JST: Smart Systems and Devices
Volume 32, Issue 2, May 2022, 014-021

Proposing Comprehensive Security Solutions for IOT Networks by Improving and Integrating Methods: DTLS, Quark Encryption and Overhearing Mechanism

Nguyen Van Tanh[1*], Ngo Quang Tri[2], Nguyen Linh Giang[3], Nguyen Ngoc Cuong[4], Tran Xuan Ban[5]
[1]VNU - International School, Hanoi, Vietnam
[2, 3]Hanoi University of Science and Technology, Hanoi, Vietnam
[4]The Ministry of Public Security, Hanoi, Vietnam
[5]University of Technology - Logistics of Public Security, Bac Ninh, Vietnam
[*]Email: tanhnv@vnu.edu.vn

Abstract

With the rise of the Internet of Things (IoT), the risk of information security is increasing. There have been many proposals for IoT security, however, so far, there is not truly effective and comprehensive solution. The study aims at lightweight encryption, with the basic goal of reducing the loops of encryption algorithms, reducing the computing requirements, and energy consumption of the system while ensuring safety, and integrating into new Protocols of IoT networks and weak resource devices. Within the framework of this article, we introduce the research results and continue to propose security solutions for IoT networks by improving and integrating DTLS protocols, Quark hash function and Overhearing mechanism, installation and testing on IoT network structure components, It shows the feasibility and effectiveness of the solution.

Keywords: Security, internet of things, wireless sensor network, DTLS, overhearing, quark lightweight

1. Introduction

The rapid development of applications for Internet of Things (or IoT) leads to the rise of threats about information security and data security with three basic characteristics including confidentiality, integrity, and availability. In IoT System, the gateway and the environment of the sensor are vulnerable to these sniffing and spoofing attacks to confidentiality and integrity, respectively, so scientists designed cryptographic mechanisms including the DTLS Protocol covering the gateway and Quark Lightweight Cryptography covering the sensor's environment. On the other hand, the sensor's environment with limited resource become vulnerable to DoS attack to the availability so scientist designs the overhearing mechanism to prevent this kind of attack. With implementation of these mechanisms, all basic characteristics are protected so it becomes a comprehensive solution.

Our research team researched and improved the overhearing mechanism [1,2], and we proposed a comprehensive security solution including the improved DTLS and the overhearing [3,4]. It is easy to recognize that this solution is not perfect because the confidentiality and integrity of information security in the sensor's environment are not protected. Therefore, we continued in research of improvement and integration. New solutions with the improved DTLS, improved Quark and overhearing can protect all vulnerable components of IoT system. The process to study this Comprehensive solution also requires deep theoretical research as well as careful experiment to find the balance between security level and resource consumption with each single security mechanism as well as a comprehensive security solution and this study concentrates on this process.

The study has 5 chapters: "*Chapter 1: Introduction*" introduces the basic overview of the study; "*Chapter 2: Comprehensive security solution with improved DTLS, Overhearing and Quark lightweight*" describes the Comprehensive security solution; "*Chapter 3: Simulation Experiments*" describes process to design and content of experiments, "*Chapter 4: Results of experiments*" describes measuring criteria, result and its evaluation and "*Chapter 5: Conclusion and future development*" concludes the study and indicated future work.

2. Comprehensive Security Solution with Improved DTLS, Overhearing and Quark Lightweight

In any IoT solution or application, IoT devices are an important factor. These IoT devices can be divided into two main categories of many resources such as servers, PCs, tablets, etc. and resource

ISSN: 2734-9373
https://doi.org/10.51316/jst.158.ssad.2022.32.2.3
Received: December 21, 2020; accepted: February 10, 2022

constraints such as sensors, RFID tags, etc. The second type of IoT device is becoming more popular because they are used in different applications and will appear more in the market, resulting in a large data exchange rate between them.

A lighter version of these solutions is lightweight cryptography, which can address these challenges to ensure communication in resource constrained IoT devices. Key challenges while deploying conventional cryptography in resource limited IoT devices

The limited problems in resource critical IoT devices, which are also challenges in implementing conventional security solutions are:

- Limited memory (register, RAM, ROM).
- Reduce computing power.
- Small physical area for assembly.
- Low battery (or no battery).
- Real-time feedback.

