Journal of Optimization of Soft Computing (JOSC)

Vol. 1, Issue 2, pp: (1-17), December-2023

Journal homepage: https://sanad.iau.ir/en/Journal/josc

Research paper

An efficient energy-aware trust-based RPL protocol for Internet of Things

Farzaneh Kaviani[1], Mohammadreza Soltanaghaei[1*], Farsad Zamani Boroujeni[2]

[1]*Department of Computer Eng., Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran.*
[2]*Department of Computer Engineering, Islamic Azad University, Science and Research Branch, Tehran, Iran.*

Article Info

Article History:
Received: 2023/11/15
Revised:
Accepted: 2024/1/7

Keywords:
Internet of Things, Trust models, Energy-aware, RPL protocol, IDS.

**Corresponding Author's Email Address: soltan@khuisf.ac.ir*

Abstract

The Internet of Things (IoT) is considered as one of the newest communication technologies for various applications. On the other hand, it has faced many challenges that one of the most important of which is related to the security. Due to many limitations, IoT is very vulnerable to attacks, and it is highly exposed to attacks due to its sensitive applications. Various studies have been introduced to improve IoT security. Most of methods have focused on improving the security of the RPL protocol (as the IoT routing standard) based on the development of trust models. However, most of these researches have considered behaviors to calculate the value of trust. This way of assessing trust is not enough due to the widespread attacks of malicious nodes. In this paper, an improved method is proposed based on RPL development utilizing trust models with intrusion detection system. The proposed method focuses on three important principles, including establishing secure and reliable routing topology, evaluating trust, and detecting malicious nodes. In the first step, the network routing topology is formed based on the trust and conditions of the nodes. In the second step, in accordance with the data exchanges, the trust of the nodes is evaluated and malicious factors are identified. The simulation results using Cooja indicated the superiority of the proposed method in improving routing reliability and data exchange over previous operations.

1. Introduction

The Internet of Things (IoT) is widely used in a wide range of areas, including transportation, military applications and emergencies [1, 2]. The most important features of these without infrastructure networks are the absence of central power and distribution of variable topology network, many deficiencies, especially in consumption resources, node self-organization and multi-hop data exchange [3, 4]. These special and unique features of these networks, have led to various issues (especially the issue of trust and support) that are different from other wireless networks. This difference, along with the specific and limited nature of IoT, has led to these networks being more vulnerable to attacks than other networks [5]. However, important and sensitive applications, such as military, have made the IoT highly susceptible to various attacks. The discussion of routing and data exchange as the most important element of the IoT is no exception to this rule. Building trust, especially in the field of routing and data exchange, is one of the most important issues of the IoT. Accordingly, extensive researches have been introduced to improve the

security and trust of IoT routing and exchange based on trust models.

Trust models are considered as a complementary tool for security systems that they provide good ability to detect malicious nodes [6]. Trust models, in addition to high efficiency to detect malicious nodes, are very compatible with the characteristics of the IoT, and they are considered as one of the most effective techniques for implementing trust in these networks [7]. In these models, the network nodes by monitoring and analyzing behaviors assess trust. Trust relations can be used to make effective decisions at the nodes, for example, selecting preferred parents or providing trusted routing. Therefore, many researches have been presented based on the importance of trust models in improving IoT security. The most purpose of these models is to improve the security of the RPL protocol. However, many researches focus on behaviors to calculate the value of trust. This method of assessing trust is not sufficient due to the widespread attacks of malicious nodes and is particularly vulnerable to intelligent attacks [8, 9].

As mentioned in trust models, the trust value of nodes is calculated based on behaviors. This evaluation method provides a cumulative value of previous behaviors of nodes that it is not sensitive enough to detect malicious elements [9]. In other words, it does not provide the ability to detect suspicious elements and deceptive attacks. In fact, malicious nodes can mask negative behaviors because of good behaviors and not be recognizable in exchange. These deceptive behaviors include a number of attacks that the most important of them are on-off attack, selective forwarding and gray hole. The purpose of this article is to improve the response to these attacks.

This paper proposes an improved method called Energy Aware Trust-based Efficient RPL for IoT (EATE-RPL) based on the development of the RPL protocol using trust models and intrusion detection systems. This method improves the reliability of trust calculations and the detection of deceptive attacks by examining the integrity of node behavior. Based on this, the proposed method identifies malicious agents and enables secure routing by removing and quarantining them.

The RPL routing protocol is accepted as the routing standard for IoT and has been widely used in various applications [10, 11]. RPL provides users with the ability to optimize and define routing according to their needs. This article focuses on the RPL capability and tries to improve it based on trust relationships. The main contribution of this article can be summarized as follows:

This paper proposes a new objective function, known as the energy and trust-aware objective function. EATE-RPL uses it to select preferred parents, which is a result of the trust and conditions of the network nodes. It introduces a mechanism to evaluate the trust of nodes, predicts complementary intrusion detection system for more effective detection of malicious agents and intelligent attacks and implements and EATE-RPL evaluates in different scenarios and compares its performance with previous researches.

In the continuation of the article, the PRL protocol will be briefly introduced. In the third section, previous researches will be reviewed. Details of the proposed EATE-RPL will be provided in Section four. In the fifth section, the proposed protocol based on Cooja software is simulated and its performance will be evaluated. The article will conclude in the sixth section.

2. RPL Routing Protocol

The IoT consists of a large number of sensor nodes and one or more specific nodes called roots. Sensor nodes send all their data and reports to the root node. However, the sensors are unable to communicate directly with the root due to radio range limitations. Accordingly, in the IoT, communications and exchanges of nodes with roots take place in a multi-hop with the participation of other nodes. So, nodes operate on the basis of routing protocols [12, 13]. Routing protocols enable communication between sensors and roots by considering and discovering intermediate routes. Among all types of routing protocols, RPL is accepted as the routing standard for the IoT [14]. This protocol has been introduced by one of the Internet Engineering Task Force (IETF) working groups called Routing Over Low Power and Lossy (ROLL) [15]. The group focuses on the routing of

Low power and Lossy Networks (LLN), including IoT.

RPL resolves the needs of IoT routing well because of its unique capabilities, but there are still many challenges. One of the most important of these challenges is related to the security. The function of this protocol is briefly discussed below.

The RPL protocol generally has three control messages including DIO (DODAG information object), DIS (DODAG information solicitation) and DAO (destination advertisement object). DIO and DAO are used to create and update the DODAG graph, and DIS is used to manage network topology changes (such as adding a new node). The RPL forms the DODAG graph through two messages of DIO and DAO, which the nodes will be able to communicate with the root through this graph [14].

To create a DODAG graph, the root node generates a DIO message and sends it all over the network nodes. Each node on the transmitter radio board receives a DIO. After receiving the DIO, the receiving node makes a decision based on evaluating the objective function (OF) in relation to selecting the sender as a parent and resending the DIO [11]. If the node selects the sender as the parent, it updates the DIO packet and resends it in broadcast. Otherwise, it will not send the packet in order to prevent looping. This process continues until all nodes receive the DIO. If a node receives a DIO from multiple neighbors, it selects its parent from the list of candidate parents according to the criteria and constraints defined by the objective function. After sending the DIOs, the node with the best objective function is selected as the preferred parent and is notified by sending a DAO message. This process continues until DAOs are received by the root. Upon receipt of DAOs by the root, the DODAG graph is created, and the nodes are able to communicate with the root through the generated graph. If a new node is added to the network, this extension is managed by sending a DIS packet. The new node sends DIS to its neighbors for requesting DIO, and after receiving it the node with the best objective function is selected as the preferred parent and a DAO packet is sent to it. This will make the new node as a member of the DODAG graph. A more comprehensive explanation is provided in [14].

3. Related works

As mentioned, the importance of IoT applications has made these networks highly susceptible to various attacks. The purpose of most of these attacks is to disrupt the routing process and data exchange, especially to disrupt the performance of the RPL protocol. Accordingly, the extensive researches have reviewed RPL protocol security and the challenges of this protocol [16 and 17]. In [18] Raoof et al. considered the security features of the RPL and the vulnerabilities of this protocol. They introduced various methods of detecting and counteracting attacks. According to this research, attacks on RPL are divided into two types of attacks from wireless sensor networks and attacks focused on RPL features. The results of this study showed that although several security features have been envisaged for the RPL protocol, this protocol still faces wide-ranging challenges. Research [19] provided a detailed review of the types of attacks on RPLs and counteraction techniques. Verma et al. divided the attacks on RPL into three categories: resource-focused, topology-oriented, and traffic-oriented.

