I. J. Computer Network and Information Security, **2021, 2, 29-38**
Published Online April 2021 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2021.02.03

An Optimized Protocol of M2M Authentication for Internet of Things (IoT)

Mohamed M. Samy
Military Technical College/Electrical Engineering Department, Cairo,11571, Egypt
E-mail: m.samy1880@yahoo.com

Wagdy R. Anis.
Ain shams university/Electrical Engineering Department, Cairo,11571, Egypt
E-mail: wagdyanis51@yahoo.com

Ahmed A. Abdel-Hafez and Haitham D. Eldemerdash
Military Technical College/Electrical Engineering Department, Cairo,11571, Egypt
E-mail: aabdelhafez@gmail.com, dr.hdawood80@gmail.com

Received: 16 November 2020; Revised: 16 January 2021; Accepted: 25 February 2021; Published: 08 April 2021

Abstract: The Internet of Things (IoT) consists of sensors, networks, and services to connect and control production systems. Machine-to-Machine (M2M) communication technology is considered as a key underlying technology for building Industrial IoT environments where devices are enabled to exchange information with each other in an autonomous way without human intervention. Resource-Constrained Devices (RCD) have found an expanding demand in the Internet of Things (IoT) applications as these gadgets are essentially working with delicate information. Thus, information security has ended up vital for both makers and clients. However, the creation of defenseless gadgets still challenging regarding the restriction of involved assets especially with the attackers ‘continuous trials to misuse these restrictions chasing important information. Hence, connecting an open key crypto-system becomes a must to extend gadget proficiency and relieve the chance of touchy data loss. Deployments of Elliptic curve cryptography (ECC) are fundamentally an open key crypto-system with the basic distinction of speedier advancing capacity whereas yielding an assortment of distinctive approaches to the arrangement of the cryptographic calculation. We will submit a proposed protocol to overcome the demands of information security and the speed of data circulation. The proposed protocol is characterized by low computational cost, communication and storage overhead, while achieving mutual authentication, session key agreement, device’s identity confidentiality, and resistance against various attacks.

Index Terms: Resource-Constrained Devices (RCD), Automated Validation of Internet Security Protocols and Applications tools(AVISPA), Internet of Things (IoT), Elliptic curve cryptography (ECC), Public Key Cryptography (PKC).

1. Introduction

Internet of Things is characterized as the next revolutionary development layer of information technologies fields after computer, Internet, and mobile telephone communication. IoT is already encountered in each activity field of our daily lives [1]. IoT has changed the life of human beings. Enormous increase in users of Internet and modifications on the internetworking technologies enable networking of everyday objects. If the settings of the environment can be made to respond to human behavior automatically, then there are several advantages [2]. The Internet of things (IoT) is considered an early innovation that focuses on the inter-connection between gadgets and people or clients to attain a few collective objectives. The Internet of Things (IoT) is the means that gives the regular gadgets a method of correspondence and another route for distinguishing proof with one another. The range of (IoT) application areas is huge including e-wellbeing, keen urban communities, shrewd homes, wearable, and so on. Subsequently, billions of gadgets could be associated. The Internet of Things (IoT) is one of the most feasible advances that have met the consideration of academic approaches together with the industrial demand, where (IoT) interconnects people with the web-accessed gadgets to attain a few common objectives. Hence, (IoT) is anticipated to become consistent coordinates into our horizon and human will be subordinate on this invention to achieve consolation and modest life fashion.

In 1976 White Diffie and Martin Hellman were the pioneers to create The Diffie-Hellman key trade convention within the editorial topic "New Direction in Cryptography"[3]. In the fundamental form, it is a proficient arrangement to

This work is open access and licensed under the Creative Commons CC BY 4.0 License.

the issue of making a common mystery between two members through an in a secure channel. Since at that point a huge assortment of secure executions in the public-key cryptography has been ended utilizing elliptic curves. In 1985, Elliptic Curve Cryptography (ECC) was offered freely by Neal Koblitz, and Victor Miller operator [4]. Elliptic curve cryptography (ECC) may be an exceptionally proficient innovation to recognize public-key cryptosystems and public key infrastructures (PKI).

The role of architecture in IOT systems has very importance with respect to develop secure system because security has become a major issue, any criminal activity can be done so these systems should be made protected unethical activities [5]. The security of a public key framework utilizing elliptic curves is founded on the hardness calculation of distinct logarithms within a bunch of focuses on an elliptic bend characterized over a limited field [6]. The need for more productive calculations rises with the expanding number of memory-limited versatile electronic gadgets. The other parts of this paper are structured as follows: Section 2 discusses the related works and Section 3 discusses the resources constrained devices while Section 4 explains the elliptic curve cryptography. Section 5 represents the generic art of (IoT), and Section 6 discusses both the key security apprehensions and the security contests at the (IoT) design. Section7delivers a categorization of the current authentication structures of the proposed (IoT) system, while Section 8 is a security analysis of (IoT) authentication schemes using (AVISPA). Finally, Section 9 develops the conclusions together with the outcomes of this work.

2. Related Works

In [7], a lightweight authentication protocol for Machine to Machine (M2M) is presented for home network services. The solution ensures various security properties such as anonymity, secure localization, and resilience to key exposures. Also, this authentication protocol requires the exchange of two messages only. However, a large number of hash operations (11) are needed to achieve mutual authentication in addition to several XOR operations. On the other hand, several authentication protocols based on Physical Layer Security (PLS) have emerged in the literature [8,9,10,11]. However, these schemes are considered insecure since they rely only on the random characteristics of wireless channels, which is not sufficient to achieve the required security level [12].

