Compatible authentication and key agreement protocol for low power and lossy network in IoT environment

Ali Peivandizadeh (apeivandizadeh@uh.edu)
Graduated Student Technology Project Management University of Houston
Behzad Molavi
Vahdat Institute of Higher Education, Torbat-e Jam

Research Article

Keywords: RPL, IoT, Security, Privacy, Key agreement, Authentication, ECC

Posted Date: September 29th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-2085426/v1

Abstract

Today, the Internet of Things can be described as the fastest-growing network that offers applications in a wide range of applications fields. This breadth has led to a wide range of IoT research. Applications of this network can be mentioned in various sectors such as e-health, smart homes, smart cities, and everything in smart cities via the Internet, where the collection and exchange of large amounts of data are undeniable. The IoT also supports large-scale low-power networks (LLNs) and uses the RPL protocol to route low-power, low-resource nodes on this large scale. Due to the exchange of sensitive data in this network, security is a critical issue. However, RPLs have many serious vulnerabilities, including the use of symmetric encryption that attackers can exploit. In addition, the privacy and security of network nodes are other challenges of this network. Therefore, there is a significant need for an effective and secure authentication scheme that enables IoT users to authenticate each other and share the session key to a secure meeting. In this paper, we aim to provide a secure protocol to enhance the security of the IoT and low-power nodes that use the RPL protocol against various network attacks. For this purpose, a key agreement protocol and authentication mechanism using ECC theory are proposed. Finally, we show that the proposed scheme is secure against routine network attacks and incurs a small computational and communication cost that is compatible with nodes with limited resources.

I. Introduction

In recent years, a new era has emerged in Internet networks called the Internet of Things (IoT) [1–2]. It is noteworthy that the Internet of Things has become extremely important, and its efficiency in connecting the billions of objects used has led to its expansion around the world [3–4]. The advent of the Internet of Things has led to the emergence of a particular category of networks that can be known as low-power networks and loss networks (LLN) [5–6]. LLNs can be used efficiently and practically in designing and manufacturing commercial devices for emerging markets. The Internet of Things includes the deployment of large-scale low-power networks (LLNs), including resource-limited devices such as sensors and RFIDs [7]. One of the challenges in LNNs is routing, which requires an effective routing protocol that meets the requirements of the program [8]. The Internet Engineering Task Force (IETF) proposed the 6LOWPAN Applicable Protocol for LLNs in the IoT environment [9]. One of the basic requirements for implementing and deploying LNNs on a large scale is routing in that infrastructure, and the protocols used for routing in WSN are not suitable for LNNs in an IoT network. Therefore, the IETF has provided a routing protocol for low power networks and loss (RPL) for LLNs in the Internet of Things. RPL is fully compatible with LLNs and supports all their traffic flow requirements in a wide range of applications [10]. The RPL routing protocol is based on IPv6 [11]. Restrictions on RPL-based networks cause network nodes to be exposed to a variety of security attacks [12]. In addition, RPL does not support security features and cannot provide complete security and routing security, thus making it vulnerable to all types of network attacks [13]. Even if encryption mechanisms are used for security, they can only prevent external attacks. When nodes in the network are compromised, they can become an internal enclosure within the network, in which case encryption techniques alone will not be able to protect the network. Extensive studies have

been conducted on IoT network security. Since a large number of devices and network nodes use the RPL protocol, a huge range of network entities is exchanging important data. So, security in RPL becomes a very important issue that needs to be addressed significantly. Because in the routing process, the data that is being transmitted should not be accessed by an intruder or an unauthorized third party on the network or leaked out of the network. Although several security measures have been considered for the security of the RPL protocol, there are threats to the security of this protocol.

In this article, the vulnerabilities and security requirements of IoT have been examined. Since IOT includes a wide range of network devices and users, information security and privacy of the entities of this network are of great importance. Because network attackers can cause significant damage to this network by accessing or even causing a delay in reaching the destination. In IoT, many nodes have low computing power and are forced to use symmetric encryption systems to implement their security policies. But due to the use of a fixed key in this type of encryption system, when the symmetric key is exposed, it puts the whole network at risk. According to the investigations, we have presented a key agreement scheme and multiple authentications to improve the security of IoT network nodes. Also, due to the high vulnerability of network nodes with low computing power, we tried to make our presented method highly compatible with these types of IoT network nodes.

The protocol provided significant features as follows.

1- Improving the symmetric encryption system

The presented protocol provides a mechanism using the ECDH theory that network nodes can create their symmetric encryption key in each connection and a fixed symmetric key is no longer used for all entities. The symmetric key generated in each connection is unique and according to ECDH theory, it is impossible to calculate by attackers.

2- Multiple authentication mechanisms based on ECDH theory

In addition to using the private parameters of the communication nodes, the presented protocol also uses the ECDH theory to strengthen the authentication mechanism of the nodes.

3- Significant reduction in the computational cost of the protocol process

Due to the presence of low-power nodes in the network, a protocol has been provided to maintain its security features by significantly reducing the calculation time of the protocol operation. The computational cost of the proposed protocol is significantly lower than the related protocols.

In the following, the theories (ECC, ECDLP, ECDH) used in the proposed protocol, security challenges of the RPL routing protocol for routing low-power network nodes, and Security challenges in IoT are described.

A. Concepts of the cryptographic system:

1. Elliptical Curve Cryptography

Elliptic curve (ECC) cryptography is one of the modern techniques in the world of public-key cryptography and encryption, which is based on the elliptic curve theory. This asymmetric encryption mechanism can be used to create faster, smaller, and more efficient encryption keys. The ECC uses a mathematical process to merge two separate keys, and its output is used to encrypt and decrypt data. This asymmetric cryptography system uses an elliptical curve called E and a set of points with coordinates, $pf \ * pf \ ()$ x, y. The points along the graph are represented by the following equations:

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

Where a,b f_p and $4a^3 + 27b^2 \ 0$

The elliptic curve cryptography system consists of the sum of points and point multiplication, which are the two main factors of this cryptographic mechanism. The point multiplication factor is also called scalar multiplication. An example of scalar multiplication by multiplying K by P is given below to better understand this factor.

KP = P + P + P + P…. +P

2. Elliptic Curve Discrete Logarithm Problem (ECDLP)

In the ECC cryptographic system, the computational problem of the discrete logarithm problem of an elliptic curve is abbreviated to ECDLP, which forms the basic block in the pairing-based and elliptic curve mechanism. Now if we have two points named P and Q on the surface of an elliptic curve, the point Q is the result of calculating the scalar multiplication of the value of K at the point P. Given the problem of discrete logarithms mentioned earlier, if we have two points P and Q, it is very difficult and even impossible to calculate the parameter k, even with those two parameters. In the ECC encryption mechanism, this difficulty and impossibility of calculating the parameter are known as ECDLP or hard ellipse curve problems [14–15].

3. Delphi-Hellman ECDH Elliptic Curve

Other sub-theories of the ECC subset include Elliptic Curve Diffie–Hellman Key Exchange (ECDH), which is a method for key agreement between two entities based on anonymity. In this mechanism, each of the two communication parties has public and private keys based on the elliptic curve, which allows them to create their common session key or secrets in a secure name channel. Other sub-theories of the ECC subset include Elliptic Curve Diffie–Hellman Key Exchange (ECDH), which is a method for key agreement between two entities based on anonymity. In this mechanism, each of the two communication parties has public and private keys based on the elliptic curve, which allows them to create their common session key or secrets in a secure name channel. Consider the elliptic curve and assume that two points $p.\ a_i$ and $p.\ b_i$ are on the surface of this curve. The Delphi-Hellmann Curve (ECDH) problem expresses the principle

that if a resident on the network has access to these two points, It is impossible for he/she to reach bi (a_i. p) and ai (b_i. p).