Lightweight security protocol for IoT includes authentication, identification, and key exchange purposes. It is suitable for installation in limited resource environments.

For devices with limited resources, conventional cryptographic algorithms are too big, too slow, and too energy intensive. Lightweight cryptographic algorithms overcome these disadvantages.

2.1. Introduction to Comprehensive Security Solution with Improved DTLS and Overhearing

2.1.1. Introduction to the comprehensive solution

Three basic characteristics of security and information safe are defined in CIA security triangle [3] including Integrity, Availability, and Confidentiality. Moreover, the extent of security 6-pointed star CIA [5] is indicated in Fig. 1 with the addition of more than 3 extended characteristics. Each extended characteristic is the interference of two basic characteristics next to it. In Fig. 1, three white peaks with upper-case-characters labels represent the basic characteristics while three black ones with lower-case-characters labels represent the extended characteristics:

The IoT system will be safe if its security solution protects both 3 basic characteristics in the security CIA triangle because the safety of 3 basic characteristics will ensure the safety of 3 other extended characteristics and it means all necessary characteristics of IoT System are in protection.

2.1.2. DoS attack in IoT network

Denial of Service Attack (or DoS Attack) is a kind of attack which targets the availability of the Internet System. There is a large number of DoS attacks and they can be classified by architecture and mechanism [6]. Our research team concentrated on DoS attacks with architecture Botnet and mechanism UDP Flood [1,2]. With architecture Botnet, the attacker tries to control the node in WSN. Thus, the node becomes Bot and attacks the target which is normally a root node and its neighbor in WSN. With mechanism UDP Flood, Bots attacks by transferring a huge number of packets to the target and making it overloaded. Thus, the victim is exhausted and loses the ability to operate necessary activities in WSN.

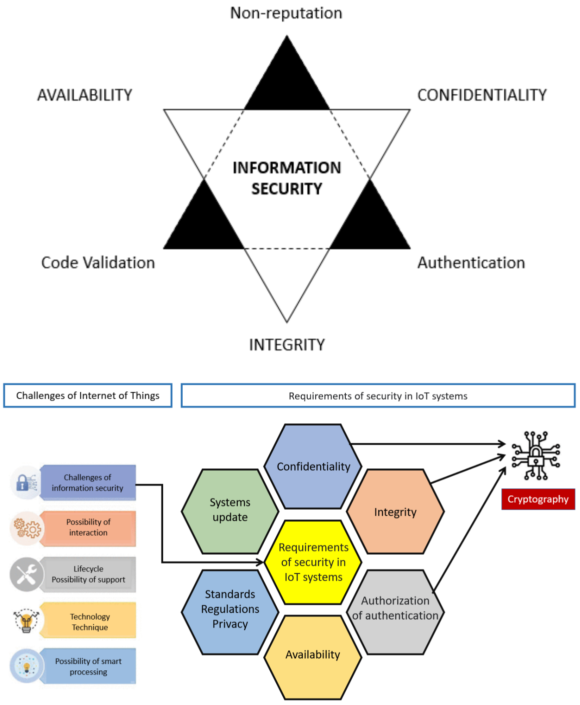
Non-reputation
AVAILABILITY
CONFIDENTIALITY
INFORMATION SECURITY
Code Validation
Authentication
INTEGRITY
Challenges of Internet of Things
Requirements of security in IoT systems
Challenges of information security
Possibility of interaction
Lifecycle Possibility of support
Technology Technique
Possibility of smart processing
Systems update
Confidentiality
Integrity
Requirements of security in IoT systems
Standards Regulations Privacy
Authorization of authentication
Availability
Cryptography

Fig. 1. Security 6-pointed star CIA.

2.1.3. Solution with improved DTLS and overhearing

DTLS was established by Netscape communications [7] concentrates to prevent all threat at the confidentiality such as sniffing attack and the Integrity such as spoofing attack. Meanwhile, the overhearing is developed by our research team [1,2] concentrated to prevent all threat at the Availability likes DoS attack by UDP flood mechanism and Botnet architecture. From approach about comprehensive security solution, we proposed combine the DTLS to the overhearing to protect all basic characteristic of information security including confidentiality, integrity with the DTLS and availability with the overhearing. During the process of implementation, we recognize that the high resource-consumption of the DTLS becomes a hard challenge, so we research and propose some improvement like reducing length of key and removing DoS Countermeasures [4].