3. Resources Constrained Devices (RCD)

The implanted computational procedures conducted inside the IoT are anticipated to be resource constrained. These resource-constrained procedures were not utilized as remembrance and handling abilities, but the low-power radio guidelines connected advanced oblige the organize interfacing. Numerous (IoT) gadgets are assets obliged, as prepared with a restricted sum of memory, computing, and vitality resources. Embedded gadgets connected within the (IoT) require displaying computational capabilities for the assignment they ought to execute and organizing capabilities permitting integration with the Internet. (IoT) devices are probably prepared through the low power implanted computational gadgets, to play down item costs. The building up of any organizing advances combined with resource-constrained devices becomes a must regarding the remembrance restraints. In this case, a negligible IP-based protocol structure should be proposed to successfully oversee the (IoT). Additionally, a critical analysis of the uncovered least characteristic set is required to keep the protocols recognizable either individually or accompanied with the existing instruments, therefore empowering genuine interoperability, whereas still being utilitarian on resource-constrained devices [13].

4. Elliptic Curve Cryptography

ECC is public decoding tool that develops both communal and secretive keys to enable the certification process. ECC, which is commonly well-known as a category of the PKC, is fundamentally constructed based on the elliptic logarithmic structure. The trouble of the elliptic bend discrete logarithm issue (ECDLP) represents a primary part within the ECC confidence nature, which could be manipulated through the range of the exponential time. In the interim, it must be included that the execution of this calculation is primarily depended on the scalar efficacy of the execution increase calculation. The Hamming weight could be a secretive basic figure in calculation adequacy concerning the calculation level scalar number juggling. Hamming weight is a well-known tool to implya scalar illustration of the non-zero digits, where the haste of the scalar increase execution improves with the decrease in the degree of Hamming weight. In like manner, a scalar cryptography strategy could be utilized to control the Hamming weight [14]. The algebraic nonsingular relationship of the elliptic curve (E) over a finite field could be generalized through the Weierstrass equation [15]:

$$E: \{(x,y)|y^2+\alpha_1 xy+ \alpha_3 y-x^3-\alpha_2 x^2- \alpha_4 x- \alpha_6=0\}U\{0\} \quad (1)$$

Whereα_1, α_2, α_3, α_4, and α_6 Є E and O the point at infinity. In this paper, the work will be limited over a finite field where [k = F* p], as represented in Figure 1, as follows.

$$y^2=x^3+ax+b \tag{2}$$

Where a, b Є k and $4a_3 + 27b_2$ ǂ 0, composed with an extra point O will be known as the point at infinity.

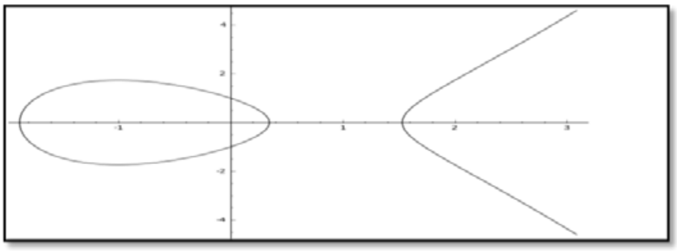


Fig.1. Graph an elliptic curve y2=x3-3x+1

5. IoT Generic Architecture

IoT features a distinctive tactic gives Machine-to-Machine (M2M) and Human-to-Machine (H2M) network, for dissimilar sorts of machines in arrange to back an assortment of uses (e.g., distinguishing, finding, following, checking, and controlling), whereas classical web interfaces individuals to a organize [16]. Interfacing several dissimilar machines [17] clues to a gigantic activity, consequently, the got to bargain with the capacity of enormous information [18, 19]. In this manner, the TCP/IP design, which is well-known for arranging networks, still unsatisfactory regarding the IoT desires concerning different viewpoints counting protection and security [20,21]. Even though various designs were projected for IoT, there are more requirements for developing reference designs [22, 23]. The fundamental design demonstrates suggested within the writing could be three-layer construction [21, 24–26], as appeared in Figure 2a. It comprises of the perception layer, the network, and the application layer.

5.1. Perception layer

It represents the mental section that faculties the atmosphere to see the surrounding properties including the temperature, location, and also moistness utilizing conclusion – hubs, through the utilize of diverse detecting innovations such as RFID, NFC, and GPS.

5.2. Network Layer

It gets information from the perception layer and then it is responsible for transmitting information to the final layer, which is the application layer, through different organize innovations (e.g., 3G, 4G, 5G, Wi-Fi, Bluetooth, Zig-Bee, etc.). It is additionally dependable of information administration from packing to preparing accompanied with the assistance of middle-wares; e.g “cloud computing”.

5.3. Application Layer

It is responsible for conveying application-specific administrations to the client. The significance of this layer is that it can cover a wide range of diverse markets [27]. Figure 2b represents an additional projected layered construction which is known as (five-layer design) [21,24–26]. The five-layer design comprises firstly of the business layer which is followed by the application layer, processing layer, and the transport layer respectively. Finally, the perception layer represents the fifth layer in this design. The role of the application layer, the transport layer, and the layer of perception is still the same as described in the three-layer design. However, the role of the other layers of the design is as follows:

5.4. Processing laye

It is also well-known as the middle-ware layer. It is capable of giving different sorts of administrations, primarily putting away, analyzing, and preparing information concerning the computed outcomes.

5.5. Business layer

It contains the generally IoT framework activities and functionality. The application layer drives the information to the commerce layer whose part is to construct commerce models, charts, and flowcharts to investigate information, in arrange to play a part in choice-making around trade procedures and roadmaps.

