A Novel Approach for Protecting RPL Routing Protocol against Blackhole Attacks in IoT Networks

Saeid Zangeneh (saeid.jamshidi@outlook.com)
University of Malayer
Rassoul Roustaei
Islamic Azad University of Hamedan

Research Article

Keywords: Low-power, Lossy networks, Security in RPL, Blackhole attacks

Posted Date: June 9th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-174724/v1

Noname manuscript No.
(will be inserted by the editor)

A Novel Approach for Protecting RPL Routing Protocol against Blackhole Attacks in IoT Networks

Saeed Zangeneh · Rassoul Roustaei

Received: date / Accepted: date

Abstract Nowadays, we are witnessing an increasing trend towards interconnected devices. This process of connecting devices instead of people is called the Internet of Things (IoT). The main concept of IoT is to connect heterogeneous objects separately and centrally in different places using standard protocols. The general idea is to create an independent world using intelligent objects that have the ability to exchange information and make decisions. Connected objects allow users to monitor and track remotely and in real-time. IoT relies on the development of a low-power, high-throughput network to support communication between objects and their connection to the Internet. These networks are characterized by limited resources in terms of energy, memory, and processing. In the true sense of the Internet of Things, networks called 6LoWPAN were created, and a new routing protocol compatible with these networks, called RPL, was introduced. Due to the limited nature of RPL-based networks, they may be exposed to a variety of internal attacks. Neighbor attacks and DIS are specific attacks in this protocol. This study proposes a trust-based RPL routing protocol which deals with blackhole threats. Besides, it is shown that while our recommended system is secure against blackhole attacks, it doesn't incur any unwanted expenses in terms of network traffic.

Keywords Low-power · Lossy networks · Security in RPL · Blackhole attacks

Saeed Zangeneh
Department of Computer, Malayer branch, Islamic Azad University, Malayer, Iran.
Tel.: +989189226088
E-mail: saeed.zangeneh.email@gmail.com

Rassoul Roustaei
Department of Computer, Malayer branch, Islamic Azad University, Malayer, Iran.

1 Introduction

Internet of Things (IoT) network is one of the most significant issues in Information Technology (IT) and Computer. As it's evident from the name, anything within the surrounding environment can turn into a node in this network and it's noteworthy that all nodes within such a network are interconnected. This communication is done through wireless networks and will provide a wireless infrastructure within any IoT network which has the potential of a sensor network as well. On the other hand, despite the variety of nodes (i.e. things), they are heterogeneous as well. Secure routing and provision of trustable communication mechanisms are considered as one of the main challenges in the heterogeneous world of IoT [1]. Since IoT includes a set of moving and constant constituents, different problems are faced in the development of routing protocols through which such devices are connected. Any smart routing protocol is capable of freeing up the innate power of any heterogeneous, dynamic, and complex network which is characterized by multiple dynamic factors including change in topology and flow; thus, to make a full range of IoT functions possible, smart protocols for the device to device connection are required in a network. Efficient and scalable routing protocols are compatible with different scenarios in terms of size and type and they're capable of finding the required optimized routes [2][3]. Routing Protocols for Low-power and Lossy Networks (RPL) routing protocol is designed for supporting cost-efficient routing on low-power and lossy networks. The current version of the RPL protocol applies a square-shaped arrangement. Such kinds of arrangements are used for non-smart and non-user attacks. The problem with such arrangements is their high error rate which makes them prone to damages in high-scale attacks. This protocol is highly suited for blackhole attacks and is not suited for other kinds of attacks, especially for repeated and high-scale attacks. To simplify this protocol against normal attacks which mainly consists of unauthorized individuals, a change in the arrangement as well as the application of applied logic is required [4]. Therefore, the RPL protocol dispatch will be optimized in this study through intrusion detection and energy observation.

The wide application of IoT devices in daily activities has many advantages and at the same time, increases the challenges related to security issues [5]. The accessibility of real-time data is necessary for IoT-based sensitive applications. This accessibility is possible only when the externally authorized users are allowed to have direct access to such data, in a way that they could directly access the sensor nodes data or other IoT devices [6]. For more than two decades, authentication and authorization protocols as well as encryption mechanisms and Intrusion Detection Systems (IDS) have been considered as significant tools to protect information networks and systems. However, using traditional intrusion detection techniques in an IoT environment is difficult considering peculiarities of this environment such as limited-resources devices, a specific protocol stack, and different standards involved. The most important issue involved here is the processing capacity and storage of network nodes.

