ISSN 2278-3091
Volume 12, No.4, July - August 2023
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse041242023.pdf
https://doi.org/10.30534/ijatcse/2023/041242023

Data Protection in IoT using CoAP based on Enhanced DTLS

[1]Sara Alayda,[2]Randa Ahmed
[1]Student, Jouf University, College of Computer and Information Sciences, Saudi Arabia sarh.alayda@gmail.com
[2]Assistant professor, Jouf University, College of Computer and Information Sciences, Saudi Arabia, rjabeur@ju.edu.sa

Received Date June 15, 2023 Accepted Date: July 27, 2023 Published Date: August 06, 2023

ABSTRACT

The Internet of Things (IoT), refers to all the infrastructures and technologies put in place to operate various objects through an Internet connection, it is about connected objects. One of the most frequently used IoT application protocols is the Constrained Application Protocol (CoAP) that matches restricted computers. CoAP is a solution for in-regulated data formats and a high security to protect government-related data from cyber-attacks. CoAP advises using DTLS (Datagram Transport Layer Security) to provide robust security of the UDP-based TLS edition. Initially, DTLS was planned for conventional networks. Therefore, a heavyweight solution is created by moving the protocols over the resource-limited computers. Unfortunately, DTLS has some security issues regarding the management of keys and its vulnerability against common cyber-attacks especially Denial of Service (DoS). Thus, a security approach is important to secure CoAP-based IoT infrastructures from these attacks. In our work, we propose to secure IoT data using enhanced DTLS protocol over CoAP. The enhancement DTLS make it possible to prevent DoS and Distributed DoS attacks. In our proposition, we apply a thrusted party (TP) to which we delegate the process of the authentication and authorization of clients. In addition, the TP is responsible of the verification of IP addresses in order to mitigate attackers from flooding the network with fake hello messages.

Key words: CoAP, DTLS, DoS and Distributed DoS attacks, Internet of Things (IoT).

1. INTRODUCTION

The Internet of Things (IoT), which produces a huge variety of technology for the benefit of a society, is one of the fastest emerging networking paradigms. The creation of (IoT) has resulted in a protracted assault involving end-to-end security methods [1-4]. IoT infrastructures cover a big application area starting from business-oriented emergencies such as insurance and banking, to mission-critical crises such as e-health and intelligent transport networks. In order for raw data to be received by an IoT platform (like the Cloud for example), we need a facade through which objects can connect and communicate. This facade is called an application interface based on application protocols. An application protocol is a set of rules defining the mode of communication between two computer applications. These rules are based on transport protocols (TCP / UDP) to initially establish routes and exchange data according to all the rules of the selected application protocol. One of the most frequently used IoT application protocols for resource discovery is CoAP that matches restricted computers [5-8]. IoT systems need CDs with energy-efficiency, limited processing capabilities, limited storage space, efficient network architecture and setup, specified data model, and a model of (IoT) implementation for effective functionality. This device, like the ocean, is manufactured and made to be environmentally friendly. CoAP is a solution for in- regulated data formats and a high security to protect government-related data from cyber-attacks.

Indeed, when CoAP is used for temperature control, the server sends some update to the client. Such attributes contribute to vast volumes of data. Otherwise, multiple problems emerge such as fragmentation and recombination. CoAP advises using to provide robust security of the UDP-based TLS edition. Initially, DTLS was planned for conventional networks. Therefore, a heavyweight solution is created by moving the protocols over the resource-limited computers. The DTLS headers are also too long to fit into a complete IEEE 802.15.4 transmission unit (MTU). Besides these technical problems, DTLS has also some security issues regarding the management of keys and its vulnerability against common cyber-attacks. The Internet of Things has a variety of security problems, but attacks against data communication infrastructure through Denial of Service (DoS) pose an especially major challenge to IoT deployments. According to the literature in the context of IoT security, much of the work presents DoS attack detection mechanisms or only mentions DoS attacks as one of the IoT ecosystem's problems. Therefore, a security approach is important to secure CoAP-based IoT infrastructures from these attacks [9-12]. The purpose of our work is to provide secure communication within the IoT environment and resilience against DoS attacks. Therefore, we propose to enhance the secure CoAP protocol with DTLS by integrating the concept of Third Party (TP). In

our work, we based our proposition on the work presented in [13], described above. We employed the idea of trusted party from that work and try to enhance it. However, in some cases, devices can be compromised and intruders will use their IP addresses to flood the network with fuzzy requests. Therefore, we plan to improve the existing proposition by adding a prevention mechanism presented in [14]. Although, the proposition of this later work was not dedicated to DTLS protocol. We believe that it provides great benefit to secure the protocol against DoS attacks. Thus, inspired by the proposal presented in [14], we opted the concept of IP addresses verification in our work and adapt it to be used by the trusted party (TP). This party is a trusted entity responsible for the verification and the authentication of the sending nodes called clients. The proposed mechanism aims to protect the IoT environment from DoS attacks as well as distributed DoS. The protection is lead on the idea of mitigating the attack by ensuring a strong authentication process between clients and server. Furthermore, the proposed mechanism aims to identify suspicious addresses that would be a trigger of such an attack.

2. RELATED WORKS

We review prior works that handled the problem of security in CoAP protocol. We study the security mechanism and approach proposed to secure the exchange of IoT data using DTLS protocol.