Other designs could also be distinguished within the writing. In [28, 29], the creators utilized a five-layer design based on Service Oriented Architecture (SOA) that makes a difference in the integration of IoT in undertaking administrations. In [30], the creators deliberated a novel non-layered approach for the five-layer design. This non-layered approach is founded upon the processing of the human brain as in the cloud architecture, fog architecture, and in the social IoT. Later on in this work, we consider the design of three-layer architecture.

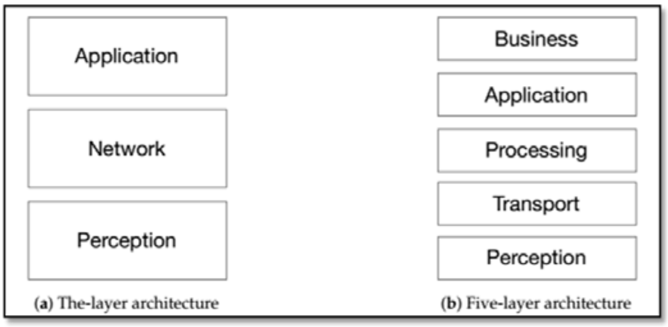


Fig.2. lot architecture models

6. Threats over Iot Layers

This part covers a different security threat that exists over a different layer of IoT as discussed in section 5 and illustrated in figure 2(a).

6.1. Perception Layer Threats

A. Tampering Node

The attacker can replace the node or can damage the sensor of the node to get access [31]. Another phase for this attack is when the device is in development the device is tempered by changing the manufacturing procedure [32]. When an attacker gets the access of node it can access the confidential information like cryptographic keys.

B. Malicious code Injection

An attacker can inject the malicious code into a node which will help him to get access to the whole network. Up-gradation of the software is the best time for the attacker to inject the code [31,33].

6.2. Network Layer Threats

A. Routing Attack

This attack is done by intermediate nodes that are malicious and can affect the whole network by just manipulating the path while data packets are being forward [31]. This attack can also change the data after manipulating the path.

B. DoS/DDoS Attack

As we know that all the devices are heterogeneous so any malicious devices can attack and made unnecessary requests to the system and make this network halt [31,32].

C. Network Injection

This attack can change the original sender with a hacker device and start sending data like it is part of the IoT network [34].

D. Man-in-Middle

All the nodes in the IoT network connect to the gateway for communication and if the gateway is in attack, then all the devices sending or receiving data are not secured [35].

6.3. Application Layer Threats

A. Data Leakage

At the application level, the security risk of data-stealing is increasing if the attacker knows the vulnerabilities of the application. This can cause the manipulating of data that is store on the cloud [31].

B. DoS/DDoS Attack

The availability of the application is destroyed by the attacker. Which will cause the network to fail and the response is not received from the application.

C. Malicious Code

If the attacker knows the vulnerability of the application, then he can upload a malicious code while up-gradation of application [31]. Like SQL Injection is the code injections in which the attacker add an extra Unnecessary field with malicious SQL query which is processed by the database. Cross-site Scripting execute the script that is malicious during the browsing the web [32].

D. Misconfiguration

IoT devices need to be properly configured with the application, if it is not configuring properly with the entire security configuration then it will cause the damage the whole Network. All the software also has to configure properly like the operating system and database system of IoT [32].

E. Sniffing Attack

A sniffer application is introducing by the attacker into the system which collects all the information from the network about the devices and communication [36].

7. Proposed Protocol

This part represents an insubstantial one-way verification and key agreement protocol based on ECDH. Our system comprises three phases: the registration phase, key Agreement phase and the text message phase.

7.1. Registration Phase

As the server is completely confidential in the framework, it is sensible to accept that the server bootstraps the entire framework. In the registration phase, the devices can register to the server via their initialization information.

Step (1), the server sends the identity to the devices (n devices).
Step (2), the devices store their identity and computes time stamp.
Step (3), the devices send their identity and time stamp to the server.
Step (4), after the server receives the identity and time stamp of the devices, the server verifies whether these identity and time stamps are legal or illegal. If they are illegal, they will be canceled. If they are legal, the identity of the device is labeled as registered. This ensures that the device's identity can only be used once and prevents illegal devices from registering to this IoT system.

Table 1. Protocol Legend

Symbol	Description	Symbol	Description
ID_S	ID for server	ID_1	ID for device 1 ....n
TS	Time Stamp	PV_S	Private Key for server
K_a	Pubic Key for server	PV_{d1}	Private Key for device 1
K_b	Pubic Key for device 1	V, V^*	Authentication Succeed
N_{S1}	Server text message	N_{D1}	Device1 text message

7.2. Key Agreement Phase

In the key agreement phase, the server Step (5), and the devices step (10), choose an elliptic curve E_G (a, b), $y^2 = x^3 + ax + b \bmod G$, where G is a generator point on E_G (a, b). The key agreement phase generates a shared key between a server and the devices. The entire key agreement process is illustrated in Figure 3.

Step (6), the server generates a private key and a public key.
Step (7), The server sends an encrypted message by Ka contain a parameter of ECDH (g, a_1, b_1), ID_S, time stamp 2 to the device 1.
Step (8), the device checks TS_2, IDS, if it illegals, it will be canceled otherwise it will begin the next step.
Step (9), the device stores K_a then it chooses the parameter of ECDH (a_2, b_2).
Step (11), the device generates a private key and a public key.
Step (12), the device sends an encrypted message by K_b contain a parameter of ECDH (a_2, b_2, ID_1, TS_3) to the server.
Step (13), the device checks ID_1, TS_3, if it illegals, it will be canceled otherwise it will begin the next step.
Step (14), the server stores K_b.
Step (15), the server computes V, then the device computes V*. The authentication between the server and the device is succeeding if V = V*.

