Pervasive and Mobile Computing 80 (2022) 101525

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

journal homepage: www.elsevier.com/locate/pmc

A lightweight distributed detection algorithm for DDAO attack on RPL routing protocol in Internet of Things

Mohsen Sheibani [a], Behrang Barekatain [a,b,*], Erfan Arvan [a]

[a] Faculty of Computer Engineering, Najafabad Branch, Islamic Azad University, Najafabad, Iran
[b] Big Data Research Center, Najafabad Branch, Islamic Azad University, Najafabad, Iran

ARTICLE INFO

Article history:
Received 5 October 2021
Received in revised form 29 November 2021
Accepted 27 December 2021
Available online 1 January 2022

Keywords:
DDAO attack
Internet of Things (ioT)
Intrusion Detection System (IDS)
RPL

ABSTRACT

A significant increase in the number of connected devices in the Internet of Things poses a key challenge to efficiently handling the attacks in routing protocols such as Routing Protocol for Low Power and Lossy Networks (RPL). The attacks on RPL are partly studied in the literature, and the proposed solutions typically overlook the appropriate trade-off among the detection rate and communication and computational overhead. This study aimed at introducing a new attack called Dropped Destination Advertisement Object (DDAO) and a new Intrusion Detection System (IDS) to counter this attack in RPL protocol. DDAO attack adversely affects the network by preventing the creation of the downward routes through not forwarding Destination Advertisement Object (DAO) messages and sending fake Destination Advertisement Object Acknowledgment (DAO-ACK) messages to the DAO source. A distributed lightweight IDS is proposed in this study to detect and counter DDAO attacks by monitoring the behavior of parents against forwarded DAO messages. According to the evaluations conducted on the Cooja simulator under different real-world conditions, the proposed IDS can detect DDAO attacks with high accuracy, precision, and True Positive Rate (TPR) and low False Positive Rate (i.e., close to zero). Additionally, compared to RPL, the proposed IDS improves Packet Delivery Rate (PDR) by 158 percent when countering attacks.

1. Introduction

The Internet of Things (IoT) is an emerging ecosystem consisting of different technologies, such as wireless sensor networks, Radio Frequency Identification (RFID), and ad-hoc networks, aiming to connect billions of devices to the Internet. IoT also enables a wide variety of useful applications such as Smart Home, Multimedia distribution, Electronic Health, and Smart City [1–5]. In the concept of IoT, the network nodes are called "Things". Each thing consists of at least a sensor that collects the information from the environment and a weak processor (i.e., limited in terms of resources) which is responsible for transferring information [6,7]. Low power and Lossy Network (LLN) [8] has a key role in realizing IoT. These networks consist of resource-constrained devices (i.e., low-cost devices with limited processing, storage, and networking capabilities, and often run on batteries). These features and limitations bring about some severe challenges for designing a routing protocol for LLNs. To provide a standard routing protocol for LLNs, the Routing Over Low power and Lossy

* Corresponding author at: Faculty of Computer Engineering, Najafabad Branch, Islamic Azad University, Najafabad, Iran.
E-mail addresses: sheibani.mohsen01@gmail.com (M. Sheibani), behrang_barekatain@iaun.ac.ir (B. Barekatain), e.arvan@yahoo.com (E. Arvan).

https://doi.org/10.1016/j.pmcj.2021.101525
1574-1192/

networks IETF (ROLL) workgroup of Internet Engineering Task Force (IETF) proposed Routing Protocol for Low Power and Lossy Networks (RPL). RPL presented in RFC-6550 [8] does the routing operations on 6LoWPAN networks.

Moreover, security is one of the most important challenges for IoT to become ubiquitous. Some studies have been conducted to achieve message security in the End-to-End (E2E) form on IoT, which guarantees message confidentiality and integrity using cryptography algorithms and authentication protocols [9–12]. Even by assuming the use of encryption at the hop-by-hop level, if the attacker obtains the network secret keys in a way such as compromising one of the network nodes, it can form internal attacks on routing protocols called routing attacks. Routing attacks are the most common attacks which can be performed on LLNs [13]. RFC-7416 [14] defines RPL security requirements based on security reference model ISO7498-2. These requirements include authentication, access control, confidentiality, and integrity. In addition to these requirements defined based on the security reference model, RFC-7416 also considers availability as another security requirement for RPL protocol.

Also, Different attacks on RPL have been introduced so far, such as Selective Forwarding, Denial of Service (DoS), Sinkhole, Hello flooding, Sybil, Rank, Version, Local Repair, Neighbor, DODAG Information Solicitation (DIS), Destination Advertisement Object (DAO) Inconsistency [15], DAO Insider [16], and DAO Induction [17].

Moreover, using common security protocols and methods that counter attacks on the Internet is not feasible in IoT because they need lots of resources, but IoT devices are resource-constrained.

This paper introduces a new attack called Dropped Destination Advertisement Object (DDAO) on RPL protocol. According to this attack, the attacker drops the DAO messages sent from the victim node and sends a fake Destination Advertisement Object Acknowledgment (DAO-ACK) message to the victim to manipulate it. This attack can cause a significant part of the network to be inaccessible. Moreover, an efficient, lightweight distributed IDS based on packet eavesdropping has been proposed to detect DDAO attacks accurately and efficiently.

The rest of this paper is organized as follows. In the next section, the related work will be reviewed. Then, in the third section, the RPL protocol is elaborated. In the fourth section, the problem statement is provided in which the DDAO is introduced. In the fifth section, the proposed IDS is introduced. In the sixth section, the proposed IDS evaluation will be addressed. Finally, in the last section, the conclusion is provided. Also, the table of acronyms is provided after the conclusion.

2. Related work

Different attacks and countermeasures have been proposed on RPL, and some of them are more related to this study; therefore, a short review of these attacks has been provided in this section. Bhalaji et al. [18] have proposed an algorithm based on trust and eavesdropping to counter the Black-Hole attack on RPL protocol. Airehrour et al. [19] proposed a trust-based algorithm to detect rank and Sybil attacks. In another study, the same authors [20] have proposed a trust-aware extension for RPL to detect and counter Black-Hole and Selective Forwarding attacks. Pongle et al. [21] have suggested several solutions to counter Selective Forwarding attacks on RPL; one is to consider separated routes among the nodes that intend to communicate with each other. Another solution is that the nodes can determine their route to their parent or children dynamically. This study clarifies that defending against all Selective Forwarding attacks is difficult, but using encryption and packet monitoring in the application layer can detect many Selective Forwarding attacks. Wallgren et al. [22] have addressed the capability of self-healing mechanisms of RPL protocol in countering Selective Forwarding attacks. They implemented the attack so that the attacker node forwards RPL control messages, but the data messages are dropped. After 24 h of the attack, it was observed that RPL self-healing mechanisms could not detect this attack and heal the network. Therefore, an IDS is needed to detect this attack. In the same study, a protocol called Heartbeat was proposed. The same authors [23] have provided an IDS called SVELTE in order to detect Selective Forwarding, Sinkhole, and Rank attacks. Karkazis et al. [24] have added Packet Forwarding Indication (PFI) criteria to the parent selection function in RPL. Djedjig et al. [25] have proposed a trust-based extension for RPL so that trust value is one of the main routing metrics in the Objective Function (OF). That study uses shared trust values between the neighbors.

Pu et al. [15] have introduced a new attack called DAO Inconsistency in which the attacker starts not forwarding data packets and returns the same packet with the setting F-flag (Forwarding error Flag); therefore, parent nodes will remove corresponding downward routes from their routing tables. They have also suggested a method using a dynamic threshold to detect this attack. Ghaleb et al. [16] have proposed a new attack called DAO Insider in which the attacker sends fake DAO packets to its parent periodically. Then, the parent itself forwards these packets towards the root. They have also suggested an algorithm to detect this attack using a threshold parameter. Baghani et al. [17] have introduced a new attack called DAO Induction in which attacker tries to send many unnecessary DAO messages. They also provided a lightweight algorithm to detect this attack.