In traditional networks, the system administrator will establish authentication and intrusion detection mechanisms in nodes with higher computational capacity. IoT networks are mainly comprised of nodes with limited resources. Therefore, finding a node with the potential to support security protocols like authentication, authorization, and intrusion detection in the IoT network is a difficult task [7].
Increasing attention of research and industrial groups to RPL protocol is evident in the recent literature and different platforms' RPL performance has been studied accordingly. The authors in [4][5] illustrated the necessity of RPL considering its low delay, quick configuration, and self-healing. Because communication links' security and nodes displacement are considered as crystal-clear issues, we're now looking for ways to facilitate the security of such protocols against attacks to solve this dilemma and optimize RPL protocol. This will consequently lead to lower energy consumption and higher reliability of the network.
Authors in [4]suggested that RPL protocol consists of networks with initial parents that attempt reproduction in later stages such that they can learn IoT networks. Blackhole attacks have resulted in lags between message receiving and sending times which is conducted through communicating the message from the protocol to fuzzy logic. Accordingly, appropriate decisions will be made and the blackhole will be identified in the case that lags exist between messages.
RPL protocol has been applied extensively. The main application of this protocol is fighting against attacks such as blackhole attacks. RPL protocol will act as a protective wall and it will enhance efficiency in case everything is arranged properly. In this study, the researcher attempts to apply RPL routing protocol which has been designed for low-power, lossy networks in rank to increase security against blackhole attacks, such that network efficiency will be improved.

2 A description of the plan

IoT is based on the interconnection between smart and routable devices, connected through an internet platform. The distribution of data in an IoT network generally depends on different applications desired and it required conscious routing protocols and automatic configuration. RPL protocol has been recommended to supervise and manage the efficiency of the network layer in the connection of wireless sensor networks to the internet. Due to their limited nature, RPL-based networks are prone to vast security attacks. One of the main attacks involved in a RPL is a blackhole attack in which a destructive node will eliminate all received packages; while it's expected to dispatch them to the next step's node.
Ahmad et al. [8] presented an approach for reducing the impacts of blackhole attacks with low package loss and high confidence. The suggested approach included a local decision and a universal authentication process. At first, each

node observes the communication behavior of its neighboring nodes by hearing the packages being transferred by its neighbors and attempts to detect the suspicious nodes from their behavior. Then, in case a node identifies another node as suspicious, it would confirm whether the suspicious node is blackhole or not and efficiently identifies the blackhole attack. The simulation results illustrate that the suggested approach increased package delivery significantly and detects blackhole attacks effectively.
The purpose of this study was to optimize RPL. This protocol is a network layer protocol and has been designed in a way to be used in line with 6LOWPAN technology. This protocol has been implemented based on different mechanisms of the communication layer including IEEE MAC 802.15.4 and PHY. IoT scenario can be implemented as a G=(N,L) scenario through RPL protocol, where N is a set of network nodes and L is a set of connections that connected these nodes. Network topology's G graph includes the routes being created and the messages being sent. For each n_i node, one A set exists which includes nodes playing the role of parent nodes for other adjacent nodes. This process runs based on the group's ranking. The ranking is a number which determines the position of a node in that topology as compared with other nodes and the graph root. The use of rankings and ranks for the nodes makes it possible for the nodes to distinguish their position, that of the parent nodes, and invading nodes. In this mechanism, a node decides about its parent node based on the lowest rank specified to the nodes. Rank is a natural number by itself and describes the position of the node in G graph. The lower the position of a node in topology, this parameter will be increased. RPL protocol is implemented through four stages including setup, route development, data communications, and revision of routes. In the RPL protocol's set up phase, the objective function is used to enable the nodes to select their parent node. This process is done based on the ranking information obtained.

3 Suggested approach

The suggested approach is based on the RPL protocol. This protocol is a distance-vector routing and origin routing has been designed to support cost-efficient routing on low-power and lossy networks. This protocol supports three different security modes including insecure, pre-installed, and authenticated. RPL acts based upon the DODAG topological concept. DODAG is an acronym for Destination Oriented Directed Acrylic Graph and it has a tree-like structure that determines the network's default routes. In DODAG, any node can be assigned more than one parent, while any usual tree has one parent node only. To construct DODAG, the graph's root will broadcast a DIO message, such that the graph's ID and rank will be determined and thus enables the other nodes to identify their position within a network. As soon as this message reaches the other nodes, they receive a DIO message in case they'd like to join the network and then:
1. They add DIO message sender to their parent list.

