will be forwarded until the end of that time slot.

Algorithm 1 DAO Attack Countermeasure 1

```
procedure Initilization
    set DAO_For_MAX_PerChild
end procedure
procedure DIO Transmitted
    for  Each child in the childern list do
        child_DAO_Counter = 0
    end for
end procedure
procedure Child's DAO Received
    if child_DAO_Counter < DAO_For_MAX_PerChild then
        forward the DAO
        child_DAO_Counter ++
    else
        discard the DAO
    end if
end procedure
```

Algorithm 2 DAO Attack Countermeasure 2

```
procedure Initilization
    set DAO_For_MAX
end procedure
procedure DIO Transmitted
    DAO_Counter = 0
end procedure
procedure Child's DAO Received
    if DAO_Counter < DAO_For_MAX then
        forward the DAO
        DAO_Counter ++
    else
        discard the DAO
    end if
end procedure
```

VII. PERFORMANCE EVALUATION AND DISCUSSION

In this section, we show the effect of the attack on the performance of the network in terms of several metrics, and to demonstrate how our proposed mechanisms can mitigate the DAO attack. A set of experiments have been carried out based on the well-known Contiki, the operating system for IoT devices [28]. Contiki has implementations for IoT communication stack including the standards of RPL, 6LoWPAN, CoAP, and IPv6.

Cooja simulator [29] which emulates exactly the binary on real IoT devices is used in our study to conduct the experiments. This has been exploited to emulate the MSPsim [30] of the Tmote sky platform, a well-known IoT sensor device with a low power IEEE 802.15.4 compliant CC2420

TABLE 1. Simulation parameters.

Parameter Name	Values
Simulation Area	100 x 000 m
Number of nodes	50
Simulation time	1800s
Mote Type	Tmote Sky Mote
Mac/Adaptation Layer	IEEE802.15.4/6LoWPAN
Radio Model	CC2420
Transmission Range(m)	30 m
Interference Range	25 m
Routing Protocol	RPL
Mode Of Operation	Storing mode
Rank Metric	MRHOF
Nominal Capacity	1000mAh
Battery Capacity	1000mAh
Voltage	3 V
Packet sent interval	60 s
Node Distribution	Uniform Distribution

radio chip. The radio protocol (UDGM), Unit Disk Graph Radio Medium, is used to simulate the propagation model. For Link layer, we used the CSMA/CA whereas the ContikiMAC was used as the radio duty cycling (RDC) protocol. The attack itself (i.e., DAO attack) has been implemented based on the ContikiRPL library within Contiki operating system. In particular, the attack was mounted by having an insider attacker send DAO messages periodically at pre-specified interval to its parent. The number of attackers in our simulation is set to three nodes.

A periodic data gathering application where sensor nodes send their readings to the DODAG root every minute was simulated at the application laye,r where the DODAG root sends a reply for each received message as a downward traffic. We simulated a stationary network with 50 nodes, the predominant pattern that you will find in a typical home network. The nodes in our simulation were distributed uniformly in an area of 100m x 100m while the DODAG root is positioned outside the deployment area. The simulation is timed out to end in 30 minutes for each simulated scenario.

Table 1 summarizes the experimental parameters used in our study.

The protocols evaluated for each scenario are RPL, RPL with attack (InsecRPL), RPL under attack with first proposed solution (SecRPL1), RPL under attack with second proposed solution (SecRPL2). In terms of the following metrics:

1) The average number of DAO messages forwarded by the parents in the network (Number of DAOs Forwarded).
2) The average power consumption in the network in milliwatts (Power Consumption (mW)).

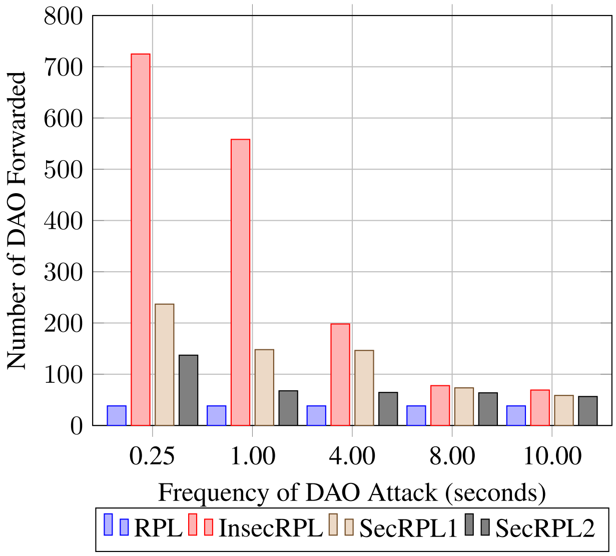

FIGURE 1. DAOs forwarding overhead vs attack intervals.

3) The Packet Delivery Ratio (PDR) of the upward traffic (i.e., from nodes to the DODAG root)
4) The PDR of downward direction (i.e., from the DODAG root to nodes)
5) The average end-to-end delay from nodes to the DODAG root in seconds (i.e. latency of the upward traffic)
6) The average end-to-end delay from the DODAG root to nodes in seconds (i.e. latency of the downward traffic)

A. THE EFFECT OF THE DAO ATTACK FREQUENCY

In the simulated scenario, three nodes located at the edge of the deployment area farther away from the DODAG root were selected to run as the attacker nodes as this will ensure covering the vast majority of forwarding paths, a phenomenon that an attacker will prefer to maximize the damage in the network. The maximum number of DAOs allowed to be forwarded for each child by a parent is set to 10 empirically (i.e., DAOMax threshold). The attack interval, the rate in milliseconds at which the malicious nodes transmits DAOs, is chosen between 250 and 10000 milliseconds. Five runs were conducted for each simulated scenarios under different random seeds for getting statistically solid results which are depicted in the following graphs.