On the other hand, extensive methods have been introduced to deal with attacks, which they are two types of intrusion detection systems (IDS) and trust-based methods. In the following, the types of methods related to each category are introduced separately and important details related to each category are discussed.

3.1. IDS-based methods

In this section, IDS-based attack response techniques will be discussed. IDS is one of the most effective intrusion detection solutions that has been widely used in IoT [16]. References [20, 21] provides comprehensive reviews of applied IDS-based models for IoT. In [22] IDS models are evaluated and classified based on parameters and applied techniques. In [23], IDS models based on learning algorithms have been evaluated and analyzed. In [24-26] methods called Compression Header Analyzer Intrusion Detection System (CHA-IDS), Hybrid Intrusion Detection System (HIDS) and Detection of routing attacks in RPL-

based IoT (DETONAR) have been introduced, respectively. Introduced methods focused on intrusion detection techniques that their aim is to detect routing attacks. Although these methods have been successful in detecting attacks, their implementation is highly complex. In [27, 28], the proposed techniques are classified based on IDS to improve RPL security and the vulnerabilities of these techniques are evaluated. Simoglou et al. [16] discussed about the design requirements of IDSs for the RPL protocol and focused on the problems of these techniques. Arış et al. [29] proposed two techniques for combating version number attacks (VNA). In [30, 31], signature-based intrusion detection methods are introduced. Although these methods are simple and fast, but due to the extent of the attacks, these methods are only resistant to some attacks. Luangoudom et al. [32] and Soni et al. [33], respectively, introduced the methods called svBLOCK: mitigating black hole attack in low-power and lossy networks, and Link Hop Value-based Intrusion Detection System (L-IDS) to detect the black-hole attacks. So, svBLOCK focuses on checking the authenticity of control messages, and L-IDS focuses on evaluating the number of hops. The disadvantage of these methods is the high delay. Mayzaud et al. [34] proposed a distributed monitoring architecture to detect DODAG incompatibility attacks. In [35] the same approach was developed to identify rank attacks. In this solution, the monitoring nodes have the ability to cooperate with each other to detect. References [36-38] proposed the Deep Learning (DL) model as IDS to identify routing attacks. The results show good performance in terms of IDS accuracy. However, the DL fitting time is very long.

Studies on intrusion detection models show that although these methods are successful in detecting attacks, they do not provide the ability to establish trust in routing and exchanges.

3.2. Trust-based methods

In this section, trust-based methods will be discussed. Trust is one of the key tools for dealing with malicious nodes and supporting routing and trusted exchanges. It has been widely used in the IoT.

In recent years, the issue of trust management has become more widely used in the IoT. In [39], Junior et al. considered trust models, especially in relation to data transmission trust, and reviewed the challenges associated with this field. Mohammadi et al. [40] considered trust-based models and these methods are classified into three different layers of the IoT based on application parameters and techniques. In [41], trust management in Social Internet of Things is discussed and the challenges in this area are reviewed and several suggestions are introduced to resolve them. In [42], the use of blockchain technologies to improve trusted exchanges is considered and these techniques are compared with traditional trust models. This study shows that the blockchain can improve trusted exchanges. Pourghebleh et al. [9] classified trust management techniques into four classes including recommendation-based, prediction-based, policy-based, and reputation-based and evaluated them based on trust criteria. Studies show that there are still widespread challenges to trust management, especially trust in routing and exchanges. Researches of [7, 8] provided comprehensive reviews of applied trust management models for IoT. These studies have been performed by considering direct and indirect observations (recommendations) based on distributed, semi-distributed and centralized designs. Verma et al. [19] examined a variety of trust models, especially applied trust models to improve trusted RPL protocol exchanges, and increasing energy consumption and incompatibility with the dynamics of nodes are introduced as the most important challenges in trust models. In reference [6] attacks on RPL and trust models against these attacks have been investigated and suggestions have been made to provide a secure routing model.

In the following, some of the most important models of trust are introduced and examined in a more specialized way.

Most previous researches for trust management in the IoT are based on social trust that the important goal of them is to improve RPL routing and exchanges trust. For example, Karkazis et al. [43] introduced the Packet Forwarding Indication (PFI) criterion as a measure of trust for RPL. In [44, 45], models based on multi-metric evaluation and fuzzy

logic are introduced, respectively. The goal of research in [44] is to improve the trust and reliability of routing, and for this purpose it operates based on trust, residual energy and ETX. Fuzzy, dynamic and hierarchical trust model (FDTM-IoT) is integrated as a objective function in RPL and its goal is to improve unreliability as one of the most important features of trust [45]. Djedjig et al. introduced a new trust-based measure for RPL routing [46, 47]. In these methods, direct trust is evaluated based on energy trust, trust in behavior, trust in link, so that the final trust is obtained based on the result of this evaluation by combining indirect trust. Muzammal et al. [48] improved routing trust and RPL exchanges. In this study, trust is estimated based on two factors of direct and indirect trust with considerations related to the dynamics and energy of the nodes. Hassan et al. [49] proposed a control layer-based trust mechanism for supporting secure routing (CTrust-RPL). CTrust focuses on the high energy consumption of trust models that to improve it, trust calculations have been transferred to the higher layer. In [50], trust is evaluated based on successful exchanges between two nodes, and based on it, decisions are made to identify malicious factors. Hashemi et al. [51]Proposed a Dynamic and comprehensive trust model for IoT and its integration into RPL (DCTM-IoT). DCTM is based on direct and indirect trust. It also includes other criteria such as energy, dynamic and ETX (Expected transmission count) in trust assessments to provide a dynamic trust model. In [52], a method for detecting black hole attacks was presented by focusing on assessing the status of graph paths relative to the ratio of successful delivery to total transmissions. Airehrour et al. [53, 54] proposed the trust-aware RPL routing protocol (SecTrust-RPL). In SecTrust, the final trust of the nodes is calculated based on the direct trust and the recommendations received from the two-hop parents. In [55] RPL trust is improved based on a logistic regression model. Logistic regression is used to predict the behavior of nodes based on the value of integrated trust.

According to what was presented in the previous sections regarding intrusion detection systems and trust models, if IDS-based methods are successful in detecting malicious nodes, these models do not provide the ability to support routing and trusted exchanges. While trust-based models have been successful in supporting routing and trusted exchanges, most of these methods deal with some attacks, including deceptive attacks (such as on-off attacks, selective forwarding, etc). In addition, most of the researches presented have focused on securing topology routing and trusted exchanges. Although this performance covers the needs of trust well, other aspects of routing, including the reliability of routing and exchanges, still need to be considered in order to maintain the quality of exchanges. Focusing only on trust, even in some situations, may lead to increased intermediate route lengths, exchange inefficiency, and reduced service quality because trust is the only criterion for decision making.

In this research, a method called Energy Aware Trust-based Efficient RPL (EATE-RPL) is proposed based on RPL optimization with a focus on models of mutual trust using IDS. EATE-RPL focuses on three important principles including establishing secure and reliable routing topology, evaluating trust, and detecting malicious nodes. On this basis, in addition to covering security needs, the reliability of transactions has also been provided.

4. Proposed EATE-RPL

The purpose of EATE-RPL is to improve RPL protocol routing and exchanges. For this purpose, the EATE-RPL operation is divided into two general steps. In the first step, based on the trust and conditions of the nodes, the focus is on creating a secure and reliable routing topology. In the second step, along with the data exchanges, the trust of the nodes is evaluated and malicious factors are identified. In addition to providing communication trust, EATE-RPL also covers the reliability of data exchanges. Overall, the EATE-RPL focus to improve reliability and trust of RPL can be divided into the following:

1-Creating secure and reliable routing topology.

2-Proposing a new objective function called Trust and Reliability Aware Object Function (TQAOF) that it is evaluated by focusing on residual energy, trust, ETX, and node rankings.

3-Establish trust by focusing on trust-based and IDS-based techniques with the aim of improving detection of malicious nodes.

In the following, first the details of TQAOF evaluation are provided and then how to develop RPL in order to implement EATE-RPL will be discussed.

4.1. Extended RPL with TQAOF

TQAOF is an objective function that provides a result of trust, reliability, and node rankings. The selection of the preferred parents is based on the evaluation result of this function. Based on previous researches, only communication security has been discussed and supporting the reliability of data exchanges has not been considered. However, TQAOF supports both needs well. This criterion is evaluated in terms of residual energy, ETX, node ranking and reliability.