2. They compute their rank using objective function 9the rank of each node must be higher than those of its parents).
3. It will update the DIO package with its rank and will broadcast this package again. This process continues until all network nodes will be assigned a rank. Any node must select a parent node among the set of its parent node for guiding the data packages toward the sink. When a node joins the DODAG graph, it can process the DIO message in three possible forms:
1. Removing the DIO package according to some of the terms and conditions.
2. Processes the message to consolidate its position within the network.
3. To optimize its position by getting a lower rank inside the DODAG graph.

Any time a node will decrease its rank, it must remove parents with lower rank from its own parent set and prevent the development of a loop in the network by so doing. After this stage, a node takes a default route toward the root and it can send its data packages toward the root. In case the performance type would be non-zero in the DIO flags message, the downward routes from roots to nodes must be supported and maintained. In this mode, any node must send a DAO message to its parent such that the information of the inverse route (i.e. downward) would be determined. Whenever DAO packages move from nodes toward the roots, they'll save the address of nodes being visited in the course of upward movement inside their DAO package and as soon as these packages arrive in the root, the complete routes between root and nodes will be developed. This message can be authenticated through a DAO authentication message by the destination[9][10][11][12].
In this suggested approach, the average throughput of each node during previous runs will be computed for the first phase. To this end, any node in the definite periods attempts to assess the number of packages sent by its neighboring nodes. Here, throughout rate is considered as the ratio of the number of packages being sent to the number of packages being received. Accordingly, in case a nose attempts blackhole attacks, the sent packages will gradually become lower than its sent packages and it will be detected as prone to attack. Since this value is defined as a probable number in [0, 1] domain, therefore the throughout value is used as the probability of a blackhole attack in the traffic pattern of a node.

$$BH_{prob}(i) = \frac{rec(i)}{send(i)}$$

Figure 1 illustrates that the input data are in the form of a time-series. A time-series is a set of statistical data that has been collected in equal and regular time intervals. The statistical approaches using such statistical data are called time-series analytical approaches. The throughput rate of each node will be determined in the decision block.

In the second phase of the suggested approach, Ant Lion Optimizer (ALO) algorithm is used to develop an RPL graph in rank to select the best rank and development of the optimized route between the origin nodes and sink

Fig. 1 determining the possibility of attack based on each node's behavior through computing the throughput.

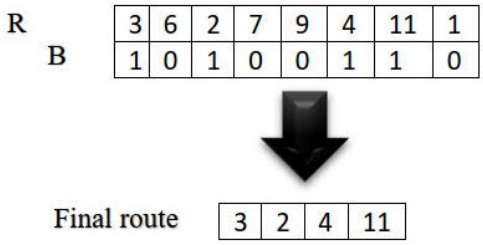

Fig. 2 The structure of a sample solution in the suggested approach.

(i.e. the ate connected to a large-scale network). ALO algorithm imitates the contrast between antlions and the entrapped ants. To model such contrast, the ants must move on the search space, and the antlions are allowed to hunt them and their fit will be increased upon using the traps. Since the ants follow the randomized movement to search for food in nature, a random movement is used to model ants' motions in the following manner [13]:

X(t)=[0,cumsum(2r(t-1)-1, cumsum(2r(t-2)-1]....,cumsum(2r(t-n)-1]

Where cumsum computes the cumulative sum, n is the maximum number of recurrences, t displays the step of random movement, and r(t) is the defined random function which is:

$$r(t) = \begin{cases} (1)if, rand & \leq 0.5 \\ (0)if, rand & \geq 0.5 \end{cases}$$

Where t is the pace of random motion and rand is a generated random number through uniform distribution in [0,1] domain. The ants are similar to particles in a PSO algorithm or individuals in a GA algorithm. The ant's location refers back to the parameters of a specific solution. The general schemata of a solution in the ant ant lion approach are displayed in the following figure. This figure illustrates that it's possible to create routes with different lengths between the origin node and the sink because the generated solution is multiplied in a vector called B. Accordingly, the limitations of meta-heuristic algorithms in the generation of similarly sized populations are eliminated.

