A Comprehensive Security Solution for IOT Network with Integrated Technology of Improved Lightweight Encryption Mechanisms

Nguyen Van Tanh
VNU - International School
Vietnam National University (VNU)
144 Xuan Thuy Str, Cau Giay Dist
Hanoi, Vietnam
tanhnv@vnu.edu.vn, tanh.nguyenvan@hust.edu.vn

Ngo Quang Tri
SOICT
Hanoi University of Science and Technology
01 Dai Co Viet Str, Hai Ba Trung Dist
Hanoi, Vietnam
Tri.ngoquang@sie.edu.vn

Nguyen Linh Giang
SOICT
Hanoi University of Science and Technology
01 Dai Co Viet Str, Hai Ba Trung Dist
Hanoi, Vietnam.
Giang.nguyenlinh@hust.edu.vn

Duy-Tien Le
VNU - International School
Vietnam National University (VNU)
144 Xuan Thuy Str, Cau Giay Dist
Hanoi, Vietnam
leduytien@vnu.edu.vn, ldtien82@gmail.com

***Abstract* - With the rapid development of the Internet of Things (IoT) network, the threats of information insecurity are increasing so there have been many proposals for IOT security, however, so far there is no one that is truly effective and comprehensive. In our previous research, we have focused on Lightweight encrypt, with the primary goal of simplifying loops of encryption algorithms, reducing computation requirements, and reducing energy consumption, the system is still safe, integrated into the new protocols of the IoT network. In this article, we proposed a comprehensive security solution including the improved DTLS in Transmission Layer, the improved Quark and the improved Overhearing in Sensor Layer. Our solution include location diagram, improvements to decrease resource consumption of the DTLS and the Quark for adapting to low-energy network. After proposed theoretical basis, our team set up simulating experiments in Contiki Operating System to deploy comprehensive security including DTLS, Quark and Overhearing as well as simulate a DoS Attack by Botnet and UDP Flood. Our team measuring criterions of WSN performance such as PDR, Latency and Energy Consumption and the their results proved the stable operation of WSN with installing this comprehensive security solution and suffering a simulated DoS Attack.**

Keywords - Internet of Things, Security, Wireless Sensor Network, DTLS, Overhearing, Quark, Lightweight security

I. INTRODUCTION

The rapid development of Application for the Internet of Things (IoT) lead to the rise of threat about information security and data security with three basic characters including Confidentiality, Integrity and Availability. In IoT System, the Gateway and the Sensors Environment is vulnerable against these Sniffing and Spoofing Attack to the Confidentiality and Integrity, respectively, so scientists designed cryptographic mechanisms including the DTLS Protocol covering the Gateway and Quark Lightweight Cryptography covering the Sensors Environment. In the other hands, the Sensors Environment with limited resource become vulnerable against DoS Attack to the Availability so scientist design the Overhearing mechanism to prevent this kind of attacks. With these mechanisms is implemented, all basic characteristics are protected so it becomes a Comprehensive solution.

The paper I divided into 6 sections: section I introduces the basic overview of study; section II on Related works cover papers related to this study and those to suggest improvements; section III deals with comprehensive security solutions with improved DTLS, overhearing and quark lightweight cryptography to describe a comprehensive security solution; section IV deals with the simulation experiments to describe the process for overall design and content of experiments, section V on results of experiments describes the measuring criterions, results and their evaluation, finally section VI deals with conclusion and future developments.

II. RELATED WORKS

In the past, our research team researched and improved the Overhearing mechanism and our study about this published in the 7th IEEE International Conference of Smart Communication in Network Technologies (SaCoNet 2018) in El Oued, Algeria [1] and Symposium of Information Security (SoIS 2018) at Da Nang, Vietnam [2]. After that, we proposed the Comprehensive security solution including the improved DTLS and the Overhearing and published in Fundamental Applied Information technology Research (FAIR 2020) in Nha Trang, Vietnam [5]. However, we recognized that this solution is not perfect and thus, we continued to research improved and integrating Quark Lightweight Cryptography to the Comprehensive solution with improved DTLS and Overhearing. Similar to the proposed solution in FAIR 2020, the process to research this Comprehensive solution also require deep theoretical research as well as careful experiment

DOI 10.5013/IJSSST.a.21.04.14 ISSN: 1473-804x online, 1473-8031 print

to find the balance between secure level and resource consumption with each single security mechanism as well as comprehensive security solution and this study concentrates on this process.

III. COMPREHENSIVE SECURITY SOLUTION WITH IMPROVED DTLS, OVERHEARING AND QUARK LIGHTWEIGHT CRYPTOGRAPHY

In this Chapter, we indicate our approach about design a comprehensive security solution based on CIA Security Triangle. Then, we introduce our previous study about the comprehensive security solution combining the DTLS and the Overhearing. After our indication about drawbacks of this solution, we introduce Quark Lightweight Cryptography as well as describe the integration of this mechanism to our previous proposal.