3. RPL

RPL [26] is a distance-vector routing protocol that organizes nodes in DODAG (Destination Oriented Directed Acyclic Graph). In DODAG, the node which provides the Internet connection is considered as root. As shown in Fig. 1, an RPL network can have several different DODAGs, forming an RPL instance and having their unique ID. Each node in RPL selects one of its neighbors as its selected parent based on Objective Function (OF), through which it sends the packets towards

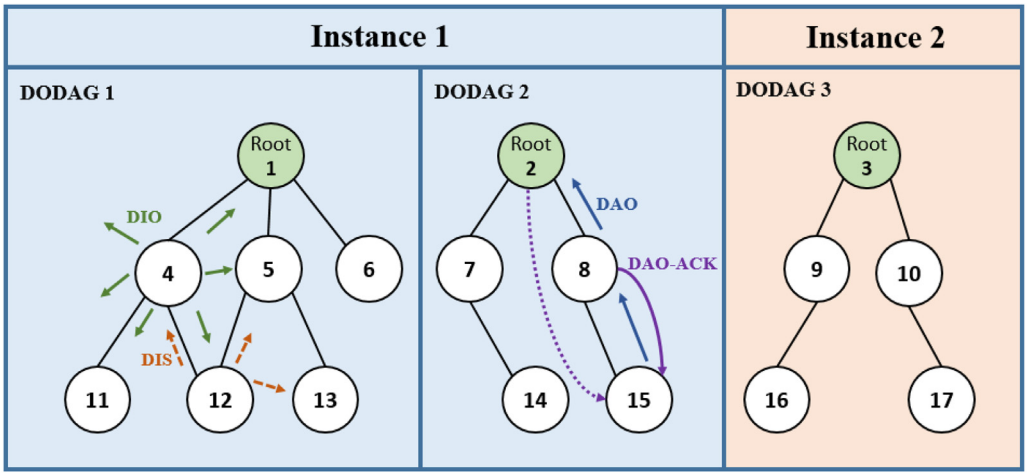


Fig. 1. Overview of RPL.

the root. Another application of OF is calculating the Rank of the nodes. Each node, after selecting its parent, starts to send DODAG Information Object (DIO) control messages and determines its Rank inside the DODAG (e.g., node 4 in Fig. 1). The existence of ranks for each node prevents loop formation in network topology. DIS messages are used to discover the neighboring nodes in DODAG (e.g., node 12 in Fig. 1. is broadcasting a DIS message). When a node wants to connect to the network, it broadcasts DIS messages in order to receive DIO messages from surrounding nodes. In RPL, after selecting a new preferred parent, each node sends a DAO message through its new parent (e.g., node 15 in Fig. 1. is sending a DAO message to its preferred parent that is node 8) upward to the root in order to help the root node and intermediate nodes form downward routes to that node; in a more detailed form, the parent node receiving the DAO message places its IP address in it and forwards it to its own parent (e.g., node 8 in Fig. 1. is forwarding the DAO message received from node 15 to its preferred parent that is Root 2), and then, this will continue until the DAO message reaches the root. When the network is configured in *storing mode*, all intermediate nodes in the path of the DAO message store the route to the DAO sender node, and send a DAO-ACK message to their previous node (e.g., in Fig. 1., node 8 is sending a DAO-ACK to node 15). On the other hand, when the network is configured in *non-storing* mode, only the root stores the routing information, and then, it sends a DAO-ACK message to the DAO sender (e.g., in Fig. 1., Root 2 is sending a DAO-ACK to node 15, which is illustrated by a dashed purple arrow).

4. Problem statement

In this study, a new attack on RPL is introduced, which is called DDAO. DDAO attack can be performed on RPL and prevents forming downward routes towards victim node(s). Accordingly, as the ancestor nodes cannot send any messages to their victim descendants, this attack can be hazardous, and the network can be almost disrupted. Also, if the attacker node has a low rank and is close to the root, it can make a big part of the network out of access. Therefore, if this attack is combined with other attacks like Rank or Sinkhole, it can be more harmful.

As mentioned before, each node, after selecting a new parent, sends a DAO message through its new parent upward to the root in order to let the root node and intermediate nodes know the route to it. In DDAO attack, the attacker is an internal attacker (i.e., a legitimate node that, in the case of encryption, has an access to the network secret keys) that starts to drop DAO messages received from the victim (i.e., its child node or one of its descendants) and replies a fake DAO-ACK message to the victim to manipulate it. In a more detailed form, when RPL is configured in *Storing mode*, the attacker node, after dropping a DAO message, sends a DAO-ACK message to the victim node, and when the network is configured in *Non-Storing mode*, the attacker node impersonates the root and sends a fake DAO-ACK to the victim node.

The nature of this attack is similar to packet-dropping attacks (e.g., Black-hole and Selective Forwarding), but the main difference is that fake DAO-ACK messages are sent from the attacker node to the victim nodes.

Fig. 2 illustrates two examples of DDAO attacks in *Storing mode* and *Non-Storing mode*. For both attacks, node B is a DDAO attacker and the parent of node D. It can be observed that in the Non-storing mode of the network, node B, after dropping a DAO message, impersonates the root and sends a fake DAO-ACK message to node D, which contains the root's IP address as the sender of the message. On the other hand, in the Storing-mode, node B sends a DAO-ACK message containing its IP address as the sender after dropping a DAO message from node D.

Furthermore, in order to show the destructive effect of DDAO attack on RPL, in Fig. 3, the impact of increasing network size on PDR in RPL networks *with one DDAO attacker* along with RPL networks *with no attackers* has been reported. Accordingly, the curve of *RPL with one attacker* shows that PDR has dramatically dropped compared to RPL with no

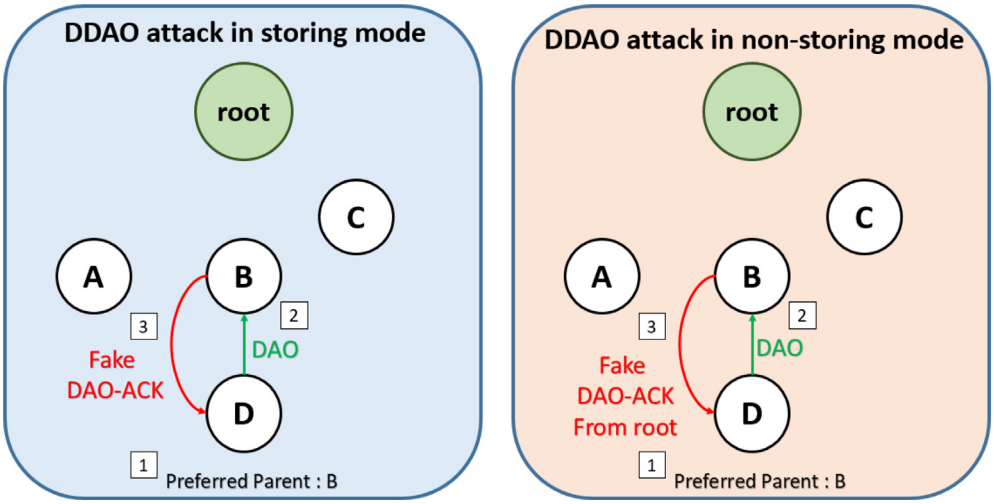


Fig. 2. DDAO attack in Storing-mode and Non-Storing mode.