This figure illustrates that the size of any solution affects the maximum number of possible steps generated through RPL in a graph. The first line of the matrix shows the number of available nodes in the network's graph as the node of the next step and the second line shows the presence or absence of the intended node in the course of data transfer. Finally, the vector of the final route will be defined for each package. Since the scatteredness of the nodes in the environment is high and the number of possible solutions is displayed exponentially, therefore not all possible solutions can be either generated or assessed. Consequently, the metaheuristic antlion optimizer approach is used. The location of ants will be stored in the following matrix and used in the course of optimization:

$$M_{ant} = \begin{pmatrix} A_{1,1} & A_{1,2} & \cdots & A_{1,d} \\ A_{2,1} & A_{2,2} & \cdots & A_{2,d} \\ \vdots & \vdots & \vdots & \vdots \\ A_{n,1} & A_{n,2} & \cdots & A_{n,d} \end{pmatrix}$$

Such that M_{ANT} displays the location of each ant, A_{ij} defines jth variable and ith ant, n defines the number of ants, and d defines the number of variables to be considered. To assess each ant, a fitness function will be applied in the course of optimization. Then, these functions are stores in the following manner:

$$M_{OA} = \begin{pmatrix} f(A_{1,1} & A_{1,2} & \cdots & A_{1,d}) \\ f(A_{2,1} & A_{2,2} & \cdots & A_{2,d}) \\ & \vdots & & \\ f(A_{n,1} & A_{n,2} & \cdots & A_{n,d}) \end{pmatrix}$$

M_{OA} is used to store the value of fitness function for each ant. Suppose that ant lions are hidden in space. To store their location as well as their objective function, the following matrices are used:

$$M_{AntLion} = \begin{pmatrix} f(AL_{1,1} & AL_{1,2} & \cdots & \cdots & AL_{1,d}) \\ f(AL_{2,1} & AL_{2,2} & \cdots & \cdots & AL_{2,d}) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ f(AL_{n,1} & AL_{n,2} & \cdots & \cdots & AL_{n,d}) \end{pmatrix}$$

$$M_{OAL} = \begin{pmatrix} f(A_{1,1}\ A_{1,2} \cdots A_{1,d}) \\ f(A_{1,1}\ A_{1,2} \cdots A_{1,d}) \\ \vdots \\ f(A_{n,1}\ A_{n,2} \cdots A_{n,d}) \end{pmatrix}$$

$M_{Antlion}$ and M_{OAL} define the location matrix and objective function matrix for each antlion. Besides, $Al_{i,j}$ is the ith and jth dimensions of the antlions, n is the number of antlions, and d is the number of existing variables.

The following conditions are applied in the course of optimization:
- The ants move in search space through different random motions.
- The random motions are applied to all ants' dimensions.
- The random motions are affected by antlion traps.
- The antlions are capable of making holes proportionate to their fit (the more heir fit, the bigger the hole will be).
- The antlions possessing larger holes are capable of catching more ants.
- Any ant can be caught by one antlion and by the selected one (the antlion with the highest fit value) in any iteration.
- The range of random motion will be reduced comparatively until it simulates the sliding motion of the ants toward the antlions.
- If an ant will gain a higher fit compared with an antlion, it means that it has been caught with the antlion and has been pulled under the soil.
- He ant lion changes its location toward the last prey being caught and it can excavate a hole to optimize its power to hunt another prey after each hunt.

To examine each solution, a fitness function (i.e. objective function) has been used throughout the optimization. It has been attempted in this study to select the next step's nodes through minimizing the probability of a black-hole attack (i.e. maximizing the throughput of nodes located on the optimized route)in an uncertainty-laden environment concerning neighboring nodes' performance (normal or invading node). Therefore, the defined fitness function acts based on the following equation:

$$fittness_{sol_j} = \frac{\sum_{i \in soi_j} BH_{prob}(i)}{|sol_j|}$$

$BH_{prob}(i)$ is the throughput of *ith* node in sol_j solution and $\|\mathrm{sol}_j\|$ is the size of this solution (the number of steps between sink and origin node) which is computed based on the number of nodes located on the route.
The ants synchronize their location upon random motions in each optimization step. Since any search space has been endowed with a boundary (variable

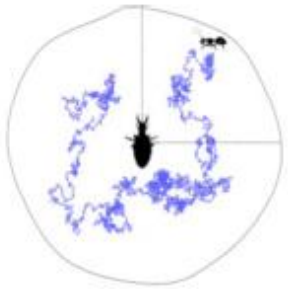

Fig. 3 the random motion of an ant inside an antlion trap.