2.2. Combining Quark Lightweight in Security Solution with DTLS and Overhearing

2.2.1. Introduction to the lightweight cryptography

One of the basic characteristics of the sensor's environment is the limit of resource. Basically, the Sensors Environment is a collection of a large number of sensor devices [8] that use independent memory and a source of energy. Since the number of sensor devices in a WSN is quite large as well as the allocation of these devices is extremely wide, these devices are designed with a simple structure and low production cost. With these principles of design, the sensor devices are designed with small batteries for reducing size as well as low memory for reducing production cost. Therefore, the resource of energy and space of memory of the sensor device in the WSN is tiny in comparison with the other network system. From this situation, the activities of a sensor device are operated by two principles including high specialization and low resource consumption [9]. Concerning the principle of high specialization, all activities of a sensor device concentrate on the unique mission which is usually gathering a specific signal and transferring it to the Gateway. For example, if the mission is measuring both temperature and moisture of a special air environment, it is irrelevant to install a sensor device that collects both temperature and moisture signals. Instead, with principle of high specialization, two sensors are installed in this environment. The temperature sensor collects data about temperature while the moisture sensor collects data about moisture of surrounding air. Regarding the principle of low resource consumption, all basic and functional activities of each sensor device in the WSN are different from the basic internet network which has lower resource consumption. For example, in the WSN, the used routing protocol is routing protocol for low-power and lossy networks (or RPL) which consumes less energy than the protocol used in the basic Internet [10]. In addition, the security mechanism is not designed in the WSN because of the exhaustion of resources. Therefore, the sensor environment becomes vulnerable before risks to the security and security of information. From this situation, some security solutions are designed to protect the security and security of information in the sensor environment. These solutions are also designed by the principle of low resource consumption to avoid the exhaustion of the WSN caused by the overload consumption.

Security uses many mechanisms to protect the security and security of information and one of them is the cryptographic mechanism. The cryptographic mechanism converts data called plain text to meaningless characters called ciphertext. Therefore, the cryptographic mechanisms have a huge role to avoid sniffing attacks, especially the confidentiality of the information security [11]. From the huge advantage of the cryptographic technology for preventing sniffing attacks, there are many published studies about the way for implementing the different cryptographic mechanisms to the WSN which has plenty of security holes. The design of cryptographic mechanisms must follow the principle of low consumption of resources as the other mechanisms implemented in the WSN. One of the cryptographic mechanisms designed in low-energy environment is the lightweight cryptography [6].

2.2.2. Introduction of Quark Lightweight Cryptography

Quark lightweight cryptography was developed by Jean-Philippe Aumasson with low resource consumption for the tiny-scale WSN such as Radio Frequency Identification (RFID) System [12]. Its advantage is suitable for meeting our requirement about lightweight cryptography with low emery consumption for combining in a comprehensive security solution. Quark uses padded sponge construction which is developed by Guido Bertoni from STMicroelectronics [13], with 6 turns of data hashed by a hash function in which the output of the previous turn would be the input of the next. As the result, the security level increases rapidly when the number of turns data hashed increases but it can reuse the volume of data, thus, decreasing resource consumption in WSN. Fig. 3 describes the padded sponge construction in Quark. Note from Fig. 2 that all block "Hash Function" represent only one hash function in the Quark but process data 6 turns.

Quark used KATAN block cryptography with the input data is a fixed number. From the length of input data, there is 3 types of Quarks: *u-Quark* is 8 bits, *d-Quark* is 16 bit and *t-Quark* is 32 bits. The larger the length is, the faster the cryptographic speed is, but the cryptography consumes more resources. In addition, the Quark could be modified number of hashed turns or the length of input data (but this value must equal to the power of base 2).