7.3. Text Messages Phase

Step (16), the server sends an encrypted message by public key K_a contain IDs, TS_4, NS_1 (Text message encrypted by server private key PV_S) to Device1 to ask about data wanted from Device1.

Step (17), Device1 sends an encrypted message by public key K_b contain ID_1, TS_5, ND_1 (text message encrypted by device private key PV_{d1}) to the server to respond with the data wanted by the server.

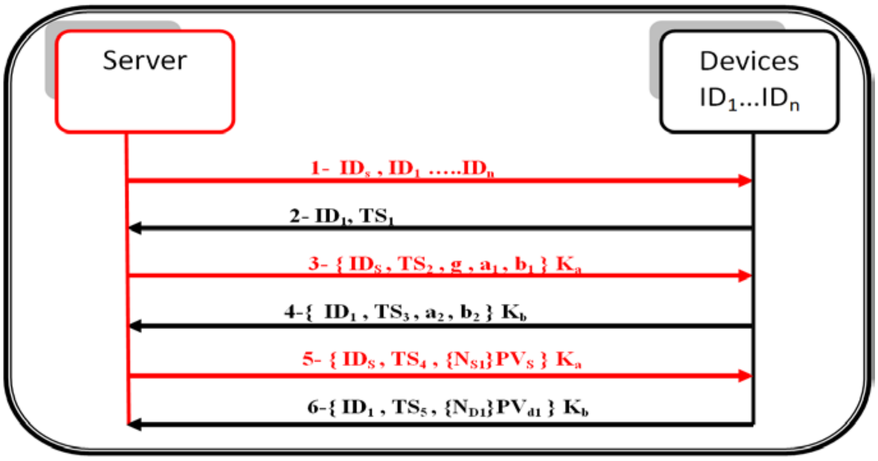

Server
Devices
$ID_1 ... ID_n$
1- ID_s , ID_1 .....ID_n
2- ID_1, TS_1
3- { ID_S , TS_2 , g , a_1 , b_1 } K_a
4-{ ID_1 , TS_3 , a_2 , b_2 } K_b
5- { ID_S , TS_4 , {N_{S1}}PV_S } K_a
6-{ ID_1 , TS_5 , {N_{D1}}PV_{d1} } K_b

Fig.3. Proposed protocol between server and devices.

7.4. Steps for the Proposed Protocol

1 - Server sends ID_S, ID_1...........IDn.
2 - Device1stores ID_S, ID_1 and generates TS_1.
3 - Device1 sends ID_1, TS_1.
4 - Server checks ID_1, TS_1. (If it refused, it canceled / if it agreed, begin step 5)
5 - Server chooses Eg(a , b) where G is generator point of Eg(a , b) [$y^2 = x^3+ax+b \bmod g$].
6 - The server generates V, K_a.
7 - Server sends {ID_S, TS_2, g, a_1, b_1} K_a.
8 - Device 1 checks TS_2, ID_S. (If it refused, it canceled / if it agreed, begin step 9)
9 - Device 1 stores K_a.
10- Device 1 chooses a_2, b_2.
11- Device 1 generates V*, K_b.
12- Device 1 sends {ID_1, TS_3, a_2, b_2} K_b.

13- Server checks ID_1, TS_3. (If it refused, it canceled / if it agreed, begin step 14)
14 - Server stores K_b.
15- $V= PV_S * K_b$ $\quad V^*= PV_{d1} * K_a$
$= PV_S * PV_{d1} * g = PV_{d1} * PV_S * g$

$V = V^*$
Authentication Succeed

16 - Server sends {ID_S, TS_4, {NS_1} PV_S} K_a.
17 - Device1 sends {ID_1, TS_5, {ND_1} PV_{d1}} K_b.

8. Security Analysis

This section presents the attack model to appear the capabilities of the foe; formal security confirmation utilizing Automated Validation of Internet Security Protocols and Applications (AVISPA) tools to appear the proposed convention is secure against different assaults additionally analyzes diverse security qualities related to the proposed convention by the casual security investigation.

8.1. Attack model

Security is attracting an increasing demand day by day concerning the IoT design. As a result, designing attack-free IoT devices became challenging to improve design security levels, and thus expanding their applications. To achieve this goal, the following issues should be addressed:

A. *Denial-of-Service attack*

A challenger could interrupt the network by over-burdening with the junk messages to corrupt the execution of the network. This will offer assistance to the enemy to create the assets inaccessible to the expecting clients.

B. *Eavesdropping attack*

A challenger could be caught the messages and examined the progressing communication between the embedded device and cloud server. In this way, the foe may store the data and utilize that to unveiling the eavesdropping attack.

C. *Password guessing attack*

Through utilizing offline dictionary assault, an enemy can attempt to figure the secret word of the legitimate gadget to create attainable the assault.

D. *Impersonation attack*

Through directing the substantial messages of the past communications within the valid entities, a foe can imitate as a lawful gadget.