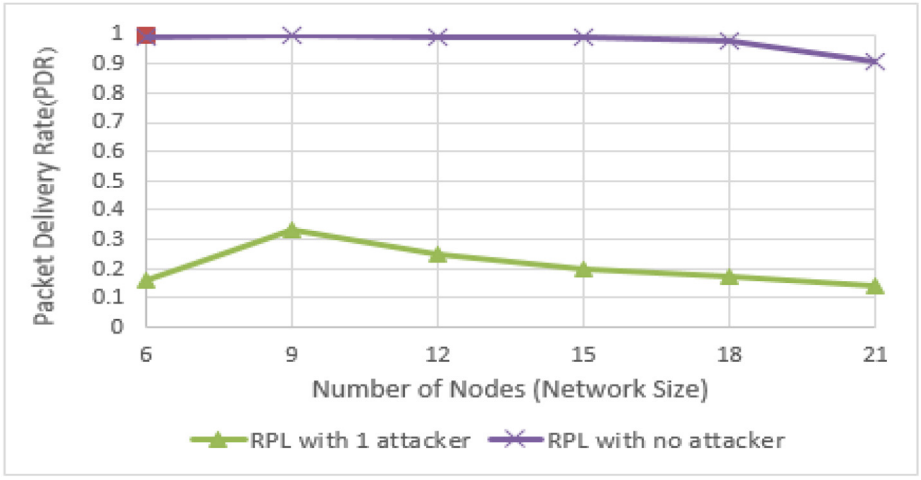


Fig. 3. Impact of network size increase on Package Delivery Rate on RPL with attacker and RPL without attacker.

attackers, which means that RPL self-healing mechanisms cannot counter this attack, and many sent messages in the network will not reach their destinations.

In the real world, network hardware in IoT is not ideal; therefore, some packets are lost in the network naturally. Hence, regarding the destructiveness of this attack, an IDS must be provided to counter it, and it should be able to adapt itself in different networks (with different probability of environmental changes). Also, the proposed IDS should also have a fair performance according to the different requirements. In such an IDS, the network nodes should be able to detect the dropping of DAO packets by their attacker parent, and they should be aware that they will receive fake DAO-ACK messages from the attacker. Moreover, considering the limitations of resources in IoT, the provided IDS should be lightweight. Finally, it should be noted that On–Off attack (i.e., an attack in which the attacker sometimes pauses the attack) cannot be combined with DDAO attack because even by forwarding a single DAO message by the attacker, the attack will be ineffective.

5. The proposed IDS for detecting DDAO attack

In this section, an IDS for detecting DDAO attack will be presented. The proposed IDS detects this attack in a distributed structure which results in more scalability. Moreover, the lossy nature of LLNs in this study has been considered; therefore, an adaptive approach has been applied to better management in different networks with different error probabilities. Nodes are considered to be static based on RFC-6550. It is also assumed that the network construction is done in a safe and supervised way, and the attackers start their attack after the formation of the network. The attacker is an internal

node and has access to the network's symmetric keys. The attacker node can capture all sent packets by the nodes in its neighborhood and send packets to them. In this attack, the attacker can perform the attack on all of its descendants. The primary approach of the proposed IDS is using packet eavesdropping and considering a threshold for the negative behaviors of nodes. Also, a punishment procedure isolates the attackers, and a forgiving procedure is also introduced to reduce the overheads caused by false detections.

Algorithm 1: Proposed IDS for DDAO attack detection

```
1.  Sent DAO message: M
2.  Next hop (Preferred Parent): j
3.  Begin
4.  IF (Watchdog (M , j)==1)
5.        n_j = 0;
6.  Else
7.     n_j + +;
8.     IF (n_j > α)
9.          Raise an Attack Alarm ;
10.        FG_j + +;
11.         IF (FG_j ≤ β)
12.              Block j for t seconds;
13.         Else
14.              Block j permanently;
15.         EndIF
16.      EndIF
17. EndIF
18. End.
```

The operation of the proposed IDS is shown in Algorithm 1, and in the following sections, its three main building blocks will be explained.

5.1. Monitoring parent's behavior

After sending a DAO message to the preferred parent, the sender node activates the promiscuous mode of its network card and monitors the preferred parent's behavior. Monitoring the parent's behavior is done using a Watchdog technique. Accordingly, when a DAO message is sent to the parent, a timer will be activated, and during this interval, all packets disregarding their data-link layer destination address are passed to the network layer. Then, suppose a packet forwarded from the parent node has been detected, and it is the same DAO message forwarded to the parent with a modification which means the IP address of the parent is added into the body of the message. In that case, the output of the algorithms will be 1. Otherwise, after timer expiration, the algorithm returns zero. Hence, based on the output of the Watchdog algorithm, there are two different cases which are explained in the following sections.

5.1.1. Packet is forwarded

In this case, the output of Watchdog algorithm is one, which means the parent node (node j) has forwarded the DAO message to its parent without any unnecessary changes; therefore, as shown in Eq. (1), the number of negative behaviors of the parent node will reset to zero (lines 4 and 5 of Algorithm 1):

$$n_j = 0 \tag{1}$$

In which n_j is the number of negative behaviors of the parent node j.

It should be noticed that if the attacker node passes the DAO message, the upper nodes will detect the DAO sender node and the attack will be ineffective.

5.1.2. Packet is not forwarded

In the second case, the output of Watchdog algorithm is zero, which means the parent (node j) has forwarded the DAO message to the next node with some unnecessary changes or it has not forwarded the message during the timer interval. Therefore, the number of negative behaviors of node j increases based on Eq. (2) (lines 6 and 7 of Algorithm 1):

$$n_j^{t+1} = n_j^t + 1 \tag{2}$$

Where n_j^{t+1} is the new value of number of negative behaviors of node j, and n_j^t is the previous value.

5.2. Detecting DDAO attack

After increasing the number of negative behaviors of node j, if (3) is satisfied, node j will be considered as an attacker (lines 8 and 9 of Algorithm 1), and the next phase of the algorithm will be run to punish the attacker (see Section 5.3 of this section). Otherwise, the child node will try to forward another DAO message to node j in order to examine its behavior again.

$$n_j > \alpha \tag{3}$$

Where α is the attack detection threshold. In the real world, some mistakes might happen during the monitoring of parent's behavior due to changes in the environment or lack of optimized network hardware. Suppose that the parent node has forwarded the received DAO message to the next node, but, at the time of eavesdropping on its behavior, a barrier has appeared between it and its child node; therefore, the forwarding of the DAO message could not be detected. As a result, a negative behavior will be counted for the parent node mistakenly. In order to reduce the impacts of these mistakes, α threshold has been provided, which means there are up to α acceptable errors. A low value for α will increase the False Positives (FP), and a high value will increase the attack detection delay. Accordingly, α is one of the contributions of the proposed IDS in comparison with other IDSs because it reduces the overheads caused by mistakenly blocking nodes in the network, which lead to a lot of parent changings.

5.3. Punishment and forgiveness

5.3.1. Increasing the number of times for a node to be an attacker

After considering node j as an attacker, to punish it, first the number of times that node j was introduced as attacker will be increased as in (4) (line 10 of Algorithm 1).

$$FG_j^{t+1} = FG_j^t + 1 \tag{4}$$

Then, the IP address of node j will be pushed in the list of blocked IP addresses, and all the communication with this node will be blocked in the future temporarily or permanently based on the explanations provided in the next two sections. By using the attack detection threshold (α), the probability of false detections will decrease. However, there is still a possibility of making some mistakes. Therefore, a forgiving procedure has also been considered to prevent the mistaken blocking of normal nodes as much as possible; hence, the FP alarms will be as low as possible in the network.

5.3.2. Temporary punishment of the node

If the number of times that node j has been selected as attacker becomes less than from or equal with a configurable threshold β, it will be blocked for τ second (lines 11 and 12 of Algorithm 1); therefore, in case of a mistake or a temporary fault, it can return to the network and continue its normal behavior.

5.3.3. Permanent punishment of the node

If the number of times that node j has been known as attacker is more than β, it will be blocked permanently (lines 13 and 14 of Algorithm 1).

5.4. Case study

In the scenario shown in Fig. 4, node A is the DDAO attacker and node *1* is the victim, the bottom dashed circle (with blue border) determines the wireless range of node *1*, and the upper dashed circle (with red border) determines the wireless range of node A.

Assume $\alpha = 2, \beta = 1, \tau = 120$ s, $n_A = 0, FG_A = 0$, and node *1* has sent the first DAO message to node A, and has started to monitor its behavior (based on line 4 of algorithm *1*). Afterward, using the watchdog algorithm provided in Section 5.1, node *1* observes that node A did not forward the DAO message and has sent a DAO-ACK message in response. Therefore, it increases the number of A's negative behaviors ($n_A = 1$), but $n_A < (\alpha = 2)$, therefore it tries to send another DAO message to node A. In other words, after sending two other DAO messages to node A, the number of A's negative behaviors will be 3 which will exceed the α; therefore, node A will be considered as an attacker, the number of times that it was introduced as attacker will increases ($FG_A = 1$), and it will be blocked temporarily for 120 s. Afterward, if node A is again considered as an attacker, it will be blocked permanently because the FG_A will set to 2 and $2 > (\beta = 1)$.