In [15], the authors studied the security features of the CoAP protocol and address the different problems that face this protocol. In addition, CoAP security over DTLS was also discussed where authors affirm that CoAP is a good choice for IoT devices. However, there are still some enhancement and improvements to be done on the protocol as on it security protocol DTLS. Regarding CoAP security as well, authors in [13] address the security issue of distributed DoS attacks. Especially, those which use amplified reflection (AR-DDoS). This type of attack threatens the CoAP security and thus the authors studied this type of attack and its influence on IoT environments.

Moreover, in the IoT environment, [16] the researchers have proposed a novel solution to prevent well-known attacks such as DoS and DDoS in the IoT, at an early stage at the Border Router node. The proposed method consists of two stages. The first one check and whether the sender is legitimate or doubtful. In the second one, the validity of the suspicious senders is verified. The authors used the Contiki Cooja simulator to simulate and implement the algorithm.

Regarding our study of the state of art, we divided the works proposed for the enhancement of CoAP security into four main categories as shown in Figure 1. Noting that, this classification is based on which mechanism or context the authors have been focused on the most. Hence, we define four main categories. The first one is security investigation, where the proposed work emphasizes the security aspect by including newer cryptographic techniques such as the Elliptic Curve Cryptography (ECC) or using external entities to ensure more security such as trusted parts and security gateways. The second category is DTLS suitability. In this category, authors tried to make DTLS more secure and more appropriate for constrained environments. This appropriation is illustrated by header compression, lightweight protocol, and the improvement of its handshake phase. The third category classifies works that focused on performance optimization. Namely, the authors aim to reduce ROM utilization and packet overhead. The last category concerns work that deals with CoAP security outside DTLS, noting that this category is out of the scope of work.

Figure 1: Related works proposed classification

In what follows, we highlight the methods proposed for each category. In the security investigation category, an approach using ECC is presented in [17] where authors suggested a scheme to create a secure session key between the remote server and IoT devices named ECC-CoAP. In their method, the authors enhanced the authentication mechanism by using a limitation technique. In other words, any device will be blocked after a specific number of fail. Hence, the authors indicate that after three fail of authentication within the server, a device will be automatically blocked by the server to prevent DoS attacks and the transmission of the fuzzy requests. In order to evaluate the applicability of their solution, the authors perform a formal security analysis using the BAN logic and presented also a security verification using the role-based AVISPA tool [18]. However, their solution was not tested in a real environment.

In [19], a smart gateway-based authentication and authorization strategy was proposed to prevent and protect more sensitive physiological information from cyber-attackers and malicious users. With the help of the Contiki Network Emulator, the enhanced-DTLS based on the smart gateway is seen showed. Moreover, basic authentication procedures are applied. The authors proposed to perform authentication using smartcards. For the formal security analysis and verification, this work uses AVISPA (Automated Validation of Internet Security-sensitive Protocols and Applications) tools and BAN (Burrows-AbadiNeedham) logic. To increase the suitability of DTLS, the authors in [20] proposed also a DTLS improvement to be used with CoAP protocol. Their method consists of the separation of the two phases: DTLS handshake and data encryption phase. Basically, the proposed solution is based on a delegation mechanism where they suggested to use Secure Service Manager (SSM) to delegate the handshake phase. Thus, they aimed to eliminate the power and the space needed for such a handshake.

An improved version of DTLS including header compression for securing IoT is proposed in [21]. Regarding CoAP, the improvement in DTLS with header compression decreases the DTLS overhead. In that way, it improves the energy consumption and the response time. In this work, the authors proposed a collaboration of DTLS and CoAP where the DTLS header compression framework has been proposed to help to minimize the packet size and to prevent fragmentation by complying with the 6LoWPAN requirements.

In [15], the authors focused on the enhancement and light weighting of the DTLS protocol. They used a Trusted Third Party (TTP) to afford improvement to E-Lithe. This concept ensures the pre-exchanging of secret keys as well as resilience against DoS attacks. However, in this work, the TTP uses a primary authentication mechanism and does not protect from DDoS attacks.

In [16], the authors established an enhanced implementation of DTLS for CoAP. They proposed to use the (ECC) optimizations and focus on reducing the use of ROM. Furthermore, they combined fragmentation and connection-oriented communication (CoC) to lightweight DTLS comparing to the standard version. Additionally, to prevent server resource consumption in case of a DoS attack, the authors applied a stateless cookie technique. This technique is based on the cookie validation and the retransmission of the Client Hello message. Hence, the DTLS handshake depends on the server's decision. To validate the feasibility of their approach, the authors applied their proposition on the MagoNode and compared it to the DTLS standard implementation. The experimental results prove that the optimized ECC solution outperforms the standard implementation and improves network lifetime. Nevertheless, the proposed solution was not tested in a real-life scenario.

In [22], the authors have enhanced DTLS implementation over CoAP for the IoT. Their implementations are based on ECC and performed on a platform named MagoNode. The results of their implementation show a reduction in ROM occupancy and computation overhead within CoAP.

An enhanced DTLS version was introduced [23], where the authors emphasize the performance aspect. Hence, their method aims to minimize DTLS communication costs and fortifies its security. The authors integrated several encryption elements inside CoAP messages while creating Client/server connections. In addition, the authors focused on extenuating DoS attacks by extending the DTLS handshake process with cookies. Hence, to prevent resource exhaustion caused by DoS attacks, it is primordial for a server to ensure the client's abilities before the resource allocation. The evaluation of the proposed method indicated that the simplification of the DTLS handshake process ensures better performance. Thus, the consumption of energy, the packet overhead, and the ROM usage have been reduced. Nevertheless, in terms of performance, the proposed model suffers from a latency problem. In addition, in terms of security, the authors does not deal with all the DoS attack scenarios such as those launching from spoofed IP addresses.