E. *Man-in-the-middle attack*

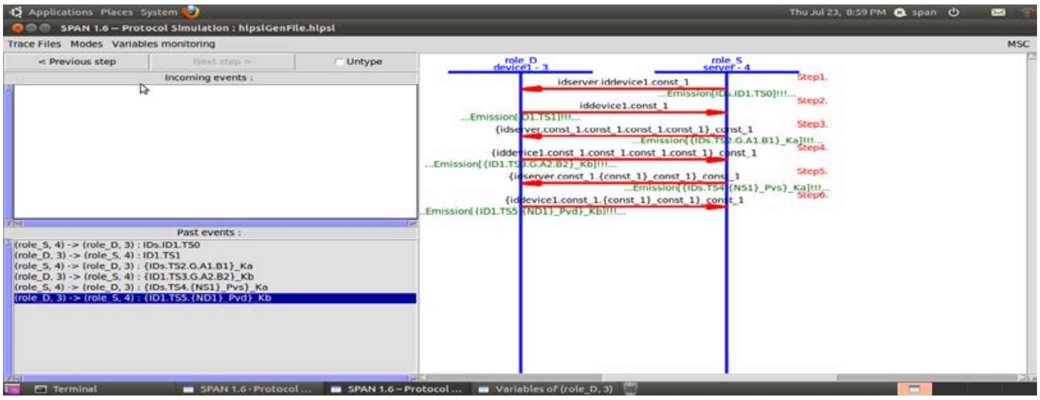
At the time of live communication is going on within two authentic substances; a foe can attempt to tune in it. Afterward, he can erase, modify, or hold the transmission messages.

8.2. *Formal security verification using AVISPA*

The proper security confirmation of the projected protocol by the reenactment utilizing the AVISPA tool was accomplished. AVISPA is a push-button apparatus for robotic validation of web security protocols, which could be a commonly acknowledged tool for proper security confirmation verification. The reenactment comes about guarantee that the proposed protocol is secure from replay and man-in-the-middle assault.

A. *Informal security analysis*

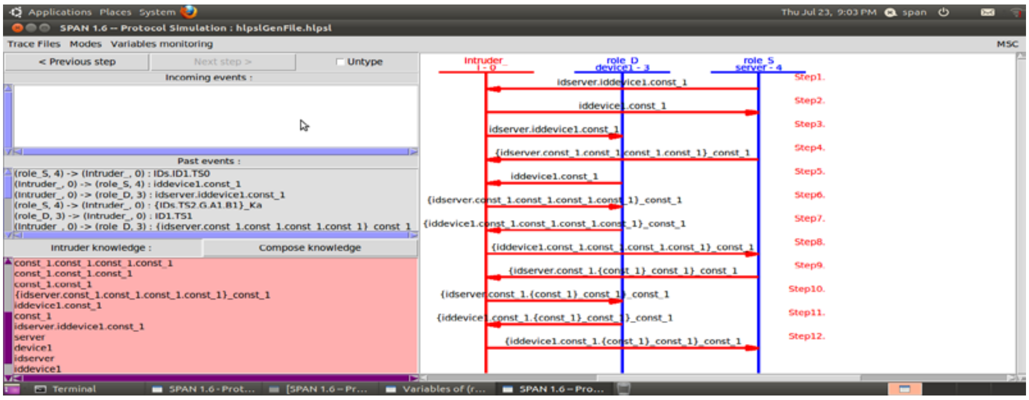
This part analyzes security property related to the proposed protocol. The result of the analysis is summarized in Figures 4, 5, 6, 7, 8.



```
(role_S, 4) -> (role_D, 3) : IDs.ID1.TS0
(role_D, 3) -> (role_S, 4) : ID1.TS1
(role_S, 4) -> (role_D, 3) : {IDs.TS2.G.A1.B1}_Ka
(role_D, 3) -> (role_S, 4) : {ID1.TS3.G.A2.B2}_Kb
(role_S, 4) -> (role_D, 3) : {IDs.TS4.{NS1}_Pvs}_Ka
(role_D, 3) -> (role_S, 4) : {ID1.TS5.{ND1}_Pvd}_Kb
```

```
Step1. idserver.iddevice1.const_1
...Emission[IDs.ID1.TS0]!!!...
Step2. iddevice1.const_1
...Emission[ID1.TS1]!!!...
Step3. {idserver.const_1.const_1.const_1.const_1}_const_1
...Emission[{IDs.TS2.G.A1.B1}_Ka]!!!...
Step4. {iddevice1.const_1.const_1.const_1.const_1}_const_1
...Emission[{ID1.TS3.G.A2.B2}_Kb]!!!...
Step5. {idserver.const_1.{const_1}_const_1}_const_1
...Emission[{IDs.TS4.{NS1}_Pvs}_Ka]!!!...
Step6. {iddevice1.const_1.{const_1}_const_1}_const_1
..Emission[{ID1.TS5.{ND1}_Pvd}_Kb]!!!...
```

