IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 22 October 2022, accepted 8 November 2022, date of publication 10 November 2022, date of current version 7 February 2023.

Digital Object Identifier 10.1109/ACCESS.2022.3221434

RESEARCH ARTICLE

Security Challenges of Selective Forwarding Attack and Design a Secure ECDH-Based Authentication Protocol to Improve RPL Security

HAITHAM Y. ADARBAH[1], MOSTAFA FARHADI MOGHADAM[2], ROLOU LYN RODRIGUEZ MAATA[1], AMIRHOSSEIN MOHAJERZADEH[3], AND ALI H. AL-BADI[1]

[1]Gulf College, Muscat 133, Oman
[2]Department of Computer Engineering, Vahdat Institute of Higher Education, Torbat-e-Jam 9576175537, Iran
[3]Department of Computer Engineering, Ferdowsi University of Mashhad, Mashhad 9177948974, Iran

Corresponding author: Haitham Y. Adarbah (Haitham.adarbah@gulfcollege.edu.om)

This work was supported by the Ministry of Higher Education, Research and Innovation (MoHERI) of the Sultanate of Oman under the Block Funding Program under Agreement MoHERI/BFP/GULF/2022, and Project BFP/RGP/ICT/22/474.

ABSTRACT Today, we could describe the Internet of Things (IoT) as the pervasive and global network that provides a system for monitoring, controlling, processing, and analyzing the data generated by IoT devices. The huge amount of data generated by IoT devices when transported and routed through the internet presents several challenges. One of the common routing protocols in IoT networks is RPL (Routing Protocol for Low Power and Lossy Networks), but it is prone to security issues and attacks. Due to the presence of sensitive data in IoT and its exchange in the open network, issues of privacy and security in this network should be given special attention. In addition, the nodes in the Internet of Things have limited resources, and the symmetric encryption key is used to encrypt the data of all nodes, which has security weaknesses. Therefore, an efficient and secure authentication scheme is needed so that IoT nodes can authenticate each other and share a secure session key. In this article, we review security aspects of RPL protocols focusing on selective forwarding attacks. Further, we propose a key agreement and authentication mechanism based on ECDH (Elliptic-Curve Diffie–Hellman). We show that our design is very secure, that it meets security requirements, and that it can withstand known attacks while having low costs for computation and communication.

INDEX TERMS IoT, RPL, selective forwarding attack, RPL, ECC, ECDH, authentication.

I. INTRODUCTION

The Internet of things (IoT) is creating a world where billions of things and smart objects are integrated into networks seamlessly. The aim of this network is to provide advanced and intelligent services to a range of sectors. These IoT nodes are usually battery-powered, wirelessly connected, and deployed in a mesh topology [1]. The devices are typically constrained by limited power, memory, and processing resources. The IoT network generally is optimized for energy-saving and operates under a variety of such working constraints [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [30], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43].

Every device and thing in the Internet of Things has its unique Internet Protocol (IP) address. The devices, such as sensors or mobile devices, monitor and collect all kinds of data on the network. The data can be further collected, processed, analyzed, and mined to extract effective information to provide intelligent and ubiquitous services. The IoT services are emerging into today's markets in wide areas, namely surveillance, health care, security, transport, food safety, and distant object monitoring and control. High interest in this paradigm has led to the deployment of large-scale low-power and loss-free networks (LLNs) such as wireless sensor networks, but there is an important issue that the existing routing protocols are not suitable to deal with IoT

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.

requirements [3]. For support of the communication layers in wireless personal area networks (WPAN) and the 6LowPAN protocol, standardized protocols have been developed, including the IEEE 802.15.4. The protocol is called RPL (Routing Protocol for Low Power and Lossy Networks), which is based on IPv6 [4].

In this article, we examined the vulnerability of the RPL protocol against various attacks. Due to the vulnerabilities of RPL, we have provided a secure key agreement and authentication schema to improve the security of this protocol, making it safe against all kinds of network attacks. One of the RPL weaknesses is the use of a symmetric encryption key for all nodes, which makes the security of all network nodes vulnerable by exposing the symmetric key [45]. In our protocol, we have a mechanism based on the ECDH theory, that for each communication, the symmetric key to encrypt information is completely different from the key of the previous communication. In addition, by completing the protocol process, nodes can have a unique session key for their communication. The dynamic feature of the symmetric key is one of the strengths of the proposed protocol compared with other similar protocols in the IoT. Another feature of the proposed method is its low computational cost, which is compatible with low computational power network nodes. The evaluations show that our protocol uses less time for its operations than other key agreement and authentication protocols. In the following, we have described the theories (ECC, ECDLP, ECDH) used in the proposed protocol, RPL concepts, RPL security challenges, and Selective Forwarding Attack.

A. BASIC CONCEPT

Currently, many IoT companies are facing a lack of information protection protocols. There is no suitable solution to protect all IoT systems because most devices use different control operating systems, servers, connection domains, and protocols. Information encryption in IoT devices is very important in terms of information security and privacy. Data is stored on the server, and whoever has access to the data must be controlled to guarantee privacy and data exclusivity. Therefore, encryption must be done to protect and isolate data between users, companies, and other individuals involved in or accessing the data. Encrypting information and encrypting it with complex and impenetrable algorithms may be a good solution to keep information more secure for us so that we don't have to worry anymore. The new information security solution based on the Internet of Things is to encrypt sensitive and important information before sending it or to send it encrypted to the destination. Cryptographic methods are an excellent way to build trust between companies and users, especially when it comes to sharing sensitive data. Therefore, encryption must be at the core of every IoT device to ensure that data is fully encrypted in memory and transit. Security is the key for IoT to be a success in the future and give people the services they need.

1) ELLIPTICAL CURVE CRYPTOGRAPHY

One of the cryptographic techniques is elliptic curve cryptography, which is a type of asymmetric cryptography of the public key. In this cryptographic system, the elliptic curve E is a set of points with coordinates $pf \subseteq * pf \subseteq()$ x, y, which is denoted by the following equations.

1) $Y^2 = x^3+ax+b$

where a,b $\subseteq f_p$ and $4a^3+ 27b^2+ \neq 0$

The elliptical curve consists of two main operations called the sum of points and point multiplication. Point multiplication is also known as scalar multiplication. Below is an example of scalar multiplication, with K multiplied by P, to help you understand it better.

1) $KP = P+P+P+P.... +P$

2) DISCRETE LOGARITHM PROBLEM OR ECDLP ELLIPTIC CURVE HARD PROBLEM

Computational Problem The problem of the discrete logarithm of an elliptic curve is abbreviated to ECDLP. This constitutes the basic building block in pair-based and elliptic curve (ECC) cryptography. Consider two points named P and Q on the elliptic curve. The point Q is calculated using scalar multiplication on the parameter k at point P. Given the discrete logarithm problem, you will see that if we have two points P and Q, calculating or obtaining the parameter k is a difficult and even impossible task. This difficulty and impossibility of calculation is known as ECDLP, or hard elliptic curve problem [43], [44], [45], [46], [47], [48], [49], [50], [51], [52].

3) THE DELPHI-HELLMAN ECDH ELLIPTIC CURVE

This encryption system is a protocol for two-way key agreement. In this encryption, each party to the key agreement has a pair of public-private keys based on the elliptic curve. The parties to the key agreement also have the possibility of agreeing on a common key in an insecure channel. Considering that the two points $p.\ a_i$ and $p.\ b_i$ are on the elliptical curve. According to the Delphi-Hellman curve (ECDH) problem, if the attacker in the network has these two points, it is impossible for him to reach the points b_i (a_i.p) and a_i (b_i.p).

B. RPL CONCEPTS

The core of the IoT protocol stack used for communication between these low-power devices is Low-Power Lossy Networks (LLNs). In most of the application scenarios, the nodes in LLNs operate independently and are unsupervised, causing a variety of attacks. To protect LLNs against these attacks, the ROLL working group at the Internet Engineering Task Force (IEFT) has designed the Routing Protocol for Low power Lossy Networks (LLNs) (RPL) [6]. The RPL protocol is a distance-vector routing protocol that is based on IPv6 and it is compatible with communication protocols like ZigBee [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [30], [32], [33], [34], [35], [36], [37], [38],

[39], [40], [41], [42], [43], [44]. Among the IoT routing protocols, it is worth mentioning the RPL routing protocol that supports IPv6 communications as in [5]. According to a particular topology, the RPL devices are connected in which the topology combines mesh and tree topologies. RPL builds a topology as a Directed Acyclic Graph (DAG) which is divided into one or more Destination Oriented DAGs (DODAGs). An example of a DAG is shown in Figure 1, where a single destination is rooted in a DAG (DODAG) root.