The performance of the network under the simulated scenarios in terms of Forwarded DAO messages and under different attacking intervals is depicted in Figure 1 where the DAOMax threshold per child is set to ten. Figure 1 shows that the overhead of forwarded DAOs in InsecRPL, SecRPL1 and SecRPL2 is higher than that of normal model (i.e., RPL) regardless of the attacking interval value. However, we can also observe from Figure 1 that SecRPL2 has performed better, especially under attack interval of 250 milliseconds, in terms of DAOs overhead compared to other models apart from normal RPL.

The same can be said in relation to the power consumption as demonstrated in Figure 2. This better performance in terms

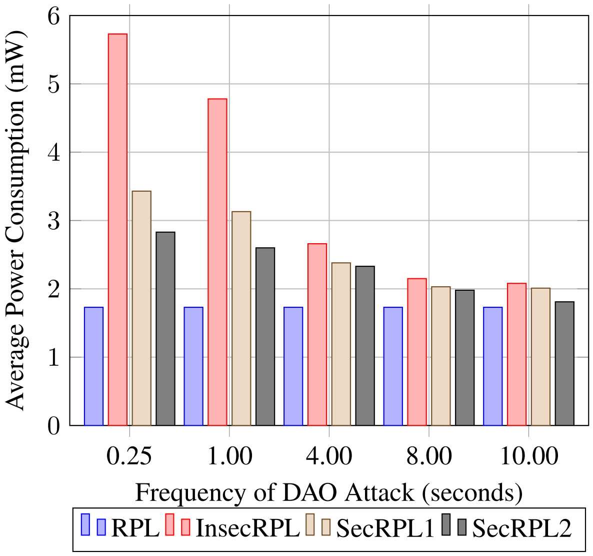

FIGURE 2. Power consumption vs attack interval.

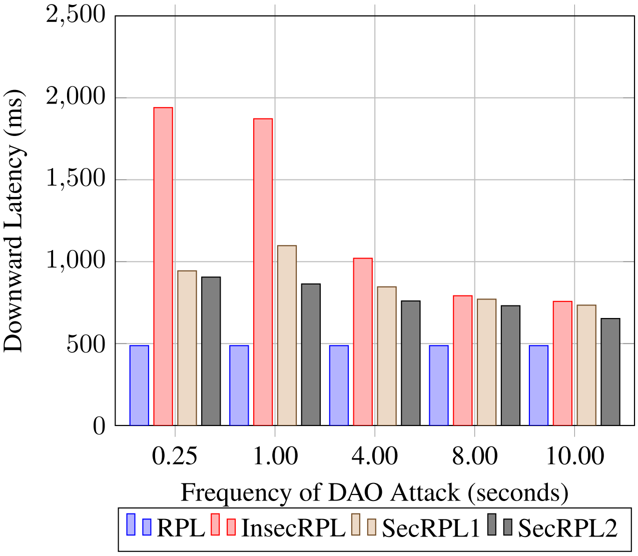

FIGURE 4. Downward latency vs attack intervals.

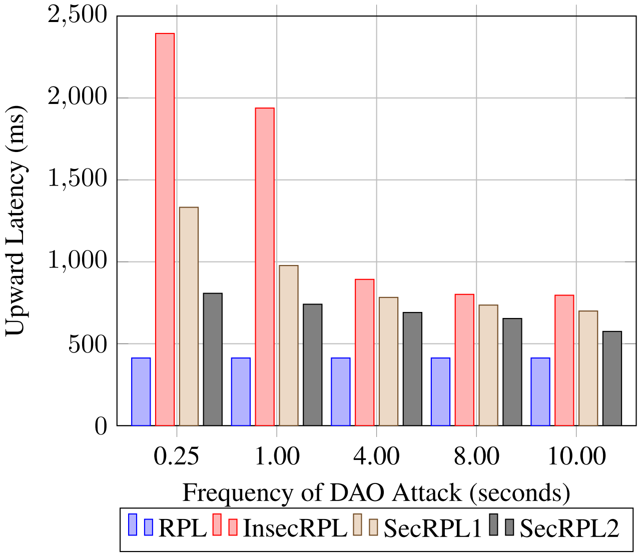

FIGURE 3. Upward latency vs attack intervals.