In general, the RPL protocol has two functions including OF0 and ETX to select the preferred parents that one of which can be used as needed. In the objective function of OF0, the selection of the preferred parents is done with a focus on proximity to the root [56], and in the objective function of ETX, this selection is based on the reliability of the link [57]. TQAOF is an improved objective function that includes the outcome of rank, reliability (residual energy and ETX) and node trust with the aim of creating a secure and reliable routing topology graph.

To detail the EATE-RPL function, in the first section the applied criteria have been formulated for calculating TQAOF, then routing and network topology is discussed for the TQAOF objective function. In the following, the details of malicious detection and isolation are described.

4.2. TQAOF Metrics

The parameters used to evaluate TQAOF reflect the trust, rank, and reliability of the nodes. These parameters are used to find the best parent and are as follows:

4.2.1. Trust

In EATE-RPL, the trust evaluation is based only on direct trust and is not used indirect trust (recommendations) due to attacks and increased overheads. Exchanges of recommendations, on the one hand, have led to an increase in overheads, which is contrary to IoT limitations, and on the other hand, will lead to attacks such as Bad-mouthing and Good-mouthing. So, in EATE-RPL, the assessment of trust has been done only with a focus on direct trust.

Direct trust is related to the behavioral history of nodes that it provides a result of trust in node communications. Nodes in IoT networks often cooperate and communicate with other nodes (neighboring nodes). Considering communication behaviors provides the ability to detect the normal or abnormal operation of nodes. However, it should be noted that due to severe IoT limitations, many causes lead to communication disruptions and data loss. In fact, the cause of failed communication may not be the only malicious behavior, and communication channel disruptions or decrease of node efficiency may be the cause. Therefore, evaluating trust with regard to the history of communication behaviors will be uncertain. In EATE-RPL, improve this issue is based on the concept of uncertainty. But at the same time, this kind of evaluation will not be safe enough, especially in the face of deceptive attacks. In this type of attack, the malicious agents act by changing their behaviors (change in right and wrong behaviors) in such a way that with performing negative behaviors, their trust is greater than the threshold value of malicious detection. This is done with the intention of deception. Considering three concepts can have great effects in improving this issue: 1) The malicious node can't gain high trust in low value transactions and is misused it in high value transactions. This refers to the need to calculate variable trust in the interaction value. 2) Trust is hard to come by and easy to lose. Trust in negative and positive transactions should not have the same effect. The effect of negative transactions on reducing trust should be greater than the effect of positive transactions on increasing trust. 3) The malicious agent can't gain high trust in the old transactions and abuse it in the current transactions. This refers to the higher value of current transactions in the calculation of trust. The EATE-RPL seeks to improve the detection of deceptive and intelligent attacks by considering these three concepts alongside the topic of uncertainty.

The EATE-RPL uses the watchdog mechanism to assess trust and to make direct observations during exchanges. Based on the results of this monitoring, the ability to analyze and detect the behavior and performance of nodes during exchanges will be provided. Then, based on the results of this study, the trust of the nodes is evaluated based on equation (1). So that $T_{i,j}$ is equal to the trust of node i to j, $NT_{i,j}$ and $PT_{i,j}$is equivalent to the new and past trust of node i to j, θ is value coefficient to the new and old trust of nodes. So that $0 <\theta <1$. The value of this coefficient in EATE-RPL is considered equal to 0.5. $PT_{i,j}$ is the past trust that it is saved in the node table. In the initial moment the trust value of nodes is equal to 0.5 (average trust).

$$T_{i,j} = \theta . NT_{i,j} + (1 - \theta) . PT_{i,j} \quad (1)$$

4.2.2. Energy Remainder (ER)

This metric is one of the reliability criteria and refers to the residual energy of the nodes. The ER criterion is evaluated based on energy consumption to the initial energy of the nodes. In equations (2) and (3), the details of energy consumption of nodes and evaluation of residual energy of nodes are provided, respectively. Thus, tx, rx, LP and cpu are equivalent to transmission, receive, low power mode (such as node sleep mode) and processing mode (when radio components are off), respectively. P_{tx}, P_{rx}, P_{cpu}, and P_{LP} are equivalent to the energy requirements associated with the four modes, respectively. T_{tx}, T_{rx}, T_{cpu}, and T_{LP} are the length of sending, receiving, processing, and low power mode, respectively [58]. In equation (3) EC_i, IE_i and ER_i are equal to the amount of energy consumed, the initial energy and the ratio of the remaining energy of node i, respectively. In IoT networks, power consumption of node is depends on its location in the network. This metric is effective in preventing the selection of low energy nodes and premature depletion of energy of some intermediate nodes.

In EATE-RPL, nodes share their remaining energy periodically in the network with their neighbors.

$$EC_i = T_{tx} \times P_{tx} + T_{rx} \times P_{rx} + T_{cpu} \times P_{cpu} + T_{LP} \times P_{LP} \quad (2)$$

$$ER_i = 1 - \frac{EC_i}{IE_i} \quad (3)$$

4.2.3. Rank

This metric refers to the position of the nodes relative to the root. If the node rank is smaller, the node is closer to the root, and vice versa. In most cases, the rank of the root node is zero, and the rank of the other nodes increases in proportion to the distance to the root. Rank, in addition to preventing looping, is one of the most important criteria for selecting parents with optimal paths. Rank of nodes in the RPL is exchanged between nodes via DIO messages. Equation (4) shows how the rank is calculated. So that R_j is equal to the rank of node j, FR_j is the rank of parent j and RI is equal to the value of the fixed rank redundant.

$$R_j = FR_j + RI \quad (4)$$

4.2.4. Expected Transmission Count (ETX)

This criterion is known as link reliability [17]. ETX refers to the certainty of the desired connection, and it is defined in terms of the probability of successful delivery of data by the receiver (DF) and the probability of successful delivery of ACK by the sender according to equation (5). So that $ETX_{i,j}$ is the reliability of nodes i and j. Using this parameter leads to the selection of routes with higher reliability. If the ETX value is lower, the link reliability is higher, and vice versa.

$$ETX_{i,j} = \frac{1}{Df_{j,j-1} \times Dr_{j,j-1}} \quad (5)$$

4.3. The process of sending DIOs in EATE-RPL

The process of sending DIO messages in EATE-RPL is consistent with sending DIOs in the RPL protocol, except for one minor difference, which is described in detail below.

In EATE-RPL, as in the RPL protocol [14], the root node generates a DIO message when it starts operating and propagates it over the network. Sending DIOs in accordance with the RPL is repeated over specific time periods to update the network topology.

In the RPL protocol, after sending the DIO message by the root, it is shared among the nodes to the extent that all members of the DIO network

receive the sent one. The process of sending DIOs in EATE-RPL follows the same rule, except that if the sender of the DIO was from a parent identified as malicious (node trust is less than the threshold value), receiving node refuses to accept or resend the DIO message. This is done with the aim of punishing malicious agents and preventing their participation in creating the network topology. In fact, when a factor is identified as malicious, it will be excluded from network interactions for a certain period of time to punish. Therefore, no packet is received from the malicious agent during the quarantine period and no packet is sent to it.

In addition, a bit flag is provided in the DIO packet called security flag (SF) that the value of it is one or zero and is specified by the root node. If the value is one, it means the need to implement security and network nodes operate in security mode. However, if it is zero, the network application is normal without security sensitivity. In fact, depending on the application and security needs, the root node specifies the value of this flag.

4.4. Parent Selection

The EATE-RPL objective function specifies how to separate and select preferred parents. OF in EATE-RPL consists of two execution steps. The first step is to start the network, which includes discovering neighbors and creating connections. The network nodes do not know about their neighbors or their trust. At the beginning of network operation, all nodes are equal to 0.5 (average trust) and their energy is the same. Therefore, only criterion used to construct the topology is the rank of the nodes. The parent with the minimum rank value is selected as the preferred parent and the network topology is created accordingly. After creating the initial topology, the second step is called and executed. The second step is to update the network topology and build trust. In this step, if safe mode is not active (or in other words, the SF flag is set to zero), the only remaining energy, rank and ETX are as decision criteria. Based on these parameters, the preferred parents are selected and the network topology is updated. However, if the security mode is enabled, the nodes first assess the trust of parents and distinguish the parents that have the most trust threshold. Then they choose the parent with the highest priority as the preferred parent.