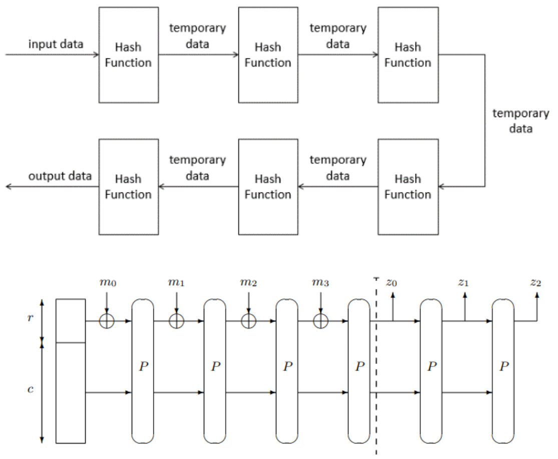

Fig. 2. Padded sponge construction in the Quark.

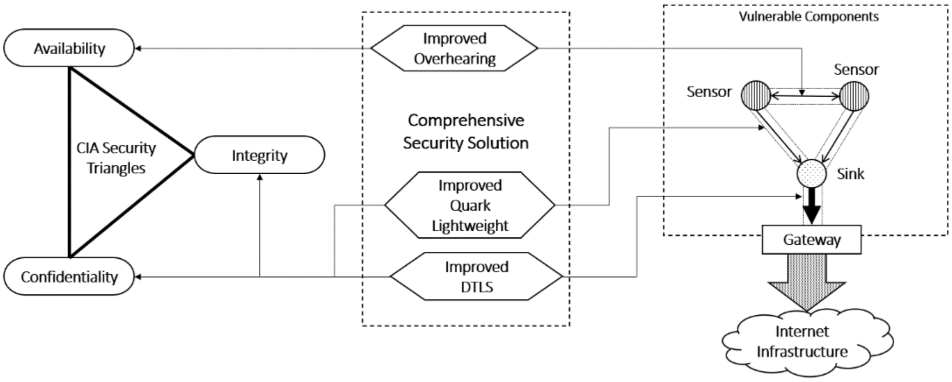

Fig. 3. Location and Target of the Comprehensive Security Solution.

2.2.3. Position of mechanisms in IoT system

In old comprehensive security solution, the DTLS Protocol is installed in transmission layer, the Overhearing mechanism is installed in sensor layer [4]. With the Quark lightweight cryptography, because it aims is protecting sensor nodes, it is installed in the sensor layer. Fig. 3 describes the position of installation and target of each mechanism:

From Fig. 3, DTLS, Overhearing, and Quark are installed in all vulnerable components including Sensor Node, Sensor Environment, and Gateway. Firstly, these components have weak bandwidth, limited resources, and weak backup mechanisms so the DoS attack destroys the IoT network easier than the Internet. Secondly, these components use IoT standards which lack effective security solutions in the current world while internet security is protected by strong security mechanisms such as TLS.

2.2.4. Challenges of the combination of DTLS, overhearing, and quark in IoT system

Combination of Quark and this old security solution has some disadvantages. Firstly, like all security solutions, Quark lightweight cryptography, DTLS mechanisms, and protocols must consume resources in operating and dominate resources of other IoT components, thus can cause that the IoT activities to be delayed or seriously, stopped. Secondly, lightweight Quark, DTLS protocol, and overhearing protocol also change data and information in IoT operation, especially, the operation of DTLS encryption converts the content of all packets to security as well as makes some difficulty for the hashing process of Quark.

3. Simulation Experiments

3.1. Implementation of Comprehensive Security Solution in Contiki Operating System

3.1.1. Combination of improved DTLS protocol and overhearing mechanism

In the previously published papers [1,2,4], our team researched and proposed overhearing including detection of bots by “Singularity point from median Algorithm” and prevention of the DoS attack by isolating bots. We deployed it in Contiki Operating System as well as simulated a DoS attack by UDP Flood and Botnet in square grid WSN. Improvement in file “*tiny-dtls*” to reduce energy consumption includes reducing the length of key and eliminating DoS Countermeasures. However, because of combining the Quark, the process for reducing length of key includes:

- *Decrease key length of Advanced Encryption Standard (AES) encryption:* The key length is decreased from 16 bits to 8 bits.
- *Decrease key length of Secure Hash Algorithm (SHA):* This decreases the key length from 32 bits to 16 bits.