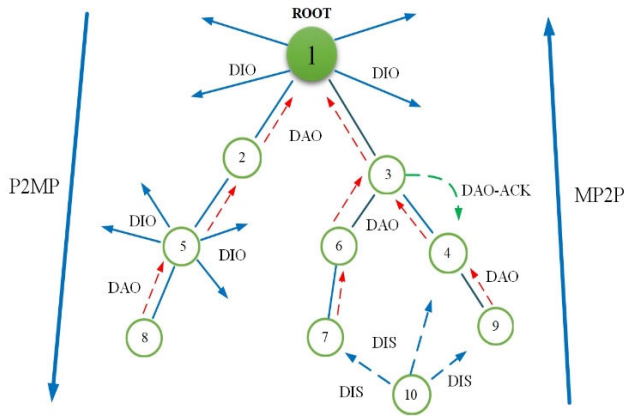

FIGURE 1. An example of a DODAG in RPL network.

RPL is considered a blend of Distance Vector (DV) and source-routing (path addressing) protocols. It uses vectors (arrays) of distances to other nodes in the network and has a router to inform its neighbors of topology changes periodically. Each node in the RPL network maintains a vector (table) of the minimum distance between every node. The RPL routing protocol uses various route metrics to calculate the cost of reaching a destination. In the RPL network, a sender can partially or completely select the route the packet will travel through the network. That is why it is a source-routing protocol.

An identifier called RPLinstanceID is used to identify and maintain the RPL topology. An RPL instance consists of a set containing one or more DODAGs of a common RPInstanceID. The same RPInstanceID is assigned to each DODAG and shares the same objective function (OF) to calculate the position of a node in the DODAG. The Objective Function Zero (OF0) and the Minimum Rank with Hysteresis OF (MRHOF) can be given as examples of OF. A DODAGID is known as a numeric version of a DODAG, which is a sequential counter and is incremented by the root to create a new version. The position of a node in DODAG relative to the root can be determined by the rank value of that node. Also, to maintain the cyclical nature of the chart, the rank values of the child nodes must be greater than the values of their parents. There are two types of DODAG: a node in a ground DODAG that meets the program target and a floating DODAG that provides only paths within the DODAG. But it should be noted that a node in the floating DODAG is expected to meet the goal. DODAG provides two modes of operation, which are storage and non-storage. When nodes are in storage, they retain nodes with a lower rank, such as 1-3, which have a larger routing table in Figure 1. Filling in these tables will lead to protocol failure. On the other hand, when in non-storage mode, ROOT sends packets to large nodes through source paths. This mode is more expensive compared with the storing mode-of- operation. The two traffic streams supported by RPL are Point-to-MultiPoint (P2MP) and MultiPoint-to-Point (MP2P), as shown in Figure 1.

C. SECURITY CONCERNS

In terms of information security transitions, plenty of challenges have been identified. Packets are routing and addressing between IoT devices, and it is a significant issue for network that the network needs to define protocols/mechanisms for routing packets from the source node and transmit across diverse network topologies to be received by the destination node [8].

The nature of the RPL devices is vulnerable in the absence of the tamper-resistant ability and gives the attackers an opportunity to be able to capture the IoT nodes. This resulted in the extraction of all cryptography information, and unauthorized nodes operated legally in the network. The attacker attempts to implement the malicious codes and break routing rules by capturing the nodes. Because of nodes, responsibility for their processing, detecting the changing and malicious effects is difficult [7]. Routing data between the nodes suffers from potential threats and security issues, and it is associated with the lives of users [9].

Another critical and challenging issue in the IoT is protecting the safety of RPL routing data. Malicious nodes carry out their own unauthorized activities by forwarding packets sent across the network and can carry out various types of attacks on the routed data [10]. However, the standards defined for RPL protocols are incapable of overcoming IoT network security issues. Given that in a network of objects, billions of devices are connected to each other and exchange information, establishing security and protection of data against various types of attacks and threats has created a vital challenge for the network [11].

D. SECURE ROUTING RPL CHALLENGES

This section addresses the challenges of RPL protocol security attacks and the mechanisms used in the RPL protocol. A large amount of information is sent by users in the network, which must be sent confidentially. To protect the privacy of users' information on the network, different encryption techniques are used for purposes such as user authentication and data privacy as a defense shield. This mechanism provides conditions for the network to prevent unauthorized people in the network from accessing information.

There are two techniques for data encryption, symmetric and asymmetric, and RPL protocols use symmetric encryption to encrypt their data. This symmetric encryption system is known as the Advanced Encryption Standard (AES) with a counter with encrypted Encryption Message

Authentication Code (Counter with CBC-MAC (CCM)) - (AES/CCM). An asymmetric encryption system uses a pre-shared secret key to exchange messages between nodes, since this type of encryption system uses a common key for all nodes, making it messages easier for an attacker to access the network. When the attackers find a way to access the secret keys, they attempt to perform any possible threats to get access and insert their nodes into the network. It will make the network vulnerable to various security attacks and compromise the nodes of the network. In such cases, the encryption system does not have the ability to protect the network [12], [13]. Due to the existing vulnerability and the availability of conditions for injecting fake data by the adversary, a significant improvement in the RPL routing protocol authentication system is required [14], [15].

The RPL routing protocol has mechanisms to repair DODAGS, detect inconsistencies, and avoid loops. Also, the protocol can use the data-path validation mechanism to detect inconsistencies [1]. However, the IETF ROLL workgroup specified the security requirements of RPL, but they did not specify security models for it. Basically, the standard RPL protocol utilizes key management in the application of sensor nodes that are already configured. The key management mechanism allows only the authenticated RPL nodes to join the network. The lack of a specification that does not define how RPL sensor nodes authenticate and securely connect among themselves, is a weakness in the security design of the standard IETF RPL. This makes the RPL protocol vulnerable to several routing attacks, which are explained in Table 1 [16], [19], [20], [22], [23], [24], [25].

TABLE 1. RPL routing protocol attacks.

Attack	Feature of the attack	Consequences on network's performance
spoofing/replaying information	Create non-existent information or partially modify data	Attracting/repelling network traffic, creating routing loops.
selective forwarding	Refusing to forward massages from selected nodes	Reducing traffic and increasing data loss
Blackhole	Failing to forward any data packets including its own	Reducing traffic and increasing data loss
sinkhole	Advertising false information to create a center of attraction for other nodes.	Compromise of transmission routes, reducing traffic and increase data loss.
node replication	Physical capturing of a node, its replication and deployment back into the network.	Compromise of transmission routes, eavesdropping on the falsely created links.
Wormhole	Create a low link tunnel between two malicious nodes in different parts of network	Sending data to the false distention, undermining cryptography protection.
hello flood	Broadcasting a hello packet to the whole network with great transmission power.	Increasing energy degradation and collisions, create false transmission routes.

E. SELECTIVE FORWARDING ATTACK

This attack captures packets that are sent on the network and sends them selectively on the network. Using this attack, the DoS (Denial of Service) attack can be implemented on a network. The purpose of the attacker is to disrupt routing and filtering protocols. In the RPL routing protocol, the adversary could forward all RPL-related control messages over the network and release the rest of the network traffic. One method that can be considered as a solution to this attack is to create a heterogeneous or dynamic path between parents and children. An encryption system can also be used as another solution by using a strong encryption technique to make the network traffic flow unrecognizable to the attacker. To detect a disturbance in the network topology, the heartbeat protocol is basically used, which can be used to detect selective sending attacks [16], [17]. Another solution is to use an intrusion detection system (IDS) that defines an End-to-End packet loss adaptation algorithm for detecting selective forwarding attacks on the network [18]. A system is needed to be able to detect and eliminate this type of attack. The RPL self-healing feature does not have the ability to modify the topology [16], [17], [18], [19].

Figure 2 shows an example of selective forwarding attacks in the RPL network. As can be seen in figure 2, node 3 does not send data packets that are received from its neighbor to the root while it forwards the routing packets.

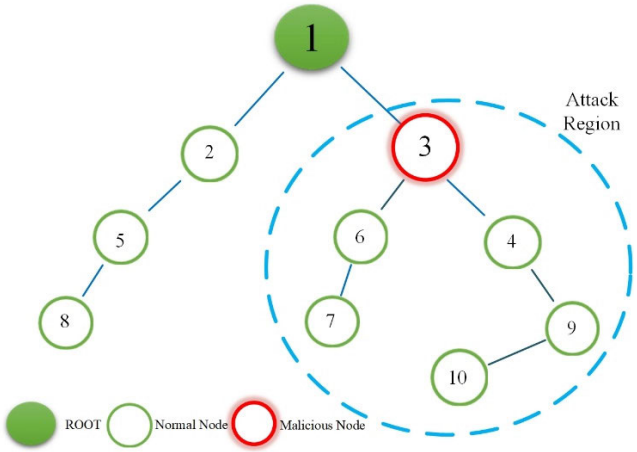

FIGURE 2. An example of selective forwarding attacks in an RPL network.