B. RPL Overview

The Routing Protocol for low power and lossy networks (RPL) is an IPv6-based routing protocol. This protocol was developed by the IETF Group and can be identified as Routing Over Low Power and Lossy Networks (ROLL) [16]. The purpose of designing this protocol is to present it as a standard for low-consumption and lossless networks that can include all sensor nodes in an IoT network. RPL works by exploring routes by setting up an RPL network, hence it is considered an active routing protocol. This routing protocol forms a tree-like topology known as the destination non-cyclical directional graph (DODAG). In an RPL network, each node selects a parent based on predefined criteria, which acts as a gateway to that node. When a node intends to send a packet to its intended destination, it does not have a routing table for it. So, he has to pass that package to his parent who has a route to the next destination or transfer. This process continues until it reaches the final destination in the tree. One of the most important factors for an RPL is the choice of path, which uses several criteria for this purpose. 3 traffic patterns can be mentioned for RPL packages. First, point-to-point (MP2P) traffic was sent from the leaves to the roots via upward paths. The second is point-to-point (P2MP) traffic from root to leaf using downward paths. Finally, the third pattern of point-to-point (P2P) traffic is represented by red dotted arrows using up and down paths.

C. RPL Security and challenges

The development and implementation of appropriate security mechanisms in low-power and lossy networks are critical [17–18]. As mentioned earlier, the IoT network has resource constraints for many network nodes, which makes the implementation and deployment of security mechanisms in RPL very complex and difficult. In the routing process, RPL transmits information between network nodes, and many security challenges have been identified. IoT network nodes exchange packets for routing and addressing, which requires the definition of protocols and security mechanisms for routing packets being transmitted. These mechanisms and protocols must be compatible with different network topologies [19]. In general, RPL devices are vulnerable due to their inability to resist tampering and allow network attackers to capture IoT nodes. In addition, it is possible to extract encrypted information and allow legal activity for an unauthorized node. An attacker with the ability to act as a network node tries to execute malicious code and try to change the routing rules. Each network node is responsible for processing, which makes it difficult to detect variable and destructive effects [20]. In the routing process between nodes, there are potential threats and security issues that cause vulnerabilities that can endanger users' lives in cases such as human health monitoring devices [21]. As in any network, the protection and security of network data are very important, so in RPL routing, this is an important and challenging issue. A malicious node sends packets that are being transmitted across the network to carry out their unauthorized activities. This enables the malicious person or node to perform all kinds of attacks on the data being routed [22]. However, research shows that the standards defined for RPL protocol security are not able to meet the security challenges of the IoT network.

Usually, there are other security mechanisms in the link layer that are used in some infrastructures. The RPL standard for security has introduced three modes that can provide security features of message confidentiality and integrity.

Unsecure mode

In this case, the control messages sent by RPL are delivered without any security mechanism in the network. It is possible to adopt security requirements and mechanisms in another layer, such as the link layer.

Pre-installed mode

In this node, any node that intends to join an RPL must have pre-defined keys. This is to ensure the security of RPL messages.

Authenticated Mode

This section is somewhat similar to the second mode, Pre-Installed. There are also pre-defined keys in this section, but with the difference that the keys are only for joining the RPL as a leaf node. The key can also be obtained from a central authentication reference.

Another security challenge in RPL is the large amount of information sent by network users, and the confidentiality of this data must be maintained. There are different encryption techniques to protect the privacy of users and the confidentiality of network users' information. These cryptographic systems are used for user authentication, privacy, and defense against a variety of network attacks. In addition, they provide conditions for the network that unauthorized persons are not able to operate and access network information. There are two techniques to use data encryption systems: symmetric and asymmetric encryption. The RPL protocol uses a symmetric encryption system to secure its data, which costs less than an asymmetric one. From the attack of symmetric encryption algorithms and standards, one can go to Advanced Encryption Standard (AES) and Message Authentication Code (CBC-MAC Counter (CCM)) - (AES / CCM) pointed out. In an asymmetric encryption system, the two sides of the communication use a secret key that is already shared between them to encrypt the data. A common key is used for all nodes, which makes it easier for the network attacker to access. If an attacker on the network has access to secret keys under certain conditions, he/she can carry out his malicious actions on the network and even insert his malicious nodes into the network. In such a case, the network becomes vulnerable to all kinds of security attacks and the security and privacy of network nodes are compromised. Once the secret keys of the network are exposed to the network attackers, the cryptographic systems will no longer be able to protect the network [23–24]. As mentioned, research shows that RPL has experienced significant vulnerabilities, so improvements in security mechanisms and the RPL routing protocol authentication system are essential [25–26]. The routing protocol requires mechanisms for identifying inconsistencies, loop avoidance, validation, and detecting inconsistencies. Although the security requirements for RPL security have been provided by the IEFT, a valid security model has not been identified, which has posed

challenges to the routing protocol security. The key management mechanism in RPL does not specify the characteristics, authentication, and secure connection of nodes, which is a weakness in the design of the security standard. This design weakness makes the RPL protocol vulnerable to a variety of attacks [27]. Table 1 shows the types of routing attacks.

Table 1
Attacks on RPL protocol

Attack	Feature of the attach	Consequences on network's performance
Rank	Rank field and strict rank rules are exploited.	Generates routing loops. Increases end-to-end delay, PDR, control packet overhead, congestion, and energy consumption. Introduces unoptimized routes.
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
Sniffing	Network traffic is eavesdropped for obtaining routing information from packets.	Introduces privacy concerns.
Sinkhole	Advertising false information to create a center of attraction for other nodes.	Compromise of transmission routes, reducing traffic and increasing 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.
Jamming	Attacker transmits with high power radio signals to introduce heavy interference.	Decreases PDR and increases energy consumption.

Attack	Feature of the attach	Consequences on network's performance
Wormhole	Create a low-link tunnel between two malicious nodes in different parts of network	Sending data to the false distention, undermining cryptography protection.
Sybil	Single nodes contain multiple logical identities.	Overcomes voting schemes, and compromises transmission routes by taking control of the network.
Hello flood	Broadcasting a hello packet to the whole network with great transmission power.	Increasing energy degradation and collisions, create false transmission routes.

D. IoT Security challenges

The Internet of Things has provided many benefits to the users of this network, but despite this, there are challenges for this network. One of the most important challenges that researchers and security experts have pointed out is the cyber security and privacy risks of the Internet of Things network. Due to the connection of networks in the Internet of Things, access from the Internet is anonymous and unreliable, common cyber security attacks have made the Internet of Things network vulnerable [11]. The Internet of Things consists of a wide variety of devices, equipment, and computers, which makes it more vulnerable to various types of attacks and security challenges. The connection of IoT devices means that if a device in this network has poor security and connectivity, it can affect the security and flexibility of the Internet internationally.

A large amount of data is exchanged on the Internet of Things, which makes information security one of the most vulnerable areas. For example, we can mention contactless credit cards. These cards provide the possibility of reading the number and name of the cards without authentication of the Internet of Things and the conditions for them to purchase goods using the bank account number of the cardholder and their identity. One of the most common IoT attacks is the man in the middle. This attack causes the bank server to recognize the performed transaction as a valid event [19].

Even though the issue of security is not new in the information and technology sector, the implementation of the Internet of Things has presented challenges that must be addressed. One of the important security features is the authentication of network entities. Unfortunately, the Internet of Things is weak in providing this feature and suffers from various vulnerabilities, which is one of the most important issues in providing security in many programs.

Paper organization

Our goal in this paper is to focus on addressing the security challenges of the RPL protocol in routing nodes in the Internet of Things and providing a secure method of exchanging session keys as well as authentication of communication parties. The article is organized as follows. Related works are presented in the second section. Section III provides a proposed protocol for securing RPL. The security simulation results of the proposed protocol using the AVISPA network protocol review tool and the protocol resistance of the protocol against common network attacks are presented in Section IVSection V compares the performance of the proposed protocol in terms of computational cost and also compares it with other protocols related to RPL and IoT security. Finally, the conclusion of the paper is reported in section VI.