Finally, we considered an example of methods that uses other security mechanism for CoAP. Namely, the Advanced Encryption Standard (AES) algorithm was used in [24] to conceive a lightweight security structure in CoAP. Authors divide their work into two sections; the first one allows lightweight security for CoAP (CoAPs-Lite). The second part permits the process of authentication in IoT devices (CoAP_auth). This solution ensures confidentiality, key management and authentication. However, it inherits security problems related to AES and it is not a standardized solution. Table 1 summarizes the related work discussed in this section.

Table 1: Related works summary

Work	Category	Proposed Solution	Advantage	Drawback
[13]	DTLS Suitability	DTLS enhancement using third trusted party (TTP)	ensures the pre-exchanging of secret keys and resilience against DoS attacks	primary authentication mechanism No protection against DDoS attacks
[16]	Performance Improvement	combine fragmentation and connection-oriented communication (CoC) to lightweight DTLS	Prevent server resource consumption in case of a DoS attack and improves network lifetime.	The proposed solution was not tested in a real-life scenario.
[19]	Security Investigation	Ensure authentication and authorization by using smart gateway-	Simple solution to protect sensitive physiological data	basic authentication procedures
[20]	DTLS Suitability	Delegation of DTLS protocols using Secure Service Manager (SSM)	eliminate the power and the space needed for such DTLS handshake to make it more suitable for constrained devices	Resulting security issues in case of SSM failure.

[21]	DTLS Suitability	DTLS header compression for securing IoT CoAP-based communication	decreases the DTLS overhead, in that way it improves the energy consumption and the response time	No prevention against cyber-attacks
[22]	Performance Improvement	ECC-based DTLS implementation	a reduction in ROM occupancy and computation overhead within CoAP	No prevention against cyber-attacks
[23]	Performance Improvement	integrate several encryption elements inside CoAP messages while creating Client/server connections and the use of cookies	minimize DTLS communication costs and fortifies its security	Didn't deal with all the DoS attack scenarios such as those launching from spoofed IP addresses.
[24]	Lightweight Security Solutions	a lightweight security structure based on AES	ensures confidentiality, key management and authentication	Nonstandard solution

In this work, we aimed to strengthen the authentication and the authorization process in DTLS by using the concept of TP. The TP is responsible for the authentication of clients; hence, it will perform a pre-exchange of a secret pre-shared key between the client and the server. Furthermore, the TP will keep a list for suspicious IP addresses or addresses that have been compromised before in order to prevent DoS attack. Thus, the main idea of this work is to prevent DoS attacks in order to mitigate their harm. In this work we have been inspired by the work presented in [15], which deals with the idea of trusted party. However, in some cases devices can be compromised and intruders will use their IP addresses to flood the network with fuzzy requests.

Therefore, our work enhances the security of the proposed method in [15] by creating the mechanism of filtering lists. Thanks to the IP addresses verification method, our protocol is more secure and can prevent DoS attacks comparing to the proposition of [15]. Our proposed enhanced DTLS uses the idea of TP to minimize the chances of DoS attack on server.

TP and server pre-share and agree a secret used for the authentication of the client as well as the server. Hence, it is considered more efficient and more secure

3. PROPOSED APPROACH

The proposed solution aims to prevent DoS and DDos attack on server in an IoT environment, using the concept of TP for DTLS over CoAP Protocol. The TP will be in charge for exchanging secret keys, authenticating the client and checking for suspicious devices. Hence, our schema defines three segments: The server, the client environment, and the trusted party as shown in Figure 2, Dos attack can be lunched in the network using spoofed IP addresses or by flooding the network with fuzzy requests (client hello message in case of DTLS). Hence, to reserve the server security and the continuity of services, clients aiming to reach the server must be validated as legitimate devices and IP addresses must be checked to classify those how are suspicious, especially for the case of distributed DoS where the attack is performed by several nodes distributed in the network.

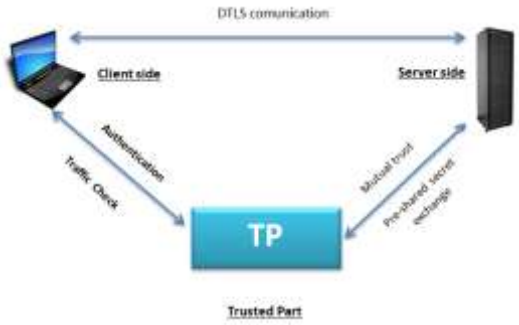

Figure 2: Segments of the proposed schema

The functioning of the proposed schema is divided into four main phases as follows:

1. *Server to TP connection (Trust Exchange phase)*

Before the beginning of the connection and the transmission of any information between the client and the server or even between the trusted party and the client, a mutual trust between the server and the trusted party must be established. This trust is expressed by the exchange of shared secret between them. Hence, the first thing to do is to guarantee that TP and the server get agreed on a pre-shared secret (Figure 2). This secret does not help for the mutual trust only, but, it will be used latter to validate clients by the TP and to authenticate their credential. Noting that, this pre-shared secret is considered as a symmetric secret key noted K.