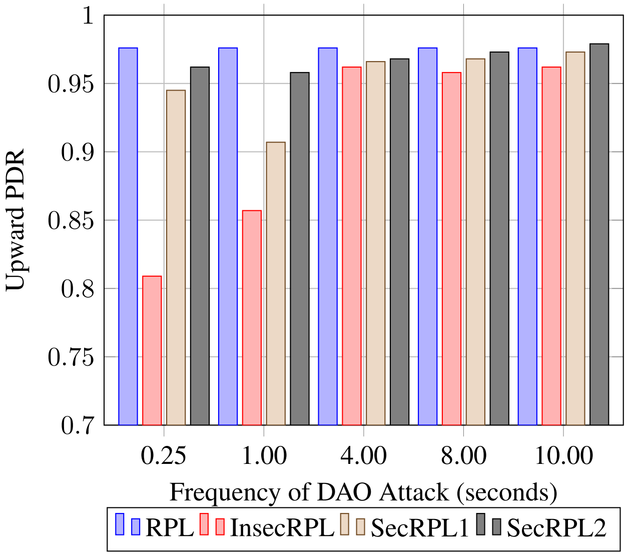

FIGURE 5. Upward PDR vs attack intervals.

of overhead and power consumption is easily justified by having the parent restricts the number of forwarded messages per child as proposed in our mechanism. It can be observed in Figure 2 that the insecure version of RPL has suffered heavily in relation to average power consumption due the attackers being able to flood the network with large amount of DAOs with no defence mechanism in place. This has been mitigated in both SecRPL1 and SecRPL2 applying the idea of threshold-based security with SecRPL1 showing relatively better performance compared to SecRPL2.

Indeed, the amount of power consumed is calculated in Contiki by adding up the power consumed in four of states of the nodes which are: power consumed in the listening state, power consumed in the idle state, power consumed in the transmission state and power consumed in the running state. Hence, the high overhead in terms of DAOs will surely lead to an increase in the power consumed in the transmission and listening states of the forwarder nodes along the path to the DODAG root, consequently increasing the average power consumption of the network.

The performance of the network in terms of upward latency is shown in Figure 3, whereas upward latency is depicted in Figure 4. Similarly, it is evident from figures that the latency in both downward and upward traffic has been adversely affected by the DAO attack. This again can be attributed to high overhead at the forwarder nodes that induces a higher congestion. In the same context, this degradation in the network performance in terms of latency has been mitigated by applying our mitigation mechanism (i.e., SecRPL1 and SecRPL2) specifically under heavy attacking intervals.

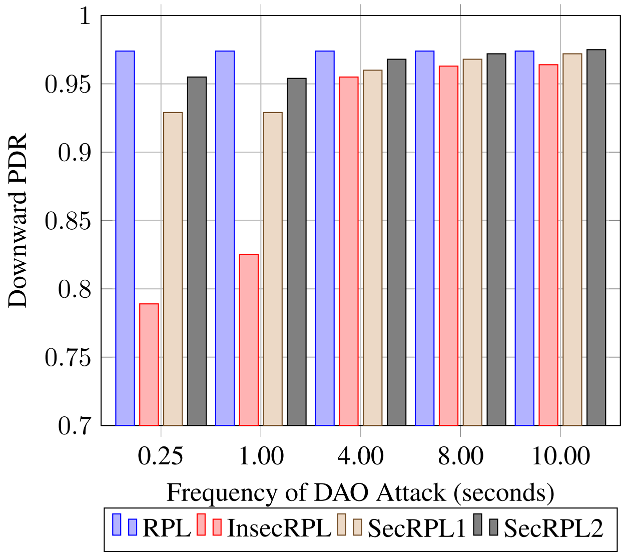

FIGURE 6. Downward PDR vs attack intervals.

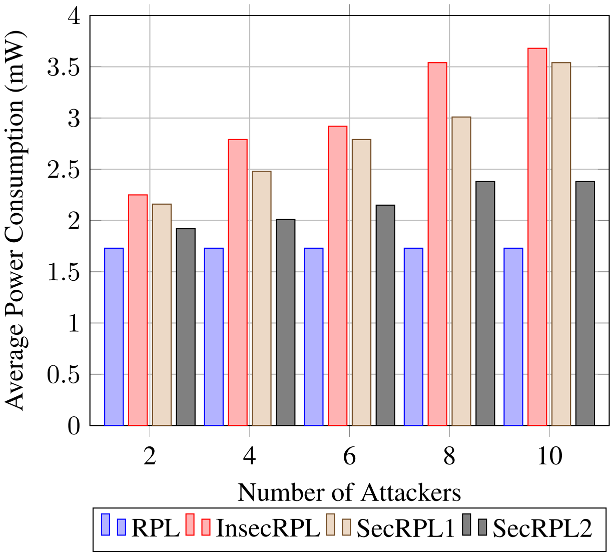

FIGURE 8. Power consumption vs number of attackers.

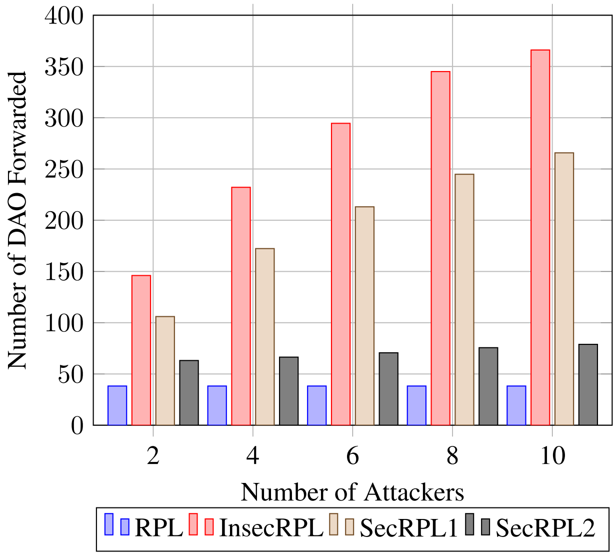

FIGURE 7. DAOs forwarding overhead vs number of attackers.