Fig.4. Protocol Complete Run

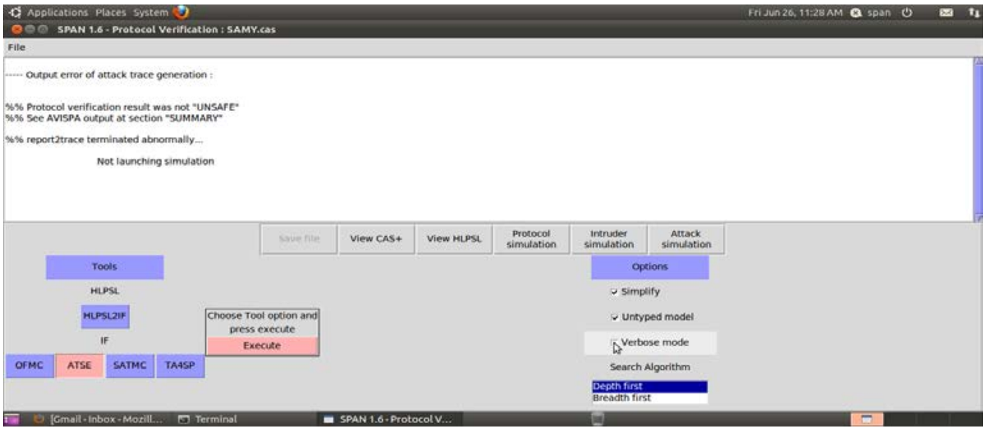


```
(role_S, 4) -> (Intruder_, 0) : IDs.ID1.TS0
(Intruder_, 0) -> (role_S, 4) : iddevice1.const_1
(Intruder_, 0) -> (role_D, 3) : idserver.iddevice1.const_1
(role_S, 4) -> (Intruder_, 0) : {IDs.TS2.G.A1.B1}_Ka
(role_D, 3) -> (Intruder_, 0) : ID1.TS1
(Intruder_, 0) -> (role_D, 3) : {idserver.const_1.const_1.const_1.const_1}_const_1
```

```
const_1.const_1.const_1.const_1
const_1.const_1.const_1
const_1.const_1
{idserver.const_1.const_1.const_1.const_1}_const_1
iddevice1.const_1
const_1
idserver.iddevice1.const_1
server
device1
idserver
iddevice1
```

```
Step1. idserver.iddevice1.const_1
Step2. iddevice1.const_1
Step3. idserver.iddevice1.const_1
Step4. {idserver.const_1.const_1.const_1.const_1}_const_1
Step5. iddevice1.const_1
Step6. {idserver.const_1.const_1.const_1.const_1}_const_1
Step7. {iddevice1.const_1.const_1.const_1.const_1}_const_1
Step8. {iddevice1.const_1.const_1.const_1.const_1}_const_1
Step9. {idserver.const_1.{const_1}_const_1}_const_1
Step10. {idserver.const_1.{const_1}_const_1}_const_1
Step11. {iddevice1.const_1.{const_1}_const_1}_const_1
Step12. {iddevice1.const_1.{const_1}_const_1}_const_1
```

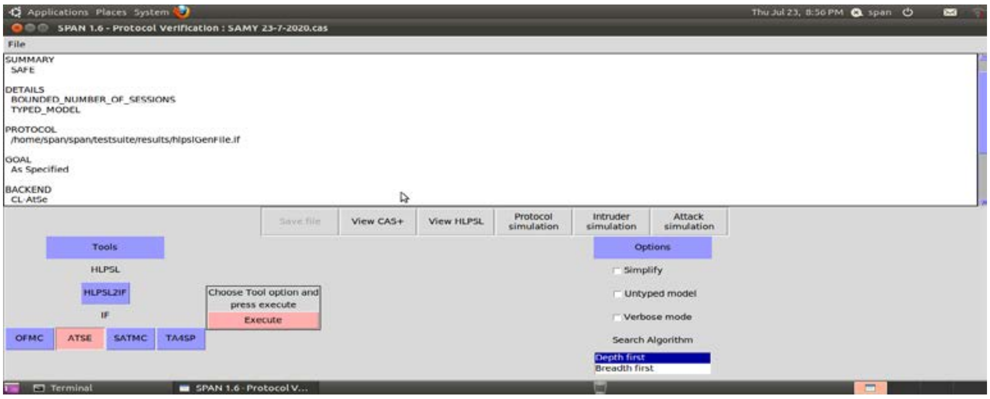
Fig.5. Attacker’s Gained Information



```
----- Output error of attack trace generation :

%% Protocol verification result was not "UNSAFE"
%% See AVISPA output at section "SUMMARY"

%% report2trace terminated abnormally...

        Not launching simulation
```

☑ Simplify
☑ Untyped model
□ Verbose mode

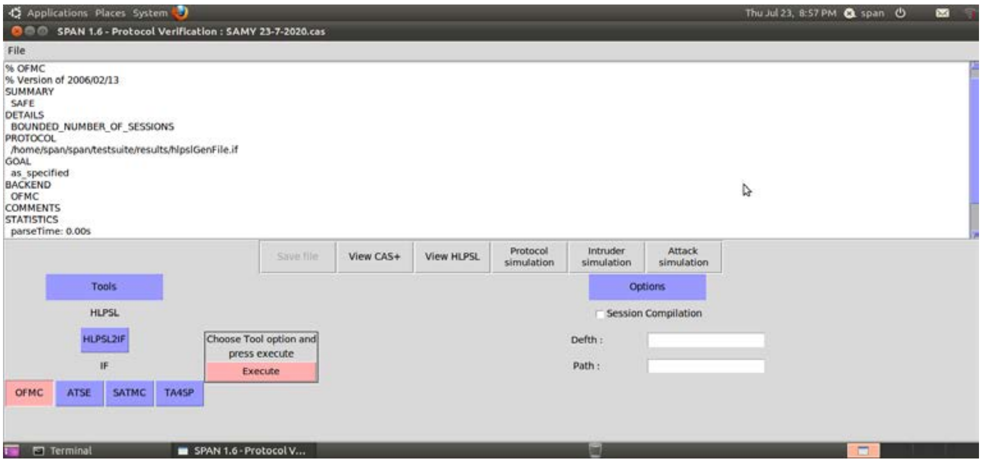
Fig.6. Attack Trace



```
SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL

PROTOCOL
 /home/span/span/testsuite/results/hlpslGenFile.if

GOAL
 As Specified

BACKEND
 CL-AtSe
```

□ Simplify
□ Untyped model
□ Verbose mode

Fig.7. CL-ATSE Attacks Searcher Result



```
% OFMC
% Version of 2006/02/13
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/hlpslGenFile.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
```

□ Session Compilation
Defth :
Path :

Fig.8. OFMC Model Checker Result

The Protocol Complete Run prove that the protocol is correct and can perform a complete run as in figure 4. The Intruder Simulation traces the intruder trials to attack the protocol and; besides, it shows the intruder knowledge with each step as in figure 5. The Attack trace reports if the intruder trials have successes in attacking the protocol or not and the attack trace. Finally, the Model Checker Results and the attacks searcher results, give feedback to the user if the protocol is safe against various malicious attacks or not and some statistics about the test, so the AVISPA could not launch a trace for any attack as illustrated in figure 6. Then the AVISPA found the protocol safe due to CL-ATSE Attacks Searcher Result as in figure 7 and OFMC Model Checker Result as in figure 8.