range), therefore, the random motions have been normalized using the following equation in rank to maintain them inside the search space:

$$X_i^t = \frac{(X_i^t - a_i) \times (d_i - c_t^i)}{(d_i - a_t^i)}$$

Where a_i is the minimum random motion of *ith* variable, b_i is the maximum random motion of *ith* variable, c_t^i is the minimum value of *ith* variable in *tth* iteration, and d_t^i is the maximum value of *ith* variable in *tth* iteration. This equation must be applied in any iteration until it guarantees the occurrence of random motions inside the search space. The random motions of the ants is affected by antlions' traps. To provide the mathematical model of this hypothesis, the following equations are recommended:

$$\mathrm{c}_i^t = Antlion_j^t + c^t$$

$$\mathrm{d}_i^t = Antlion_j^t + d^t$$

Where c_t is the minimum of all variables in *tth* iteration, d_t is the vector including all variables in *tth* iteration, c_t^i is the minimum of all variables for *ith* ant, d_t^i is the maximum of all variables for *ith* at, and $Antlion_t^i$ is the location of selected *jth* antlion in *tth* iteration. Such equations show that the ants move around a selected antlion inside a cloud sphere using c and d vectors. Through such recommended mechanisms, the antlions are capable of making traps proportionate to their fit index and the ants must take on random motions. However, just when the antlions perceive that an ant is entrapped, they throw the soil to a location outside the center of the hole. This behavior makes the entrapped ant slide downward. To model the hunting potential of the antlions, the swirling wheel structure will be used.

Whenever an ant is entrapped, the antlion will throw stones toward the ends of the hole. To develop the mathematical model of this behavior the ra-

dius of the cloud sphere of ants' random motion will be comparatively reduced. The following equations are recommended:

$$C_i = \frac{C^t}{I}$$

$$d_i = \frac{d^t}{I}$$

Where I is a proportion, c_t is the minimum of all variables in *tth* iteration, and d_t is the vector including the maximum of all variables in *tth* iteration. In these equations,

$$I = 10^w * t/T$$

where t is the current iteration, T is the maximum number of iterations and W is a constant which is defined as the following based on current iteration:

$$r(t) = \begin{cases} 2, when\ t & > 0.1T \\ 3, when\ t & > 0.5T \\ 4, when\ t & > 0.75T \\ 4, when\ t & > 0.9T \\ 6, when\ t & > 0.95T \end{cases}$$

Constant W can adjust the precision of utilization. These equations minimize the synchronization radius of ants' locations and simulate the process of ants sliding toward the holes.
The final stage of hunting is exactly when the ant arrives at the lower end of the hole and is caught by the antlion. After this phase, the antlion pulls the ant inside the soil and the body would swallow that. T imitate this process, it's supposed that hunting the prey happens when the ants appear with a higher fit than their corresponding antlion (i.e. they go inside the soil). Then, the antlion must synchronize its location compared with the location of the last hunted ant to enhance its chance to hunt new prey. The following equation is recommended accordingly:

$$\text{Antlion}_j^t = Ant_i^t, if, f(Ant_i^t) > f(Antlion_j^t)$$

Where t is the current iteration, Antlion_i^t is the location of j_{th} selected antlion n_t^{th} iteration and Ant_i^t is the location of i_{th} ant in t_{th} iteration.
Selectivity is a significant characteristic of evolutionary algorithms that allows

them to maintain the best solutions obtained in each stage of the optimization process. In this study, the best antlion in each recurrence is stored and considered as a selected one. Since this selected antlion, is the highly fitted antlion, must be capable of affecting the motions of all ants in all iterations. Therefore, it's supposed that each ant moves randomly around the roulette wheel selected antlions and simultaneously selected antlions in the following manner:

$$Ant_i^t = \frac{R_A^t + R_E^t}{2}$$

Where, R_{i^t} is the random motion around the selected antlion through roulette wheel in tth iteration, R_E^t is the random motion around the selected in t_th iteration, and $\mathrm{An}t_i^t$ is the location of i_th ant in t_th iteration. In reinforcement learning, an objective is defined for the learning agent until it achieves it. Then, the mentioned agent learns how to achieve the determined target through conducting trial and error with its environment. One of the methods of reinforcement learning is the stochastic learning automata. Stochastic learning automata attempts to find the solution to a problem without any information regarding the optimal action (i.e. through considering the uniform probability for one's actions at the beginning of a task). An automata action is selected stochastically and is applied within the environment. Then, the environment's reaction is received and the possibility of actions are updated based on the learning algorithm and the above mentioned procedure is repeated. In the third phase, using the stochastic learning automata, the probability of a blackhole attack in nodes' working pattern will be updated based on reward and punishment mechanisms.
A stochastic automaton is defined in the form of$SA = \{\alpha, \beta, F, G, \phi\}$quintuple; where r is the number of automata actions, $SA = \{\alpha_1, \alpha_2, ..\alpha_r\}$ is the set of all automata actions, $SA = \{\beta_1, \beta_2, ..\beta_m\}$ is the set of automata inputs,$F = \phi \times \beta \to \phi$ is the function of new state generation, $G = \{\phi \to \alpha\}$ is the output function which maps the current state to the next output, and $G = \{\phi_1, \phi_2, .., \phi_k\}$ is the set of automata's internal states at n moment. At the beginning of automata activity, the probability of its actions is equal to $\frac{1}{r}$ (where r is the ttal number of automata actions).
The probability vector is assigned values at first using the computed values in the first phase regarding the throughput of any node; however, over time, it will be assigned new values based on the feedback it received from the environment. The process within this phase is such that in any attempt of sending data, in case the node i will successfully select a package to be passed through a mediating node of j toward the sink, the probability of an attack in all nodes located on DODAG graph, for RPL protocol, will be reduced then. The reasoning behind this is that the node which successfully sent a package toward the sink in several steps can't be the invader in the blackhole attack. This is considered as a reward mechanism in the following equation:

$$\begin{aligned} \mathrm{P}_i(n+1) &= p_i(n) + a[1_{pi}(n)] \\ P_i(n+1) &= (1-\alpha)p_i(n), \forall j \neq i \end{aligned}$$

However, in case the occurrence of a blackhole attack by the mediating nodes will result in the package loss, therefore, the automata will be punished and the probability of $BH_{prob}(i)$ will be increased. However, in case that the recommendation wouldn't be accepted by the tourist, the automata will be punished and it will be updated using the following equation:

$$\begin{aligned} \mathrm{P}_i(n+1) &= (1-b)p_i(n) \\ P_i(n+1) &= \tfrac{b}{r-1} + (1-b)p_j(n), \forall j \neq i \end{aligned}$$

Accordingly, the updated probability values of attack within the graph matrix will dynamically change during the process of automata model learning, such that the resulting graph will be more resistant against attacks.

4 Implementing the suggested approach

4.1 Simulation environment and evaluation parameters

Evaluation parameters of the suggested approach include the number of detected attacks, end-to-end attacks, and the rate of successful package delivery to the destination (PDR) in terms of the number of successfully delivered packages to the total packages being sent which are among the service quality parameters for IoT-based networks. The rate of data delivery will be computed through the following equation (1-4):

$$PDR = \frac{Receive - Pckt}{Sent - pckt}$$

The rate of package loss which is expressed through the proportion of eliminated packages to the total packages being sent is computed through the following equation:

$$P_{Lost} = 1 - PDR$$

The average end-to-end delay in package delivery is defined as the amount of time required to deliver a package right after the formation of the DODAG graph and defining the optimized parent for each node and directing the package through the mediating nodes toward he destination. The characteristics of the system being used, parameters being used in the implementation phase,

and the values of the antlion approach's parameters are displayed in the flowing table.

Table 1 simulation parameters

Simulation parameters	Value
Number of nodes	10, 15, 20, 25, 30
Number of packages being sent through a node	500
Network dimensions	50*50 square meters
The radius of each signal sending node	20

Table 2 ALO approach parameters

Simulation parameters	Value
Maximum number of iterations	10 cycles
Population size	30

5 Simulation results

The authors in this study attempt to study the efficiency of the suggested approach in terms of attack detection and service quality indices such as end-to-end delay and successful package delivery rate (PDR) through sending 500 packages from the origin to the specified destination (i.e. the sink located at the coordinates' origin). Some attacks occur randomly in some simulation runs, in which a node attempts to modify the DODAG graph by declaring a false rank (a higher rank as compared with other odes) and attract user traffic toward this invading node.

To study this particular situation, the number of detected attacks has been studied in two separate modes (the number of attacks detected per each network node and the total number of detected attacks). In the second mode, we have a network consisting of 10, 15, 20, 25, and 30 nodes, while 10% of them are invading by their nature and attempt sending rank messages to their neighbors in different periods to change the package delivery route toward the sink. As it's evident from Figure 4, the suggested approach is highly precise in detecting the attacks made by invading nodes, such that the number of attacks being detected through the suggested approach is higher in most of the network nodes. To clarify the superiority of an approach compared to another, the total number of detected attacks will be illustrated here. As it's evident from Figure 5, the number of attacks detected through the suggested approach is comparatively higher than the basic plan in all five modes (with different numbers of nodes) using ALO and RPL meta-heuristic methods. Thus, the suggested approach can successfully detect and isolate rank attacks during