The parent selection mechanism based on TQAOF is presented in Algorithm (1). When a node intends to select or change its parent, EATE-RPL selects the most appropriate option from the set of candidate parents based on the parents' preference. Prioritization and selection are based on the TQAOF objective function. If the priority of two parents is equal, trust is the selection criterion and the parent with high trust is selected as the preferred parent. The parent selection mechanism based on TQAOF and trust criteria is presented in Algorithm (1). The algorithm first creates a set of candidate parents as a list. The network security conditions are checked based on the SE flag check (Line 3). If network conditions are not secure, parental priority is assessed by energy, ETX, and rank (Lines 4 and 5). Otherwise, if the network conditions are in a secure state, first the trust of the parents is measured and the untrusted parents are removed from the list of candidates (lines 7 and 8). Then the priority of the trusted parents considering the energy, ETX, and rank is assessed (lines 11 and 12). The node with the highest priority is then selected as the preferred parent (lines 14 to 16). If the priority of the two parents is equal to each other, the parent with higher trust will be selected as the preferred parent (lines 17 and 18). At the end, the preferred parent is returned as the selected parent by the algorithm (line 22).

Algorithm (1) Preferred parent selection mechanism

Input: DIO Message from nodes;
Output: Preferred parent (P_p) selection of node i;
1: TQAOF = 0;
2: **For** each j ∈ candidate fathers list
3: **If** (SF = 0) then // SF = Security Flag
4: $TQAOF_j = w_1 \times ER_j + w_2 \times \frac{1}{ETX_{i,j}} + w_3 \times \frac{1}{R_j}$;
5: $w_1 + w_2 + w_3 = 1$; // w is metrics weight
6: $w_1 + w_2 + w_3 = 1\ ,\ 0 \le w_1, w_2, w_3 \le 1$
7: **Else**
8: **If** ($T_j \le TH_T$) then
9: Discard node of parent candidate list;
10: **Else**
11: $TQAOF_j = w_1 \times ER_j + w_2 \times \frac{1}{ETX_{i,j}} + w_3 \times \frac{1}{R_j} + w_4 \times T_j$;
12: $w_1 + w_2 + w_3 + w_4 = 1\ ,\ 0 \le w_1, w_2, w_3, w_4 \le 1$
13: **End if**;
14: **If** (TQAOF < $TQAOF_j$) Then
15: $P_p = Father_j$;
16: TQAOF = $TQAOF_j$;

```
17:      Else if (TQAOF = = TQAOF_j) Then
18:           P_p = node with maximum trust;
19:      End if;
20:    End if;
21: End for
22: Return P_p;
```

4.4.1. Complementary intrusion detection system

In the EATE-RPL, in addition to the discussion of trust, a complementary intrusion detection systems (IDS) are envisaged to increase the accuracy of malicious node detection. This is because some attacks, especially intelligent attacks, may not be detected by high-reliability trust models. In other words, trust is an accumulated value based on the nodes' past behaviors and reflects an overall evaluation of the nodes. This accumulation is not sensitive enough to detect intelligent attacks, because it takes time to reduce accumulated trust. Designing an intrusion detection system based on assessing the ratio of negative behaviors and behavioral changes can be effective in counteracting these attacks.

Designing such an intrusion detection system can affect the behavior of malicious nodes, especially when they are aware of the rules of trust assessment and try to maintain a certain amount of trust value by fluctuating between their behaviors. Therefore, we use the intrusion detection system based on the evaluation of the ratio of negative behaviors with the use of the concept of entropy [59].

Methods designed based on intrusion detection systems (IDS) are based on a set of anomaly detection rules [60, 61]. As mentioned, EATE-RPL uses this system to increase the accuracy of intelligent attack detection. If IDS generates warning for a node, the node will be identified as malicious.

Since most intelligent attacks focus on behavioral changes, the proposed IDSs are based on this. In EATE-RPL, IDS warns when the ratio of negative behaviors and node behavior changes exceeds a certain threshold. Equations (6) to (9) provide details of this detection. Where $IDS_{i,j}$ is a warning symbol. $D_{i,j}$ (t-1, t) is equal to the ratio of the value of incorrect behaviors to the sum of the values of node j behaviors for node i requests in time period t-1 to t. TH_E is equivalent to the energy threshold, TH_D is the intrusion detection threshold and β is the error control index. Energy threshold and intrusion detection in terms of repetition of experiments in the proposed method are considered equal to 0.2 and 0.5, respectively. The error control index (β) is used when the node energy is in the critical state. In this case, since the negative behaviors of a node may be due to a decrease in performance, by considering the error control index, it tries to prevent the misdiagnosis of these nodes as malicious. If the change in node behavior is high during interactions, the probability of IDS warning is high, and vice versa. In fact, this IDS is designed and predicted with a focus on analyzing behavioral changes.

$$IDS_{i,j} = \begin{bmatrix} 1 \text{ If } (ER_j \geq TH_E) \text{ and } (D_{i,j}(t-1,t) > TH_D) \\ 0 \text{ If } (ER_j < TH_E) \text{ and } (D_{i,j}(t-1,t) > TH_D + \beta) \end{bmatrix} \quad (6)$$

$$D_{i,j}(t-1,t) = \frac{VNB_{i,j}(t-1,t)}{VCB_{i,j}(t-1,t) + VNB_{i,j}(t-1,t)} \quad (7)$$

$$VCB_{i,j} = \sum_{a=1}^{No.of\ transaction} S(a)_{i,j} \times V(a)_{i,j} \quad (8)$$

$$VNB_{i,j} = \sum_{i=1}^{No.of\ transaction} N(a)_{i,j} \times V(a)_{i,j} \quad (9)$$

In equation (8) and (9), $VCB_{i,j}$ and $VNB_{i,j}$are equal to the sum of the value of positive and negative interactions, respectively. No. of transaction is the sum of interactions between nods of i and j in period of time t. $S(a)_{i,j}$ and $N(a)_{i,j}$are equivalent to satisfaction and dissatisfaction with the interaction of (a) (in successful interaction $S(a)_{i,j} = 1, N(a)_{i,j} = 0$ and in case of failure $S(a)_{i,j} = 0, N(a)_{i,j} = 1$). $V(a)_{i,j}$ is equivalent to the value of interactions of (a) for nodes i and j, which will be equal to 1 and 0.5 for control and data messages, respectively. Note that packets sent in the IoT can generally be divided into data and control. Control messages are more valuable than data messages due to their important role in topology formation [47]. Considering the value of interaction in calculations, the node can't gain high trust in low-value transactions and abuse it in high-value transactions.

4.4.2. DODAG Construction and Trust Update

In EATE-RPL, trust updates are reactively and dynamic. Reactive and dynamic trust updates are based on behaviors. In this type of update, nodes are encouraged and punished for their right and wrong behaviors by increasing and decreasing trust. Details of the evaluation and update of trust were discussed earlier. Based on this assessment, if a node's trust falls below the threshold value, the faulty node is identified as malicious and added to the malicious list. In this case, the desired node will be excluded from the network exchanges for a certain period of time.

5. Simulation and experimental results

In this section, the efficiency and performance of EATE-RPL will be evaluated. For this purpose, EATE-RPL is implemented with cooja 2.7 simulator software (simulator designed based on Contiki [62]) and with protocols of RPL [14], CT-RPL [49] and SecTrust [53] has been compared. Experiments were repeated for variable of malicious agent as well as different attacks and scenarios to evaluate the performance of methods. The details of the simulation scenarios are discussed in the next section.

5.1. Simulation setup

As mentioned, open source simulation software of Contiki 2.7 / Cooja simulator was used [63]. The configured scenarios for evaluating the methods include 40 nodes of Sky mote type (TelosB) and one root node and they are located in a network with a size of 200m * 200m. The root node is in the center of the network and the other nodes are randomly placed around it. Each network node has a 16-bit microcontroller of Texas Instruments MSP430 with a frequency of 8 MHz with 10 KB of RAM and 48 KB of flash memory. To evaluate the methods, two types of attacks, black-hole and selective-forwarding, have been considered. The performance of the methods against these two types of attacks has been examined. Also, the number of malicious nodes in different scenarios is considered between 1 to 10 nodes.

The trust threshold is set to 0.5 and the γ coefficient is set to 0.5 for indefinite behaviors. The values of coefficients (w) in SE = 1 are equal to w_1, w_2, w_3, w_4 = 0.25 and in SE = 0 are equal to w_1, w_2, w_3 = 0.333. Other details of the simulation parameters are given in Table (1).

Table 1. Simulation parameters.