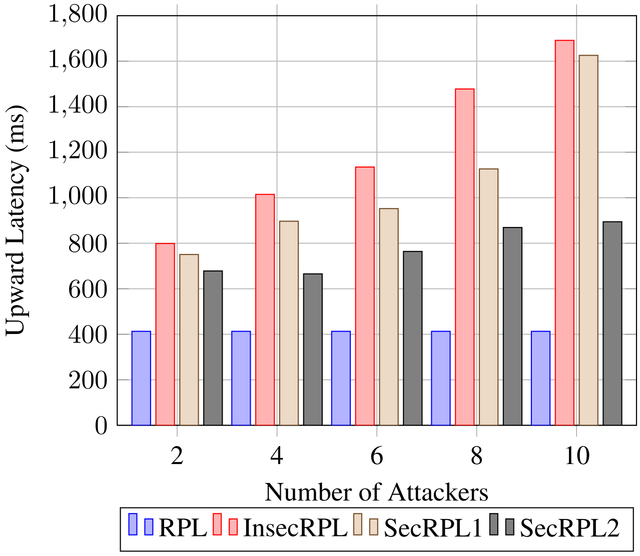

FIGURE 9. Upward latency vs number of attackers.

The PDRs of the upward traffic and downward traffic are shown in Figure 5 and Figure 6 respectively. It is again evident from both figures that the PDR in both directions suffer heavily when running the attack under a high attack interval. Note, however, that this may not hold true when mounting the attack under different data rates or topologies. This degradation can be mainly justified by the congestion incurred due to the high overhead at the forwarder nodes under the effect of the attack which again has been alleviated applying our proposed mitigation mechanisms. Both RPLSec1 and RPLSec2 have shown comparable PDR rates in both directions to that of the reference model. The insecure version of RPL (i.e., InSecRPL) has experienced the worst results in terms of PDR, with 7% lower than that of the reference model of RPL. Both SecRPL1 and SecRPL2 have managed to enhance the performance in terms of PDR by up 4% and 6% respectively.

B. THE EFFECT OF INCREASING THE NUMBER OF ATTACKERS

In this scenario, the attack will be implemented by increasing the number of attackers, starting with two attackers and incrementing it by two to a maximum of 10. The value of DAOMax threshold in all cases was fixed to 10 in both RPLSec1 and RPLSec2.

The DAO overheads in terms of the average number of forwarded messages per node with different attacking intervals is depicted in Figure 7. The figure demonstrates that InsecRPL have increased the DAO overhead in comparison with SecRPL2 and RPL. In fact SecRPL1, SecRPL2 have managed to mitigate the effect of the DAO attack, especially in the case under ten attacking nodes with 76.36% and 205% respectively decrease in the DAO overhead compared to the InsecRPL.

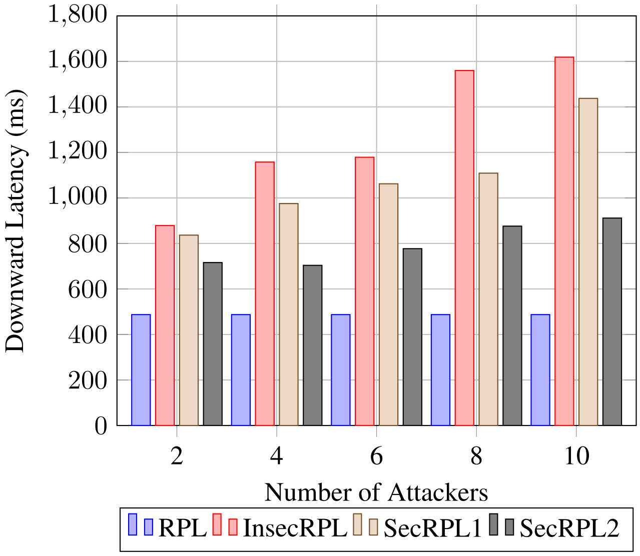

FIGURE 10. Downward latency vs number of attackers.

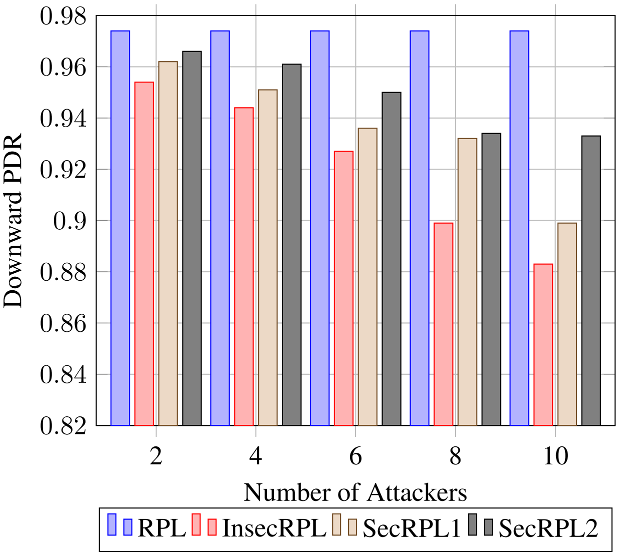

FIGURE 12. Downward PDR vs number of attackers.