3.1.2. Integrating improved quark lightweight cryptography to the security solution.

Like the DTLS, the Quark has a version in the Contiki OS and it was organized in folder “*quark-master*” [12]. Folder “*quark-master*” contains 3 files: file “*quark.c*” with Quark operating functions, file “*quark.h*” with configuration parameters and file “*main.c*” storing application programming interface to be used in outside components. Folder “*quark-master*” is also located in folder “*apps*” with folder “*tiny-dtls*” in “*contiki-master*”. Despite saving of resource by hash-functions mechanism, the Quark still needs to improve to reduce more resource consumption to integrate with the DTLS and the overhearing which consume a lot of resource. The improvement of Quark is shown below:

- *Decrease length of input data block:* As the below mention, the bigger length of input data block is, the higher resource consumption is. To do this improvement, we create a new type of Quark called “*i-Quark*” (improved Quark) which the length of input data block is **8 bits**.

- *Decrease number of hashed turns:* The decrease of length of input data block causes a side-effect which reduces operation speed so we must eliminate this by reducing number of hashed turns from *6 turns* to *5 turns*

With the second improvement which decrease number of hashed turns, we change threshold argument in for loop code to loop the hashing process in file "*quark.c*". This source code in below rectangle shows this improvement:

```
    memcpy(data_block,input_data_block,
DATA_BLOCK_WIDTH);
    //  for( i=0; i < 6; ++i ){
    /* Add this code */
     for( i=0; i < 5; ++i ){
    /* Add this code */
        cipher_KATAN_block(data_block);
    }
```

With the first improvement which decreases the length of the input data block, it is more complicated than the second one because it requires creating a new data structure "*IQUARK*" representing i-quark and attaching it to the Quark functions with the role of Quark type (like "*UQUARK*" representing u-Quark, "*DQUARK*" representing d-Quark and "*TQUARK*" representing t-Quark). All changes in source code are implemented in file "*quark.h*". This source code in the below rectangle creates the data structure "*IQUARK*":

```
#if  defined(UQUARK)
#define DATA_BLOCK_WIDTH  8
#elif           defined(TQUARK)
#define DATA_BLOCK_WIDTH  16
#elif           defined(DQUARK)
#define DATA_BLOCK_WIDTH  32
/* Add this code */
#elif           defined(IQUARK)
#define DATA_BLOCK_WIDTH  8
/* Add this code */
```

This source code in the below rectangle attaches it to the Quark functions:

```
    //  #define           QUARK_FAMILY{
&uquark, &tquark, &dquark, &iquark }
    /* Add this code */
    #define QUARK_FAMILY{ &uquark,
&tquark, &dquark }
    /* Add this code */
    #endif
```

In conclusion, both DTLS and Quark had suitable improvements with the target of reducing resource consumption. In the DTLS, we decrease the length of some keys and remove DoS Countermeasures while in the Quark, we decrease the length of the input data block and build a new type of Quark with the lower length of the input data block. From these improvements, the operation of the comprehensive security solution with DTLS, Quark, and Overhearing will consume fewer resources enough to avoid causing the out of resource phenomenon in WSN System.

3.2. Design and installation of the simulation and experiment

3.2.1. Design schedule of experiments

Like the abovementioned, the target of this study is to prove the realizability, the effectiveness, and the optimization in the combination of DTLS, Quark, and overhearing in the IoT System in a comprehensive security structure for IoT, thus, we simulate our combining solution in Contiki-OS. Source code "*tiny-dtls*" and "*quark-master*" are adequate for almost IoT simulations in the Contiki OS. It is necessary to validate whether the DTLS and the Quark prevented the overhearing activities in suffering DoS Attack by Botnet and UDP flood, although its encryption is independent of the overhearing. We designed 6 simulation test cases where 3 of them run in normal transmission and the rest runs in overload transmission for simulating a DoS Attack.

- *Scenario 1 (TC1):* The network works normally, does not install Overhearing, and does not install DTLS and Quark.

- *Scenario 2 (TC2):* The network works normally, installs overhearing, and installs the original DTLS and Quark.