Ii. Related Work

Security is very important in any network, and IoT routing also exchanges a significant amount of data. In addition, the security of nodes in the IoT is a critical issue. Due to the vulnerabilities of RPL and IoT, a lot of security research has been done.

In 2017, Airehrour et al. [28] proposed a trust-based routing protocol for Low-Power and Lossy Networks to identify Blackhole attacks and selective forwarding attacks. In the method provided by them, each node needs trust to operate and access the network, and the calculated value for each node is a criterion for parent selection. In addition, their results show that the protocol provided by them does not incur additional costs on network traffic. In the same year, Tomić and McCann [29] presented their research on the deployment of WSN, in which the authors focused on key security mechanisms and their effects on WSN protocols and standards. They discuss personal networks, RPL routing protocols, potential security threats, and countermeasures that can be taken for threats at each layer. In addition, they have been simulated using Cooja to express the effects of attacks and network performance. In addition to the previous author, Shrinovas et al. [30] Investigated the vulnerabilities of routing protocols for low-power networks. As a result of these investigations, they identified attacks in which the attacker's goal was to disrupt the RPL protocol routing process. The authors proposed a hacking system in 6LoWPAN networks intending to improve security. In addition, they have proposed the use of geographical hints to identify malicious nodes in an ETX-based network.

In 6LoWPAN networks, due to the need for low bandwidth and limited resources, the Internet Protocol version 6 and RPL are used in the wireless sensor network. RPL exchanges data without using an authentication mechanism, which leads to network disruption. An example is the Sinkhole attack. In 2018, Mahmoud et al. [31] examined these vulnerabilities and developed a hybrid monitoring method that aimed to detect abnormal behaviors in RPL-based networks. The model presented by them consists of two phases, in the first phase the information of the adjacent node is collected and in the second phase it is responsible for identifying the sink node. Different mechanisms and standards have been proposed for IoT security, and the centralized trust approach is one of the proposed mechanisms for security in this

network. Therefore, Mehta et al. [32] proposed a trust mechanism based on trust to prevent the execution of Wormhole and Grayhole attacks in the IoT network. Their proposed system has two approaches: direct and indirect trust, which uses the node properties in direct trust and the indirect trust from the perspective of neighboring nodes. Features of this method are compatibility with RPL protocol in terms of energy consumption and low overhead in network traffic. Airehrour et al. [33] proposed a time-based trust model to protect the IoT network from routing attacks such as Rank and Sybil. This model provides a framework for IoT nodes that can exchange and communicate with each other on a trust basis. In the method proposed by the authors, the network environment is divided into smaller areas that help the network nodes to interact and trust.

One of the most challenging security issues is ensuring security in IoT routing protocols because the devices in this network are limited and have heterogeneous resources. Hashemi et al. [34], due to limited resources for security, proposed a routing protocol that is participatory and based on conscious trust. In their proposed method, they have integrated a dynamic trust model with the RPL protocol that uses the required criteria and activities in combination to counter network security attacks. This combination of criteria was used to calculate the level of trust and help improve network performance. Moraly et al. [35] Focusing on the Sybil attack, which allows the adversary to compromise nodes and create illegitimate identities, they presented a Sybil attack modeling and a lightweight intrusion detection algorithm. They used artificial bee colonies for modeling, and their proposed algorithm can counter Sybil's attack in the mobile RPL protocol. In their modeling, they have considered three different types of Sybil attacks that are based on behavior. In addition, they examined the performance of RPL under attack with respect to packet delivery ratio factors, traffic control overhead, and power consumption. The Internet has provided a platform where a wide range of different devices and services can exchange information and provide different services to each other. However, the confidentiality of the information and the lack of proper security requirements in the network causes numerous attacks that endanger the security of network users. Jain, Akanksha, and Sweta Jain [36] have examined traditional methods of routing security in terms of factors such as limitations, secure routing problems, and existing techniques.

The IPv6-based RPL protocol uses DODAG (DIO) information objects to propagate routing information between network nodes. A malicious node can access these messages by eavesdropping and sending them over and over again at different times on the network. Verma A, Ranga V [37] introduced an intrusion detection system called CoSec-RPL to prevent this attack. A non-fake copy attack can significantly increase the average delay and packet delivery on the network. But the authors show that their proposed method is not only resistant to attacks, but can also effectively reduce network power consumption and add overhead to nodes. Due to the compactness of the 6LoWPAN and RPL protocols, several attacks, including wormhole, blackhole, sinkhole, Sybil, rank, selective forwarding, and various denial of service attacks, put them at risk. V. Neerugatti et al. [38] proposed a multi-diagnostic scheme to secure these protocols and reduce attacks. The proposed design is based on artificial intelligence, which used the ContikiCooja simulator implemented with Sky motes to implement its design. Patel et al. [39] focus on selective transmission attacks and increase the security of the RPL protocol by providing a method in which a reputation-based mechanism is embedded in the RPL routing protocol. The reputation

criterion in the method presented by them is calculated by evaluating the behavior of the node in the Internet of Things. This behavior is based on sending node data in the network, which evaluates the actual and estimated number of lost packets. The calculated reputation value is used to select the parent in the network. IoT network security is an important issue and due to the scalability of this network, so-called security mechanisms such as encryption techniques, key management, intrusion detection system, and anomaly detection have many challenges to implement. Prathapchandran et al. [40] Using the trust mechanism, they presented a lightweight approach that can be effective in ensuring IoT security. In their method of targeting network malicious nodes, they have used random forest (RF) and mental logic (SL). Agiollo, Andrea, et al. [41] Introduced an intrusion detection system (IDS) to reduce RPL overhead and energy consumption. Their proposed method, called DETONAR - Detector of Routing Attacks in RPL, uses a combination of signature and expression anomalies to detect illegal behavior in the network. In addition, they used RADAR - Routing Attacks Dataset for RPL to evaluate their intrusion detection system.

Iii. Proposed Schema

Numerous studies have been conducted on the security of the RPL and network routing protocols as well as the IoT, and have shown that weak devices with limited resources have created many security problems for the IoT network and the network routing protocol. As mentioned in the previous sections, RPL has a vulnerable nature that provides the right conditions for all types of network attacks. One of the most important issues that have weakened this routing protocol is the lack of an authentication mechanism and the use of symmetric encryption for the entire network.

In this part of the article, we present a robust authentication protocol with a key exchange mechanism to secure the RPL protocol based on our RPL security reviews. In our proposed method, we have used ECC techniques and theories that are compatible with the resource quality of weak IoT devices. The proposed method consists of two phases, the registration phase in which each node must be entered by a node to enter the network. Do parent or Root. This phase verifies the authorized identity of each network node.

The second phase, which is authentication and key exchange, is a process for this phase in which two related entities, in addition to being able to generate different encryption keys for each session, authenticate each other with private parameters. Table 2 explains the definition of the parameters used in the proposed protocol.

Table 2
describes the parameters used in the proposed protocol.

Symbol	Definition
ID	Nod Identity
PU	Public Key
PV	Private Key
$d_i,f_i,e_i,a_i,b_i,g_i,c_i,z_i,l_i$	Random Numbers
H	Hash Function
P	Base Point
AC	Authentication Certificate
SK	Session Key
E	Encrypt by Symmetric Key

A. Registration phase

The first step of the proposed protocol is the registration phase, in which any node intending to enter the network must do at least one of these steps. If a node is completely out of the network for a long time, it must also go through the registration phase again to enter the network. In the first step, the node selects two random numbers c_i and l_i. The next step produces the value N_i, which is an anonymous type of node private key. The reason for producing this parameter is that it is used in generating the Authentication Certificate parameter and is a step of authentication based on the private parameters of both parties to the entity. In addition, it helps the protocol withstand the Forgery of identity attacks.