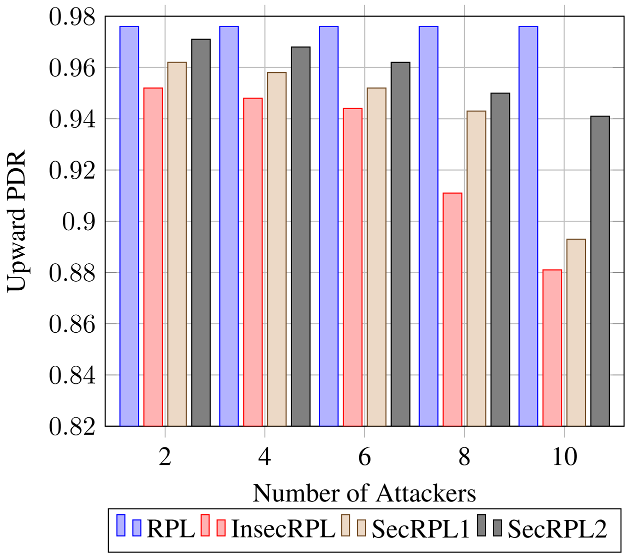

FIGURE 11. Upward PDR vs number of attackers.

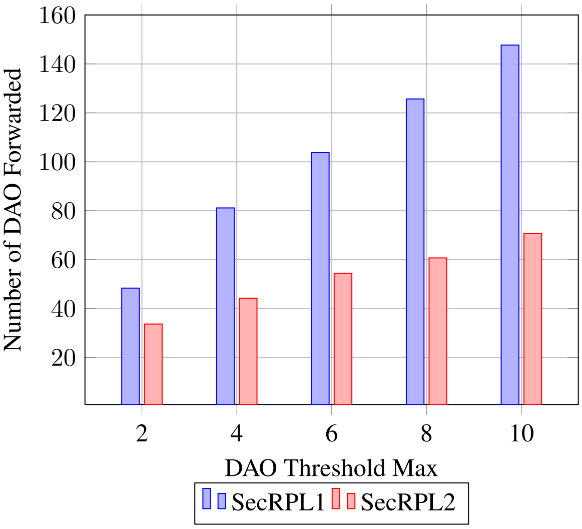

FIGURE 13. DAOs forwarding under various DAO threshold.

The superior performance of SecRPL2 over SecRPL1 is related to the value of the DAOMax chosen as SecRPL2 can only forward up to 10 DAOs in total in a given interval while SecRPL1 can forward 10 DAOs per destination, hence, the superiority of SecRPL2 over SecRPL1. This has been translated into a decrease in the power consumption under the proposed schemes as depicted in Figure 8 which can be easily justified by the capacity of secure versions of RPL (i.e., SecRPL1 and SecRPL2) to restricted the number of forwarded DAOs per child due to the attack. Both mitigation schemes SecRPL1 and SecRPL2 were able to reduce the effect of the attack by 24% and 87% respectively; however, both consumed more power than the reference network (RPL).

Figures 9 and 10 demonstrate the latency of the upward and downward traffic respectively for protocols under comparison. Similarly, it is evident that the latency has suffered significantly under the attack for both traffic patterns as a result of the significant congestion at the forwarder nodes. SecRPL1 has improved the upward latency by 65.88% and the downward latency by 181.19%. With SecRPL2 both upward and downward latency are greatly reduced outperforming SecRPL1 which can be attributed again to the DAO threshold chosen.

The PDRs of upward and downward traffic for the four models are depicted in Figure 11 and Figure 12 respectively. The figures again demonstrate that the PDRs of both traffic patterns have been affected negatively and the amount of the affect is proportional to the number of the attackers in the network, which can be attributed to the congestions experienced by the forwarder nodes. The degradation in the PDR rate has been overcome by the proposed solutions, in which we almost restore the same efficiency of the reference model. From Figure 11 and Figure 12, we can conclude that SecRPL1 has

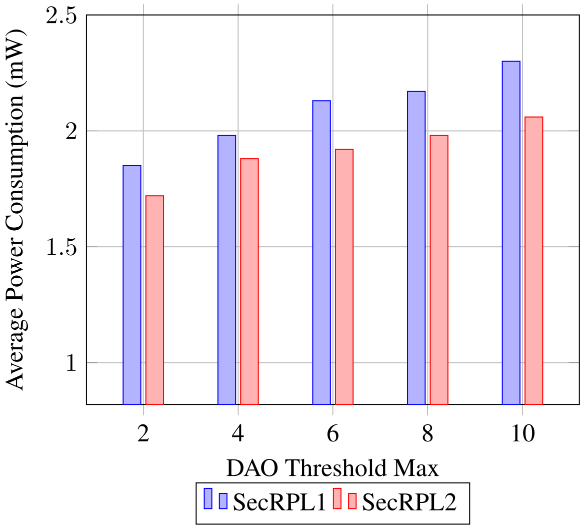

FIGURE 14. Power consumption under various DAO threshold.

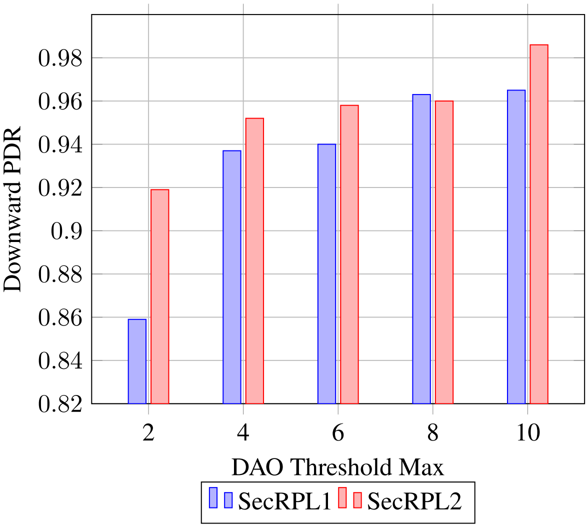

FIGURE 15. Downward PDR under various DAO threshold.