9. Conclusion

In this paper, an authentication protocol has been proposed for the IoT environment. Our proposed protocol is suggested to form more security and higher speed while the computational load isn't expanded; it is needed to be not only secure but also practical and uncostly. Simulation for the formal security analysis of the proposed protocol utilizing the AVISPA tool guarantees that the protocol is safe and secure from different security assaults. Our proposed protocol is implemented three phases (registration phase, key agreement phase, and text message phase) by six messages between server and devices which minimized the number of messages that are used in the M2M authentication. So, it is recommended also for RCD as it has a small memory size and large battery life, low computation power, and smaller cost ratio. Thus, our proposed protocol is an optimized protocol of M2M authentication for IoT.

As a future work, we will study more in machine to machine mutual authentication advanced signal processing and try to perform hardware implementation for machine to machine mutual authentication and use it as truly random key to encrypt the transferred messages between them to authenticate each other's.

References

[1] Rashid G. Alakbarov, Mammad A. Hashimov,"Application and Security Issues of Internet of Things in Oil-Gas Industry", International Journal of Education and Management Engineering, Vol.8, No.6, pp.24-36, 2018.

[2] Jyotir Moy Chatterjee, Raghvendra Kumar, Manju Khari, Dao Thi Hung, Dac-Nhuong Le,"Internet of Things based system for Smart Kitchen", International Journal of Engineering and Manufacturing, Vol.8, No.4, pp.29-39, 2018.

[3] Nissa Mehibel, M'hamed Hamadouche, "A New Approach of Elliptic Curve Diffie- Hellman Key Exchange", The 5th International Conference on Electrical Engineering – Boumerdes (ICEE-B) October 29-31, 2017, Boumerdes, Algeria.

[4] Tanushree Banerjee and M. Anwar Hasan," Energy Efficiency Analysis of Elliptic Curve based Cryptosystems", 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications, 12th IEEE International Conference On Big Data Science And Engineering.

[5] Syed Kashan Ali Shah, Waqas Mahmood, " Smart Home Automation Using IOT and its Low Cost Implementation ", International Journal of Engineering and Manufacturing, Vol.10, No.5, pp.28-36, 2020.

[6] Technical Guideline BSI TR-03111,"Elliptic Curve Cryptography", Version 2.10, 1 June – 2018.

[7] P. Gope, "Anonymous mutual authentication with location privacy support for secure communication in M2M home network services," Journal of Ambient Intelligence and Humanized Computing, pp. 1–9, 2017.

[8] M. Liu et al., "TBAS: Enhancing wi-fi authentication by actively eliciting channel state information," in IEEE Int. Conf. Sensing, Commun. and Netw. (SECON), June 2016, pp. 1–9.

[9] M. Pospl and R. Mark, "Experimental study of wireless transceiver authentication using carrier frequency offset monitoring," in Int. Conf. Radioelektronika (RADIOELEKTRONIKA), April 2015, pp. 335–338.

[10] F. Liu et al., "A two dimensional quantization algorithm for CIR-based physical layer authentication," June 2013, pp. 4724–4728.

[11] X. Wu et al., "Artificial-noise-aided physical layer phase challenge response authentication for practical OFDM transmission," IEEE Trans. Wireless Commun., vol. 15, no. 10, pp. 6611–6625, Oct 2016.

[12] R. Melki, H. N. Noura, M. M. Mansour, and A. Chehab, "A survey on ofdm physical layer security," Physical Communication, vol. 32, pp. 1 – 30, 2019.

[13] AnujSehgal, Vladislav Perelman, SiarheiKuryla, and Jürgen Schönwälder, "Management of Resource Constrained Devices in the Internet of Things", Jacobs University Bremen, IEEE Communications Magazine, December 2012.

[14] Md. Yosuf Zamil, and Ditee Yasmeen, "Prime Field over Elliptic Curve Cryptographyfor Secured Message Transaction", International Journal of Computer Science and Mobile Computing, Vol.5 Issue.9, September- 2016, pg. 81-88.

[15] William Stallings, "Cryptography and Network Security", Fifth Edition, 2011.

[16] Liu, R.; Wang, J. Internet of Things: Application and Prospect. In MATEC Web of Conferences; Zhao, L., Xavior, A., Cai, J., You, L., Eds.; EDP Sciences France: Les Ulis, France, 2017; Volume 100, p. 02034.

[17] Taynitskiy, V.; Gubar, E.; Zhu, Q. Optimal impulse control of bi-virus SIR epidemics with application to heterogeneous Internet of Things. In Proceedings of the 2017 Constructive Nonsmooth Analysis and Related Topics (CNSA), St. Petersburg, Russia, 22–27 May 2017.

[18] Rajakumari, S.; Azhagumeena, S.; Devi, A.B.; Ananthi, M. Upgraded living think-IoT and big data. In Proceedings of the 2017 2nd International Conference on Computing and Communications Technologies (ICCCT), Chennai, India, 23–24 February 2017.

[19] Dineshkumar, P.; SenthilKumar, R.; Sujatha, K.; Ponmagal, R.; Rajavarman, V. Big data analytics of IoT based Health care monitoring system. In Proceedings of the 2016 IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics Engineering (UPCON), Varanasi, India, 9–11 December 2016.