F. ORGANIZATION OF THE PAPER

In this research, we focus on the impact of selective forwarding attacks on the performance of RPL-based IoTs and drop the data packets only, not the routing packets. To secure the RPL protocol against selective forward attacks and other

common network attacks, we have provided a key agreement and authentication protocol. The presented protocol enhances the mechanism of using RPL symmetric encryption, which uses a fixed key for all nodes, and a dynamic mechanism is provided for the symmetric encryption system. Also, the provided protocol has been considered in the protocol process to prevent the activity of unauthorized nodes in the network through multiple authentication mechanisms. The rest of the paper is organized as follows: Section II presents the related work; In Section III the proposed protocol is presented. The results of the security simulation of the proposed protocol using the AVISPA authentication tool and the review of common attacks are given in Section IV. Section V presents the performance of the protocol and the computational cost of the protocol, as well as the cost-related protocols. Finally, the conclusions of the article are presented in Section VI.

II. RELATED WORK

Due to the growing trend of IoT and the importance of RPL protocol security because of the limited resources of network nodes, a significant number of research papers have been presented to provide security solutions for the RPL protocol.

Similarly, Chris and Wagner [21] describe the routing security features in wireless sensor networks. They demonstrate that the various attractors to ad-hoc and peer-to-peer networks can be turned into powerful attacks against sensor networks and suggest countermeasures and design considerations. The research work in [22] and [23] discussed selective forwarding attacks and some of the mitigation schemes to defend against them, but their work was without any simulation experiments. In [24], the authors implemented and demonstrated attacks against 6LoWPAN networks running IoT protocols, and they showed the impact of routing attacks against RPL and how some attacks can be avoided by RPL's self-healing mechanisms. Linus et al. [25] provide an analysis of IoT technologies and their new security capabilities that could be exploited by attackers and IDSs. To detect the selective forwarding attacks based on the reply to messages that are received from the node, they offered the Heartbeat protocol. Their proposed protocol works only when IPsec is used in the network.

Tomić and McCann [16] studied the main security mechanisms and their effects on standards and the most popular protocols that are used in WSN deployments. In their work, they quantified the effect of attacks on the performance of the network using the Cooja simulator. Shreenivas et al. [26] attempted to detect intrusions aimed at disrupting the routing protocol for low-power networks. To improve security on 6LoWPAN networks, they have developed SVELTE, an IoT intrusion detection system with an intrusion detection module that uses the ETX (Expected Transfer) metric. Airehrour et al [27] attempted to propose a solution to detect the blackhole and selective forward attacks, which are essential security attacks on the routing of data in the IoT. To address these security features, they proposed trust-aware RPL. The value of trust calculated for network nodes is used in the parent selection. A new centralized mechanism for managing trust in the IoT network has been proposed by Airehrour et al [28]. In this framework, the effort is to enable IoT nodes to communicate with each other on a trustworthy basis. In order for the IoT nodes to have a reliable interaction, the system divides the network environment into small areas called clusters. This cluster contains the main node called MN, which consists of a large number of CN cluster nodes and acts as a local trust manager. One of the mechanisms used to provide a suitable solution in the field of IoT security is the centralized trust approach. A multi-link paradigm to detecting the Wormhole and Grayhole attack in Routing Protocol for LLNs based IoT networks was proposed by Mehta et al [29]. Their proposed system uses direct and indirect trust, which the direct trust is based on node attributes and the indirect trust is determined according to the neighboring nodes' viewpoint. Also, the offered method is adaptable with RPL because it is energy-friendly and does not subject the network to excessive traffic overload. Mahmood et al [30] proposed a hybrid monitoring method to detect abnormal behavior in RPL-based networks. The model that is presented by the authors consists of two phases: the first phase collects information about the neighboring node, and the second phase is responsible for identifying the sinkhole node.

The routing protocol for low-consumption and wasted networks (RPL) is vulnerable to routing attacks and also the use of a metric in routing disrupts network performance. To overcome the limitations and ensure the security of the Hashemi et al [31] offered a trust-aware and cooperative routing protocol for the network. In their proposed method, they have used a comprehensive hierarchical model to evaluate the trust of nodes, which provides a multidimensional perspective on trust. To overcome the attacks, they have defined a combination of metrics and required activities to calculate the level of trust in the network. To counter the Sybil attack, Murali and colleagues [32] proposed a novel Artificial Bee Colony (ABC) inspired by Sybil mobile attack modeling and a lightweight intrusion detection algorithm in RPL. In their approach, they define three different behavioral categories for Sybil attack that evaluate the performance of the RPL routing protocol under Sybil attacks based on packages delivered, traffic soldier, and energy consumption. In addition, they have evaluated the performance of their proposed algorithm based on three factors: accuracy, sensitivity, and specificity. Because information confidentiality is critical, a lack of strong security facilities in the network exposes information and entities to a variety of attacks and security threats. Jain, Akanksha, and Sweta Jain [33] gave an overview of how traditional routing methods deal with security issues like constraints, secure routing problems, and techniques that can be used to make routing more secure.

Several attacks in the RPL protocol include: wormhole, black hole, sink hole, sybil, rank, selective post, various denial of service attacks, and so on. V. Neerugatti et al. [34] introduced a novel artificial intelligence-based detection

method with the aim of detecting the selective forward attack that usually happens in the 6LoWPAN-based RPL protocol. To evaluate the performance of their proposed system, they used the ContikiCooja simulator, which was implemented with Sky motes. Given the importance of security, Verma et al. [19] have examined the various attacks that seriously threaten the security of the RPL routing protocol on the network, and have provided defensive solutions that can provide security features. A classification of RPL attacks is shown for better understanding, taking into account key features such as resources, topology, and traffic. In addition, the study of defense solutions based on cross-dedicated network layer and RPL has been proposed in the literature. A malicious node within the network is able to eavesdrop on messages containing routing information about each of its neighboring nodes and then replay them over and over again at regular intervals. Verma A, Ranga V [35] examined this attack in their article and showed that the attack significantly increases the average delay and packet delivery in the network. They proposed an intrusion detection system called CoSec-RPL to address the security issues of non-spoofed copycat attacks. They compared the effectiveness of their proposed intrusion detection system with the standard RPL protocol, and the results show that CoSec-RPL effectively reduces network traffic.

In Patel et al. [36], they enhanced the capabilities of the RPL protocol to overcome the selective forwarding attack. They introduced a reputation-based RPL protocol that is embedded in the RPL protocol. A network node is known for evaluating, the data it sends over the network, and for this evaluation the data behavior of the nodes is examined. This data transmission behavior is the result of the difference between actual and normal packets that are lost. Due to the vastness and dynamism of the IoT environment, conventional security mechanisms such as encryption techniques, key management, intrusion detection systems, anomaly detection, etc. are not applicable in the scalable and dynamic IoT environment, because these mechanisms consume more energy in the network. To cover security features due to the energy limit of the nodes in the network, Prathapchandran et al. [37] introduced a lightweight RFTrust model based on trust, which was originally designed to withstand depression. The authors' proposed model uses random forest (RF) and Subjective Logic (SL) to improve the performance of the network while identifying a sinkhole attack. Agiollo, Andrea, et al. [38] tried to develop an intrusion detection system (IDS) to deal with multiple attacks on the network as well as provide a mechanism to reduce troops in the RPL. Their proposed system is based on packet sniffing, which they call DETONAR - Detector of Routing Attacks in RPL. The proposed DETONAR looks for bad behavior in a network by using rules based on signatures and rules for unusual behavior.

III. PROPOSED SCHEMA

As mentioned in the RPL Security Challenges section, this protocol uses symmetric encryption, which is one key for encrypting information between network entities. Using the one encryption key for all the network creates security issues that endanger the entire network information and the security of network entities.

In this section, with respect to the security issues raised by the RPL protocol, we present the key exchange protocol using ECC encryption techniques and theorems. During the registration phase, each node that wants to join the network must perform the registration step with the root node or the node that controls the network so that it can work as an authenticated and authorized node in the network. In the authentication and session key exchange phase, we have considered a process in which the two entities agree on the secure session key after performing mutual authentication and exchanging private parameters. But there is a notable point about the proposed protocol, and is that the generated symmetric key is dynamic and different for each session. These conditions for the use of a dynamic symmetric key make up for the security flaws in the network's fixed symmetric key.

TABLE 2. Describes the parameters used in the proposed protocol.