6. Simulation, analysis and evaluation of results

In this section, first, the evaluation metrics are introduced. Second, the simulator and simulation parameters are provided. Then, the proposed IDS will be evaluated based on different scenarios in comparison with RPL.

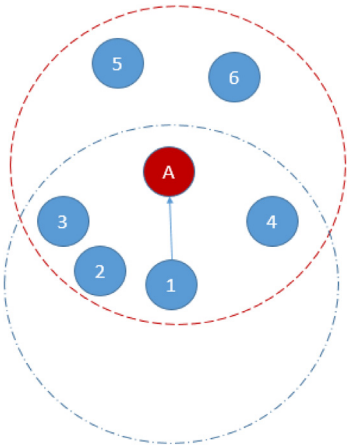


Fig. 4. A part of network as a case study to describe how the proposed IDS detects DDAO attack.

6.1. Evaluation metrics

The evaluation metrics used in this study include Accuracy, Precision, TPR, FPR, PDR and Power Consumption.

Attacks are labeled as Positive, and normal behaviors are labeled as Negative. For different simulations, True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN) are calculated and according to them, Accuracy, Precision, TPR and FPR are calculated based on the following equations ((5)–(8)):

$$TPR = \frac{TP}{TP + FN} \tag{5}$$

$$FPR = \frac{FP}{FP + TN} \tag{6}$$

$$\Pr ecision = \frac{TP}{TP + FP} \tag{7}$$

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{8}$$

Calculation of power consumption was done by analyzing data provided by PowerTrace tool in Cooja simulator. Power consumption of network is calculated based on (9).

$$\begin{aligned} &Power\ (\text{mW}) = \\ &= \frac{Energest\_Value \times Current \times Voltage}{RTIMER\_SECOND \times Runtime} \\ &= \frac{(transmit \times 19.5\ \text{mA} + listen \times 21.8\ \text{mA} + CPU \times 1.8 + LPM \times 0.0545) \times 0.33 \times 3}{4096 \times 8 \times 3600} \end{aligned} \tag{9}$$

Where, voltage and current values are extracted from the Tmote-Sky hardware datasheet, RTIMER-SECOND is the number of clock ticks in each second that is also extracted for Tmote-Sky hardware, Runtime is the simulation time in seconds. Moreover, *Energest_Value* represents the values obtained from Powertrace tool in Cooja simulator for when the simulation ends, and it can be divided into four categories; transmit, listen, CPU, and LPM, which respectively are the number of clock ticks which node n was transmitting packets, was receiving packets, was processing, and was in the Low Power Mode (LPM).

PDR is the ratio of the number of received packets to the total number of sent packets which is calculated using (10):

$$PDR = \frac{R}{S} \tag{10}$$

Where S is the total number of sent packets in the network and R is the number of the packets received at the destination. Note that the RPL does not have any detection algorithm; therefore, the TPR, FPR, Precision, and Accuracy results are presented only for the proposed IDS in all sections.

6.2. Simulator and simulation parameters

All simulations in this study have been conducted using the Cooja simulator, which simulates nodes that use Contiki operating systems, and is the most practical simulator in the field of IoT. Table 1 shows the simulation parameters.

Table 1
Simulation parameters.

Parameter	Value
Simulator	Contiki Cooja
Node type	Sky mote
Simulation time	60 m
Radio interface model	UDGM
The area covered by each node	50 m
Packet size	40 Bytes
Frequency of sending data packets	60 s
α parameter (i.e., attack detection threshold)	Based on the values in (Table 2)
B parameter (i.e., number of temporary punishments for attacker)	2
watchdog timer value	500 ms
τ parameter (i.e., attackers' temporary punishment timer value)	120 s
Nodes arrangement	Four client nodes in each row + one server node (root node) at the top of the first row
Layers 1 and 2	IEEE 802.15.4 standard
Number of repetitions of each simulation	10
Attack detection threshold	Based on the values in (Table 2)

Based on our observations, choosing a high value for β parameter (i.e., the number of temporary punishments of attackers) slightly decreases PDR because we allow attackers to repeat their attacks more times. Consequently, more packets to the victims may be lost before detecting the attackers and punishing them. More specifically, in our simulations, PDR decreased by choosing a value higher than two for β parameter (e.g., for $\beta = 3$, PDR decreased by almost 1.5% on average). On the other hand, by choosing a small value for β parameter, the number of times that a normal node is considered as an attacker may exceed the β threshold. Therefore, that normal node may be blocked permanently, and it would itself decrease the PDR too (e.g., in our simulations, by choosing $\beta = 1$, PDR decreased by nearly 2% on average). Hence, the β parameter is considered to be two in our simulations.

Furthermore, based on our observations, choosing a high value for τ parameter may decrease the PDR because if a normal node is considered as an attacker mistakenly, we are punishing it for a longer time, and during this time, more sent packets to this node are lost. In contrast, by choosing a small value for τ parameter in real-world, we may not allow the normal nodes which are temporarily defected and are mistakenly considered as attackers, maintain themselves and resume their normal behavior again; therefore, they may be considered as attackers again until the number of being considered as attackers for them exceeds the τ threshold. Consequently, they will be blocked permanently, and the network PDR will decrease. In our simulations, we observed that by choosing a value higher than 120 s for τ parameter, we could be sure that the temporary malfunction of the normal nodes, which are mistakenly considered as attackers, has finished, in fact, by choosing $\tau = 60$ s, and $\tau = 180$ s PDR slightly decreased; hence, the proper value for τ in our simulations was 120 s.

To determine a proper value for α, each topology was run once with normal nodes; then, the maximum number of consecutively lost DAO messages in the whole network was considered as the value of α for that topology (Table 2 shows the obtained α value related to each scenario). This approach will decrease the false-positive alarms because it decreases the possibility for α parameter to be falsely exceeded in the real simulations. Also, as mentioned in Section 4, the On–Off attack cannot be performed along with DDAO attack; therefore, even by choosing a big value for α, either the attacker will eventually be detected, or the attack will be ineffective. However, choosing a big value for α will increase the false-negative alarms and the attack detection delay.

Finally, the amount of the used timer in the watchdog algorithm is set to 500 ms which was observed to be the maximum one-hop delay in all simulations.

6.3. Evaluation scenarios

In this section, the impact of 5 different independent parameters on evaluation metrics is measured. The independent parameters are: (1) Network size (i.e., number of nodes), (2) Error probability during eavesdropping, (3) Number of attackers, (4) The distance between nodes (to evaluate the impact of network density).

Table 2 shows the 24 different scenarios of the evaluations.

6.4. The impact of increasing the network size

In this section, the impact of increasing the number of nodes on evaluation metrics is evaluated. Three cases with different networks sizes are evaluated (i.e., 10, 15, and 20), in this regard, the average of the results of scenarios with No. 1 to 8 in Table 2 represents the results of the first network size case (10 nodes), and that of scenarios with No. 9 to 16 and 17 to 24 respectively represents the results of 15 and 20 nodes cases. According to Fig. 5, the TPR for 10 nodes is close to 1 and by increasing the number of nodes, TPR decreases a little. Moreover, according to Fig. 6, for all of the

Table 2
Evaluation scenarios.