[20] Shang, W.; Yu, Y.; Droms, R.; Zhang, L. Challenges in IoT Networking via TCP/IP Architecture; Technical Report 04, NDN, Technical Report NDN-0038; Named Data Networking. Available online: http://nameddata.net/techreports.html (accessed on 10 August 2018).

[21] Khan, R.; Khan, S.U.; Zaheer, R.; Khan, S. Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. In Proceedings of the 2012 10th International Conference on Frontiers of Information Technology, Islamabad, India, 17–19 December 2012.

[22] Weyrich, M.; Ebert, C. Reference Architectures for the Internet of Things. IEEE Softw. 2016, 33, 112–116. [CrossRef]

[23] Bauer, M.; Boussard, M.; Bui, N.; Loof, J.D.; Magerkurth, C.; Meissner, S.; Nettsträter, A.; Stefa, J.; Thoma, M.; Walewski, J.W. IoT Reference Architecture. In Enabling Things to Talk; Springer: Berlin/Heidelberg, Germany, 2013; pp. 163–211.

[24] Mashal, I.; Alsaryrah, O.; Chung, T.Y.; Yang, C.Z.; Kuo, W.H.; Agrawal, D.P. Choices for interaction with things on Internet and underlying issues. Ad Hoc Netw. 2015, 28, 68–90. [CrossRef]

[25] Said, O.; Masud, M. Towards Internet of things: Survey and future vision. Int. J. Comput. Netw. 2013, 5, 1–17.

[26] Wu, M.; Lu, T.J.; Ling, F.Y.; Sun, J.; Du, H.Y. Research on the architecture of Internet of Things. In Proceedings of the 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Chengdu, China, 20–22 August 2010.

[27] Nastase, L. Security in the Internet of Things: A Survey on Application Layer Protocols. In Proceedings of the 21st International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, 29–31 May 2017; pp. 659–666.

[28] Wang, F.; Hu, L.; Zhou, J.; Zhao, K. A data processing middleware based on SOA for the Internet of things. J. Sens. 2015, 2015, 827045. [CrossRef]

[29] Spiess, P.; Karnouskos, S.; Guinard, D.; Savio, D.; Baecker, O.; de Souza, L.M.S.; Trifa, V. SOA-Based Integration of the Internet of Things in Enterprise Services. In Proceedings of the 2009 IEEE International Conference on Web Services, Los Angeles, CA, USA, 6–10 July 2009.

[30] Sethi, P.; Sarangi, S.R. Internet of things: Architectures, protocols, and applications. J. Electr. Comput. Eng.2017, 2017, 9324035. [CrossRef]

[31] Mario Frustaci, Pasquale Pace, “Evaluating Critical Security Issues of the IoT World: Present and Future Challenges”, IEEE INTERNET OF THINGS JOURNAL, VOL. 5, NO. 4, AUGUST 2018, pp. 2483-2495.

[32] Syed Rizvi, Joseph Pfeffer III, Andrew Kurtz, Mohammad Rizvi, “Securing the Internet of Things (IoT): A Security Taxonomy for IoT” 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference On Big Data Science and Engineering, 2018, pp 163-168.

[33] Sudeendra kumar K, Sauvagya Sahoo, Abhishek Mahapatra, “Security Enhancements to System on Chip Devices for IoT Perception Layer”, IEEE International Symposium on Nanoelectronic and Information Systems, 2017, pp 151-156.

[34] Trusit Shah, S. Venkatesan, “Authentication of IoT Device and IoT Server Using Secure Vaults”, 17thIEEE International Conference On Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference On Big Data Science and Engineering, 2018, pp 819-824.

[35] Santhosh Krishna B V, Gnanasekaran T, “A Systematic Study of Security Issues in Internet -ofThings (IoT)”, International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), 2017, pp. 107-111.

[36] Sowmya Nagasimha Swamy, Dipti Jadhav, Nikita Kulkarni, “Security Threats in the Application layer in IOT Applications”, International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), 2017, pp. 477-480.

Authors’ Profiles

Mohamed M. Samy: He received his B.Sc. from the Electrical Engineering Department, Military Technical College, Cairo, Egypt in 2003, master student in Ain Shams University Communication and Electronics Department. Currently, Egyptian Armed Forces.

Wagdy R. Anis: He received his B.Sc. from the Electrical Engineering Department, Ain shams university, Cairo, Egypt. M.Sc. from Ain shams university in 1977. Ph.D. in 1985 Currently Emeritus Professor at Electronics Engineering and Electrical Communications.

Ahmed A. Abdel-Hafez: He received his B.Sc. and M.Sc. from the Department, Military Technical College, Cairo, Egypt in 1990., 1997 respectively. Ph.D. from Ottawa University in 2003. Currently Head of cryptography research center since 2012, Egyptian Armed Forces. His research interests including Applied cryptograph and Information Security.

Haitham D. Eldemerdash: He received his B.Sc. and Ph.D. from the Communication Engineering Department, Military Technical College, Cairo, Egypt in 2002, 2014 respectively and the M.Sc. from Arab academy for science and technology, Cairo, in 2011. Currently, member of cryptography research center since 2014, Egyptian Armed Forces.

How to cite this paper: Mohamed M. Samy, Wagdy R. Anis., Ahmed A. Abdel-Hafez, Haitham D. Eldemerdash, "An Optimized Protocol of M2M Authentication for Internet of Things (IoT)", International Journal of Computer Network and Information Security(IJCNIS), Vol.13, No.2, pp.29-38, 2021. DOI: 10.5815/ijcnis.2021.02.03