Parameter	Value
Simulator	Cooja-Contiki 2.7
Loss Model	Distance loss
Sensors	Skymote
Adaptation	6LoWPAN
Communication protocol	CSMA, ContikiRPL, IPv6
Traffic rate	1 packet sent every 10 seconds by every node
number of nodes	40
Network area	200m*200m
Data packet size	64 bytes
Range of nodes	RX: 50%, TX: 50m, interference: 60m
Number of attacker nodes	1-9
Transmission layer	UDP
Attacks	Blackhole, Selective forwarding
Simulation time	1 h
Radio model	Unit Disk Graph Medium (UDGM)
Trust Threshold	0.5

In experiments, the methods competed with each other despite different attacks and a variable number of malicious nodes in different scenarios. The following metrics have been used to compare the results:

1-Packet Delivery Ratio (PDR): This metric is the result of the ratio of successful received packets by the root to the total of sent packets.

2-Throughput: This metric is evaluated based on the total number of bits received during the time interval *t*.

3- Average Rank Changes (ARC): This metric provides a result of the average number of parent switches.

4-End-to-End Delay (EED): This metric is evaluated based on the average sending time of all packets received correctly by the root.

5- Average Energy Consumption (AEC): This metric presents the result of the average energy.

5.2. Result

This section contains the results of the simulations performed. Each chart is displayed with an average of 20 runs with a 95% confidence interval.

5.2.1. Packet Delivery Ratio (PDR)

Figures 1 and 2 show the PDR results under black-hole and selective forwarding attacks, respectively. The results show that in all four methods, with increasing the number of malicious nodes, PDR decreased. The reason for this is the increase in the

negative effects of the presence of malicious nodes for network exchanges and especially data loss. However, the reduction ratio for the proposed EATE-RPL was lower than for other methods. This is due to the high efficiency of EATE-RPL in supporting trusted exchanges, especially in dealing with malicious nodes, which has been more effective in scenarios with more malicious nodes. In addition to effectively detecting malicious nodes and supporting trust, the proposed method also supports the reliability of routing and exchanges, which has been another to improve successful exchanges. EATE-RPL selects parents with more trust and secure routes for sending data based on measures that it provides to evaluate nodes' trust and reliability. This performance has significant effects on improving exchanges and results the increased PDR. The effects are greater as the number of malicious nodes increases. However, despite selective forwarding attacks, EATE-RPL has provided far better results than other methods. This is due to the effective performance of EATE-RPL in counteracting deceptive behaviors. The other three methods do not provide effective measures to counter these attacks. CT-RPL has been more successful than SecTrust in assessing trust and countering attacks, resulting in better PDR performance. However, like SecTrust and RPL, this method, in addition to being vulnerable to deceptive behaviors, does not provide measures to evaluate QoS metrics but EATE-RPL also solves QoS requirements well.

Under the attack of the black-hole, when the number of malicious node was 1 node, EATE-RPL had about 94% successful delivery, which was 3.7%, 5.1% and 9.6% more successful than that of CT-RPL, SecTrust and RPL. However, in the presence of 9 malicious nodes, the successful delivery of EATE-RPL was 71%, which was 7.8%, 14.3% and 51.5% more successful than that of CT-RPL, SecTrust and RPL. But under selective forwarding attack, when the number of malicious node was 1, EATE-RPL had about 93.2% successful delivery that was 3.2%, 4% and 7.2% more successful than that of CT-RPL, SecTrust and RPL. In the presence of 9 malicious nodes, EATE-RPL successful delivery was 65.6%, which compared to CT-RPL, SecTrust and RPL was 9.7%, 15.9% and 32.5% more successful. These results explain two important points. The first one is that EATE-RPL has a stable operation with increasing number of malicious nodes. Second, the proposed method is well resistant to deceptive behaviors.

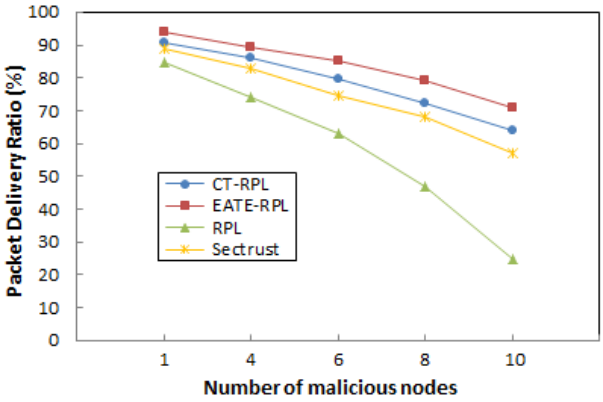

Figure 1. Packet delivery ratio under black hole attack

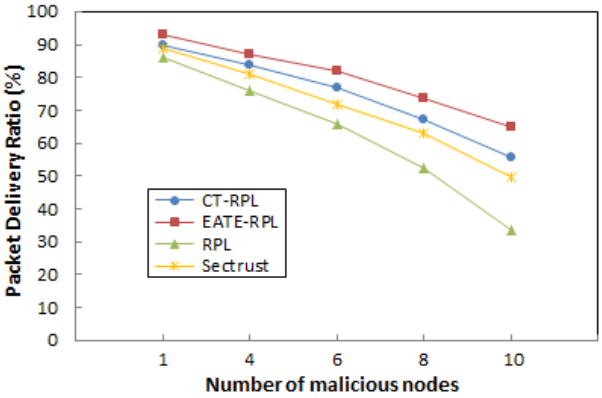

Figure 2. Packet delivery ratio under selective forwarding attack

5.2.2. Throughput

Figures 3 and 4 show the results of the throughput under black hole attacks and selective forwarding, respectively. Because increasing the number of malicious nodes leads to increased topology instability and data loss, with the increase of malicious nodes, the network throughput has decreased in both types of attacks. However, the increase in malicious nodes had less effect on the throughput during EATE-RPL operation. The result of this successful operation is the measures taken by EATE-RPL to establish trust and identify attacks. The effects of these measures on network throughput in the presence of selective forwarding attack are more obvious than other methods. RPL is extremely vulnerable to attacks and in this regard, with increasing malicious nodes, the

throughput for this method had decreased significantly. Although CT-RPL and SecTrust have been successful in building trust, these two methods are particularly inefficient and vulnerable to deceptive behaviors. The existence of this issue has caused a decline in these two methods. According to the results in the presence of black hole attack, EATE-RPL and CT-RPL had better results compared to the other two methods. EATE-RPL and CT-RPL had been more successful in detecting malicious nodes and had provided a more stable network than SecTrust and RPL. Therefore, packet loss for these two methods was reduced and network throughput was increased.