No.	Scenario parameters				α parameter
	N[a] (Qty)	A[b] (%)	D[c] (m)	E[d] (%)	
1	10	10	30	10	2
2	10	10	30	25	2
3	10	30	30	10	2
4	10	30	30	25	2
5	10	10	40	10	2
6	10	10	40	25	3
7	10	30	40	10	2
8	10	30	40	25	3
9	15	10	30	10	2
10	15	10	30	25	3
11	15	30	30	10	2
12	15	30	30	25	3
13	15	10	40	10	2
14	15	10	40	25	3
15	15	30	40	10	2
16	15	30	40	25	2
17	20	10	30	10	3
18	20	10	30	25	3
19	20	30	30	10	3
20	20	30	30	25	3
21	20	10	40	10	2
22	20	10	40	25	3
23	20	30	40	10	2
24	20	30	40	25	3

[a]N = Number of the nodes.
[b]A = Attacker ratio in %.
[c]D = Distance between nodes.
[d]E = Error probability.

simulations FPR is less than or equal to 0.005, however, increasing the number of nodes, FPR increases slightly. Also, Figs. 7 and 8 show that by increasing the number of nodes in the network, the Precision and Accuracy went down to 0.9628. According to Fig. 9, by increasing the size of network, PDR for RPL has drop to less than 0.5 which means DDAO attack has had a very destructive effect on the network. But, when the proposed IDS is used, the PDR remains near to RPL without attacker. Moreover, in this figure, the results of RPL without attackers are also presented to explain the impact of memory limitations on PDR even when there is no attacker. Accordingly, as the sent data packets are sent downward from the root to client nodes, the root had to store the routes to all client nodes, but the used hardware in simulations is limited in terms of memory, and the used version of Contiki-OS allocated a limited space for storing routes to client nodes, which results in some stored routes being overwritten, and subsequently some packets being lost. According to Fig. 10, there is an overhead for the proposed IDS in detecting DDAO attacks. Also, the curve of RPL without attacker is presented to explain the impact of successfully performed attacks on RPL; the power consumption of 'RPL with attacker' is lower than that of 'RPL without attacker' because in 'RPL with attacker' DDAO attacks are performed successfully, and many packets are lost which lead to lower power consumption; therefore, the low power consumption of RPL with attacker cannot be considered as an advantage.

6.5. The impact of increasing the error probability

An error might happen during the eavesdropping DAO messages for example because of emerging a barrier between sender node and eavesdropper node. Therefore, the Error Probability parameter is considered to simulate the probability of occurring error in eavesdropping DAO messages. It should be noticed that in the figures of this section, only the figures related to the proposed IDS have been provided because this parameter is only meaningful in the proposed IDS.

Two cases with different error probabilities (10% and 25%) are evaluated; in this regard, the average of the results of odd-numbered scenarios (i.e., No. 1, 3, …, and 23) represents the results of the first error probability case (10%), and that of even-numbered scenarios (i.e., No. 2, 4, …, and 24) is used for the second error probability case (25%). According to Fig. 11, when Error Probability in eavesdropping DAO packets is 10%, the TPR remains to 1, and correspondingly in Fig. 12, a very low FPR has been observed in detection (i.e., 0.0004). With the increase of this parameter to 25%, the TPR decreases a little, but, FPR remains steady as before. As it can be seen in Figs. 13 and 14, when this parameter increases, the Precision and Accuracy decrease slightly; however, accuracy remains almost close to 1. According to Fig. 15, despite the increase of Error Probability to 25%, PDR decreases slightly for the proposed IDS. Finally, according to Fig. 16, the Power Consumption increases by increasing the Error Probability.

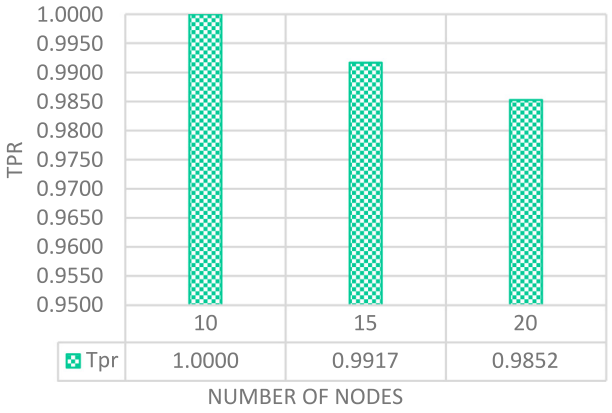


Fig. 5. The impact of increasing the number of nodes on TPR for Proposed IDS.

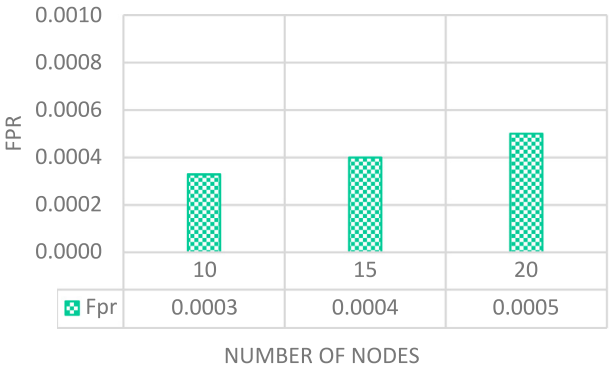


Fig. 6. The impact of increasing the number of nodes on the FPR for proposed IDS.

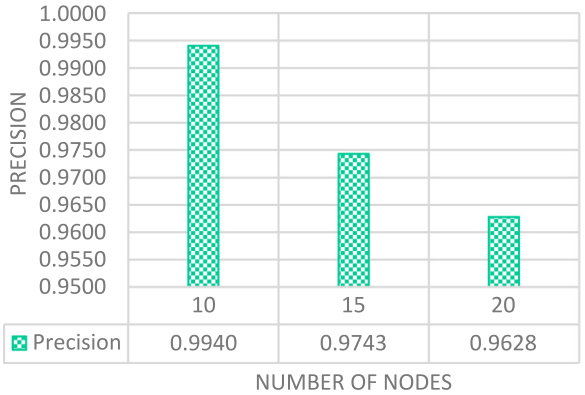


Fig. 7. The impact of increasing the number of nodes on Precision for proposed IDS.

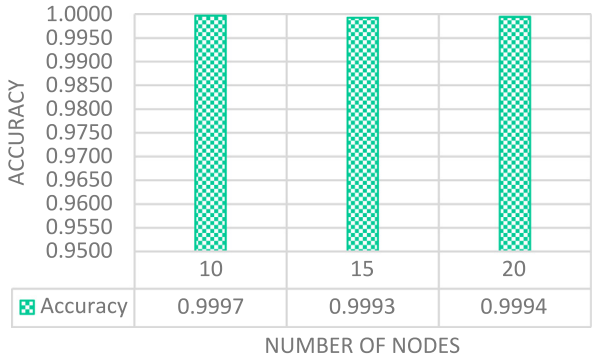


Fig. 8. The impact of increasing the number of nodes on Accuracy for proposed IDS.

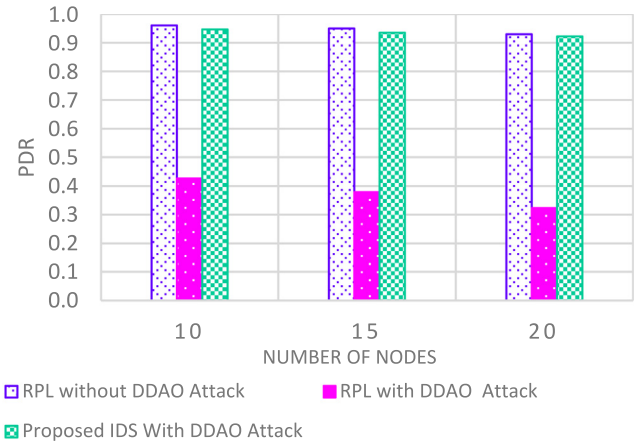


Fig. 9. The impact of increasing the number of nodes on the PDR.

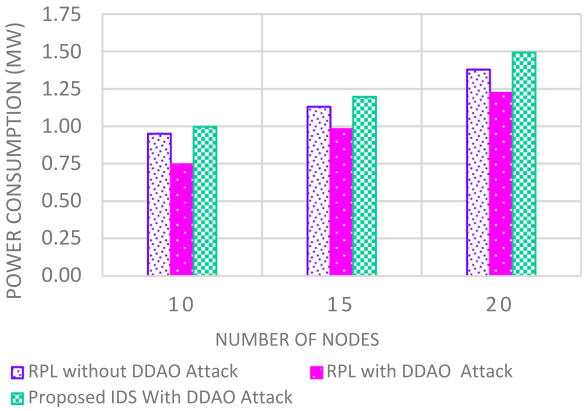


Fig. 10. The impact of increasing the number of nodes on Power Consumption.