- *Scenario 3 (TC3):* The network works normally, installs overhearing, and installs improved DTLS and Quark.

- *Scenario 4 (TC 4):* The network works when attacked by a DoS attack, does not install Overhearing, and does not install DTLS and Quark.

- *Scenario 5 (TC 5):* The network works when attacked by a DoS attack, installs overhearing, and installs the original DTLS and Quark.

- *Scenario 6 (TC 6):* The network works when attacked by a DoS attack, installs overhearing, and installs improved DTLS and Quark.

From these 6 scenarios, easily compared and collated between cases, the time is 50 minutes each.

3.2.2. Topology of simulation

The IoT Network uses the grid topology which is extremely popular in IoT Systems because of increasing the number of neighbors of each node and thus increasing the flexibility in routing.

In Fig. 4a and 4b, nodes with black background and white characters are Server nodes while nodes with white background and black characters are Client nodes. A node can be transmitted directly to all its side-by-side nodes in vertical, horizontal, and 2 diagonal lines [4]. In Fig. 4b, there are 3 Bot nodes with dark-upward-diagonal background patterns which launch DoS Attack by sending a large amount of UDP Packets to dominate the resource of the Server. The location of Bot is various to ensure the DoS Attack effects all IoT Network. In experiments, the Sensor nodes must send a data message to a Sink node with a fixed frequency. The total time in each test case is 50 minutes.

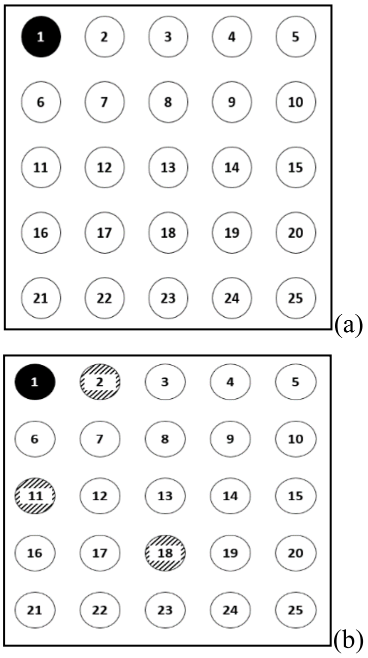

Fig. 4. Topology IoT Network Simulation Test cases. (a) Normal transmission Test cases, (b) Overload transmission Test cases

4. Results of experiments

4.1. Measurement Criterions

Three measuring criteria are Packet Delivery Ratio, Latency, and Energy Consumption.

4.1.1. Packet Delivery Ratio

The Packet Delivery Ratio (PDR) is the rate between the number of received packets and the number of sent packets. The unit of PDR is percent (%). Formula (1) calculates PDR:

$$PDR = \frac{R}{S}\, x\, 100 \qquad (1)$$

In (1), S is the number of packets the calculating node sent while R is the number of packets the other nodes received from the calculating node.

4.1.2. Latency

Latency is the average time between departing a packet from the sender (calculating node) and arriving at the receiver. The basic unit of Latency in milliseconds (ms). Formula (2) calculates Latency:

$$Latency = \frac{\sum_{i=1}^{n} \frac{TR_i - TS_i}{D_i}}{n} \qquad (2)$$

In (2), *n* is the number of successful transmission packets, *i* is the index of packet, *T(S)i* is the time the calculating node sent packet index *i* while *T(R)i* is the time the receiver received packet index *i*.

4.1.3. Energy Consumption

Energy Consumption is the abstract criterion that represents the amount of energy consumed in different simulation activities. In Contiki, the energy consumption is calculated by the rate between the time node for different tasks (sending packets, receiving packets) and a total time of the simulation. However, Source forge proposed (3) to calculate energy consumption measured by mile Joule (mJ) from the abstract value [14].

$$E = (Tx\,.\,E_t + Rx\,.\,E_r + CPU\,.\,E_o + LPM\,.\,E_l)\,\tau \qquad (3)$$

In (3), *Tx* is the rate between the time a node uses to send packets and total simulation time while *Rx* is the rate between the time a node uses to receive packets and total simulation time. CPU is the energy consumption of CPU for simulation (different kinds of node has different CPU value) and LPM is the rate between the time a node uses for basic tasks of node and total simulation time.