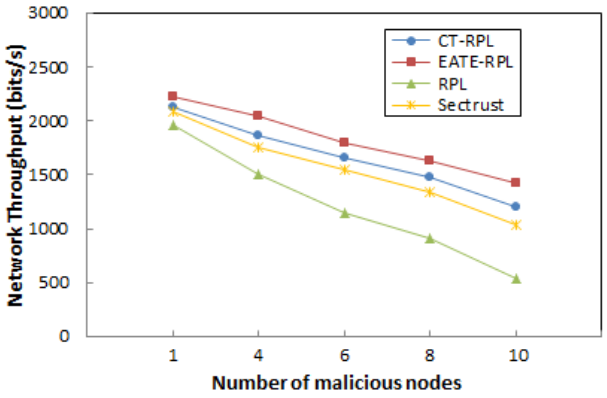

Figure 3. Network throughput under black hole attack

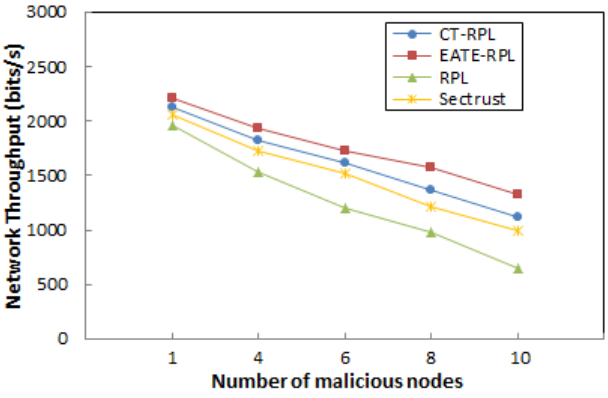

Figure 4. Network throughput under selective forwarding attack

5.2.3. Average Rank Changes (ARC)

Figures 5 and 6 show the ARC results under black hole attacks and selective forwarding, respectively. ARC provides network topology instability ratio. If the network topology is more unstable and the changes are more, the ARC is increased and vice versa. The increasing malicious factors had a direct impact on increasing ARC as it had exacerbated instability. At the same time, this increase had been more pronounced for comparable methods in the presence of selective forwarding attack. The reason for this is that due to the vulnerability of methods against selective forwarding attack, the possibility of choosing parents from malicious nodes is high. According to the results, ARC for RPL protocol is high compared to other methods that this difference is increased by increasing malicious nodes. RPL did not have a mechanism to deal with the malicious nodes, which was the main reason for the increase of ARC in this method. Note that in the selective forwarding attack, the malicious agents only for part of the sent packets have malicious behavior, so the instability for the RPL in the presence of this attack was relatively less than that of the black hole. Among other methods, Sectrust and CT-RPL performed weaker than EATE-RPL. These methods, in particular Sectrust, were less effective in detecting malicious nodes and countering attacks compared to the EATE-RPLs, and therefore ARC is increased for these protocols. To control topological instability due to malicious behaviors, nodes changed their parents frequently, leading to an increase in the rate of rank change. EATE-RPL has been more successful in reducing the negative effects of attacks and maintaining network stability in terms of measures to improve the accuracy of detecting various attacks and prevent the presence of malicious nodes. CT-RPL offers better results than Sectrust, which leads to greater stability, but this method is also sometimes vulnerable to deceptive behaviors, which has led to a slight increase in ARC.

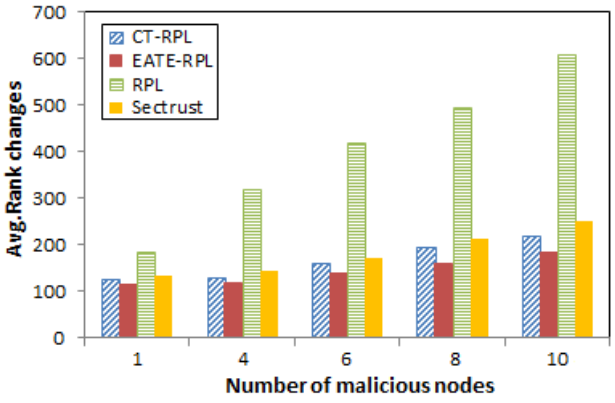

Figure 5. Average rank changes under black hole attack

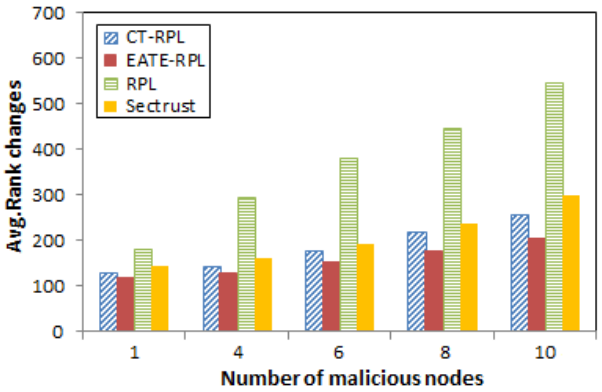

Figure 6. Average rank changes under selective forwarding attack

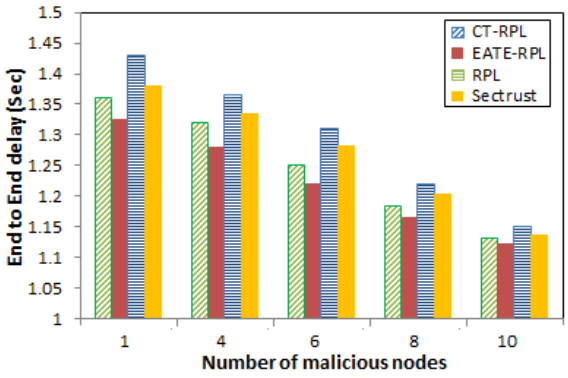

Figure 7. End-to-End delay under black hole attack

5.2.4. End to End Delay (EED)

Figures 7 and 8 show the results of end-to-end delays under black hole attacks and selective forwarding, respectively. Delay in experiments is estimated in terms of the average time to send data packets that have been successfully received by the root. Delay has generally decreased with increasing malicious nodes, because with the increase of malicious nodes, the probability of successful receptions from shorter routes is higher than longer routes, so delay is reduced. In other words, in scenarios with more malicious nodes, the probability of the presence of malicious nodes and data loss in long routes is higher, and in this regard, most data is received from shorter paths (with less delay). Since delay has been calculated for the received data successfully, it has been reduced in scenarios with more malicious nodes. In addition, the results showed that delay for EATE-RPL was lower than that of Sectrust and CT-RPL. In addition to trust, EATE-RPL considers QoS criteria for parental selection. This selection has led to improved exchanges and delay for the proposed method. In addition, EATE-RPL has been more successful in maintaining network topology stability, resulting in reduced disturbances leading to increased delay. However, in scenarios with more malicious nodes, delay for EATE-RPL is closer to other methods. Improved trusted exchanges in exchange for EATE-RPL performance have made it more likely to receive data from longer routes than other protocols in scenarios with more malicious nodes. Therefore, delay in these scenarios for the proposed method is closer to other protocols compared to the scenarios with less malicious nodes.

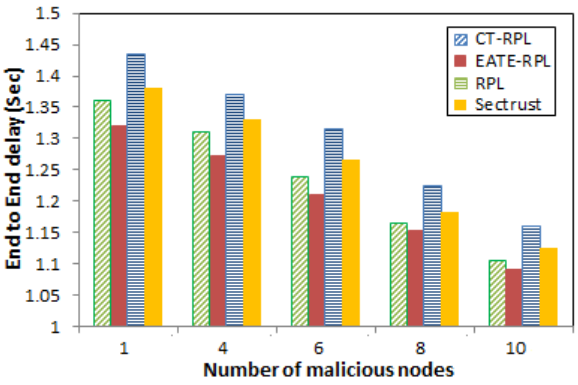

Figure 8. End-to-End delay under selective forwarding attack

5.2.5. Average Energy Consumption (AEC)

The AEC results are shown in figures 9 and 10 for the 60 and 20 minutes of simulations under selective forwarding attack, respectively. Energy consumption had increased with increasing density of malicious nodes due to increased instabilities, topological changes and rank of parental replacement. According to the results of figure 9, with increasing malicious nodes, EATE-RPL had more successful performance and less AEC increase compared to the other methods. EATE-RPL had been more successful in maintaining network topology stability in terms of identifying and preventing malicious nodes, resulting in better AEC, which is more tangible for scenarios with more malicious nodes. In RPL, the AEC has been increased significantly with the increase of malicious nodes. The lack of a mechanism to deal with malicious nodes has led to increased instabilities and topological changes resulting in an increase in AEC. CT-RPL was more successful than SecTrust in dealing with malicious nodes, and AEC was less successful in this respect.

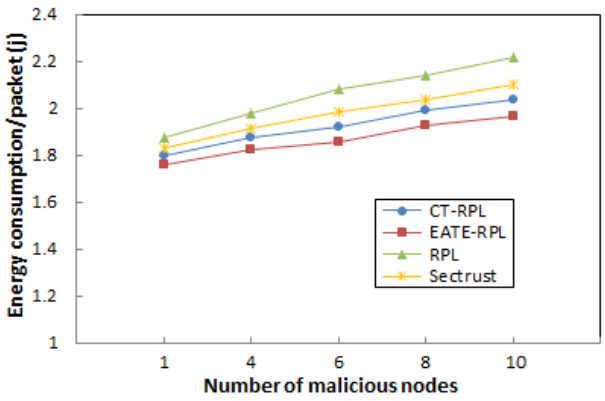

Figure 9. Average energy consumption under selective forwarding attack with simulation time 60 minutes.

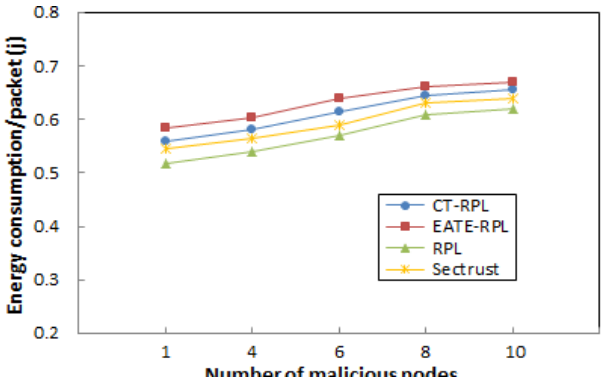

Figure 10. Average energy consumption under selective forwarding attack with simulation time 20 minutes.