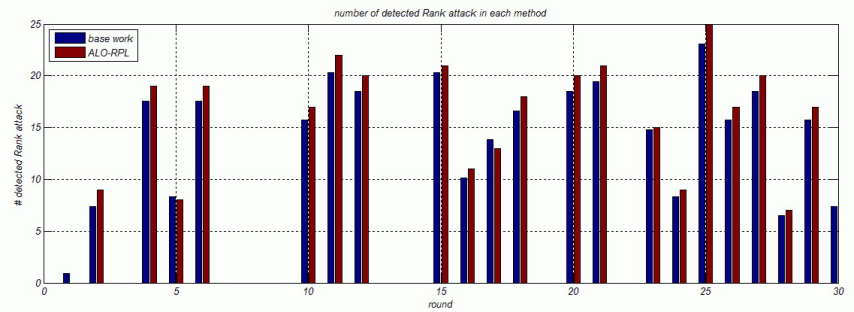

Fig. 4 Suggested approach's efficiency in detecting attacks

routing operations. Before network convergence, RPL will be full of control packages and routing information as an active routing protocol. This will result in a higher transfer of routes and control packages, facilitating it for the destructive nodes to use them for conducting their destructive behaviors. In RPL routing, a node will select its intended parent upon investigating its potential parents with lower values. This low degree uniformity is maintained among the nodes to remove the routing loop. Therefore, the change of node rank will occur when an offspring node will depict itself once again with another low-rank parent node. A rank invader gains a better rank compared with its neighbors and misuses this RPL feature to attract neighboring nodes and deceive them. In this mode, the neighboring nodes will detach themselves from their previous parents and will select the destructive node as their new parent instead.

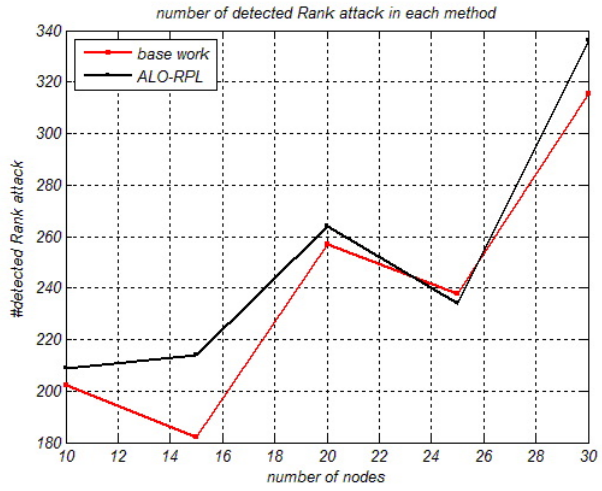

Fig. 5 comparison between the suggested approach's efficiency in detecting invading users

In the following, we compared the successful Package Delivery rate (PDR) to the sink in the suggested approach with the basic one. In the suggested approach, a DODAG graph has been created using antlion meta-heuristic capability in determining each node's suitable [aren't and using teachability and high adjustment rate in learning automata approach, we could select routes for sending packages through distinguishing invading nodes from normal ones. It's noteworthy that the invading nodes haven't been used as mediating nodes. Figure 6 illustrates that the PDR rate of the suggested approach is always higher than any other approach. Therefore, we could reduce the number of lost packages by selecting a suitable route for sending data through the mediating nodes.

One of the main objectives pursued in different routing approaches is guar-

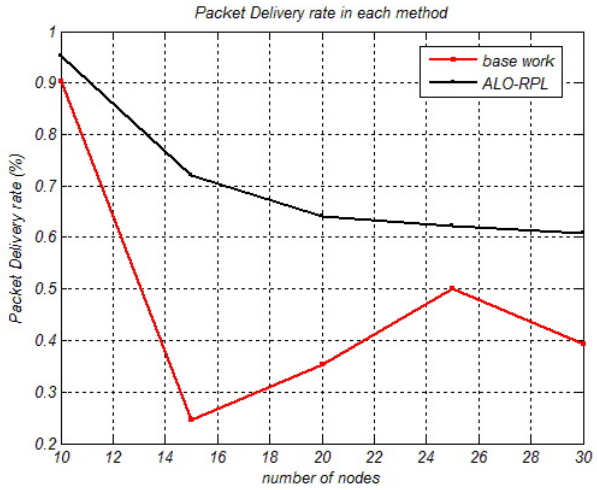

Fig. 6 suggested approach's efficiency in terms of PDR

anteeing a favorable end-to-end delay to satisfy the service level agreements (SLA). Even if the suggested approach detects and isolates the destructive nodes (rank attacks), it mustn't incur additional load on the network's performance. In sections to follow, the same scenario is studied in terms of delays in package delivery by the users. The simulation results in Figure 7 illustrate the performance of the suggested approach.