Symbol	Definition
ID_{nod}	Nod Identity
PU_{nod}	Nod Public Key
S_{nod}	Nod Private Key
S_{root}	Root Private Key
PU_{root}	Root Public Key
$d_i,f_i,e_i,a_i,b_i,g_i,c_i,z_i$	Random Numbers
H	Hash Function
P	Base Point
NAP	Nod Authentication Parameter
AM_i	Authentication Message
SK	Session Key
$E_{A2(x)}$	Encrypt by Symmetric Key

A. NODE AND ROOT REGISTRATION PHASE

In this phase of the protocol, which is performed once, each node that intends to enter the network must perform this step. In the first step of this phase, the new node first specifies its ID number and public key. In the second step, the node selects a random number called d_i. After selecting the random number, the node calculates parameter N as follows and sends the public key, the ID, and the generated value of N in the secure channel to the root.

$$N = H(d_i||PU_{nod})$$

The ROOT entity, after receiving the parameters sent by the node, first generates the random numbers f_i, e_i. After selecting the random numbers, the ROOT entity generates T_i, which uses the private key ROOT. The reason for using random numbers is to be able to create anonymity for the private key of the ROOT. This technique helps us, in addition to being able to take advantage of the security features of the private key, ensure its security against attacks by computing protocol

parameters and generating private parameters by attackers on the network. In the next step, the ROOT entity generates the R_i and S_i parameters, which are prerequisites for an important parameter called the Node Authentication Parameter (NAP). NAP is a unique value is generated separately for each node. It is generated by random numbers, the private key of the ROOT entity, and the value of N sent by the node. Using NAP is for security and to prevent unauthorized nodes from entering the network. Random numbers and nodes provide the condition that if the values are changed, the NAP value will be changed and the node will not be able to exchange information over the network. The same conditions apply to the private key of the ROOT entity. In general, the NAP parameter can be considered as a special permission to be present in the network, which consists of private and random parameters. Figure 3 shows the registration fee process and the output values of the parameters used in the registration step.

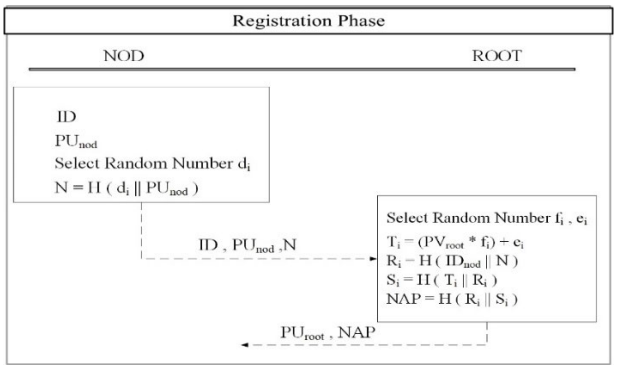

FIGURE 3. Phase of registration of entities.

B. AUTHENTICATION AND KEY EXCHANGE PHASE

In the authentication and key exchange phase, a mechanism is considered for the two entities that can generate their session key after exchanging parameters and undergoing multiple authentication processes. The generated session key is a type of symmetric cryptographic key that is different for each communication session.

Step 1:

In the first step of the key exchange and authentication phase, the node generates random numbers a_i, b_i and g_i. These random numbers aim to generate different values for the protocol output parameters in each session. In the next step of this phase, the node generates two parameters, A_1 and A_2 using the random number ai. These two parameters are used to generate dynamic symmetric keys in the protocol, which are used on the node side to encrypt information and on the ROOT side to decrypt it.

$$A_1 = a_i.P \; A_2 = a_i.PU_{Root}$$

In this step, after generating parameter A_2, the x dimension of this point is selected as the encryption key. In the next step, the node generates a value of U using its private key and the random numbers b_i and g_i, which aim to create private key anonymity. This helps to prevent the private key from being used directly in the computational and exchange parameters, and prevents attackers from accessing the private key through various network attacks.

$$U = (S_{nod} * b_i) + g_i$$

After calculating the U parameter, the node generates AM_1, which is calculated using the U, $A_{2(x)}$ and NAP parameters. This parameter is intended for node authentication by root. Finally, the node encrypts the AM_1 and U parameters with $A_{2(x)}$ and sends them to the root entity along with A_1.

Note: A_2 is a point, and the cryptographic key is $A_{2(x)}$. This is because of the ECDH theorem, which was explained in the Basic Concepts section.

Step 2:

After receiving the message sent by the node, the root entity calculates the freshness of the message by calculating T, and if the message is not new ($|T_2 - T_1| \Delta T$), the connection is disconnected. After checking the freshness of the message, the root node needs to decrypt the message encrypted by the node, which requires the calculation of $A_{2(x)}$. The root entity calculates the encryption key as follows, and then the x dimension selects as the cryptographic key.

$$A_2 = S_{root}.A_1$$

Keep in mind that, according to the ECDH theorem, the attacker will not be able to calculate and reach A_2 even if he/she has the value A_1. In order to reach A_2, the private key of the Root entity is required, which at this stage, according to the ECDLP theorem of ECC encryption, it is not possible for the attacker to calculate A_2.

When A_2 is calculated, the root entity calculates the encryption key and can decrypt the incoming message. Then after decrypting the message, the root authenticates the node in the first step. For this purpose, it calculates AM'_1 with the available parameters and compares its value with AM_1, which is sent encrypted by the node. If these two values are equal, it will continue the protocol process and in If the two values are not the same, the connection will be disconnected. After checking the node identity, the root entity selects two random numbers, ci and z_i, and generates the value of R, which is an anonymous type of private ROOT key.

After that, the root calculates the value of R. It first generates the Session Key using its private parameters and node. Also, in order to establish multiple authentication mechanisms, ROOT generates an AM_2 to verify its authenticity and sends it encrypted to the node. SK and AM_2 values are calculated as follows.

$$SK = H(R||U||A_{2(x)}||NAP) AM_2 = H(SK||NAP||A_{2(x)})$$

After the session key values and the authentication parameter are generated by the root entity, the R and AM2 values are sent encrypted to the node.

$$E_{A2(x)}\{AM_2, R\}$$

Step 3:

In this step, the node receives a message encrypted by Root, which, as in the previous steps, first checks the freshness of the received message by calculating ΔT. After checking the freshness of the message, the node needs to calculate the session key and authenticate the sender of the message. The node needs the parameters R, U, $A_{2(x)}$ and NAP to generate the session key. The R parameter is sent by the root in an encrypted message to the node, and the U and $A_{2(x)}$ parameters are generated by the node itself in the previous steps. The last parameter used is NAP, which is only generated and available to the node at the registration stage. The node must then verify the identity of the message's sender by checking AM_2, which for this purpose calculates the value of AM'_2 as follows.

$$AM'_2 = H(SK'||NAP||A_{2(x)})$$

The calculated value by the node must be the same as the value sent by the ROOT entity, otherwise the node will disconnect the connection. If AM_2 and AM'_2 have the same value, it means that ROOT sent the information and that the value of the session key calculated by the node and the existence of the root are the same. Finally, the node selects the calculated value SK′ as the Session Key. Figure 4 shows the authentication process and key-encryption process of the proposed protocol.

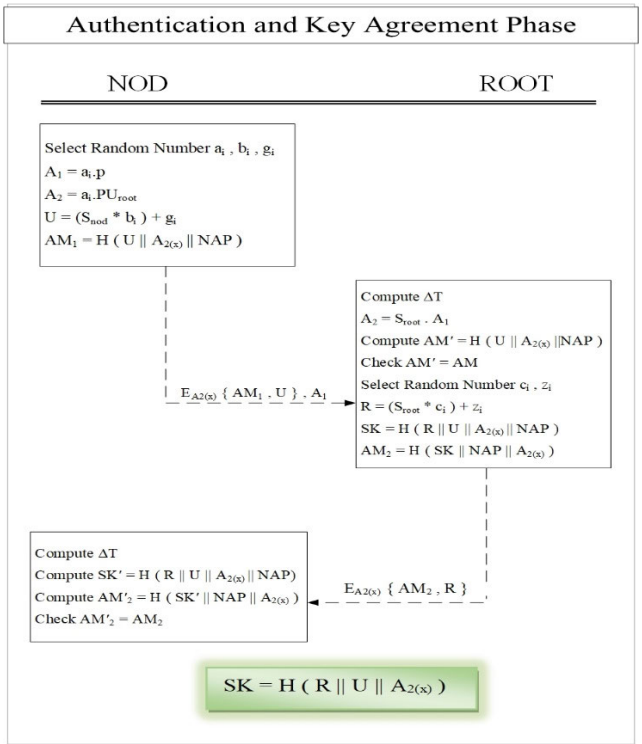

FIGURE 4. Authentication and key agreement phase.

IV. SECURITY ANALYSIS OF THE PROPOSED SCHEME

In this section, we examine the security of our proposed method, both formally and informally. To analyze and prove the security of the term plan parameters used in the protocol and its security aspects, we have formally implemented our proposal with the AVISPA tool. In the section on the informal security analysis of the protocol, we also talk about common attacks and how the proposed method can protect against them.