Fig. 11. The impact of increasing Error Probability on TPR for Proposed IDS.

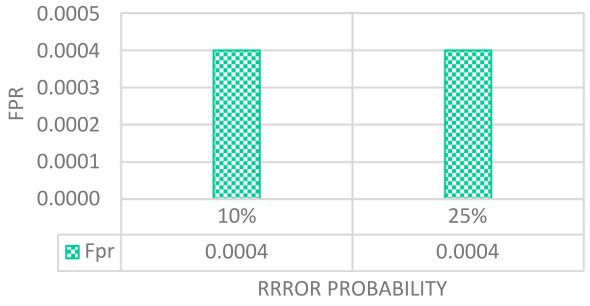


Fig. 12. The impact of increasing Error Probability on the FPR for proposed IDS.

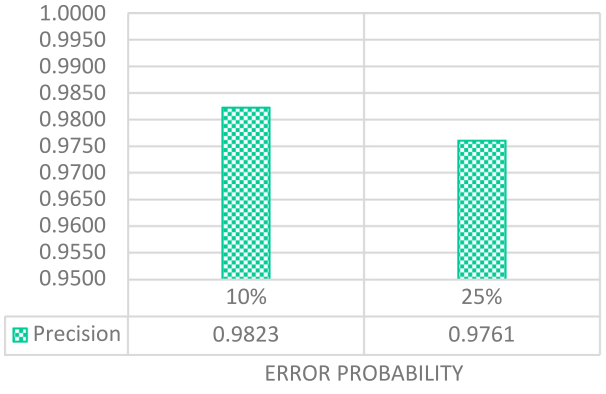


Fig. 13. The impact of increasing Error Probability on Precision for proposed IDS.

Fig. 14. The impact of increasing Error Probability on Accuracy for proposed IDS.

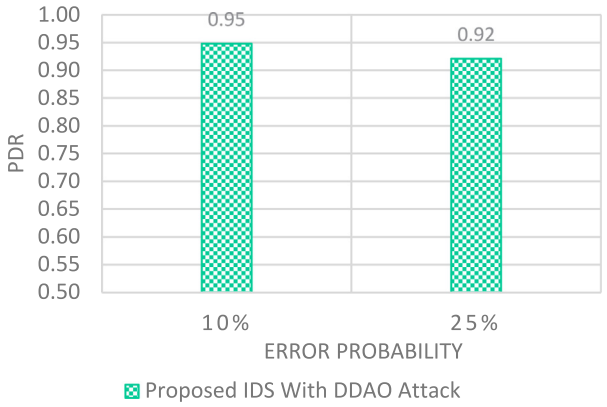


Fig. 15. The impact of increasing Error Probability on the PDR.

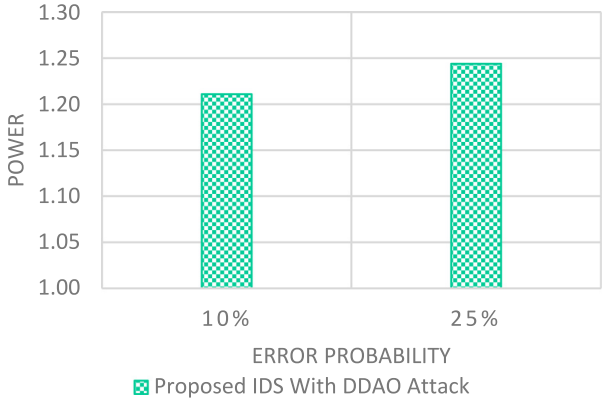


Fig. 16. The impact of increasing Error Probability on Power Consumption.

6.6. The impact of increasing the number of attackers

In this section, the impact of increasing the rate of attackers (the ratio of number of attackers to the total number of nodes in the network) on evaluation metrics is investigated. Two cases with different attacker rates (10% and 30%) are evaluated; in this regard, the average of the results for scenarios with 10% attackers in Table 2 (i.e., No. 1, 2, 5, 6, 9, 10, 13, 14, 17, 18, 21, 22) represents the results of the first error probability case (10%), and that of other scenarios is used to represent the second case (30%). According to Figs. 17 to 20, the proposed IDS, even when 30% of the network are attackers, detects almost all the attacks effectively. According to Fig. 21, by increasing the rate of attackers in the network, the PDR for the proposed IDS decreases. Also, as it can be seen in Fig. 22, by increasing the number of attackers in the network, the power consumption for the proposed IDS increases slightly because of the increase in the amount of processing needed to counter the attacks. On the other hand, for RPL, a high decrease in power consumption can be observed by increasing the rate of attackers, which in fact is not a disadvantage for the proposed IDS as explained in Section 6.4.

6.7. The impact of increasing the distance between nodes

In this section, the impact of increasing the distance between nodes on evaluation metrics is evaluated. Two cases with different values of distance between nodes are evaluated (30 m and 40 m), in this regard, the average of the results for scenarios with 30 m distance in Table 2 (i.e., No. 1 to 4, 9 to 12, 17 to 20) represents the results of the first case (30 m), and that of other scenarios is used to represent the second case (40 m). According to Figs. 23–26, increasing the distance between nodes does not have a considerable impact on detecting the attackers in the proposed IDS. According to Fig. 27, it is observed that by increasing the distance between nodes, PDR for proposed IDS remained close to RPL without attacker.

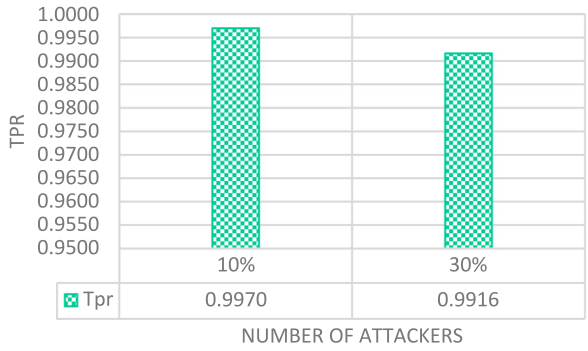


Fig. 17. The impact of increasing Attacker Rate on TPR for Proposed IDS.

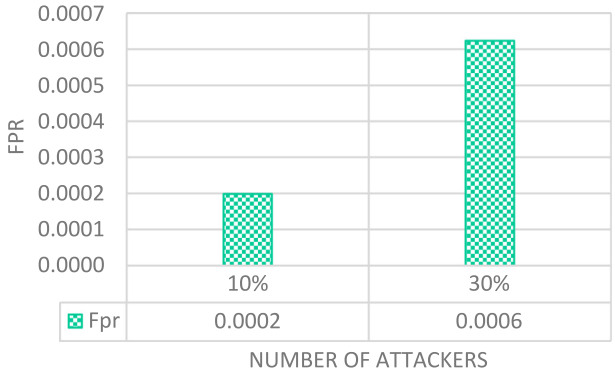


Fig. 18. The impact of increasing the Attacker Rate on the FPR for proposed IDS.

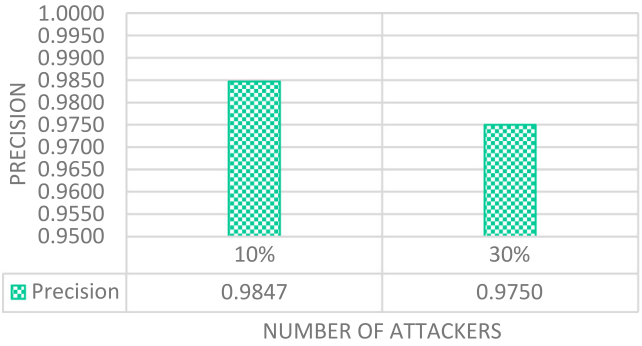


Fig. 19. The impact of increasing Attacker Rate on Precision for proposed IDS.