6 Conclusion

In the suggested approach, the RPL routing protocol has been optimized by using ALO and Stochastic Learning Automata to detect the unauthorized access of invading nodes in receiving the data packages and defining the shortest paths to the sink (blackhole attack). The simulation results showed that

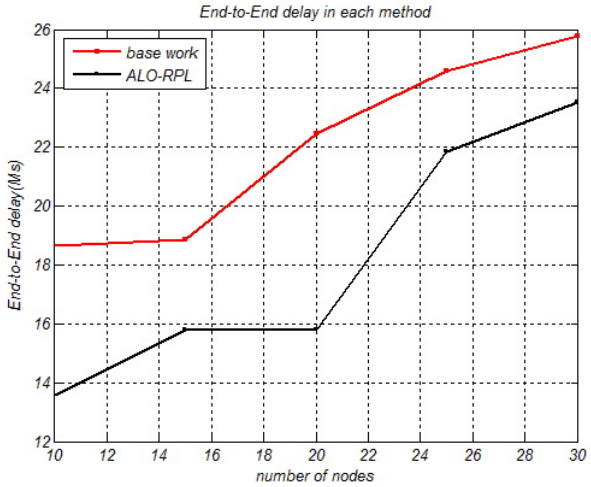

Fig. 7 A comparison between the delays of the suggested approach with the basic plan

the suggested approach was efficient in terms of detecting more attacks; however, PDR has been always higher in the suggested approach compared with the other ones. Besides, the delay in sending packages by the user has been investigated. The simulation results proved the superiority of the suggested approach.

7 Recommendations for future studies

It has been recommended to extract new features which will illustrate the situation of users in terms of being invading or not. I addition, it's recommended to prepare the grounds for detecting other common attacks in the IoT environment using machine learning techniques, such that the attacks would be detected with higher precision in an IoT environment.

8 conflict of interest

No conflict of interest was declared by the authors.

References

1. S. Zhu, S. Setia, S. Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks," ACM Transactions on Sensor Networks, vol.2, nol. 4, pp.62-72 , Nov.2006.
2. H. Chan and A. Perrig, "PIKE: peer intermediaries for key establishment in sensor networks," Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies., vol. 1, pp. 524-535, Aug. 2005.

3. L. Eschenauer, V.D. Gligor," A key-management scheme for distributed sensor networks." In Proceedings of the 9th ACM conference on computer and communications security., pp. 41-47, Nov.2002.
4. D. Airehrour, J. Gutierrez, S. Kumar Ray. "A trust-based defence scheme for mitigating blackhole and selective forwarding attacks in the RPL routing protocol." 2018.
5. M.Ammar, G.Russello, B.Crispo," Internet of Things: A survey on the security of IoT frameworks," Journal of Information Security and Applications,Vol.38, pp.8-27, Feb.2018.
6. M. Wazid, A. Kumar Das, R.Hussain, G.Succi, J.J.P.C. Rodrigues," Authentication in cloud-driven IoT-based big data environment: Survey and outlook,"Journal of Systems Architecture,Vol. 97, pp. 185-196, Aug.2019.
7. T. Sherasiya, H. Upadhyay, H.B. Patel, "A survey: Intrusion detection system for internet of things", International Journal of Computer Science and Engineering (IJCSE), vol. 1, no. 5, pp. 81-90, 2016.
8. A.Firoz, Y.B. Ko. "Mitigation of black hole attacks in routing protocol for low power and lossy networks." Security and Communication Networks, Vol.9, no.18, pp.5143-5154, Oct.2016.
9. F. Raue, W. Byeon, T. M. Breuel and M. Liwicki, "Parallel sequence classification using recurrent neural networks and alignment," 2015 13th International Conference on Document Analysis and Recognition (ICDAR), pp. 581-585, Aug. 2015.
10. I.Boussad, J.Lepagnot, P.Siarry," A survey on optimization metaheuristics," Information Sciences,Vol. 237, pp. 82-117, July. 2013.
11. A.Gogna, and A. Tayal, "Metaheuristics: review and application,"Journal of Experimental Theoretical Artificial Intelligence,Vol.25, No.4, pp.503-526,May. 2013.
12. I.Scharf, A.Subach, O.Ovadia,"Foraging behaviour and habitat selection in pit-building antlion larvae in constant light or dark conditions," Animal Behaviour,Vol. 76,pp 2049-2057,Dce.2008.
13. S. Mirjalili, " The Ant Lion Optimizer," Advances in Engineering Software, Vol.83, pp.80-98,2015.