A. SECURITY REVIEW OF THE PROPOSED METHOD AGAINST COMMON TYPES OF NETWORK ATTACKS

1) REPLY ATTACK

One of the most common attacks on the network is the response attack. This attack allows attackers to record valid data being sent over the network and send it frequently or with a delay on the network. This duplication or delay of data being sent is done by the sender or malicious network nodes.

To prevent this common network attack, we used the time-lapse protocol in the proposed protocol to check the freshness of the messages sent on the network. As stated in the protocol description section, each entity receives the message first with the value $| T_2 - T_1 | < \Delta T$ Examines. If the message is not fresh, the connection is disconnected and the message is discarded. Also, we used random numbers to prevent the repetition and constant value of the messages. Random numbers make the variables calculated in the protocol process to be completely different in each session. Using random numbers and checking the freshness of the message causes the receiver to disconnect with the sender by receiving duplicate values and the message outside the approved time frame ($| T_2 - T_1 | < \Delta T$).

2) IMPERSONATION ATTACK

In this type of attack, the attacker tries to introduce himself as an authorized node in the network and establishes his communication with other network entities. To avoid this loophole in the proposed design, we have implemented multiple authentication mechanisms. In the proposed protocol, three very important parameters examine the authorized numbering and authentication of entities in the sent messages. These parameters are AMP, AM1and AM2.

Therefore, the attacker needs to obtain the private key and the value of A. For the security of these two parameters in the protocol, their combination with random numbers is used, which makes it impossible for attackers to calculate and reach these two parameters. In addition, according to the theory of ECDLP and ECDH, the attackers will not be able to access the multiplied parameters and their results by having point A.

AMP parameter, which is generated in the registration phase is unique for each node and is known only to the ROOT. The node entity is aware of AMP and is used only in the production of parameters. To generate AM1 and AM2 parameters, the private keys of the two entities are used, which are only available to the entities. To ensure the

confidentiality and security of these parameters, they are not sent on the channel and are used only in the generation of authentication parameters. In addition to authentication messages, the dynamic symmetric key generation mechanism is also an authentication process. Using the ECDLP theorem, the ROOT entity can calculate the key when it uses its private key, otherwise, it is not possible to calculate the dynamic symmetric key and it makes it impossible for the attacker to calculate the parameters even with a sending point in the network (ECDH theory).

3) PERFECT FORWARD SECRECY

In the proposed method to implement the Perfect Forward Secrecy feature, random number parameters are used, which makes the value of the parameters used in session key generation to be different in each session. In addition, by combining the private key with random numbers, we prevented the direct use of the entities private parameters in generating the parameters. This action makes it impossible for the network attacker to reach the session key using parameter analysis methods. $A_{2(x)}$, R, and U parameters have been used in the generation of session keys, and according to the explanations given in the key agreement and authentication section, a random number has been used to generate each of these parameters. These characteristics of the parameters in the process of the presented protocol provide conditions that the session key generated in each connection is completely different from the previous connections and makes it impossible to analyze the generated values to reach the private parameters.

4) MAN-IN-THE-MIDDLE ATTACK

A Man-in-the-Middle attack (also known as MITM, MitM, MIM, or MITMA) is one of the most dangerous attacks on computer networks. Unfortunately, during the execution of this attack, the user does not notice it and it leads to the misuse of the user's information. The attacker's goal of the Man-in-the-Middle attack is to collect information and manipulate the information that is exchanged between these two devices or network entities. In addition, the attacker can access the network traffic. To deal with this attack, information encryption is one of the best solutions to deal with attacks that can maintain the confidentiality of information during transmission in the network. In the proposed protocol, using the advantages of ECDH theory, a dynamic symmetric key is used to encrypt information. The selected symmetric encryption key is the X dimension of the A_2 parameter. One of the notable features of the symmetric key selection in the proposed protocol is that random numbers are used to generate A_2, which makes the symmetric key selected unique in each connection. This key is different for each session, making it impossible for an attacker to obtain or even calculate the symmetric encryption key. Also, multiple authentication mechanisms are considered in the proposed protocol process. If the adversary has the sent message, he/she needs to encrypt it. The encryption key used in the presented protocol is based on the ECDH theory and can only be obtained by using the private key of the ROOT entity. Also, according to this theory, it is impossible to calculate it even with having the value of A_1. As a result, this process is an authentication mechanism, and the encryption key generation system is secure.

5) SECURE AGAINST THE DOS ATTACK

This attack helps the attacker send repeated and consecutive messages in the network or a specific node. The purpose of this attack is to disable the network, reduce performance and cause network delay. In the proposed protocol, to prevent this attack, random numbers are used to generate parameters and also check the time stamp by the receiver of the message. Random numbers prevent messages from being duplicated, and timestamps allow the receiver to recognize the allowed time frame of the message. Now, if an attacker sends duplicate messages or sends a large number of messages on the network, the receiver of the message will notice the duplicate message first because it has already received it. Also, by calculating $\Delta T|T_2\text{-}T_1|$, the receiver realizes that the sent message is related to the past and disconnects.

6) SELECTIVE FORWARDING ATTACK

As explained in the Introduction section, this attack captures the packets sent to the network and selectively chooses them in the network. To prevent this attack, the proposed protocol first provides an authentication mechanism that prevents unauthorized nodes from sending information. In certain circumstances, if an attacker finds the possibility of sending a message in the network and intends to execute the said attack, checking the freshness of the message as well as random numbers for the provided protocol are considered. Random numbers provide the conditions that the parameters generated in each connection are completely different and the receiver of the message disconnects from the sender of the message by receiving duplicate packets. Also, checking the freshness of the message by the receiver in the process of the provided protocol causes any packet received outside the approved time frame to be discarded and cut off the connection.

B. RESULT AND FORMAL ANALYZE

In this part of the article, we used AVISPA software for security analysis to prove the security of our proposal against passive and active attacks. This software is one of the reliable evaluation tools that is used to validate and analyze security protocols in the network. This security tool evaluates protocols under various attacks. On-the-Fly Modeler (OFMC) and Constraint-Logic (Cl-AtSe) are two of AVISPA's automated security analysis and backend servers. Given the remarkable capabilities of this software, we decided to use the AVISPA tool to check the security of our protocol against all kinds of attacks and the confidentiality of private values among the relevant factors [32]. Figure 5 shows the security result.

As can be seen from Figure 5, the proposed protocol is secure against all types of active and inactive attacks on the network. The AVISPA tool has two outputs, OFMC and CL-ATSE, which show the privacy of private parameters

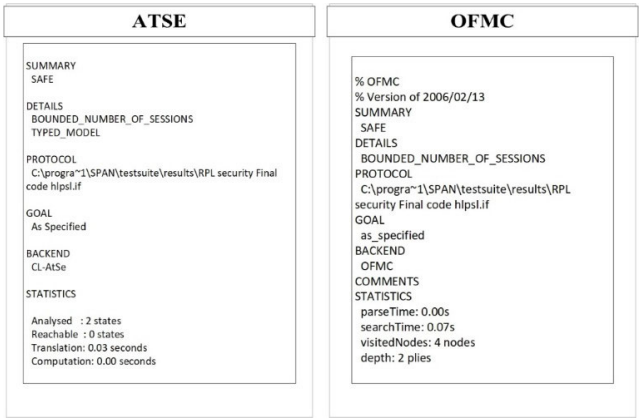

FIGURE 5. AVISPA results. (a) ATSE (b) OFMC.

of communication entities. This analyzed result shows that attackers can't get to the parameters that were made when the protocol was put into place, so they are safe. In Table 3, we have compared our design with similar protocols based on security features and security attacks. As can be seen, the related protocols have security weaknesses and our proposed method can provide security features and be resistant to network attacks.

TABLE 3. Security features comparison.