4.2. Results and Evaluation

4.2.1. Table of results

In total WSN, we will measure three criteria and take the average value of all nodes in WSN from TC1 to TC6. The result is indicated in Table 1.

4.2.2. Evaluation of results

This is an evaluation of the results of experiments indicated in Table 1:

- In case WSN works normally, the integration of Overhearing mechanism, DTLS protocol and Quark light encryption will reduce network performance. Energy is the parameter that is increased fastest. However, communication-related parameters such as PDR and Latency still ensure the network's normal operation. Even the energy gain is not too large to cause energy depletion.

Table 1. Results of experiments

	Condition	**Overhea ring**	**DTLS Quark**	**PDR (%)**	**Latency (ms/m)**	**Energy (mJ)**
TC 1	Normal transmission	Yes	Yes	98.43	613.14	147.92
TC 2		No	Original	84.50	2539.46	361.66
TC 3		Yes	Improved	**95.01**	**714.25**	**299.52**
TC 4	Overload transmission under DoS Attack	No	No	16.67	51064.53	1000.02
TC 5		Yes	Original	79.14	3145.97	505.38
TC 6		Yes	Improved	**93.91**	**821.02**	**371.64**

- In the case of a DoS attack, the overhearing mechanism also detects early and limits the consequences of a DoS attack, although the network parameters are reduced, it still ensures that the network maintains communication activities. This shows that the Quark lightweight code does not affect the operation of the overhearing mechanism.

- In both the case of DoS attack and non-DoS attack, the WSN network that installs the security solution with DTLS, and Quark natively reduces the encryption key, there is a decrease in performance and is not satisfactory for the network to operate stably. This shows the need for improvements, including that reducing key lengths can reduce the security of security mechanisms.

- In summary, the simulation experiment of a general security solution has achieved the research goal set out. The reliability and efficiency of the overhearing mechanism have been verified again by the parameters shown in the simulation experiment, even when the data is affected by the Quark lightweight code. The IoT network that installs both DTLS protocol, Quark hash function and Overhearing mechanism reduces performance but not too much (less than 10%) and still maintains IoT network operation stability and improves security somewhat, information security for the system. Power consumption and performance loss are unavoidable when installing security mechanisms, and the results show that the ratio is acceptable in existing networks. In addition, through comparison and contrast between the network installed what security solution with DTLS and Quark native and modified it, shows the importance of improvements to reduce cipher length to avoid WSN network performance degradation. capacity due to resource depletion has been demonstrated.

The DTLS and the overhearing were validated by monitoring WSN performance in overload transmission caused by a DoS attack and the unavoidable challenges of this comprehensive security solution appeared as well as the effectiveness of our improvement. The experiment simulating a comprehensive security solution completes all tasks.

5. Conclusion and Future Development

The proposed solution includes a location model, and improvements to allow DTLS and Quark protocols to adapt to IoT with low-power WSN networks. In this study, we also deploy a DoS attack simulation experiment as well as a network with DTLS and Overhearing protocol to demonstrate the advantage of the proposal. Measurements of network traffic, latency, and loss rate of information show that the network remains stable, the solution has effectively prevented attacks when simultaneously installing DTLS, Quark and Overhearing. In terms of resource-constrained IoT, the proposed model shows newness, safety, and stability in the system for which no previous studies have been published.

The results in the solution presented are all done in the ideal environment provided by the Contiki OS support simulation, however in reality there may be some errors due to the impact of the environment, weather, and surrounding waves. Due to the practical conditions that do not allow the authors to carry out simulation experiments on real equipment models and the actual environment, there are still many limitations. In the near future, the authors and colleagues will continue to study and develop solutions to further optimize the proposed model, have more thorough and convincing analysis of real environmental conditions, develop solutions for specific devices with higher configuration with stronger, higher intensity attacks to assess the correctness of the model on a large scale, our proposal also keeps its effectiveness.