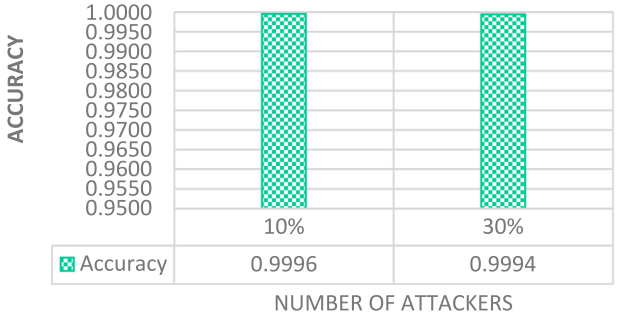


Fig. 20. The impact of increasing Attacker Rate on Accuracy for proposed IDS.

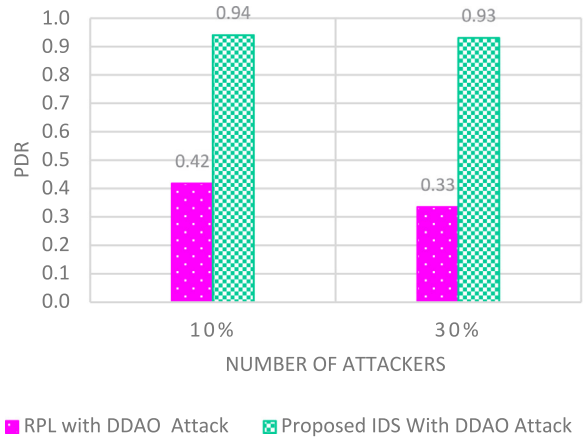


Fig. 21. The impact of increasing the Attacker Rate on the PDR.

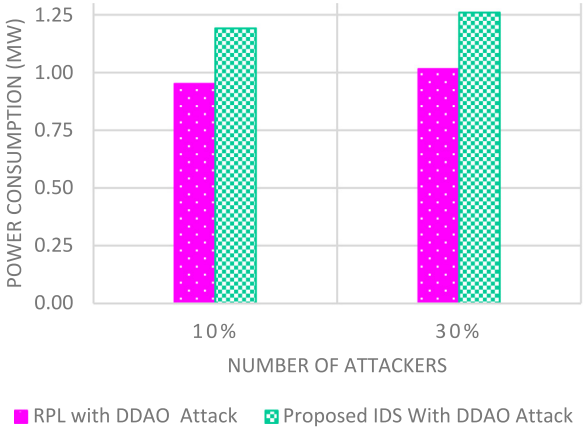


Fig. 22. The impact of increasing the Attacker Rate on Power Consumption.

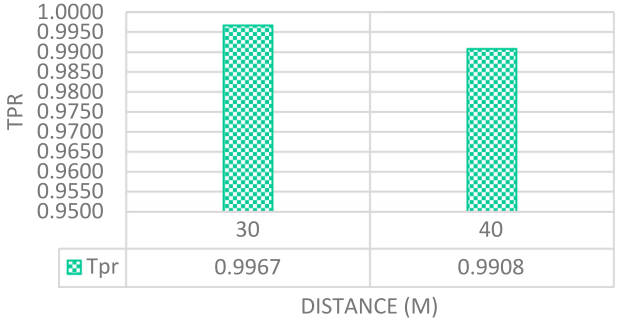


Fig. 23. The impact of increasing distance between nodes on TPR for Proposed IDS.

It is also observed that RPL protocol has had very low efficiency in case of attacker existence. In Fig. 28, it can be seen that the power consumption of proposed RPL is close to that of RPL without attacker for both two scenario sets.

6.8. Summary of the results

The evaluation results show that the proposed IDS can detect DDAO attacks with TPR mostly higher than 0.99, and with FPR close to the zero. It has also a very high Accuracy and Precision even in dense, big, with high rate of attackers, and with high probability of error networks. The reason is that the proposed IDS is fully distributed, and it can also adapt itself

Table 3
Average PDR results of proposed IDS compared with RPLFigure 2.

Scenario No.	PDR of Proposed IDS	PDR of RPL	Improvement (%)
1	0.98	0.46	113.04%
2	0.89	0.45	97.78%
3	0.94	0.40	135%
4	0.95	0.38	150%
5	0.99	0.47	110.64%
6	0.97	0.44	120.45%
7	0.93	0.41	126.83%
8	0.92	0.40	130%
9	0.93	0.42	121.43%
10	0.82	0.39	110.26%
11	0.95	0.35	171.43%
12	0.92	0.33	178.79%
13	0.98	0.44	122.73%
14	0.96	0.43	123.26%
15	0.95	0.37	156.76%
16	0.97	0.30	223.33%
17	0.88	0.38	131.58%
18	0.86	0.37	132.43%
19	0.92	0.33	177.27%
20	0.90	0.29	210.34%
21	0.96	0.39	146.15%
22	0.94	0.37	154.05%
23	0.97	0.24	304.17%
24	0.95	0.21	352.38%
Average	**0.93**	**0.38**	**158.3375%**

Table 4
Table of acronyms.

Acronym	Description
DAO	Destination Advertisement Object
DAO-ACK	Destination Advertisement Object Acknowledgment
DDAO	Dropped Destination Advertisement Object
DIO	DODAG Information Object
DIS	DODAG Information Solicitation
DODAG	Destination Oriented Directed Acyclic Graph
DOS	Denial of Service
E2E	End-to-End
FN	False Negative
FP	False Positives
FPR	False Positive Rate
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IoT	Internet of Things
LLN	Low power and Lossy Network
OF	Objective Function
PDR	Packet Delivery Rate
PFI	Packet Forwarding Indication
ROLL	Routing Over Low power and Lossy networks IETF
RPL	Routing Protocol for Low Power and Lossy Networks
TN	True Negative
TP	True Positive
TPR	True Positive Rate
Average	**0.93**

to different conditions by using two configurable thresholds. Also, the proposed IDS has a higher PDR in comparison to RPL. Table 3 shows the improvement in PDR for the proposed IDS compared to RPL for all scenarios presented in Table 2. Accordingly, the average improvement of the proposed IDS is 158% in comparison to RPL with attacker. These results show that the proposed IDS can efficiently counter the DDAO attacks. Finally, the power consumption of the proposed IDS is close to the RPL without attacker, which shows the proposed IDS is lightweight and has a little overhead. Finally, Table 4 depicts the used acronyms in this research.

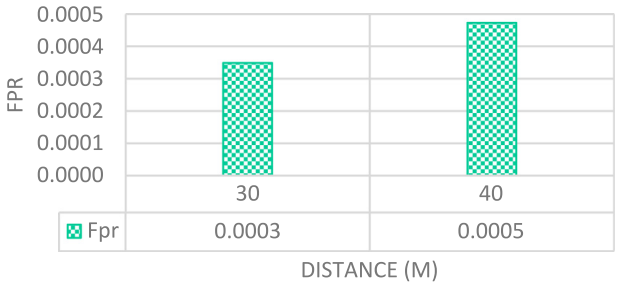


Fig. 24. The impact of increasing the distance between nodes on the FPR for proposed IDS.

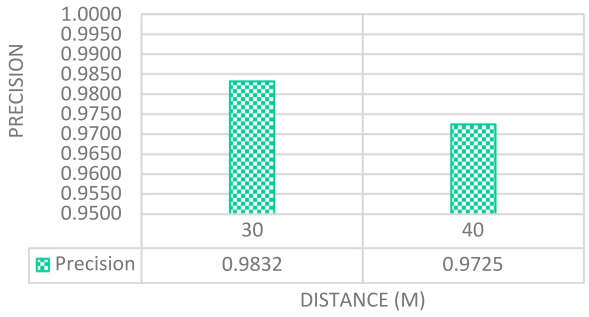


Fig. 25. The impact of increasing distance between nodes on Precision for proposed IDS.