2. *Traffic check (Authorization phase)*

Once a client wants to initiate a DLTS communication, it will send an authentication request (AuthREQ) message to the TP. When receiving a packet, the TP perform a traffic check to decide whether the incoming packet is legitimate or not. In other words, this step is considered as an authorization phase, where only authorized device with legitimate IP addresses are allowed to communicate with the server. Hence, to ensure that, the TP analyzes the source IP addresses of incoming traffic

from the external network. This analysis is performed in order to classify IP address in one of these three lists:

• Blocked list (BL): contain a list of IP sources addresses that are not allowed to send any traffic inside the network. Traffic coming from this address is denied and automatically dropped.

• Suspicious list (SL): contain a list of IP sources addresses that may present a potential danger. Hence, the traffic coming from these addresses is suspicious and can be harmful for the network security as it can lunch DoS attacks.

• Trusted List (TL): contain a list of IP sources addresses that are considered as trusted or safe. Hence, traffic coming from these addresses is legitimate.

Consequently, the TP extract the packet header (Main algorithm, line 1) and check if the source IP (IPS) of the incoming packet figures into one of the lists defined above, and decide whether accepting the traffic or drop it. Thus, if the IP address belongs to the BL list (Main algorithm, line 2) then the TP will drop the connection with this device even after it has been authenticated (Main algorithm, line 3). Otherwise, it will check the packet payload (PL). If it is greater than the size of other non-suspicious packets, it will be considered as malicious packets (Main algorithm, line 5). The comparison is conducted with a predefined threshold called Payload threshold (PLT). Accordingly, the TP drop the packet and the source IP is added to SL list. If the problem of payload is originating from the same IP of a previous suspicious packet, then DoS attack will be detected (Main algorithm, line 11) and the IP address will be moved the BL list. Else, if it comes from different IPs, then a Distributed DoS attack will be detected (Main algorithm, line 14), and all IPs addresses will be moved to the SL list (Main algorithm, line 16). Later, for packets that are coming from SL, the TP checks whether the packet shares the same features as the previous ones originating from the same IP. If it is the case, the IP address will be added to the BL list. In case where no problem has detected neither in the IP address nor in the packet payload, this address will be moved to TL list (Main algorithm, line 20) and the incoming traffic will be considered as legitimate. In what follow, we present the algorithm that translates the function of this stage.

Proposed Algorithm

Input: Packet P: [IPS, IPD, PL],
begin
Extract (P, [header]); // extracting the IP add from the packet header
if *IPS ∈ BL then*
Drop P; // Dropping the packet
else
if *PL > PLT then //payload comparison*
Drop Packet;
Add (IPS, BL); //moving the address to the blacklist
elseif IPS ∈ SL then
if *PL = PL'then // PL'is a payload of a previous suspicious packet*
if *IPS = IPS' then // IPS' is a Src address of a suspicious packet*
Alert('DoS attempt detected');
Add (IPS, BL);
elseif *multiple (IPS)then //problem originating from several addresses*
Alert('DDoS attempt detected');
For each IPS do
Add (IPS, SL); //add all the Adr to the SL
Endif
Endif
Endif
Add (IPS, TL); //when no problem is detected add the adr to the TL list
End

3 TP to client connection (Authentication phase)

This phase is the last step that precedes the DTLS handshake. This stage is considered as the authentication phase. It consists of a secure double checking to enforce the server security. After the confirmation of the device legitimacy, the TP will respond to the client AuthREQ message with an AuthREP message containing a sequence number (SN), the identity of the client and a key session generating from the pre-shared key K. When receiving this message, the client will respond with a message containing the key K along with the same sequence number (SN). In this way, the TP first authenticate this client as well as its credentials (Figure 3).

4 Client to server connection (Communication phase)

When the authentication of the client is ensured, the client HELLO message is forwarded to the server, which has a mutual trust with the TP. After this stage, the client sends a handshake request to the server. On its turn, the server compares the authentication key. If it matches, the process is followed by server hello message, thus, the client/server communication starts. Otherwise, the whole communication is dropped (Figure 3).

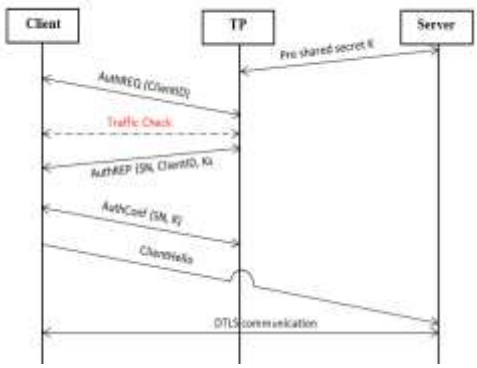

Figure 3: Messages Exchange

Our proposed enhanced DTLS use the idea of TP to minimize the chances of DoS attack on server. TP and server pre-share and agree a secret used for the authentication of the client as well as the server. Before the phase of authentication, the TP check firstly if the traffic is legitimate, to authorize (or not) a device to communicate. This authorization is given according to an IP addresses list. After that, the device is authorized; the TP authenticates the client for server. Consequently, server offers services only for a client that is considered as legitimate user. In addition to the attack prevention, the proposed method reduces the authentication of client overhead on the server. Figure 4 summarizes the functioning of our secure solution for DTLS protocol.