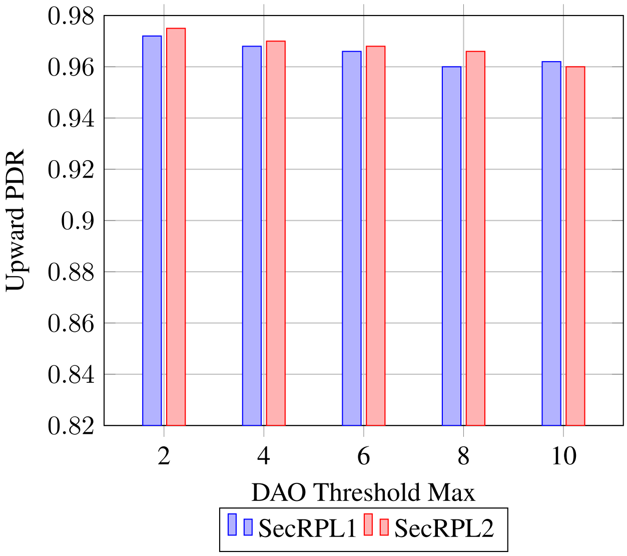

FIGURE 16. Upward PDR under various DAO threshold.

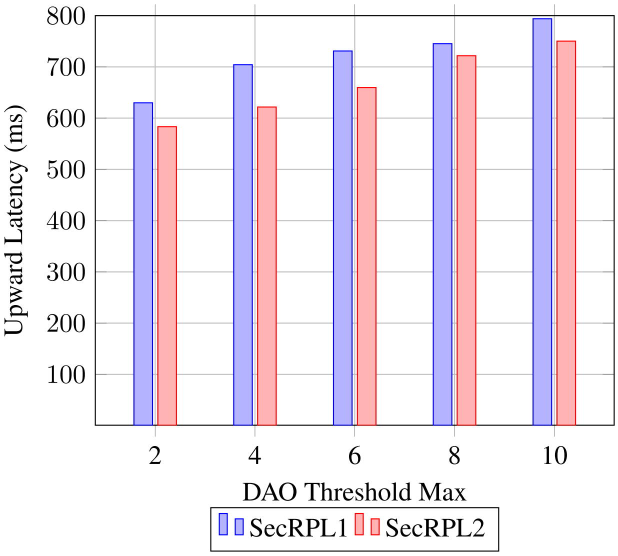

FIGURE 17. Upward latency under various DAO threshold.

slightly improved PDR over InsecRPL with a 2% increase. SecRPL2, however shows an increase of 3% indicating best performance comparable to the reference model with 3% difference.

C. THE EFFECT OF THE THRESHOLD PARAMETER (DAOMAX)

We also investigated the effect of the threshold value (i.e. DAO threshold Max) on the network reliability in terms of PDR. Intuitively, the smaller the value of the threshold, the lower the DAO overhead and power consumption but at the expense of network reliability. We have depicted how setting the threshold value can affect the performance of the network in terms of mentioned metrics in Figure 13 and Figure 14. It is clear from Figure 13 and Figure 14 that selecting a very small value for the threshold has reduced the control overhead and power consumption in both mitigation mechanisms with SecRPL2 again being more efficient in overcoming the effect of the attack, reducing the DAO overhead and the power consumption to up to 48.5% and 18% respectively compared to SecRPL1.

However, this has impacted the PDR of the downward traffic negatively as illustrated in Figure 15 and Figure 16. This holds true for any value of the threshold less than four. This can be explained easily by the fact that the small value of the threshold will lead into preventing the forwarding of critical DAO messages necessary to build more efficient downward routing paths, hence, the lower PDR of the downward traffic. The figures show also that SecRPL2 performs better than SecRPL1 under both traffic patterns in terms of PDR as the DAO threshold are only restricted partially.

Fig. 17 and 18, show the effect of both mechanisms on downward and upward latency. It indicates that assigning lower threshold values will reduce the latency. SecRPL2 was

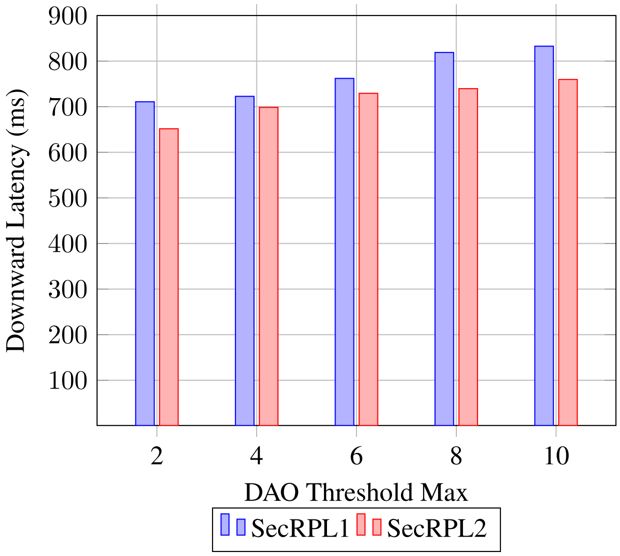

FIGURE 18. Downward latency under various DAO threshold.

able to much better overcome the effect of the attack, decreasing upward and downward latency by 53.57% and 53.71%, respectively in comparison to SecRPL1.