(1) $N_i = H((PV_{node} * c_i) || l_i)$

In the last step of this phase, the node sends the value N to Root with its public key.

Root selects the random numbers a_i and b_i in the first step after receiving the parameters sent by the node. After selecting random numbers, it generates an anomaly from its private key, which stores its value in T_i. This technique of generating anonymity from the private keys of communication institutions helps us, in addition to using the features of private keys, to maintain their security in the absence of disclosure and accessibility of network attackers. In the next step, the Root entity generates an Authentication Certificate (Parameter AC) for the node using its private parameters and the node (N_i and T_i). This certificate is for nodes only and this value is different for each node because it uses the private key of each node in its production. Figure 2 illustrates the registration process and the values used in the registration process.

B. Authentication and key exchange phase

In this stage, which includes 3 steps, the communication parties exchange parameters to authenticate each other and securely generate the Session key.

Step 1:

In the proposed protocol is the start of communication with the node. For this purpose, the node first generates random numbers d_i, e_i, and f_i. The next step is to use node private parameters to authenticate as well as prevent attackers from forging attacks. For this operation, we use the private key of the node. But for the security of the private key, it should not be used directly in the production of parameters, and therefore we use anonymity techniques or generate a root of the private key. To implement this technique, we used a combination of random numbers and a private key. The parameter U_i is the result of this combination, which is calculated as follows.

(1) $U_i = H((PV_{node} * d_i) || e_i)$

In the third act of this step, the node produces parameter A, which is the product of the scalar multiplication of the random number f and the base point. This parameter is used in generating the session key and is also effective in the protocol authentication mechanism. After generating parameter A, we need to create multiple authentication mechanisms as well as a process to ensure the accuracy of the values received on the root side, and for this purpose, we generate parameter S as follows.

(2) $S = H(AC || U_i || A)$

At the end of the node, it encrypts the parameters S, A, and U_i with the symmetric key received from Root during the registration step and sends them to the Root entity.

Step 2:

In this step, the Root entity receives the encrypted message by the node, which carries the parameters S, A, and U_i. In the first step, Root examines the freshness of the message by calculating the value of $\Delta T=|T_2 - T_1|$. Checking the freshness of the message is done to prevent Send repetitive messages and reply attacks. After checking the freshness of the message, it is necessary to check the node identity and its sent parameters. For this purpose, Root calculates the value of S' and compares it with the parameter S sent by the node. Any changes in the parameters will cause a non-equality of the parameter calculated by the root and the value received from the node, which mismatch is a reason for the disconnection between communication entities. If the values are equal, which means the information is correct, the root will continue the protocol process. After verifying the information, Root selects a random number g and generates the session key as follows.

(1) $SK = H(AC || S ||R || g_i.A)$

After calculating the session key, the Root entity generates a value R to authenticate itself and verify the sent parameters by the node. Finally, it sends a message encrypted with a symmetric key that contains the parameters R and g_i .p to the node.

(2) R = H(S || SK || AC)

Note

The values A and g_i .p play a role in generating the session key and these points are sent encrypted in the channel. But it is noteworthy that if under certain conditions the network symmetric key is exposed and the points A and g_i .p are in the possession of the attacker, according to the ECDH theorem described in the concepts section, it will not be possible to calculate g_i .f_i .p. In addition, these points play an important role in the identification of entities.

Step 3:

This is the last step in the authentication and key agreement process. The node first examines the freshness of the message by calculating $\Delta T=|T_2 - T_1|$. If not new, disconnect. The next step for the node is to authenticate the Root node and its submitted parameters. For these operations, it first generates the session key node and calculates the value of R' after generating the session key. How to calculate the parameters is as follows.

(1) SK' = H(AC || S || R || g_i.f_i.p)

(2) R' = H(S || SK' || AC)

The parameter AC is generated for the node at the registration stage, and S is generated by the node itself. The node generates the session key using the parameters it has and is sent by Root, and then generates the R' parameter. Now it is time to check the accuracy of the parameters and root authentication, which is done by checking the two values of R' and R. If these two values are equal, it means that the information sent is correct and the sender of the information is Root, otherwise the connection will be lost. Finally, by confirming the accuracy of the information, the value of the generated SK is selected as the session key. Figure 3 shows the authentication process and key-agreement process of the proposed schema.

Iv. Security Analysis Of The Proposed Scheme

In this part of the article, we have reviewed the security of our proposed method, which we have formally and informally evaluated. To prove the security of the private parameters used in the protocol, as well as the types of active and passive network attacks, we have implemented the proposed protocol with the official AVISPA tool, which is to check the security of the protocol. In addition, in the informal analysis

section, we introduce the common types of network attacks and state that the proposed protocol is safe against these attacks.

A. Informal review of the proposed protocol security

Reply attack

This attack can be introduced as one of the most common network attacks. In this attack, the adversary reaches the messages and packets sent on the network and steals them for himself. It then sends these packets frequently over the network at other times. This iteration and delay that occurs in sending can be done by the sender or network nodes. In the proposed protocol to prevent this attack, two factors are considered to check the novelty of the message and random numbers. As stated in the protocol process description section, communication entities first send a message with the value Receives $\Delta T = | T2 - T1 |$ examine. If the incoming message is not fresh, the connection will be lost. In addition, the random numbers used to generate the parameters make a difference in each session, which prevents the duplication of messages and parameters.

Impersonation Attack

This attack helps the adversary in the network to identify itself as an authorized node and to be able to communicate with other nodes in the network. To prevent this attack, we have used multiple authentication mechanisms and private parameters in the proposed protocol. For multiple authentications, we have considered the S and R parameters, which are used by both parties to the authentication. In addition, in the registration section, we have considered the AC parameter, which is unique to each authentication node and is used in the production of authentication parameters and session keys. It is important to note that the AC parameter is never sent to the channel during the phase-authentication and key exchange process. The strongest parameter we have considered for authentication is points A and g_i .p, which according to the ECDH theorem, it is not possible to reach the session key even with the exposure of points. Because they are incalculable and the correct calculation of the session key can only be done by an authenticated and authorized entity.

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 implementation of this attack, the user does not notice it and it leads to misuse of the user's information. The attacker's goal of the Man-in-the-Middle attack is to gather 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 for information encryption. The selected symmetric encryption key is the X dimension of the N parameter. One of the notable features of the

symmetric key selection in the presented protocol is that random numbers are used to generate N, which makes the selected symmetric-key unique in each connection. This key is different in each session, which makes it impossible for an attacker to obtain or even calculate the symmetric encryption key.

Session Key Computation Attack

In this attack, the attacker tries to calculate the session key generated by the communication parties. In the presented protocol, the session key is calculated as follows.

$SK = H(AC \,||\, S \,||\, R \,||\, g_i.f_i.p)$

ECDH theory, random numbers, and the private key of the communication parties are used to generate the session key. According to the ECDH theorem, even with the values of f_i. p and g_i. p, the attacker cannot calculate $g_i.f_i.p$. The presence of random numbers makes the values of S and R to be completely different in each connection. In addition, in generating the mentioned parameters, the private key of the communication parties has been used along with its combination with random numbers, which makes it impossible for the attacker to access. The proposed protocol is resilient against session key computation attacks.

Perfect Forward Secrecy

This security feature is very important in authentication and key agreement protocols, and every protocol must have this feature to be able to protect session keys and private parameters. In addition, the Perfect Forward Secrecy feature creates different session keys with no connection between the keys of each session. In the proposed method, random numbers are used to implement this feature and create conditions for generating parameters whose value in each session is different from the previous session. This factor helps the protocol to generate the session keys in each entity relationship that are completely different and independent. Therefore, if the attacker obtains the keys generated in previous sessions under certain conditions, he/she will not be able to calculate the key and create a connection between the keys of the session.