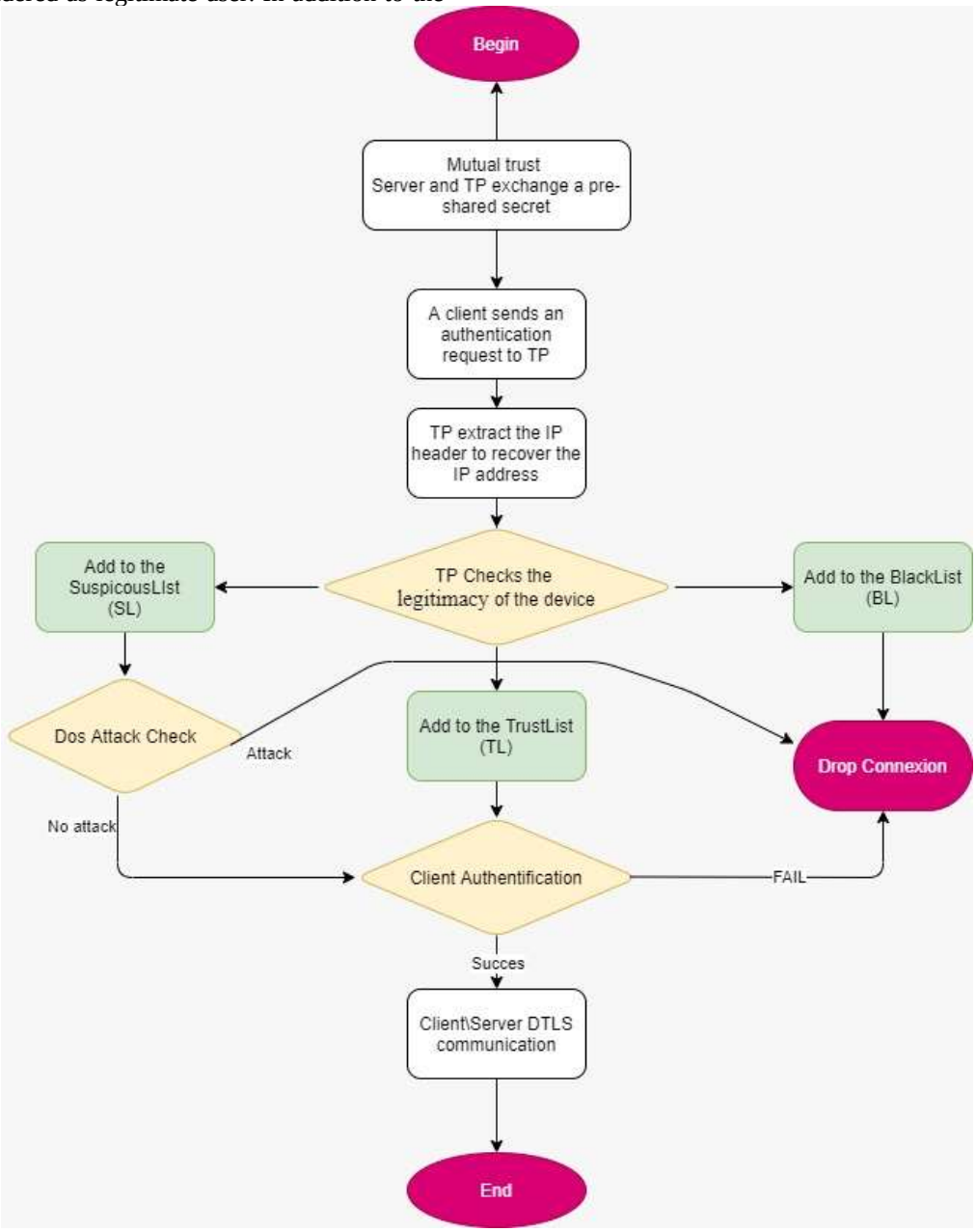

Figure 4: Flowchart of the proposed solution

3. RESULTS AND DISCUSSION

In this section, we illustrate our proposed solution which aims to enhance the security the CoAP protocol with DTLS by integrating the concept of Third Party (TP). Indeed, we focus on the implementation of the proposed solution and the evaluation of the enhanced DTLS protocol performances. More details are given in the following sections.

1 Implementation of the proposed solution

In order to check the efficacy and the efficiency of our proposed enhanced DTLS protocol, we opted for an implementation of the protocol using the MATLAB tool. For this purpose, we implement the algorithm proposed on MATLAB using special libraries for the manipulation of the CoAP protocol. As a result, the principle of noting implementation is the use of Internet Protocol (IP) principles over DTLS to secure the CoAP protocol. Additionally, we used the MATLAB simulator SIMULINK. It represents a functional diagram environment for multi-domain simulation and the Model-Based Design approach. It supports system-level design and simulation, automatic code generation, and continuous testing and verification of on-board systems. Also, SIMMULINK [25] offers a graphics editor, a customizable set of block libraries and solvers for modeling and simulating dynamic systems.