	Impersonation Attack	Mutual Authentication	Session Key Security	Anonymity	Perfect Forward	Reply Attack	Man-In-The-Middle attack	Safe from DOS attack	Formal security	Key agreement
[47]	×	✓	✓	×	✓	✓	×	×	✓	✓
[48]	×	✓	✓	✓	✓	✓	✓	✓	✓	✓
[49]	×	×	✓	×	✓	✓	×	✓	✓	✓
[50]	×	✓	✓	×	×	✓	✓	×	✓	✓
[51]	×	✓	✓	×	✓	✓	×	×	✓	✓
[53]	✓	×	✓	✓	✓	✓	✓	×	✓	✓
[54]	×	✓	✓	✓	✓	×	✓	×	✓	✓
[55]	✓	✓	✓	×	✓	✓	✓	×	✓	✓
[56]	✓	×	✓	✓	✓	✓	✓	✓	×	✓
[57]	×	✓	✓	×	✓	✓	×	✓	✓	✓
[58]	×	×	✓	✓	✓	✓	✓	×	✓	✓
[59]	×	✓	✓	×	✓	×	×	✓	✓	✓
[60]	×	✓	✓	×	×	✓	✓	✓	✓	✓
[62]	×	✓	✓	✓	×	✓	✓	✓	✓	✓
[63]	✓	×	×	✓	✓	✓	✓	✓	✓	✓
[64]	×	✓		×	✓	✓	✓	✓	×	✓
[65]	×	✓	×	×	✓	✓	✓	✓	✓	✓
[66]	✓	✓	✓	×	✓	✓	✓	✓	✓	✓
[67]	✓	×	✓	✓	×	✓	✓	✓	✓	✓
Our protocol	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

V. PERFORMANCE EVALUATION

A. COMPUTATIONAL COST

In this section, the temporal complexity of the proposed protocol operation is investigated. For this purpose, the results were obtained on a system with a 2.20 GHz Intel Pentium E2200 processor, and 2 GB of RAM. According to the report in [45] and [46], The execution times for each cryptographic element are listed in Table 4. Table 5 compares the computational costs of the related protocols based on the information in Table 4 and the operations that each one does.

TABLE 4. Execution time of cryptographic elements.

Notation	Description	Time cost (ms)
T_H	Time for a general hash operation	≈ 0.0023
T_{SE}	Time for a symmetric encryption/decryption	≈ 0.0046
T_{AE}	Time for an asymmetric encryption/decryption	≈3.85
T_E	Time for an exponentiation	≈3.85
T_M	Time for an EC point multiplication	≈2.226
T_A	Time for an EC point addition	≈0.0288
T_P	Time for a bilinear pairing	≈5.811
T_{HM}	Time for an HMAC operation	≈0.0046
T_{FB}	fuzzy extraction/biohashing	≈2.226

TABLE 5. Extensive comparison of the related protocols.

	Computations	Computational cost (ms)
[47]	$12T_M + 6T_H + 3T_A$	26.8122
[48]	$5T_M + 4T_A + 22T_H + 2T_{SE}$	11.305
[49]	$4T_E + 12T_M$	42.112
[50]	$5T_H + 6T_M + 4T_{SE}$	13.3859
[51]	$6T_H + 4T_E + 6T_{SE}$	15.41656
[53]	$12T_H + 14T_M$	31.1916
[54]	$10T_H + 18T_M + 4T_{SE}$	40.1094
[55]	$12T_M + 4T_A + 15T_H$	26.8617
[56]	$8T_E + 9T_H$	30.8207
[57]	$8T_M + 2T_P + 10T_H$	29.453
[58]	$7T_M + 21T_H + 3T_P$	33.0633
[59]	$13T_M + 15T_H$	28.9725
[60]	$6T_M + 8T_H + 2T_A$	13.432
[61]	$8T_M + 12T_H$	17.8356
[62]	$8T_M + 45T_H + 4T_A$	18.0267
[63]	$1T_{FB} + 3T_M + 17T_H$	8.9431
[64]	$4T_M + 6T_P + 17T_H$	43.8091
[65]	$14T_H + 16T_{SE} + 7T_M$	15.6878
[66]	$17T_H + 6T_S + 7T_M$	15.6487
[67]	$28T_H + 6T_M$	13.4204
Proposed Protocol	$3T_M + 6T_H + 2T_{SE}$	6.701

As can be seen in Table 5, the proposed method uses less time than the other proposed methods. This decrease in execution time is very helpful for network nodes that don't have a lot of resources and are given the RPL protocol because of this.

B. COMMUNICATION COST

In this section, we compare the communication costs of our protocol with previous related protocols. For communication

cost purposes, the bits sent through the communication media and the number of messages exchanged between the two parties are taken into account. Assuming the SHA-1 hash algorithm is used, the identity is 160 bits, a random number of 160 bits, the hash output is 160, and the time stamp is 32 bits. It is also assumed that an elliptic curve point of the form P = (Px; Py), with Px and Py representing the x and y coordinates, respectively, is (160 + 160) = 320 bits, since ECC security is 160 bits remain [47]. In the proposed protocol process, two messages ($MSG_1 = E\{AM_1, A_1, U\}$ $MSG_2 = E\{R, AM_2\}$) are exchanged. The communication cost is as follows.

$$MSG_1 = (160 + 320 + 320) MSG_2 = (160 + 320)$$

TABLE 6. Communication cost comparison.

Protocol	No. of Messages	Total Cost in bit
[47]	3	3296
[48]	2	2212
[49]	2	4256
[51]	5	1312
[53]	3	2528
[54]	2	1024
[55]	2	2144
[56]	2	11712
[57]	3	1696
[58]	4	4384
[59]	4	3904
[60]	3	1760
[62]	4	5568
[63]	4	1856
[64]	6	5344
[65]	6	2176
[66]	4	2304
[67]	4	2584
Proposed Protocol	2	1280

According to Table 6, our proposed protocol has a lower communication cost than other related protocols. In reference 56, the communication cost is lower than our method, but the method presented in reference 56 is vulnerable to impersonation, replay, and DOS attacks. Also, this method has a computational cost of 40.1094 milliseconds, while our proposed method is 6.701 milliseconds.

VI. CONCLUSION

The features and capabilities of IoT devices allow them to be used and included everywhere: in healthcare, smart cities, smart homes, and industrial environments. They have become important targets for attackers because computational constraints and security vulnerabilities in the routing protocol (RPL) make them vulnerable. In this article, we have examined the destructive effects of one of the most important security attacks on the RPL protocol, which is the selective forwarding attack, and evaluated its destructive effects on the routing process.

Based on the simulation results and analysis, it can be concluded that in selective forwarding attacks, the malicious nodes are active during the network lifetime because the malicious nodes drop data packets only, so the control packets are not affected. Consequently, the RPL will not run the self-healing mechanisms for rebuilding the topology to enhance the network performance. So, when coming up with solutions for this kind of attack in the future, the application layer needs to be taken into account.

Obviously, in a varying number of attackers' scenarios, the malicious nodes have decreased the average of both packet delivery ratio and end-to-end delay. Some data packets are dropped by the malicious nodes, so the other data packets travel faster to the root. However, in the density scenario, the malicious nodes have more negative effects because they decrease the packet delivery ratio.

REFERENCES

[1] B. Ghaleb, A. Y. Al-Dubai, E. Ekonomou, A. Alsarhan, Y. Nasser, L. M. Mackenzie, and A. Boukerche, "A survey of limitations and enhancements of the IPv6 routing protocol for low-power and lossy networks: A focus on core operations," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1607–1635, 2nd Quart., 2018.

[2] I. Butun, P. Osterberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 616–644, 1st Quart., 2020.

[3] A. J. Witwit and A. K. Idrees, "A comprehensive review for RPL routing protocol in low power and lossy networks," in *Proc. Int. Conf. New Trends Inf. Commun. Technol. Appl.* Cham, Switzerland: Springer, Oct. 2018, pp. 50–66.

[4] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander, *RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks*, document RFC 6550, IETF, 2012.

[5] K. F. Haque, R. Zabin, K. Yelamarthi, P. Yanambaka, and A. Abdelgawad, "An IoT based efficient waste collection system with smart bins," in *Proc. IEEE 6th World Forum Internet Things (WF-IoT)*, Jun. 2020, pp. 1–5.

[6] T. Winter, P. Thubert, and R. Kelsey, *RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks*, document RFC 6550, Internet Engineering Task Force (IETF). Accessed: Apr. 8, 2018. [Online]. Available: https://tools.ietf.org/html/rfc6550

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

[8] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of Things security: A top-down survey," *Comput. Netw.*, vol. 141, pp. 199–221, Aug. 2018.

[9] B. N. Silva, M. Khan, and K. Han, "Internet of Things: A comprehensive review of enabling technologies, architecture, and challenges," *IETE Tech. Rev.*, vol. 35, no. 2, pp. 205–220, 2018.

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

[11] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber security threats and vulnerabilities: A systematic mapping study," *Arabian J. Sci. Eng.*, vol. 45, no. 4, pp. 3171–3189, Apr. 2020.

[12] P. O. Kamgueu, E. Nataf, and T. D. Ndie, "Survey on RPL enhancements: A focus on topology, security and mobility," *Comput. Commun.*, vol. 120, pp. 10–21, May 2018.

[13] A. Kamble, V. S. Malemath, and D. Patil, "Security attacks and secure routing protocols in RPL-based Internet of Things: Survey," Presented at the Int. Conf. Emerg. Trends Innov. ICT (ICEI), Pune, India, Feb. 2017.