Selective Forwarding Attack

This attack is one of the common attacks of RPL routing protocol, the attacker captured the sent packets in the network and resends them selectively. The first security factor needed to prevent this is the authentication mechanism to prevent malicious nodes from operating on the network. As previously described, the proposed protocol is implemented by multiple authentication mechanisms. But certain circumstances may arise where an attacker has the opportunity to send a message on the network and intend to implement a Selective Forwarding Attack on the network. The protocol presented in each step first examines the freshness of the message and also uses random numbers in the protocol process. Therefore, it allows communication entities to identify duplicate and outdated messages and disconnect them.

Secure against the DOS attack

This attack helps the attacker send repeated and consecutive messages on the network or a specific node. The purpose of this attack is to disable the network, reduce performance and cause latency in the network. To prevent this attack, in the presented method, random numbers and also the time stamp of the recipient of the message have been used. Random numbers prevent messages from being duplicated, and the time stamp allows the recipient to recognize the allowed time frame of the message.

Now, if an attacker sends duplicate messages or sends a large number of messages in the network,

The recipient of the message first notices the duplicate message because he has already received it. Also, by calculating ΔT, the receiver realizes that the sent message is related to the past and disconnects the connection.

B. Result and Formal Analyze

In this section, we have formally analyzed our proposed method. To formally check security, we have used AVISPA software, which is a reliable tool for evaluating security and analyzing Internet security protocols. It uses an automated security analysis system and esoteric servers such as On-the-Fly Modeler (OFMC) and Constraint-Logic (Cl-AtSe). In addition, AVISPA can evaluate protocols under various attacks. Given the 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 [42]. Figure 4 shows the results of security checks on the AVISPA tool.

The formal evaluation and the results of Fig. 4 show that the proposed method can resist all types of active and passive network attacks. The AVISPA tool has two outputs, OFMC and CL-ATSE, which indicate that the private parameters used in the protocol are protected and cannot be accessed and calculated by network attackers.

V. Performance Evaluation

A. COMPUTATION COSTS COMPARISON

As mentioned in the previous sections, IoT network nodes have limited resources, so RPL requires a security mechanism that has a less computational cost. In this section, we have calculated the time complexity of the proposed method for the authentication and key exchange process. In addition in Table 4, we have compared our proposed protocol with other IoT network security protocols in terms of computational cost. To implement the results, a system with a 2.20 GHz Intel Pentium E2200 processor, and 2 GB of RAM is considered. According to the report in [43–44], the time of performing different operations for each cryptographic element is shown in Table 3.

Table 3
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

Table 4
Extensive comparison of the related protocols.

	Computations	Computational cost (ms)
Ashok Kumar, et al. [45]	$7T_M + 6T_H + 3T_A$	15.6822
Ming, et al [46]	$3T_M + 4T_P + 4T_H + T_A$	29.96
Li, Fagen [47]	$3T_M + 5T_P + 2T_H + 2T_A$	35.7952
Majumder. et al. [48]	$5T_H + 6T_M + 4T_{SE}$	13.3859
Dey, S. and Hossain, A [49]	$6T_H + 4T_E + 6T_{SE}$	15.41656
Gupta, Daya Sagar, et al. [50]	$3T_M + 2T_p$	18.3
Safkhani, Masoumeh, et al.[51]	$9T_M + 10T_H$	20.057
Nikravan et al. [52]	$23T_H + 10T_M + 4T_p$	45.5569
Vinoth et al. [53]	$12T_H + 2T_P + 4T_{SE} + 2T_M$	16.12
Proposed Protocol	$3T_M + 7T_H + 2T_{Se}$	6.703

The results of the data in Table 4, which compares our proposed protocol with other IoT protocols in terms of computational cost, show that our proposed method has much less time than other protocols.

Since IoT network nodes have limited resources and less power, they need security mechanisms that do not spend a lot of energy when calculating protocol operations when routing by RPL protocol. Therefore, our proposed method, which takes less computation time to perform authentication and key agreement operations, is more suitable and compatible for RPL network nodes.

B. COMMUNICATION COSTS COMPARISON

In this section, the communication cost of the proposed protocol is compared with other related protocols. 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 [45]. In the presented protocol, two messages (MSG_1 = E {S, A_1, U} MSG_2 = E {R, g_i.p}) are exchanged and their communication cost are as follows.

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

Table 5
Comparison of communication costs.

Protocol	No. of Messages	Total Cost in bit
Ashok Kumar, et al. [45]	3	3296
Ming, et al [46]	2	3040
Li, Fagen [47]	2	3488
Majumder. et al. [48]	5	1312
Safkhani, Masoumeh, et al. [51]	3	1728
Vinoth et al. [53]	4	2336
Proposed Protocol	2	1120

Table 5 compares the communication cost of the proposed protocol with other related protocols. As can be seen, the communication cost of the proposed method is lower compared to other related methods. This low communication cost reduces overhead and lower energy consumption, which makes the proposed protocol more compatible with IoT nodes with limited computing resources.

Vi. Conclusion

The Internet of Things is a global infrastructure that supports a variety of standard communication protocols. In addition, its features and capabilities provide the conditions for its use in a wide range of services. Examples include healthcare, smart cities, smart homes, and industrial environments. This breadth of services has made the network an important target for network attackers. On the other hand,

resource and computational constraints have created vulnerabilities for some elements of this network, most of which can be seen in the Routing Protocol (RPL). In this article, we tried to address the security challenges and vulnerabilities of IoT, especially RPL. Finally, we proposed a scheme to cover RPL vulnerabilities under limited node conditions. Formal and informal reviews that assessed the security of the proposed method show that the proposed protocol has been able to provide security against a variety of network attacks and cover RPL vulnerabilities. In addition, due to the low energy of RPL nodes, the proposed protocol had the lowest computational time compared to other proposed protocols.

Declarations

Compliance with Ethical Standards

We acknowledge that:

- All authors have participated in (a) conception and design, or analysis and interpretation of the data; (b) drafting the article or revising it critically for important intellectual content; and (c) approval of the final version.
- This manuscript has not been submitted to, nor is under review at, another journal or other publishing venue.
- The authors have no affiliation with any organization with a direct or indirect financial interest in the subject matter discussed in the manuscript

Author's name	Affiliation
Ali Peivandizadeh	Graduated Student Technology Project Management University of Houston
Behzad Molavi	Department of Computer Engineering, Vahdat Institute of Higher Education, Torbat-e Jam, Iran

Research Data Policy and Data Availability Statements :

"Data sharing not applicable to this article as no datasets were generated or analysed during the current study."

References

1. Harb, Hassan, et al. "Wireless sensor networks: a big data source in internet of things." International Journal of Sensors Wireless Communications and Control 7.2 (2017): 93-109.
2. Darabkh, Khalid, and Ramazan Aygün. "TCP traffic control evaluation and reduction over wireless networks using parallel sequential decoding mechanism." EURASIP Journal on Wireless Communications and Networking 2007 (2007): 1-16.