2 Implementation steps

The proposed enhanced protocol uses the idea of TP to minimize the chances of DoS attack on server. By default and to secure subsequent communications, the TP and server pre-share and agree a secret used key for the authentication of the client as well as the server. Knowing that, this secret key is only shared between these trusted peers. Basically, before the phase of authentication, the TP check firstly if the traffic is legitimate, to authorize (or not) a device to communicate. This authorization is given according to an IP addresses list. After that, the device is authorized; the TP authenticates the client for server. Consequently, server offers services only for a client that is considered as legitimate user. Hence, for the implementation of DTLS enhanced protocol, we apply the principle of the TP on the DTLS protocol in order to filter the incoming CoAP packets. For this reason, we employ the CoAP MATLAB library to manipulate CoAP requests and responses. Then, we add the principle of the third part that will build the three filtering lists: Blocked list, suspicious list and Trusted List. Therefore, the third-party server, after the authentication phase, will check the traffic each time. The server verification aim to classify the IP addresses according to the traffic behavior. This latter is defined according to packets received previously. Noting that comparison is conducted with a predefined threshold called Payload threshold (PLT). Hence, our code consists in making comparison between the IP addresses and also between the traffic behaviors. Thus, the TP server checks whether the packet shares the same features as the previous ones originating from the same IP.

3 Implementation model

We introduce the three lists of the protocol as well as a server as a secure and trusted third party. So, we make transmissions from three different machines: a trusted machine, a suspicious machine and a machine with blocked IP address. Figure 5 shows this model in Simulink, where the three machines try to transmit different packets over time destined to the host server with the IP address 192.168.1.3 and the black bar presented the improved DTLS protocol which will filter the traffic received from the three machines to update the lists of IP addresses. This model is used in Simulink to extract the results that will be explained in the next section.

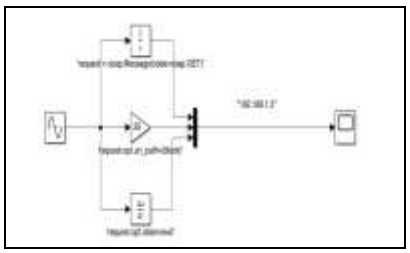

Figure 5: the proposed model in Simulink

4 Simulation results

For the simulation, running the previous model in the MATLAB simulator, Simulink have given the result shown in figure 6. As shown in the figure, the results are quite positive concerning the efficiency of the proposed method. The server of the third party lets through the traffic of a single machine (the trusted machine) and consequently we can find its IP address registered in the trusted list. On the other hand, the traffic of the two other machines is blocked. For the suspicious machine, its IP address is added to SL and the traffic TLP is used for future comparison. Moreover, with regard to the machine with blocked IP, the traffic is immediately bypassed by the protocol.

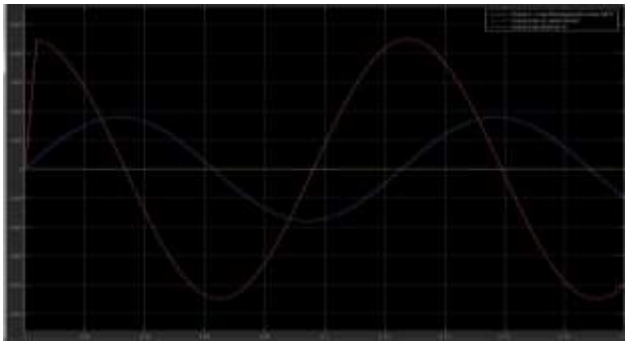

Figure 6: Results of the packet filtering simulation using one user

As shown in the figure 7, the results are quite positive concerning the efficiency of the proposed method. The server of the third party lets through the traffic of a single machine (the trusted machine) and consequently we can find its IP address registered in the trusted list. On the other hand, the traffic of the two other machines is blocked. For the suspicious machine, its IP address is added to SL and the traffic TLP is used for future comparison. Moreover, with regard to the machine with blocked IP, the traffic is immediately bypassed by the protocol.

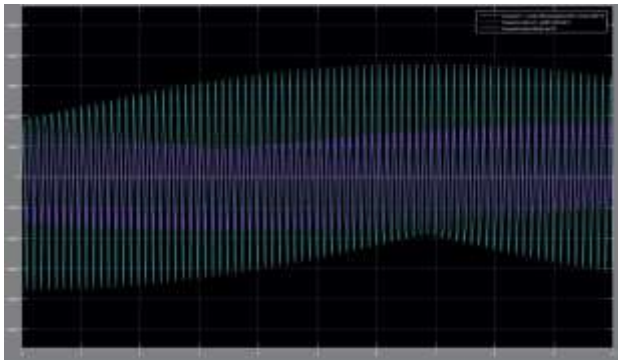

Figure 7: Results of the packet filtering simulation using 30 users

Regarding results in figure 7, we can see that it defines 3 different types of traffic: yellow for trusted traffic, blue for suspicious traffic, and red for the blocked traffic. Noting that, in our experience, we used 90 users which are divided into three categories, 30 users for each one. Hence, we have defined a database which contains all the IP addresses of these users belonging to the 3 different categories and we have started the traffic transmission. As a result, on their arrival at the server, the improved DTLS protocol begins the operation of verifying the IP addresses. Subsequently, it will classify these addresses according to the filtering lists already predefined. According to this classification, the server of the TP decides if the traffic can pass or not. Therefore, the server allowed the traffic of all 30 IP addresses classified in the trusted list to pass, in addition to some users with suspicious behavior. On the other hand, none of the blocked users were able to pass their traffic through the server TP.