[14] M. F. Razali, M. E. Rusli, N. Jamil, R. Ismail, and S. Yussof, "The authentication techniques for enhancing the RPL security mode: A survey," in *Proc. 6th Int. Conf. Comput. Informat.*, Kuala Lumpur, Malaysia, 2017, pp. 735–743.

[15] D. Airehrour, J. Gutierrez, and S. K. Ray, "Securing RPL routing protocol from blackhole attacks using a trust-based mechanism," Presented at the 26th Int. Telecommun. Netw. Appl. Conf. (ITNAC), Dunedin, New Zealand, Dec. 2016.

[16] L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and countermeasures in the RPL-based Internet of Things," *Int. J. Distrib. Sensor Netw.*, vol. 2013, 2013.

[17] S. Singh and H. S. Saini, "Learning-based security technique for selective forwarding attack in clustered WSN," *Wireless Pers. Commun.*, vol. 118, no. 1, pp. 789–814, May 2021.

[18] S. P. Lal and P. M. J. Prathap, "Retraction note to: A provenance based defensive technique to determine malevolent selective forwarding attacks in multi-hop wireless sensor networks," *J. Ambient Intell. Hum. Comput.*, vol. 12, no. 5, pp. 5589–5597, Jun. 2022.

[19] V. Neerugatti and A. R. M. Reddy, "Artificial intelligence-based technique for detection of selective forwarding attack in RPL-based Internet of Things networks," in *Emerging Research in Data Engineering Systems and Computer Communications*. Singapore: Springer, 2020.

[20] J. E. Rubio, C. Alcaraz, R. Roman, and J. Lopez, "Current cyber-defense trends in industrial control systems," *Comput. Secur.*, vol. 87, Nov. 2019, Art. no. 101561.

[21] T. Tsao, R. Alexander, M. Dohler, V. Daza, A. Lozano, and M. Richardson, *A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)*, document RFC 7416, Jan. 2015.

[22] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," in *Proc. 1st IEEE Int. Workshop Sensor Netw. Protocols Appl.*, May 2005, pp. 113–127.

[23] L. K. Bysani and A. K. Turuk, "A survey on selective forwarding attack in wireless sensor networks," in *Proc. Int. Conf. Devices Commun. (ICDeCom)*, Feb. 2011, pp. 1–5.

[24] H.-M. Sun, C.-M. Chen, and Y.-C. Hsiao, "An efficient countermeasure to the selective forwarding attack in wireless sensor networks," in *Proc. IEEE Region 10 Conf. (TENCON)*, Oct. 2007, pp. 4–7.

[25] L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and countermeasures in the RPL-based Internet of Things," *Int. J. Distrib. Sens. Netw.*, vol. 2013, pp. 1–11, 2013.

[26] I. Tomić and J. A. McCann, "A survey of potential security issues in existing wireless sensor network protocols," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1910–1923, Jun. 2017.

[27] D. Shreenivas, S. Raza, and T. Voigt, "Intrusion detection in the RPL-connected 6LoWPAN networks," in *Proc. 3rd ACM Int. Workshop IoT Privacy, Trust, Secur.*, USA, Apr. 2017, pp. 31–38.

[28] D. Airehrour, J. A. Gutierrez, and S. K. Ray, "A trust-aware RPL routing protocol to detect blackhole and selective forwarding attacks," *Austral. J. Telecommun. Digit. Economy*, vol. 5, no. 1, pp. 50–69, 2017.

[29] D. Airehrour, J. A. Gutierrez, and S. K. Ray, "SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things," *Future Gener. Comput. Syst.*, vol. 93, pp. 860–876, Apr. 2019, doi: 10.1016/j.future.2018.03.021.

[30] R. Mehta and M. M. Parmar, "Trust based mechanism for securing IoT routing protocol RPL against wormhole & grayhole attacks," in *Proc. 3rd Int. Conf. for Converg. Technol. (I2CT)*, Apr. 2018, pp. 1–6.

[31] M. Alzubaidi, M. Anbar, Y.-W. Chong, and S. Al-Sarawi, "Hybrid monitoring technique for detecting abnormal behaviour in RPL-based network," *J. Commun.*, vol. 13, no. 5, pp. 198–208, Oct. 2018.

[32] S. Y. Hashemi and F. S. Aliee, "Dynamic and comprehensive trust model for IoT and its integration into RPL," *J. Supercomput.*, vol. 75, no. 7, pp. 3555–3584, Jul. 2019.

[33] S. Murali and A. Jamalipour, "A lightweight intrusion detection for Sybil attack under mobile RPL in the Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 379–388, Jan. 2020.

[34] A. Jain and S. Jain, "A survey on miscellaneous attacks and countermeasures for RPL routing protocol in IoT," in *Emerging Technologies in Data Mining and Information Security*. Singapore: Springer, 2019, pp. 611–620.

[35] A. Verma and V. Ranga, "Security of RPL based 6LoWPAN networks in the Internet of Things: A review," *IEEE Sensors J.*, vol. 20, no. 11, pp. 5666–5690, Jun. 2020.

[36] A. Verma and V. Ranga, "CoSec-RPL: Detection of copycat attacks in RPL based 6LoWPANs using outlier analysis," *Telecommun. Syst.*, vol. 75, no. 1, pp. 43–61, Sep. 2020.

[37] A. Patel and D. Jinwala, "A reputation-based RPL protocol to detect selective forwarding attack in Internet of Things," *Int. J. Commun. Syst.*, vol. 35, no. 1, Jan. 2022, Art. no. e5007.

[38] K. Prathapchandran and T. Janani, "A trust aware security mechanism to detect sinkhole attack in RPL-based IoT environment using random forest—RFTRUST," *Comput. Netw.*, vol. 198, Oct. 2021, Art. no. 108413.

[39] A. Agiollo, M. Conti, P. Kaliyar, T.-N. Lin, and L. Pajola, "DETONAR: Detection of routing attacks in RPL-based IoT," *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 2, pp. 1178–1190, Jun. 2021.

[40] *Cooja Simulator*. Accessed: Oct. 20, 2019. [Online]. Available: https://github.com/contiki-os/contiki/wiki/AnIntroduction-to-Cooja

[41] J. Polastre, R. Szewczyk, and D. Culler, "Telos: Enabling ultra-low power wireless research," in *Proc. 4th Int. Symp. Inf. Process. Sensor Netw. (IPSN)*, 2005, pp. 364–369.

[42] L. Lassouaoui, S. Rovedakis, F. Sailhan, and A. Wei, "Evaluation of energy aware routing metrics for RPL," in *Proc. IEEE 12th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2016, pp. 1–8.

[43] A. Le, J. Loo, A. Lasebae, A. Vinel, Y. Chen, and M. Chai, "The impact of rank attack on network topology of routing protocol for low-power and lossy networks," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3685–3692, Oct. 2013.

[44] M. F. Moghadam, M. Nikooghadam, M. A. B. A. Jabban, M. Alishahi, L. Mortazavi, and A. Mohajerzadeh, "An efficient authentication and key agreement scheme based on ECDH for wireless sensor network," *IEEE Access*, vol. 8, pp. 73182–73192, 2020.

[45] M. Nikooghadam, H. Amintoosi, S. H. Islam, and M. F. Moghadam, "A provably secure and lightweight authentication scheme for Internet of Drones for smart city surveillance," *J. Syst. Archit.*, vol. 115, May 2021, Art. no. 101955.

[46] M. F. Moghadam, M. Nikooghadam, A. H. Mohajerzadeh, and B. Movali, "A lightweight key management protocol for secure communication in smart grids," *Electr. Power Syst. Res.*, vol. 178, Jan. 2020, Art. no. 106024.

[47] M. M. Farhdi, A. Mohajerzdeh, H. Karimipour, H. Chitsaz, R. Karimi, and B. Molavi, "A privacy protection key agreement protocol based on ECC for smart grid," in *Handbook of Big Data Privacy*. Cham, Switzerland: Springer, 2020, pp. 63–76.

[48] A. K. Das, M. Wazid, A. R. Yannam, J. J. P. C. Rodrigues, and Y. Park, "Provably secure ECC-based device access control and key agreement protocol for IoT environment," *IEEE Access*, vol. 7, pp. 55382–55397, 2019.

[49] A. Ostad-Sharif, D. Abbasinezhad-Mood, and M. Nikooghadam, "A robust and efficient ECC-based mutual authentication and session key generation scheme for healthcare applications," *J. Med. Syst.*, vol. 43, no. 1, pp. 1–22, Jan. 2019.

[50] J. Singh, A. Gimekar, and S. Venkatesan, "An efficient lightweight authentication scheme for human-centered industrial Internet of Things," *Int. J. Commun. Syst.*, Nov. 2019, Art. no. e4189.