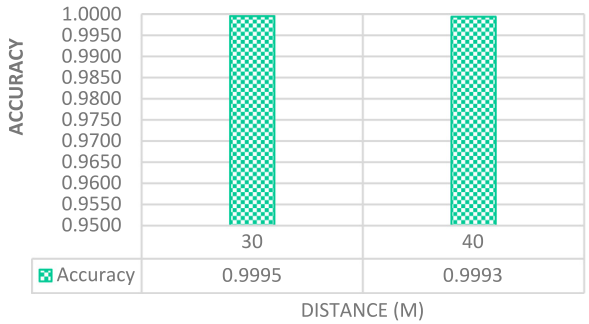


Fig. 26. The impact of increasing distance between nodes on Accuracy for proposed IDS.

7. Conclusion

In this paper, a new attack on RPL protocol called DDAO is introduced, in which the attacker prevents downward routes to the victims from being formed by dropping DAO messages and sending fake DAO-ACK messages to the victims. Based on the evaluations, DDAO attack is a harmful attack that can drop all of the downward packets destined to a big portion of the network and decrease PDR dramatically. Moreover, a fully distributed lightweight IDS is proposed, which can counter DDAO attacks by monitoring parents' behavior against forwarded DAO messages. According to evaluations, the proposed IDS can detect and counter DDAO attacks efficiently (i.e., with high accuracy, precision, and TPR, and with low FPR) even when the network size, network density, attackers' ratio, and error probability are increased.

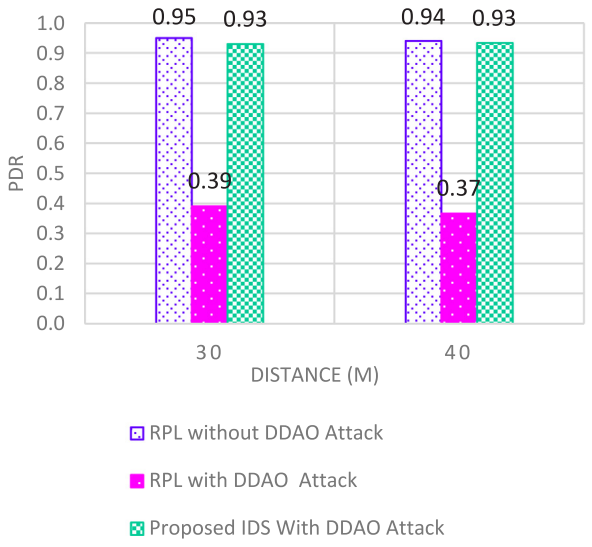


Fig. 27. The impact of increasing the distance between nodes on the PDR.

Fig. 28. The impact of increasing the distance between nodes on Power Consumption.

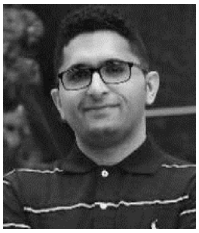
Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] I.F. Akyildiz, et al., Wireless sensor networks: a survey, Comput. Netw. 38 (4) (2002) 393–422.
[2] L.M. Oliveira, J.J. Rodrigues, Wireless sensor networks: A survey on environmental monitoring, J. Commun. 6 (2) (2011) 143–151.
[3] Barekatain, B, Performance evaluation of routing protocols in live video streaming over wireless mesh networks, J. Teknol. 62 (1) (2013).
[4] H.R. Ghaeini, B. Akbari, B. Barekatain, An adaptive packet loss recovery method for peer-to-peer video streaming over wireless mesh network, in: Emerging Technologies for Information Systems, Computing, and Management, Springer, 2013, pp. 713–721.
[5] S. Dehghani, B. Barekatain, M. Pourzaferani, An enhanced energy-aware cluster-based routing algorithm in wireless sensor networks, Wirel. Pers. Commun. 98 (1) (2018) 1605–1635.
[6] J.H. Nord, A. Koohang, J. Paliszkiewicz, The internet of things: Review and theoretical framework, Expert Syst. Appl. 133 (2019) 97–108.
[7] F. Wortmann, K. Flüchter, Internet of things, Bus. Inf. Syst. Eng. 57 (3) (2015) 221–224.
[8] T. Winter, et al., RPL: IPv6 routing protocol for low-power and lossy networks, Rfc 6550 (2012) 1-157.

[9] Z. Liu, et al., Elliptic curve cryptography with efficiently computable endomorphisms and its hardware implementations for the internet of things, IEEE Trans. Comput. 66 (5) (2016) 773–785.
[10] D. He, S. Zeadally, An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography, IEEE Internet Things J. 2 (1) (2014) 72–83.
[11] T. Kothmayr, et al., DTLS based security and two-way authentication for the internet of things, Ad Hoc Netw. 11 (8) (2013) 2710–2723.
[12] V. Rao, K. Prema, A review on lightweight cryptography for internet-of-things based applications, J. Ambient Intell. Humaniz. Comput. (2020) 1–23.
[13] A. Kamble, V.S. Malemath, D. Patil, Security attacks and secure routing protocols in RPL-based internet of things: Survey, in: 2017 International Conference on Emerging Trends & Innovation in ICT, ICEI, IEEE, 2017.
[14] T. Taso, et al., A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs) RFC 7416, IETF trust, 2015.
[15] C. Pu, Mitigating DAO inconsistency attack in RPL-based low power and lossy networks, in: 2018 IEEE 8th Annual Computing and Communication Workshop and Conference, CCWC, IEEE, 2018.
[16] B. Ghaleb, et al., Addressing the DAO insider attack in rpl's internet of things networks, IEEE Commun. Lett. 23 (1) (2018) 68–71.
[17] A.S. Baghani, S. Rahimpour, M. Khabbazian, The DAO induction attack against the RPL-based internet of things, 2020, arXiv preprint arXiv: 2003.11061.
[18] N. Bhalaji, K. Hariharasudan, K. Aashika, A trust based mechanism to combat blackhole attack in RPL protocol, in: International Conference on Intelligent Computing and Communication Technologies, Springer, 2019.
[19] D. Airehrour, J.A. Gutierrez, S.K. Ray, SecTrust-RPL: A secure trust-aware RPL routing protocol for internet of things, Future Gener. Comput. Syst. 93 (2019) 860–876.
[20] D. Airehrour, J. Ray, S.K. Ray, A trust-aware rpl routing protocol to detect blackhole and selective forwarding attacks, 2017.
[21] P. Pongle, G. Chavan, A survey: Attacks on RPL and 6LoWPAN in IoT, in: 2015 International Conference on Pervasive Computing, ICPC, IEEE, 2015.
[22] L. Wallgren, S. Raza, T. Voigt, Routing attacks and countermeasures in the RPL-based internet of things, Int. J. Distrib. Sens. Netw. 9 (8) (2013) 794326.
[23] S. Raza, L. Wallgren, T. Voigt, SVELTE: Real-time intrusion detection in the internet of things, Ad Hoc Netw. 11 (8) (2013) 2661–2674.
[24] P. Karkazis, et al., Design of primary and composite routing metrics for RPL-compliant wireless sensor networks, in: 2012 International Conference on Telecommunications and Multimedia, TEMU, IEEE, 2012.
[25] N. Djedjig, D. Tandjaoui, F. Medjek, Trust-based RPL for the internet of things, in: 2015 IEEE Symposium on Computers and Communication, ISCC, 2015, p. IEEE.
[26] O. Gaddour, A. Koubâa, RPL in a nutshell: A survey, Comput. Netw. 56 (14) (2012) 3163–3178.



Mohsen Sheibani received the M.S. degree in computer science from Islamic Azad University, Najafabad Branch, Isfahan, Iran, in 2019. His main research interests are IoT Security and Machine Learning.

Dr. Behrang Barekatain earned his BSC and MSC in computer software engineering in 1996 and 2001, respectively. He has more than 20-year experience in computer networking and security. He is as a faculty member in Najafabad Branch, Islamic Azad university, Iran, for 17 years. He received his Ph.D. and post-doc in computer networks from Ryerson University, Canada. His research interests encompass wire and wireless systems, VANETs, FANETs, SDN, NDN, IoT, Peer-to-Peer networking; network coding, video streaming, Network security and wireless mesh networks using network coding.

Erfan Arvan received the M.S. degree in computer science from Tarbiat Modares University, Tehran, Iran, in 2018. His main research interests are Network security, IP-based Internet of Things and machine learning applications in IoT.