The results of detection made by the server are shown in figure 8 and details of these results are presented in Table 5.1

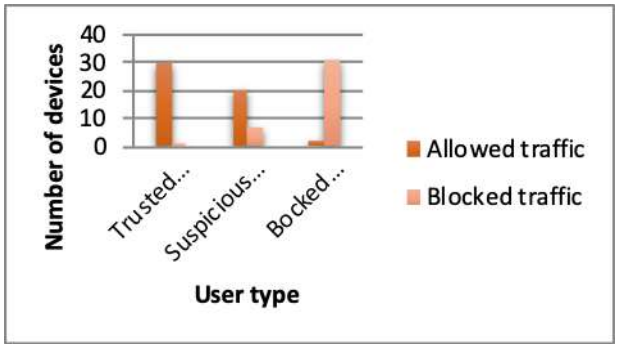

Figure 8: Blocked and allowed traffic by TP server

We can also notice that the number of false positives and false negatives is very small to a point that it is almost negligible. Regarding the detection, the server was able to detect all the 30 trusted users. However, there was a difference of 3 users from 30 in the detection of suspicious. Despite this the server has classified them as blocked users and therefore even in the case of false negative the algorithm still remains secure. As presented in the table, this gives us almost 7% false positive percentage while the classification of suspicious and blocked Users**.** Regarding the traffic filtering, we measured a percentage of 6.45% false negative**.**

Table 2: TP server Detection results

	Trusted users	**Suspicious Users**	**Blocked Users**	**Total**
Defined users	30	30	30	90
Server classification	30	27	33	90
Classification false positives	00%	00%	10%	6.66 %
Classification false negatives	00%	10%	00%	6.66 %
Allowed traffic	30	20	02	52
Blocked traffic	00	07	31	38
false positives	00%	00%	00%	00%
false negatives	00%	00%	6.45%	6.45 %

These signals are created as a result of the simulation. Noting that the rising and falling signals are excluded from transmission, only the yellow line is stable and therefore the traffic has arrived at its destination. Therefore, we observe that the protocol only lets the traffic in yellow pass, i.e. the trusted machine. These results assert the proper functioning of the enhanced DTLS protocol and confirm its security against DoS attacks that can be launched by untrustworthy machines

5 Comparison

The contrast between our proposition and the similar works is described in this subsection. For this objective, we used the method proposed in [15] and then replicated the experiment under the same conditions. Besides that, we used 30 users divided into three groups, each with ten members. As consequence, we created a database that comprises all of these users' IP addresses from the three separate groups, and we

started the traffic transmission. The simulation is carried out using standard DTLS, the approach given in [15], and our proposed protocol. The percentage of false negatives and false positives is used as a comparison criterion. Figure 9 depicts the outcomes of this experiment.

We can notice that our method presents the minimum of false negatives/false positives (1,31% / 3,75%) compared to conventional DTLS (6,21% / 9,22%) and the method in [15] (3,98% / 5,06%). This experience further demonstrates the effectiveness of our proposed protocol and ensures the interest of our contribution.

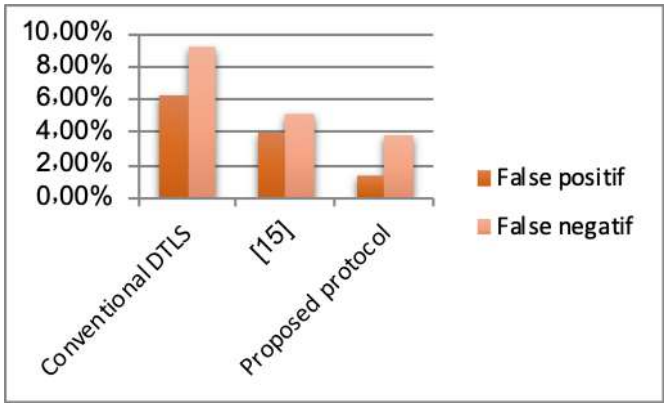

Figure 9: Related works comparison

5. CONCLUSION AND FUTURE WORK

Securing the Internet of Things is not all about guarding against the leakage of sensitive data. The IoT, like any information service, requires protection that considers the three fundamental properties of security: confidentiality, integrity and availability. The CoAP protocol is used with the IoT in conjunction with DTLS to ensure its security. DTLS has some security issues regarding the management of keys and its vulnerability against common cyber-attacks. Therefore, in this work, we proposed a method to secure IoT data using enhanced DTLS protocol over CoAP. The enhancement DTLS made it possible to prevent DoS and Distributed DoS attacks. In our proposition, we used a thrusted party (TP) to which we delegated the process of the authentication and authorization of clients. In addition, the TP is responsible of the verification of IP addresses in order to mitigate attackers from flooding the network with fake hello messages. The goal of our work was achieved since our enhanced protocol proves its security and efficiency in detecting malicious and harmful traffic. In addition, the protocol was able to identify DoS traffic behavior in order to mitigate this attack. To the best of our knowledge, the proposed protocol has only a percentage of 6.45% false negative rates and 0% of false positives rates when filtering the traffic.

As future work, we propose to further improve the system of verification of IP addresses by using other sophisticated methods such as the Artificial Intelligence (AI). In addition, the detection of DoS attacks may also be improved by creating a smarter detection system.

REFERENCES

[1] K. Khalil, K. Elgazzar, A. Abdelgawad, and M. Bayoumi, A security approach for CoAP-based internet of things resource discovery, in 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), 2020, pp. 1–6.

[2] Humayun, Mamoona, N. Z. Jhanjhi, Bushra Hamid, and Ghufran Ahmed. "Emerging smart logistics and transportation using IoT and blockchain." IEEE Internet of Things Magazine 3, no. 2 (2020): 58-62.