VIII. CONCLUSION

In this study, we have evaluated the effect of the DAO flooding attack on the network performance in terms of power consumption, packet delivery ratio and latency under different scenarios and operating conditions. The DAO attack can be mounted in IoT networks by having an attacker node transmitting periodically DAO messages to its preferred parent which in turn will forward the received DAOs to its own parent and so on until the DAOs reach the final destination which is the DODAG root. The DAOs in the context of the RPL protocol are transmitted in end-to-end approach (i.e., from sensors to the sink) which makes them different from other RPL's flooding attacks including the DIO and DIS attacks. Hence, not only the immediate neighbors of the attackers will get affected and harmed by the attack, but also all forwarding nodes to the DODAG root. In fact, an attacker node located at the network edge and transmitting a DAO message will prompt all other nodes in the forwarding path to the DODAG root to forward such a message. The simulation results have shown how the attack can damage the network performance by significantly increasing the DAO overhead and power consumption. The results have also demonstrated that the DAO attack may moderately affect the reliability of the downward traffic under specific conditions. To overcome the effect of the attack, two mitigation mechanisms have been proposed and evaluated showing a good capacity in restoring the optimal performance of the network in terms of the respective metrics.

REFERENCES

[1] J. Hui and P. Thubert, *Compression Format for IPv6 Datagrams over IEEE 802.15. 4-Based Networks*, document RFC 6282 Internet Engineering Task Force RFC 6282, 2011.

[2] J. W. Hui and D. E. Culler, "Extending IP to low-power, wireless personal area networks," *IEEE Internet Comput.*, vol. 12, no. 4, pp. 37–45, Jul. 2008.

[3] J. Hui and J. Vasseur, *The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams*, document RFC 6553, Mar. 2012.

[4] T. Clausen, U. Herberg, and M. Philipp, "A critical evaluation of the IPv6 routing protocol for low power and lossy networks (RPL)," in *Proc. IEEE 7th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2011, pp. 365–372.

[5] IETF ROLL Working Group. *Charter for Working Group*. Accessed: Nov. 29, 2019. [Online]. Available: https://datatracker.ietf.org/wg/roll/charter

[6] A. Dvir, T. Holczer, and L. Buttyan, "VeRA–Version number and rank authentication in RPL," in *Proc. IEEE 8th Int. Conf. Mobile Ad-Hoc Sensor Syst.*, Oct. 2011, pp. 709–714.

[7] L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and countermeasures in the RPL-based Internet of Things," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 8, Jan. 2013, Art. no. 794326.

[8] M. Landsmann, M. Wahlisch, and T. Schmidt, "Topology authentication in RPL," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2013, pp. 73–74.

[9] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schönwälder, "Mitigation of topological inconsistency attacks in RPL-based low-power lossy networks," *Int. J. Netw. Manage.*, vol. 25, no. 5, pp. 320–339, Jun. 2015.

[10] A. Mayzaud, R. Badonnel, and I. Chrisment, "Detecting version number attacks in RPL-based networks using a distributed monitoring architecture," in *Proc. 12th Int. Conf. Netw. Service Manage. (CNSM)*, Oct. 2016, pp. 127–135.

[11] F. Ahmed and Y.-B. Ko, "Mitigation of black hole attacks in routing protocol for low power and lossy networks," *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 5143–5154, Oct. 2016.

[12] A. Aris, S. F. Oktug, and S. B. O. Yalcin, "RPL version number attacks: In-depth study," in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp. (NOMS)*, Apr. 2016, pp. 776–779.

[13] D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for Internet of Things: A survey," *J. Netw. Comput. Appl.*, vol. 66, pp. 198–213, May 2016.

[14] P. Perazzo, C. Vallati, G. Anastasi, and G. Dini, "DIO suppression attack against routing in the Internet of Things," *IEEE Commun. Lett.*, vol. 21, no. 11, pp. 2524–2527, Nov. 2017.

[15] U. Herberg and T. Clausen, "A comparative performance study of the routing protocols LOAD and RPL with bi-directional traffic in low-power and lossy networks (LLN)," in *Proc. 8th ACM Symp. Perform. Eval. Wireless Ad Hoc, Sensor, Ubiquitous Netw. (PE-WASUN)*, 2011, pp. 73–80.

[16] D. Sharma, I. Mishra, and S. Jain, "A detailed classification of routing attacks against rpl in Internet of Things," *Int. J. Advance Res., Ideas Innov. Technol.*, vol. 3, no. 1, pp. 692–703, 2017.

[17] B. Ghaleb, A. Al-Dubai, E. Ekonomou, M. Qasem, I. Romdhani, and L. Mackenzie, "Addressing the DAO insider attack in RPL's Internet of Things networks," *IEEE Commun. Lett.*, vol. 23, no. 1, pp. 68–71, Jan. 2019.

[18] S. M. Bellovin and R. Housley, "Guidelines for cryptographic key management," in *Proc. Symp. Res. Secur. Privacy*, 2005, pp. 1–7.

[19] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Commun. ACM*, vol. 47, no. 6, pp. 53–57, Jun. 2004.