Reducing the key length and reducing loops in encryption algorithms affect the safety of the algorithm. Nevertheless, the goal of the system is to integrate a variety and overcome the limitations of weak resource equipment characteristics for the solution to be feasible and the system needs to operate under installation conditions. Through the measurement results, showed that the solution model has had very positive results, limiting the basic attacks under binding conditions as mentioned. The authors compared the previous options and found that the results are similar and have solved the limitations that previous works are lacking. This proposal can be considered as a model solution, the choice of a solution is holistic and minimizes the consequences of basic attacks in the scope, the object of research as proposed is clearly a valuable solution. Compared to the original models that have not been modified customizing improvements in the solutions, the results are remarkable.

Acknowledgments

Our team sends gratefulness to tutors and colleagues for providing adequate support about infrastructure and advice during the research process. They work in Bach Khoa Cipher Security Center and other faculties in School of Information Communication Technology, Hanoi University of Science and Technology as well as Vietnam National University, Hanoi.

References

[1] Nguyen Van Tanh, Ngo Quang Tri, Nguyen Gia Tuyen, Tran Quang Duc, Tran Hai Anh, Bui Trong Tung, The flooding attack in low power and lossy networks: a case study, the 7th International Conference on Smart Communications in Network Technologies", Internet Engineering Task Force, El Oued, Algeria, October 2018. https://doi.org/10.1109/SaCoNeT.2018.8585451.

[2] Nguyen Van Tanh, Ngo Quang Tri, Nguyen Gia Tuyen, Nguyen Linh Giang, Nguyen Viet Tien, design a security system for internet of things with detecting and eliminating denial of service attack based on overhearing mechanism, the 3rd Symposium of Information Security, Vietnam Ministry of Information and Communication, Danang City, Vietnam, December 2018.

[3] Samonas S, Coss D, The CIA strikes back: redefining confidentiality, integrity and availability in security, Journal of Information System Security, vol 10, no 3 (2014), p. 21-45.

[4] Nguyen Van Tanh, Ngo Quang Tri, Nguyen Ngoc Cuong, Nguyen Linh Giang, Nguyen Anh Tuan, Design of comprehensive security solution on internet of things with improved DTLS protocol and overhearing mechanism, Fundamental Applied Information Technology Research, Vietnam Ministry of Information and Communication, Nha Trang, Vietnam, October 2020.

[5] Allan Pratt, CIA Triad and New Emerging Technologies: Big Data and IoT, Los Angeles City College and Consultant, 2015.

[6] Lovepreet Kaur Somal, IIKaranpreet Singh, Virk, Classification of distributed denial of service attacks – architecture, taxonomy and tools, Computer Science & Technology (IJARCST 2014).

[7] T Dierks, E. Rescorla, The transport layer security (TLS) protocol version 1.2. RFC 5246, Proposed Standard, Internet Engineering Task Force, 8/2008. https://doi.org/10.17487/rfc5246.

[8] J. Yashaswini, A review on IoT secrity issues and countermeasures, Orient Journal Computer Science and Technology 10.2 (2017): 454-459. http://dx.doi.org/10.13005/ojcst/10.02.28.

[9] Hai-Ying Zhou, Dan-Yan Luo, Yan Gao, De-Cheng Zuo, Modeling of node energy consumption for wireless sensor networks, Scientific Research, p18 – 23, 2011. https://doi.org/10.4236/wsn.2011.31003.

[10] Atul Kahate, Cryptography and Network Security, Third Edition, Computer Science, Pune University and Symbiosis International University, 2013.

[11] William J. Buchanan, Shancang Li, Rameez Asif, Lightweight cryptography methods, Journal of Cyber Security Technology, Volume 1, Issue 3 – 4, March 2018. https://doi.org/10.1080/23742917.2017.1384917.

[12] Jean-Philippe Aumasson, Luca Henzen, Willi Meier, Marıa Naya-Plasencia, Quark: A Lightweight Hash, Nagravision S. A., Cheseaux, Switzerland, 2010.

[13] Bertoni G, Daemen J, Peeters M, Assche G V, On the indifferentiability of the sponge construction, Volume 4965 of LNCS, Springer (2008), p. 181–197.

[14] Mohammad Abdellatif, Power Consumption, Contiki Developer, 2017.