[3] Ullah, Ata, Muhammad Azeem, Humaira Ashraf, Abdulellah A. Alaboudi, Mamoona Humayun, and N. Z. Jhanjhi. "Secure healthcare data aggregation and transmission in IoT—A survey." IEEE Access 9 (2021): 16849-16865.

[4] Khan, Azeem, N. Z. Jhanjhi, Mamoona Humayun, and Muneer Ahmad. "The Role of IoT in Digital Governance." In Employing Recent Technologies for Improved Digital Governance, pp. 128-150. IGI Global, 2020.

[5] F. A. Alhaidari and E. J. Alqahtani, Securing Communication between Fog Computing and IoT Using Constrained Application Protocol (CoAP): A Survey, J. Commun., vol. 15, no. 1, 2020.

[6] Humayun, M., N. Z. Jhanjhi, and M. Z. Alamri. "Smart secure and energy efficient scheme for e-health applications using IoT: a review." International Journal of Computer Science and Network Security 20, no. 4 (2020): 55-74.

[7] Humayun, M. (2020). Role of emerging IoT big data and cloud computing for real time application. Int. J. Adv. Comput. Sci. Appl., 11(4), 1-13.

[8] Humayun, M., N. Jhanjhi, and M. Alamri. "IoT-based Secure and Energy Efficient scheme for E-health applications." Indian J Sci Technol 13, no. 28 (2020): 2833-2848

[9] N. F. Syed, Z. Baig, A. Ibrahim, and C. Valli, Denial of service attack detection through machine learning for the IoT, J. Inf. Telecommun. 2020, pp. 1–22.

[10] Shafiq, Maryam, Humaira Ashraf, Ata Ullah, Mehedi Masud, Muhammad Azeem, N. Z. Jhanjhi, and Mamoona Humayun. "Robust Cluster-Based Routing Protocol for IoT-Assisted Smart Devices in WSN." CMC-COMPUTERS MATERIALS & CONTINUA 67, no. 3 (2021): 3505-3521.

[11] Ullah, Ata, Muhammad Azeem, Humaira Ashraf, N. Z. Jhanjhi, Lewis Nkenyereye, and Mamoona Humayun. "Secure Critical Data Reclamation Scheme for Isolated Clusters in IoT enabled WSN." IEEE Internet of Things Journal (2021).

[12] Almufareh, Fahhad. "IoT Wireless Intrusion Detection and Network Traffic Analysis." Computer Systems Science & Engineering, vol.4, no.3, 2021

[13] Haroon, A., Akram, S., Shah, M. A., & Wahid, A. (2017, September). E-Lithe: A lightweight secure DTLS for IoT. In 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall), 2017, pp. 1-5

[14] Kajwadkar, S., & Jain, V. K. A novel algorithm for DoS and DDoS attack detection in internet of things. In Conference on Information and Communication Technology (CICT), 2018, pp. 1-4. IEEE.

[15] A.Chavan and M. K. Nighot, Secure CoAP using enhanced DTLS for Internet of things, Int. J. Innov. Res. Comput. Commun. Eng., vol. 2, no. 12, 2014, pp. 7601–7608.

[16] Maleh, Y., Ezzati, A., & Belaissaoui, M. An enhanced DTLS protocol for Internet of Things applications. In 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM) (pp. 168-173). IEEE.

[17] Majumder, S., Ray, S., Sadhukhan, D., Khan, M. K., & Dasgupta, M. (2021). ECC-CoAP: Elliptic curve cryptography based constraint application protocol for internet of things. Wireless Personal Communications, 116(3), 1867-1896

[18] Armando, A., Basin, D., Boichut, Y., Chevalier, Y., Compagna, L., Cuéllar, J., ... & Vigneron, L. (2005, July). The AVISPA tool for the automated validation of internet security protocols and applications. In International conference on computer aided verification (pp. 281-285). Springer, Berlin, Heidelberg.

[19] P. M. Kumar and U. D. Gandhi, Enhanced DTLS with CoAP-based authentication scheme for the internet of things in healthcare application, J. Supercomput., pp. 1–21, 2020.

[20] Park, J., & Kang, N. (2014, October). Lightweight secure communication for CoAP-enabled internet of things using delegated DTLS handshake. In 2014 International Conference on Information and Communication Technology Convergence (ICTC) (pp. 28-33). IEEE.

[21] A.Chavan and M. K. Nighot, Secure CoAP using enhanced DTLS for Internet of things, Int. J. Innov. Res. Comput. Commun. Eng., vol. 2, no. 12, pp. 7601–7608, 2014.

[22] Capossele, V. Cervo, G. De Cicco, and C. Petrioli, Security as a CoAP resource: an optimized DTLS implementation for the IoT, in 2015 IEEE international conference on communications (ICC), 2015, pp. 549–554.

[23] Y. Maleh, A. Ezzati and M. Belaissaoui, An enhanced DTLS protocol for Internet of Things applications, 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM), 2016, pp. 168-173, doi: 10.1109/WINCOM.2016.7777209..

[24] Ukil, A., Bandyopadhyay, S., Bhattacharyya, A., Pal, A., & Bose, T. (2014). Lightweight security scheme for IoT applications using CoAP. International Journal of Pervasive Computing and Communications.

[25] KARRIS, Steven T. Introduction to Simulink with engineering applications. Orchard Publications, 2006.