[20] A. Le, J. Loo, Y. Luo, and A. Lasebae, "The impacts of internal threats towards routing protocol for low power and lossy network performance," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2013, pp. 000789–000794.

[21] A. Mayzaud, R. Badonnel, I. Chrisment, and I. G. Est-Nancy, "A taxonomy of attacks in RPL-based Internet of Things," *Int. J. Netw. Secur.*, vol. 18, no. 3, pp. 459–473, May 2016.

[22] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schonwalder, "Using the RPL protocol for supporting passive monitoring in the Internet of Things," in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp. (NOMS)*, Apr. 2016, pp. 366–374.

[23] K. Weekly and K. Pister, "Evaluating sinkhole defense techniques in RPL networks," in *Proc. 20th IEEE Int. Conf. Netw. Protocols (ICNP)*, Oct. 2012, pp. 1–6.

[24] D. Airehrour, J. Gutierrez, and S. K. Ray, "Securing RPL routing protocol from blackhole attacks using a trust-based mechanism," in *Proc. 26th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Dec. 2016, pp. 115–120.

[25] F. I. Khan, T. Shon, T. Lee, and K. Kim, "Wormhole attack prevention mechanism for RPL based LLN network," in *Proc. 5th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2013, pp. 149–154.

[26] P. Pongle and G. Chavan, "A survey: Attacks on RPL and 6LoWPAN in IoT," in *Proc. Int. Conf. Pervas. Comput. (ICPC)*, Jan. 2015, pp. 1–6.

[27] C. Pu, "Mitigating DAO inconsistency attack in RPL-based low power and lossy networks," in *Proc. IEEE 8th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2018, pp. 570–574.

[28] A. Dunkels, B. Gronvall, and T. Voigt, "Contiki–a lightweight and flexible operating system for tiny networked sensors," in *Proc. 29th Annu. IEEE Int. Conf. Local Comput. Netw.*, Nov. 2004, pp. 455–462.

[29] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, "Cross-level sensor network simulation with COOJA," in *Proc. 31st IEEE Conf. Local Comput. Netw.*, Nov. 2006, pp. 641–648.

[30] J. Eriksson, A. Dunkels, N. Finne, F. Osterlind, and T. Voigt, "Mspsim—An extensible simulator for msp430-equipped sensor boards," in *Proc. Eur. Conf. Wireless Sensor Netw. (EWSN)*, vol. 118, 2007, pp. 1–2.

ISAM WADHAJ received the B.Eng. degree in computer networks and distributes systems, and the M.Sc. degree in advanced networking from Edinburgh Napier University (ENU), U.K., in 2010 and 2013, respectively. He is currently working as a Lecturer with the School of Computing, ENU. His research interests include wireless sensor networks, the Internet of Things, security of the IoT, and low power and lossy networks.

BARAQ GHALEB (Student Member, IEEE) received the B.Sc. degree in computer science from the University of Jordan, Amman, Jordan, in 2009, and the M.Sc. degree from the Jordan University of Science and Technology, Irbid, Jordan, in 2013, and the Ph.D. degree in applied computing from Edinburgh Napier University, Edinburgh, U.K. His current research interests include routing protocols in low-power and lossy networks and the Internet of Things (IoTs), security of LLNs, and the IoT in addition to data mining. He holds one patent in the field of the IoT Routing.

CRAIG THOMSON received the B.Eng. degree (Hons.) from Edinburgh Napier University (ENU), U.K., in 2016, where he is currently pursuing the Ph.D. degree in applied computing. His research interests include Mobile Wireless Sensor Networks, the Internet of Things, and Low Power and Lossy Networks. He is also an Associate Fellow of the Higher Education Academy (AFHEA). He was a recipient of the University Medal for his B.Eng. degree.

AHMED AL-DUBAI received the Ph.D. degree in computing from the University of Glasgow, Glasgow, U.K., in 2004. In 2004, he joined the University of West London, London, U.K. In 2005, he joined Edinburgh Napier University, Edinburgh, U.K., where he became a Professor and the Programme Leader of the Post-Graduate Research degrees with the School of Computing. He is currently the Head of the Networks Research Group. He has been published in world leading journals and in prestigious international conferences. He has also been involved with research in the area of group communication algorithms, smart spaces, and high-performance networks. He is a Fellow of the Higher Academy, U.K. He was a recipient of the several academic awards and recognitions, and a member of several Editorial Boards of scholarly journals. He has served as a Guest Editor for more than 20 special issues in scholarly journals and chaired and co-chaired more than 30 international conferences/workshops.

WILLIAM J. BUCHANAN was appointed as an Officer of the Order of the British Empire (OBE) in the 2017 Birthday Honours for services to cybersecurity. He is currently a Professor with the School of Computing, Edinburgh Napier University (ENU). He is also leading the Centre for Distributed Computing, Networks, and Security, ENU, The Cyber Academy, and the Blockpass ID Lab. His main research interests include around information sharing, the IoT, e-health, threat analysis, cryptography, and triage within digital forensics. He is a Fellow of the Britich Computer Society (BCS) and a Principal Fellow of the Higher Education Academy (PFHEA). In 2018, he received an Outstanding Contribution to Knowledge Exchange at the Scottish Knowledge Exchange awards. One of his most recent achievements is the creation of a Blockpass Identify Lab and which is one of the first of its type in the world, and has significant industry funding. This has led to several World-wide patents, and in three highly successful spin-out companies Zonefox, Symphonic Software, and Cyan Forensics.