[51] S. Majumder, S. Ray, D. Sadhukhan, M. K. Khan, and M. Dasgupta, "ECC-CoAP: Elliptic curve cryptography based constraint application protocol for Internet of Things," *Wireless Pers. Commun.*, vol. 116, no. 3, pp. 1867–1896, Feb. 2021, doi: 10.1007/s11277-020-07769-2.

[52] S. Dey and A. Hossain, "Session-key establishment and authentication in a smart home network using public key cryptography," *IEEE Sensors Lett.*, vol. 3, no. 4, pp. 1–4, Apr. 2019.

[53] J. H. Silverman, *The Arithmetic of Elliptic Curves*. Springer, 2009.

[54] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E.-J. Yoon, and K.-Y. Yoo, "Secure signature-based authenticated key establishment scheme for future IoT applications," *IEEE Access*, vol. 5, pp. 3028–3043, 2017.

[55] M. Karthigaiveni and B. Indrani, "An efficient two-factor authentication scheme with key agreement for IoT based E-health care application using smart card," *J. Ambient Intell. Hum. Comput.*, pp. 1–12, Oct. 2019.

[56] S. Malani, J. Srinivas, A. K. Das, K. Srinathan, and M. Jo, "Certificate-based anonymous device access control scheme for IoT environment," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9762–9773, Dec. 2019.

[57] Y. Tian, J. Yuan, and H. Song, "Efficient privacy-preserving authentication framework for edge-assisted Internet of Drones," *J. Inf. Secur. Appl.*, vol. 48, Oct. 2019, Art. no. 102354.

[58] B. Bera, D. Chattaraj, and A. K. Das, "Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment," *Comput. Commun.*, vol. 153, pp. 229–249, Mar. 2020.

[59] X. Jia, D. He, N. Kumar, and K.-K. R. Choo, "Authenticated key agreement scheme for fog-driven IoT healthcare system," *Wireless Netw.*, vol. 25, no. 8, pp. 4737–4750, May 2019.

[60] M. Ma, D. He, H. Wang, N. Kumar, and K.-K. R. Choo, "An efficient and provably secure authenticated key agreement protocol for fog-based vehicular ad-hoc networks," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8065–8075, Oct. 2019.
[61] B. A. Alzahrani, S. A. Chaudhry, A. Barnawi, A. Al-Barakati, and T. Shon, "An anonymous device to device authentication protocol using ECC and self certified public keys usable in Internet of Things based autonomous devices," *Electronics*, vol. 9, no. 3, p. 520, Mar. 2020.
[62] X. Gong and T. Feng, "Lightweight anonymous authentication and key agreement protocol based on CoAP of Internet of Things," *Sensors*, vol. 22, no. 19, p. 7191, Sep. 2022.
[63] S. A. Eftekhari, M. Nikooghadam, and M. Rafighi, "Security-enhanced three-party pairwise secret key agreement protocol for fog-based vehicular ad-hoc communications," *Veh. Commun.*, vol. 28, Apr. 2021, Art. no. 100306.
[64] D. Kaur and D. Kumar, "Cryptanalysis and improvement of a two-factor user authentication scheme for smart home," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102787.
[65] Y. K. Ever, "A secure authentication scheme framework for mobile-sinks used in the Internet of Drones applications," *Comput. Commun.*, vol. 155, pp. 143–149, Apr. 2020.
[66] A. Kumari, V. Kumar, M. Y. Abbasi, S. Kumari, P. Chaudhary, and C.-M. Chen, "CSEF: Cloud-based secure and efficient framework for smart medical system using ECC," *IEEE Access*, vol. 8, pp. 107838–107852, 2020.
[67] S. S. Sahoo, S. Mohanty, and B. Majhi, "A secure three factor based authentication scheme for health care systems using IoT enabled devices," *J. Ambient Intell. Hum. Comput.*, vol. 12, no. 1, pp. 1419–1434, Jan. 2021.
[68] C.-M. Chen, Y. Huang, K.-H. Wang, S. Kumari, and M.-E. Wu, "A secure authenticated and key exchange scheme for fog computing," *Enterprise Inf. Syst.*, vol. 15, no. 9, pp. 1200–1215, Oct. 2021.

HAITHAM Y. ADARBAH received the bachelor's degree in computer science from the Al-Zaytoonah University of Jordan, Amman, Jordan, in 2004, the master's degree in computer science from Amman Arab University, Amman, in 2009, and the Ph.D. degree in wireless networks from De Montfort University, Leicester, U.K., in 2015. He is currently an Assistant Professor and the Programme Leader of the Center for Training and Community Relations, Gulf College. He joined the Gulf College as a Computing Lecturer, in April 2009. He held the programme leader position with the Faculty of Computer Sciences for two years and a half and he worked as the Programme Leader of IT and Mathematics with the Centre of Foundation Studies for a year. He also served as a Moodle Coordinator for a year. As an Assistant Professor, he is also very much interested in mobile ad hoc networks (MANET): route discovery schemes, routing techniques, bandwidth utilization, power consumption, delay, security wireless networks, and network simulation and modeling. He has authored several research papers, which were all published in various international journals and conferences.

MOSTAFA FARHADI MOGHADAM received the B.S. degree in computer science from the University of Applied Science and Technology, Mashhad, Iran, and the M.Sc. degree from Imam Raza University (IRU), Mashhad. She is currently a Lecturer at the Vahdat Institute of Higher Education. Her research interests include smart grid, data security, and cryptography.

ROLOU LYN RODRIGUEZ MAATA is currently pursuing the Ph.D. degree.

She is the book author, a fellow of Advanced SHE U.K., a Certified SAP Lecturer, a Licensed Professional Teacher, a Research Reviewer, and a Computer Science Professor in various higher education institutions (HEIs). She has more than 20 years of administrative and teaching experience in the academy and has held various positions, such as the Dean, the Associate Dean, and the Department Head of Information Management and Computer Science. She is also a Certified SAP Lecturer issued by SAP University, Munich, Germany, and once served as the main contact of SAP University Alliances EMEA, Bahrain. She attended SAP ERP Training at Napier University, U.K., and SAP University, Waldorf, Germany. She is currently an Associate Professor and a Final Year Project (FYP) Coordinator with the Faculty of Computing Sciences, Gulf College, Oman, in academic affiliation with Cardiff Metropolitan University, U.K. She is an Active Research Reviewer of The Research Council (TRC) of Oman and the Institute of Informing Science, USA. She has presented and published numerous research papers in several reputable journals and peer-reviewed conference proceedings that are indexed in Scopus, IEEE, Google Scholar, and other research databases. Her research interests include the areas of educational technologies, business analytics, computer security, software engineering, and enterprise resource planning. She was awarded nine research project grants by the government of the Sultanate of Oman, on which she served as a principal investigator and a co-principal investigator, in 2018 and 2021. In January 2021, she has published a book titled *IT Application Tools in Business* as a textbook for university students taking up business courses in Philippines.

AMIRHOSSEIN MOHAJERZADEH received the B.S., M.S., and Ph.D. degrees from the Ferdowsi University of Mashhad, Mashhad, Iran, in 2005, 2007, and 2013, respectively. He has been a Computer Network Engineer with several networking projects with the Iran Telecommunication Research Center (ITRC), since 2008. Currently, he is an Assistant Professor at the Computer Engineering Department, Ferdowsi University of Mashhad. He is the author of one book in Farsi language in networking field. He has published more than 30 international conferences and journal articles. His research interests include cellular networks (5G), wireless sensor networks (WSNs), software defined networking (SDN), smart grid, target tracking, modeling and analyzing computer networks, quality of services (QoS), and fuzzy logic control.

ALI H. AL-BADI is currently working as a Full Professor and the Deputy Dean of Academic Affairs and Research at the Gulf College, Muscat, Oman. He worked as an Associate Professor in information systems and the Assistant Dean of Postgraduate Studies and Research at the College of Economics and Political Science, Sultan Qaboos University, Muscat. He received his education in Oman, Saudi Arabia, U.K., and USA. He has more than 29 years of practical and academic experience in information technology. After graduated from Reading University, U.K., he started working with the Centre for Information Systems (CIS), Sultan Qaboos University. He has held various positions in the centre, since then, where he gained most of his practical experience working on and overseeing different IT projects. From September 2007 to March 2011, he held the CIS director's position, sharing his time between managing the centre and performing his academic duties. From September 2012 to September 2015, he was the Head of the Information Systems Department, College of Economics and Political Science, Sultan Qaboos University. Furthermore, he contributed to different committees at both university and national levels. He has been continually active in research. He has published his work in several reputable peer-reviewed journals and presented papers at various local, national, and international conferences. He served as an editorial board member of several highly reputed international conferences and refereed journals.