According to the results of figure 10, for the simulation time of up to 20 minutes, EATE-RPL consumed more energy than other methods. One reason for this is that the EATE-RPL under attack consumes more energy to calculate and transmit DIO packets, but after identifying and preventing the malicious nodes, the topology stability is maintained and consumption is reduced. Another reason is that over time, the energy consumption of the nodes in EATE-RPL becomes more efficient and balanced. In this method, the residual energy and rank for selecting the preferred parents, respectively, lead to balance energy consumption and optimize the intermediate routes.

6. EATE-RPL Analysis

The proposed method provides the ability to support both of trust and reliability and it is an adaptive method with multi-application capability. The reason for this is the reliability metric review, in addition to the trust in selecting preferred parents, the SE flag prediction to determine security needs, the adaptive evaluation of trust, and the thresholds for trust and intrusion detection.

In EATE-RPL, nodes can meet different needs in different applications due to the SF flag and the proportional value to the weights (w_i). According to security needs, variable rigor of trust can be applied by giving proportional value to trust threshold and intrusion detection. Accordingly, depending on the conditions and environment of the IoT network, an effective trade-off between the effectiveness of trust and reliability can be provided, and on the other hand, a proportional stricter of trust can be applied. For example, in normal applications, the routing and interaction process can only be done by focusing on QoS metrics (rank, residual energy, and ETX). For another example, trust and reliability are supported at the same time as starting the network by giving equal weight to w_i, or by increasing the value of w_i, the value of trust or reliability in decisions is increased. In another scenario, if energy has high importance for an application, routing can be done by focusing on energy by increasing the weight of this parameter. It is also possible to increase the rigor of trust and accuracy in detecting malicious nodes by giving appropriate value to the trust and intrusion detection thresholds accordingly. There is no set value for trust and intrusion detection thresholds, and depending on the application and security needs it is defined. It is worth noting that increasing the trust threshold and decreasing the intrusion detection threshold can be more effective in identifying malicious nodes. But it also increases error, which may mistakenly detect some normal nodes as malicious. Such an issue will cause topological instability, decrease network efficiency and increase network energy consumption. On the other hand, if the trust threshold is low and the intrusion detection threshold is high, the detection accuracy will be reduced and the detection of malicious nodes will take longer.

An important issue and limitation of EATE-RPL include the storage space required for calculations and trust. As mentioned, nodes in the EATE-RPL store and maintain a list of their neighbors in which the nodes' trust and related updates are stored. This storage, however, does not create high overhead for small networks and requires little memory

consumption, but when the network is scalable and implemented over a large geographical area, it requires a lot of memory and heavy overheads is imposed on the network. it is noteworthy that in the proposed method, trust assessment is limited to direct trust and recommendations are not used. In this respect, EATE-RPL performs better than other trust models, which is one of the important features of EATE-RPL. However, storing and updating trust requires high memory consumption. To overcome this limitation, measures should be envisaged that, while establishing effective trust, make the best use of network resources. In future work, focus on improving EATE-RPL by focusing on applying the proposed method to scalable networks.

7. Conclusion and future work

Many studies have been done to ensure trust in routing and IoT data exchanges and this issue is an important tool for identifying malicious nodes and ensuring the accuracy of network performance. However, establishing effective trust is a very complex issue because the nodes' trust is determined based on their behavior. This way of assessing trust is not enough due to the widespread attacks of malicious nodes, especially in the face of deceptive attacks. To improve this issue, this paper presents an improved protocol called dual data-communication trust mechanism for RPL (EATE-RPL). EATE-RPL focuses on creating secure and reliable routing topology and detecting malicious agents with high accuracy. For this purpose, a new objective function has been introduced to select the preferred parents, taking into account the trust and reliability of the nodes and the routing topology is created based on this function. The objective function of the proposed method is created in such a way that the selection of parents from nodes will be done with the most trust and reliability. Data exchanges are then initiated through the network communication graph, and trust models combined with intrusion detection system are used to detect malicious nodes. This design increases the accuracy of assessing and detecting malicious nodes. The results of EATE-RPL simulation using Cooja in different scenarios indicate the high efficiency of the proposed method in detecting malicious nodes, improving trust and other influential metrics of reliable exchanges compared to previous researches. In future work, an attempt has been made to improve the efficiency of EATE-RPL for use in mobile applications by developing a proposed method considering the dynamics of nodes.

References

[1] Hassan, Rondik J., et al. "State of art survey for iot effects on smart city technology: challenges, opportunities, and solutions." *Asian Journal of Research in Computer Science* 22 (2021): 32-48.

[2] Hassan, Rosilah, et al. "Internet of Things and its applications: A comprehensive survey." *Symmetry* 12.10 (2020): 1674.

[3] Khanna, Abhishek, and Sanmeet Kaur. "Internet of things (IoT), applications and challenges: a comprehensive review." *Wireless Personal Communications* 114.2 (2020): 1687-1762.

[4] Al-Emran, Mostafa, Sohail Iqbal Malik, and Mohammed N. Al-Kabi. "A survey of Internet of Things (IoT) in education: Opportunities and challenges." *Toward social internet of things (SIoT): enabling technologies, architectures and applications* (2020): 197-209.

[5] Abiodun, Oludare Isaac, et al. "A review on the security of the internet of things: challenges and solutions." *Wireless Personal Communications* 119.3 (2021): 2603-2637.

[6] Muzammal, Syeda M., Raja Kumar Murugesan, and N. Z. Jhanjhi. "A comprehensive review on secure routing in internet of things: Mitigation methods and trust-based approaches." *IEEE Internet of Things Journal* 8.6 (2020): 4186-4210.

[7] Sharma, Avani, et al. "Towards trustworthy Internet of Things: A survey on Trust Management applications and schemes." *Computer Communications* 160 (2020): 475-493.

[8] Chahal, Rajanpreet Kaur, Neeraj Kumar, and Shalini Batra. "Trust management in social Internet of Things: A taxonomy, open issues, and challenges." *Computer Communications* 150 (2020): 13-46.

[9] Pourghebleh, Behrouz, Karzan Wakil, and Nima Jafari Navimipour. "A comprehensive study on the trust management techniques in the Internet of Things." *IEEE Internet of Things Journal* 6.6 (2019): 9326-9337.

[10] Solapure, Sharwari S., and Harish H. Kenchannavar. "Design and analysis of RPL objective functions using variant routing metrics for IoT applications." *Wireless Networks* 26 (2020): 4637-4656.

[11] Lamaazi, Hanane, and Nabil Benamar. "A comprehensive survey on enhancements and limitations of the RPL protocol: A focus on the objective function." *Ad Hoc Networks* 96 (2020): 102001.

[12] Dey, Amlan Jyoti, and Hiren Kumar Deva Sarma. "Routing techniques in internet of things: A review."

Trends in Communication, Cloud, and Big Data (2020): 41-50.

[13] Marietta, J., and B. Chandra Mohan. "A review on routing in internet of things." *Wireless Personal Communications* 111.1 (2020): 209-233.

[14] Gaddour, Olfa, and Anis Koubâa. "RPL in a nutshell: A survey." *Computer Networks* 56.14 (2012): 3163-3178.

[15] Kushalnagar, Nandakishore, Gabriel Montenegro, and Christian Schumacher. "IPv6 over low-power wireless personal area networks (6LoWPANs): overview, assumptions, problem statement, and goals." (2007): 1-11.

[16] Simoglou, George, et al. "Intrusion detection systems for RPL security: a comparative analysis." *Computers & Security* (2021): 102219.

[17] Almusaylim, Zahrah A., Abdulaziz Alhumam, and N. Z. Jhanjhi. "Proposing a secure RPL based internet of things routing protocol: a review." *Ad Hoc Networks* 101 (2020): 102096.

[18] Raoof, Ahmed, Ashraf Matrawy, and Chung-Horng Lung. "Routing attacks and mitigation methods for RPL-based Internet of Things." *IEEE Communications Surveys & Tutorials* 21.2 (2018): 1582-1606.

[19] Verma, Abhishek, and Virender Ranga. "Security of RPL based 6LoWPAN Networks in the Internet of Things: A Review." *IEEE Sensors Journal* 20.11 (2020): 5666-5690.