3. Iova, Oana, et al. "Rpl: The routing standard for the internet of things... or is it?." IEEE Communications Magazine 54.12 (2016): 16-22.
4. Al-Zubi, Raed, et al. "Markov-based distributed approach for mitigating self-coexistence problem in IEEE 802.22 WRANs." The Computer Journal 57.12 (2014): 1765-1775.
5. 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.
6. Pavkovic, Bogdan, et al. "Efficient topology construction for RPL over IEEE 802.15. 4 in wireless sensor networks." Ad Hoc Networks 15 (2014): 25-38.
7. Ma, Huadong, et al. "On networking of internet of things: Explorations and challenges." IEEE Internet of Things Journal 3.4 (2015): 441-452.
8. Darabkh, Khalid A., et al. "EA-CRP: a novel energy-aware clustering and routing protocol in wireless sensor networks." Computers & Electrical Engineering 72 (2018): 702-718.
9. Kobo, Hlabishi I., Adnan M. Abu-Mahfouz, and Gerhard P. Hancke. "A survey on software-defined wireless sensor networks: Challenges and design requirements." IEEE access 5 (2017): 1872-1899.
10. Zarpelão, Bruno Bogaz, et al. "A survey of intrusion detection in Internet of Things." Journal of Network and Computer Applications 84 (2017): 25-37.
11. Lin, Jie, et al. "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications." IEEE internet of things journal 4.5 (2017): 1125-1142.
12. T. Tsao, R. Alexander, M. Dohler, V. Daza,A Lozano, and M. Richardson, A Security ThreatAnalysis for Routing Protocol for Low-power and Lossy Networks (RPLs), RFC 7416, Internet Engineering Task Force, 2015.
13. 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.
14. Moghadam MF, Nikooghadam M, Al Jabban MA, Alishahi M, Mortazavi L, Mohajerzadeh A. An efficient authentication and key agreement scheme based on ECDH for wireless sensor network. IEEE Access. 2020 Apr 13;8:73182-92.
15. J. H. Silverman, The arithmetic of elliptic curves. Springer Science & Business Media, 2009.
16. Shakhatreh, Hazim, et al. "Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges." Ieee Access 7 (2019): 48572-48634.
17. Adat, Vipindev, and Brij B. Gupta. "Security in Internet of Things: issues, challenges, taxonomy, and architecture." Telecommunication Systems 67.3 (2018): 423-441.
18. Winter, Tim, et al. RPL: IPv6 routing protocol for low-power and lossy networks. No. rfc6550. 2012.
19. D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," Computer Networks, vol. 141, pp. 199-221, 2018.
20. A. Mayzaud, R. Badonnel, and I. Chrisment, “A taxonomy of attacks in rpl-based internet of things,” International Journal of Network Security, vol. 18, no. 3, pp. 459–473, 2016.

21. B. N. Silva, M. Khan, and K. Han, "Internet of Things: A Comprehensive Review of Enabling Technologies, Architecture, and Challenges," IETE Technical Review, Review Article vol. 35, no. 2, pp. 205-220, 2018.
22. D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for internet of things: A survey," Journal of Network and Computer Applications, vol. 66, pp. 198-213, 2016.
23. P. O. Kamgueu, E. Nataf, and T. D. Ndie, "Survey on RPL enhancements: A focus on topology, security and mobility," Computer Communications, vol. 120, pp. 10-21, 2018.
24. A. Kamble, V. S. Malemath, and D. Patil, "Security attacks and secure routing protocols in RPL-based Internet of Things: Survey," presented at the 2017 International Conference on Emerging Trends & Innovation in ICT (ICEI), Pune, India, 3-5 February, 2017.
25. 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 Proceedings of the 6th International Conference on Computing & Informatics, Kuala Lumpur, Malaysia, 2017, pp. 735-743.
26. D. Airehrour, J. Gutierrez, and S. K. Ray, "Securing RPL routing protocol from blackhole attacks using a
trust-based mechanism," presented at the 2016 26th International Telecommunication Networks and Applications Conference (ITNAC), Dunedin, New Zealand, 7-9 December, 2016.
27. Rubio JE, Alcaraz C, Roman R, Lopez J. Current cyber-defense trends in industrial control systems. Computers & Security. 2019 Nov 1;87:101561.
28. Airehrour, David, Jairo Gutierrez, and Sayan Kumar Ray. "A trust-aware RPL routing protocol to detect blackhole and selective forwarding attacks." Journal of Telecommunications and the Digital Economy 5.1 (2017): 50-69.
29. Tomić, Ivana, and Julie A. McCann. "A survey of potential security issues in existing wireless sensor network protocols." IEEE Internet of Things Journal 4.6 (2017): 1910-1923.
30. D. Shreenivas, S. Raza, and T. Voigt, “Intrusion Detection in the RPL-connected 6LoWPAN Networks” In Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security (IoTPTS ’17), USA, 2017, pp. 31-38.
31. Alzubaidi M, Anbar M, Chong YW, Al-Sarawi S. Hybrid monitoring technique for detecting abnormal behaviour in rpl-based network. J. Commun.. 2018 Oct;13(5):198-208.
32. [32] R. Mehta, M.M. Parmar, Trust based mechanism for Securing IoT Routing Protocol RPL against Wormhole & Grayhole Attacks, in: 2018 3rd International Conference for Convergence in Technology (I2CT), 2018.
33. D Airehrour, J.A. Gutierrez, SK Ray, SecTrust-RPL: a secure trust-aware RPL Routing protocol for Internet of Things, Future Gener. Comput. Syst. (2018), https://doi.org/10.1016/j.future.2018.03.021.
34. 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.

35. Murali, Sarumathi, and Abbas Jamalipour. "A lightweight intrusion detection for sybil attack under mobile RPL in the internet of things." IEEE Internet of Things Journal 7.1 (2019): 379-388.
36. Jain, Akanksha, and Sweta Jain. "A survey on miscellaneous attacks and countermeasures for RPL routing protocol in IoT." Emerging Technologies in Data Mining and Information Security. Springer, Singapore, 2019. 611-620.
37. Verma, Abhishek, and Virender Ranga. "CoSec-RPL: detection of copycat attacks in RPL based 6LoWPANs using outlier analysis." Telecommunication Systems 75.1 (2020): 43-61.
38. Neerugatti, Vikram, and A. Rama Mohan Reddy. "Artificial intelligence-based technique for detection of selective forwarding attack in rpl-based internet of things networks." Emerging Research in Data Engineering Systems and Computer Communications. Springer, Singapore, 2020. 67-77.
39. Patel, Anshuman, and Devesh Jinwala. "A reputation-based RPL protocol to detect selective forwarding attack in Internet of Things." International Journal of Communication Systems 35.1 (2022): e5007.
40. Prathapchandran, K., and T. Janani. "A trust aware security mechanism to detect sinkhole attack in RPL-based IoT environment using random forest–RFTRUST." Computer Networks 198 (2021): 108413.
41. 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.
42. AVISPA. Automated Validation of Internet Security Protocols. Available: www.avispa-project.org. (Accessed 1 April 2016).
43. [43] Moghadam MF, Nikooghadam M, Mohajerzadeh AH, Movali B. A lightweight key management protocol for secure communication in smart grids. Electric Power Systems Research. 2020 Jan 1;178:106024.
44. [44] Farhdi Moghadam M, Mohajerzdeh A, Karimipour H, Chitsaz H, Karimi R, Molavi B. A privacy protection key agreement protocol based on ECC for smart grid. InHandbook of Big Data Privacy 2020 (pp. 63-76). Springer, Cham.
45. Das AK, Wazid M, Yannam AR, Rodrigues JJ, Park Y. Provably secure ECC-based device access control and key agreement protocol for IoT environment. IEEE Access. 2019 Apr 24;7:55382-97.
46. Luo, Ming, et al. "Secure and efficient access control scheme for wireless sensor networks in the cross-domain context of the IoT." Security and Communication Networks 2018 (2018).
47. Li, Fagen, Yanan Han, and Chunhua Jin. "Practical access control for sensor networks in the context of the Internet of Things." Computer Communications 89 (2016): 154-164.
48. Majumder, S., Ray, S., Sadhukhan, D. et al. ECC-CoAP: Elliptic Curve Cryptography Based Constraint Application Protocol for Internet of Things. Wireless Pers Commun 116, 1867–1896 (2021). https://doi.org/10.1007/s11277-020-07769-2
49. Dey, Shreya, and Ashraf Hossain. "Session-key establishment and authentication in a smart home network using public key cryptography." IEEE Sensors Letters 3.4 (2019): 1-4.