[20] Khraisat, Ansam, and Ammar Alazab. "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges." *Cybersecurity* 4.1 (2021): 1-27.

[21] Hajiheidari, Somayye, et al. "Intrusion detection systems in the Internet of things: A comprehensive investigation." *Computer Networks* 160 (2019): 165-191.

[22] Arshad, Junaid, et al. "A review of performance, energy and privacy of intrusion detection systems for IoT." *Electronics* 9.4 (2020): 629.

[23] Seyfollahi, Ali, and Ali Ghaffari. "A review of intrusion detection systems in RPL routing protocol based on machine learning for internet of things applications." *Wireless Communications and Mobile Computing* 2021 (2021).

[24] Napiah, Mohamad Nazrin, et al. "Compression header analyzer intrusion detection system (CHA-IDS) for 6LoWPAN communication protocol." *IEEE Access* 6 (2018): 16623-16638.

[25] Smys, S., Abul Basar, and Haoxiang Wang. "Hybrid intrusion detection system for internet of things (IoT)." *Journal of ISMAC* 2.04 (2020): 190-199.

[26] Agiollo, Andrea, et al. "DETONAR: Detection of routing attacks in RPL-based IoT." *IEEE Transactions on Network and Service Management* 18.2 (2021): 1178-1190.

[27] Pasikhani, Aryan M., et al. "Intrusion Detection Systems in RPL-based 6LoWPAN: A Systematic Literature Review." *IEEE Sensors Journal* (2021).

[28] Boyanapalli, Arathi, and A. Shanthini. "A Comparative Study of Techniques, Datasets and Performances for Intrusion Detection Systems in IoT." *Artificial Intelligence Techniques for Advanced Computing Applications*, 2021. 225-236.

[29] Arış, Ahmet, Sıddıka Berna Örs Yalçın, and Sema F. Oktuğ. "New lightweight mitigation techniques for RPL version number attacks." *Ad Hoc Networks* 85 (2019): 81-91.

[30] Ioulianou, Philokypros, et al. "A signature-based intrusion detection system for the internet of things." *Information and Communication Technology Form* (2018).

[31] Kfoury, Elie, et al. "A self organizing map intrusion detection system for rpl protocol attacks." *International Journal of Interdisciplinary Telecommunications and Networking (IJITN)* 11.1 (2019): 30-43.

[32] Luangoudom, Sonxay, et al. "svBLOCK: mitigating black hole attack in low-power and lossy networks." *International Journal of Sensor Networks* 32.2 (2020): 77-86.

[33] Soni, Gaurav, and R. Sudhakar. "A L-IDS against dropping attack to secure and improve RPL performance in WSN aided IoT." *2020 7th International Conference on Signal Processing and Integrated Networks (SPIN)*. IEEE, 2020.

[34] Mayzaud, Anthéa, et al. "Using the RPL protocol for supporting passive monitoring in the Internet of Things." *NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 2016.

[35] Mayzaud, Anthéa, Rémi Badonnel, and Isabelle Chrisment. "Detecting version number attacks in RPL-based networks using a distributed monitoring architecture." *2016 12th International Conference on Network and Service Management (CNSM)*. IEEE, 2016.

[36] Yavuz, Furkan Yusuf, Ü. N. A. L. Devrim, and G. Ü. L. Ensar. "Deep learning for detection of routing attacks in the internet of things." *International Journal of Computational Intelligence Systems* 12.1 (2018): 39-58.

[37] Li, Yuxi, et al. "Deep learning in security of internet of things." *IEEE Internet of Things Journal* (2021).

[38] Thamilarasu, Geethapriya, and Shiven Chawla. "Towards deep-learning-driven intrusion detection for the internet of things." *Sensors* 19.9 (2019): 1977.

[39] Junior, Franklin Magalhães Ribeiro, and Carlos Alberto Kamienski. "A Survey on Trustworthiness for the Internet of Things." *IEEE Access* 9 (2021): 42493-42514.

[40] Mohammadi, Venus, et al. "Trust-based recommendation systems in Internet of Things: a systematic literature review." *Human-centric Computing and Information Sciences* 9.1 (2019): 1-61.

[41] Kuseh, Simon Wewoliamo, et al. "A Survey of Trust Management Schemes for Social Internet of Things." *Inform* 7.1 (2022).

[42] Kumar, Rajesh, and Rewa Sharma. "Leveraging blockchain for ensuring trust in IoT: A survey." *Journal of King Saud University-Computer and Information Sciences* (2021).

[43] Karkazis, Panagiotis, et al. "Evaluation of RPL with a transmission count-efficient and trust-aware routing metric." *2014 IEEE International Conference on Communications (ICC)*. IEEE, 2014.

[44] Sankar, S., et al. "Trust-Aware Routing Framework for Internet of Things." *International Journal of Knowledge and Systems Science (IJKSS)* 12.1 (2021): 48-59.

[45] Hashemi, Seyyed Yasser, and Fereidoon Shams Aliee. "Fuzzy, Dynamic and Trust Based Routing Protocol for IoT." *Journal of Network & Systems Management* 28.4 (2020).

[46] Djedjig, Nabil, et al. "New trust metric for the RPL routing protocol." *2017 8th International Conference on Information and Communication Systems (ICICS)*. IEEE, 2017.

[47] Djedjig, Nabil, et al. "Trust-aware and cooperative routing protocol for IoT security." *Journal of Information Security and Applications* 52 (2020): 102467.

[48] Muzammal, Syeda Mariam, Raja Kumar Murugesan, Noor Zaman Jhanjhi, and Low Tang Jung. "SMTrust: proposing trust-based secure routing protocol for RPL attacks for IoT applications." In *2020 International Conference on Computational Intelligence (ICCI)*, pp. 305-310. IEEE, 2020.

[49] ul Hassan, Temur, et al. "CTrust-RPL: A control layer-based trust mechanism for supporting secure routing in routing protocol for low power and lossy networks-based Internet of Things applications." *Transactions on Emerging Telecommunications Technologies* 32.3 (2021): e4224.

[50] Patel, Anshuman, and Devesh Jinwala. "A Trust-Integrated RPL Protocol to Detect Blackhole Attack in Internet of Things." *International Journal of Information Security and Privacy (IJISP)* 15.4 (2021): 1-17.

[51] Hashemi, Seyyed Yasser, and Fereidoon Shams Aliee. "Dynamic and comprehensive trust model for IoT and its integration into RPL." *The Journal of Supercomputing* 75.7 (2019): 3555-3584.

[52] Zangeneh, Saeid, and Rassoul Roustaei. "A Novel Approach for Protecting RPL Routing Protocol against Blackhole Attacks in IoT Networks." (2021).

[53] Airehrour, David, Jairo A. Gutierrez, and Sayan Kumar Ray. "SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things." *Future Generation Computer Systems* 93 (2019): 860-876.

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

[55] Prathapchandran, K., and T. Janani. "A Trust-Based Security Model to Detect Misbehaving Nodes in Internet of Things (IoT) Environment using Logistic Regression." *Journal of Physics: Conference Series*. Vol. 1850. No. 1. IOP Publishing, 2021.

[56] Thubert, Pascal. "Objective function zero for the routing protocol for low-power and lossy networks (RPL)." (2012).

[57] Gnawali, Omprakash, and Philip Levis. "The minimum rank with hysteresis objective function." *RFC 6719* (2012).

[58] Amirinasab Nasab, Mehdi, et al. "Energy-efficient method for wireless sensor networks low-power radio operation in internet of things." *Electronics* 9.2 (2020): 320.

[59] Weng, Jianshu, Chunyan Miao, and Angela Goh. "An entropy-based approach to protecting rating systems from unfair testimonies." *IEICE TRANSACTIONS on Information and Systems* 89.9 (2006): 2502-2511.

[60] Leloglu, Engin. "A review of security concerns in Internet of Things." *Journal of Computer and Communications* 5.1 (2016): 121-136.

[61] Abbas, Adeel, et al. "A new ensemble-based intrusion detection system for internet of things." *Arabian Journal for Science and Engineering* 47.2 (2022): 1805-1819.

[62] Dunkels, Adam, Bjorn Gronvall, and Thiemo Voigt. "Contiki-a lightweight and flexible operating system for tiny networked sensors." *29th annual IEEE international conference on local computer networks*. IEEE, 2004.

[63] Tsiftes, Nicolas, Joakim Eriksson, and Adam Dunkels. "Low-power wireless IPv6 routing with ContikiRPL." *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks*. 2010.