50. Gupta, Daya Sagar, et al. "A provably secure and lightweight identity-based two-party authenticated key agreement protocol for IIoT environments." IEEE Systems Journal 15.2 (2020): 1732-1741.
51. Safkhani, Masoumeh, et al. "RESEAP: an ECC-based authentication and key agreement scheme for IoT applications." IEEE Access 8 (2020): 200851-200862.
52. Nikravan, Mohammad, and Akram Reza. "A multi-factor user authentication and key agreement protocol based on bilinear pairing for the internet of things." *Wireless Personal Communications* 111.1 (2020): 463-494.
53. Vinoth, R., and Lazarus Jegatha Deborah. "An efficient key agreement and authentication protocol for secure communication in industrial IoT applications." *Journal of Ambient Intelligence and Humanized Computing* (2021): 1-13.

Figures

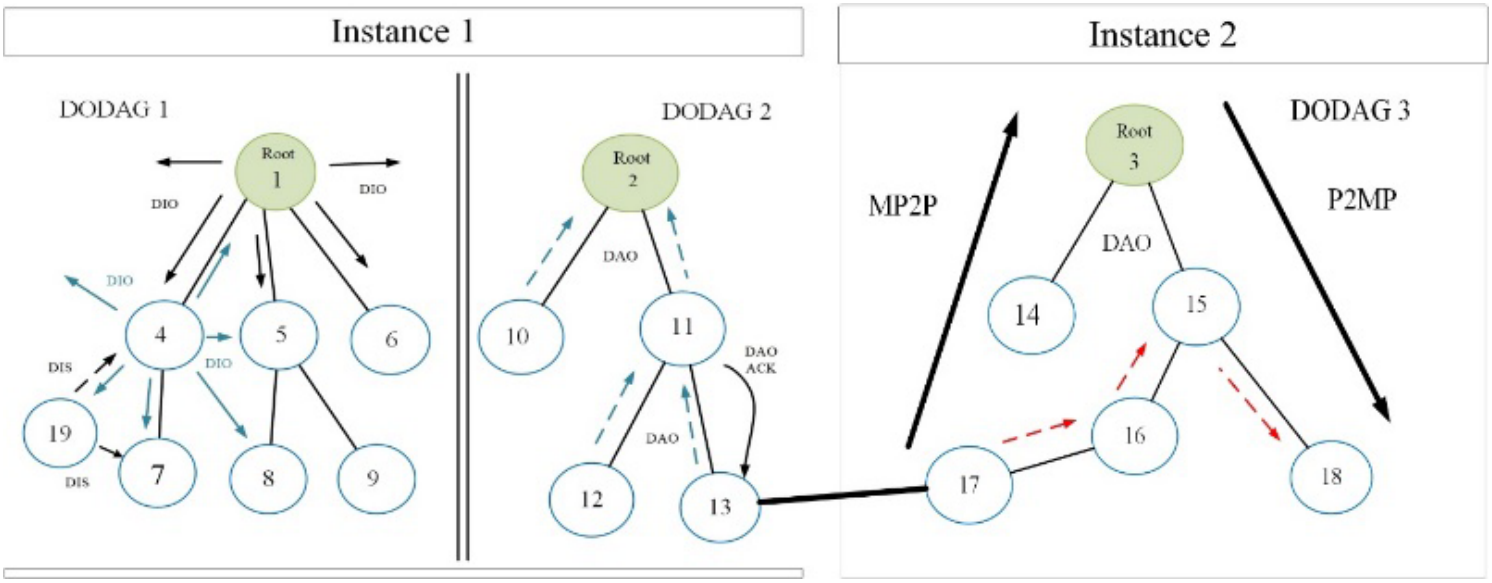

Figure 1

Two instances of RPL network and three DODAG

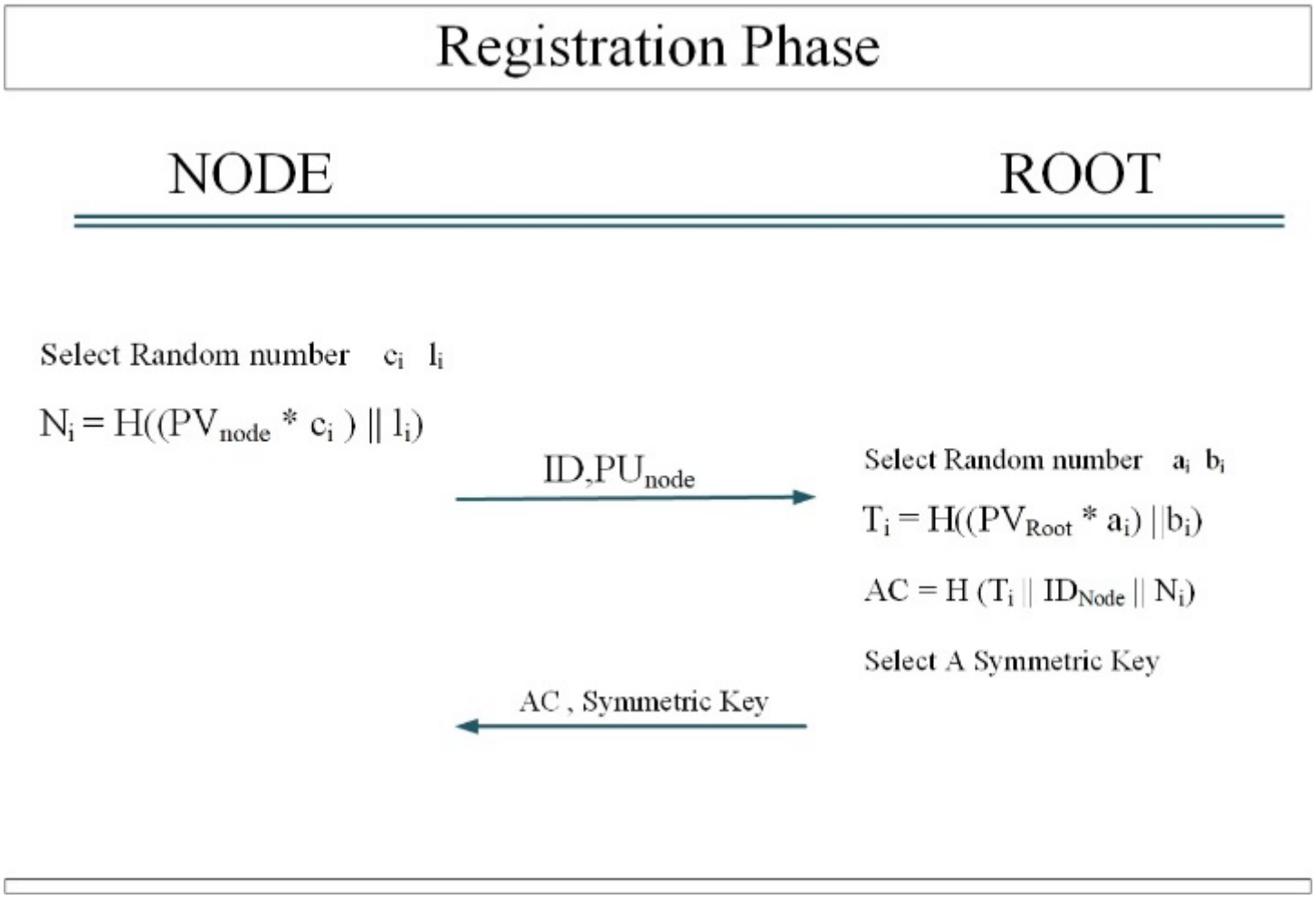

Figure 2

Registration phase

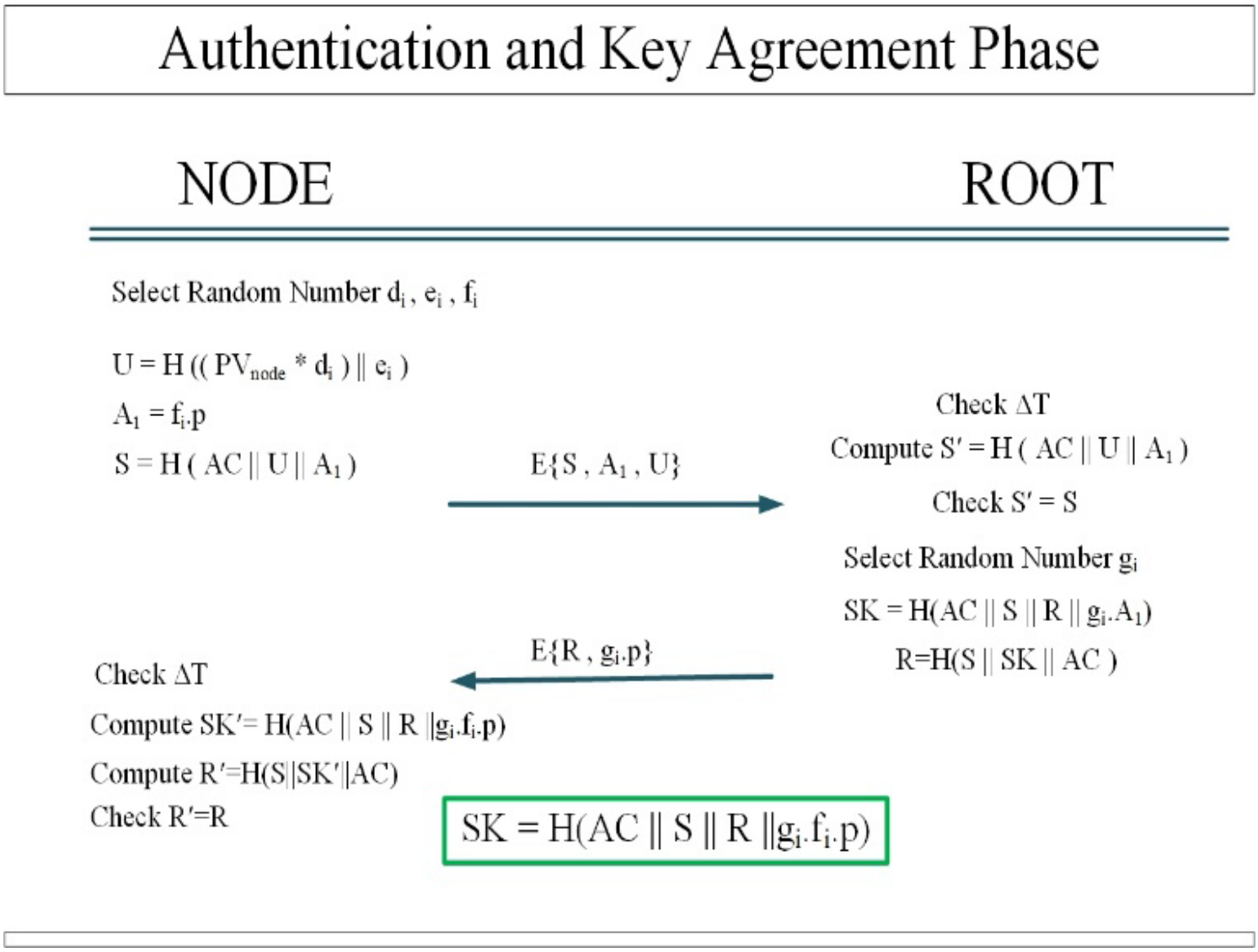

Figure 3

Authentication and key agreement phase

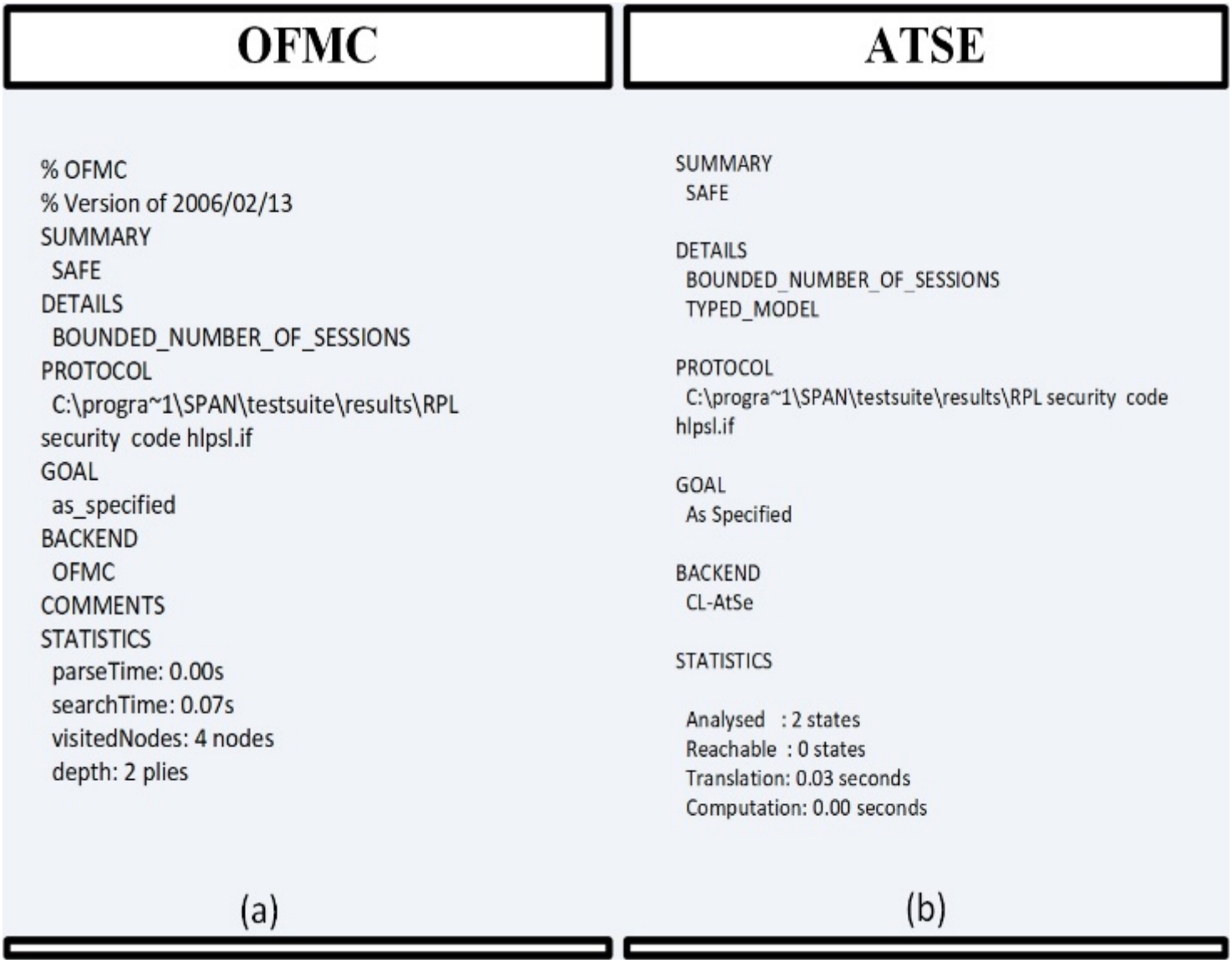

Figure 4

AVISPA results. (a) OFMC (b) ATSE