A. Comprehensive Security Solution with Improved DTLS and Overhearing)

A1. Comprehensive Security Solution

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

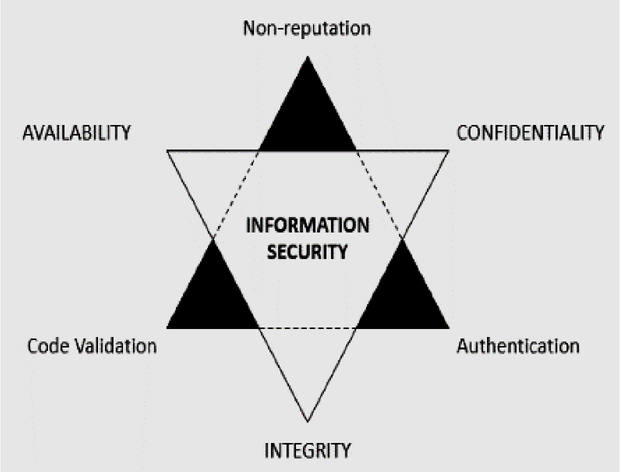


Fig. 1. Indication of extend Security 6-pointed star CIA

The IoT system will be absolutely safe if its security solution protect both 3 basic characteristics in the Security CIA Triangle because the safety of 3 basic characteristics will ensure the safety of 3 other extend characteristics and it means all necessary characteristics of IoT System are in protection.

A2. Comprehensive Security Solution with Improved DTLS and Overhearing

DTLS was established by Netscape Communications [4] concentrates to prevent all threats 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] concentrates 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 the Comprehensive security solution, the high resource consumption of the DTLS becomes a hard challenger and our team must research and propose some improvement like reducing length of key and remove DoS Countermeasures [5].

A3. Disadvantage of Comprehensive Security Solution

We recognize the protection area of DTLS cover only the Gateway and but the transmission in Sensors Environment is not protected by cryptographic mechanism. As the result, the Sensors Environment become vulnerable against threat at Confidentiality and Integrity. This problems is serious because the volume of transmission in Sensors Environment is much higher than this in the Gateway. Moreover, the Overhearing works at the Sensors Environment, this vulnerability facilitate the rise of danger in DoS Attack when Barmaster might use sniffing and spoofing Attack to weaken the Overhearing mechanism before launching DoS Attack. Therefore, it is necessary to integrate a cryptographic to protect the Confidentiality and Integrity of Information Security in Sensors Environment. Our team researched and select Quark Cryptographic as a final piece for the Comprehensive security solution.

B. Combined Quark Lightweight Cryptography in Comprehensive Security Solution with DTLS and Overhearing

B1. Comprehensive Security Solution with Improved DTLS and Overhearing

Quark Lightweight Cryptography was developed by Jean-Philippe Au Masson with low resource consumption for the tiny-scale WSN such as Radio Frequency Identification (RFID) System [8] with the advantage is suitable meet our requirement about lightweight cryptography with low energy consumption for combining in comprehensive security solution. Quark uses padded sponge construction which is developed by Guido Bertoni from STMicroelectronics [9], with 6 turns data is hashed by a hash function which the output of previous turn would be the input of the next. As the result, the secure level increases rapidly when the number of turns data is hashed increases but it can reuse volume of data, thus, decrease resource consumption in WSN. Fig 2 describes the padded sponge construction in Quark. It noted from Fig 2 that all block "Hash Function" represent only one hash function in the Quark but process data 6 turns.

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

B2. 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 [5]. With the Quark Lightweight Cryptography, because it aim is protecting sensor nodes so it is installed in Sensor Layer. Fig 3 describes position of installation and target of each mechanism.

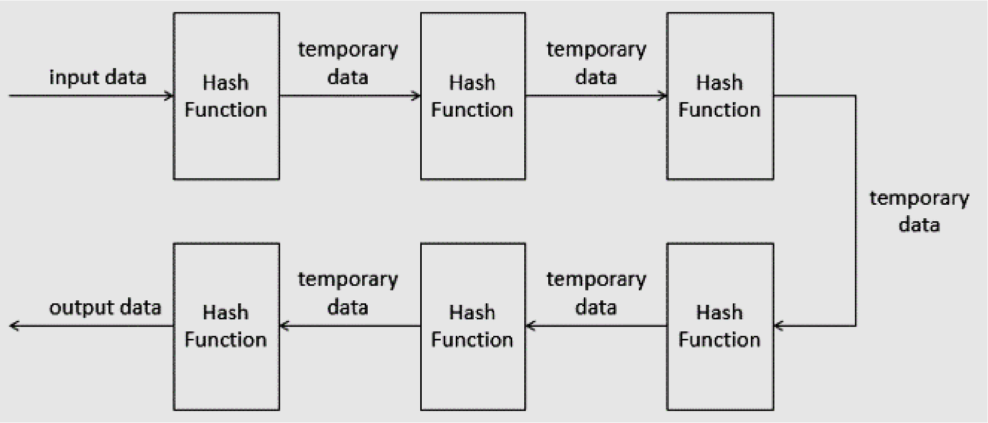


Fig.2. Padded sponge construction in the Quark.

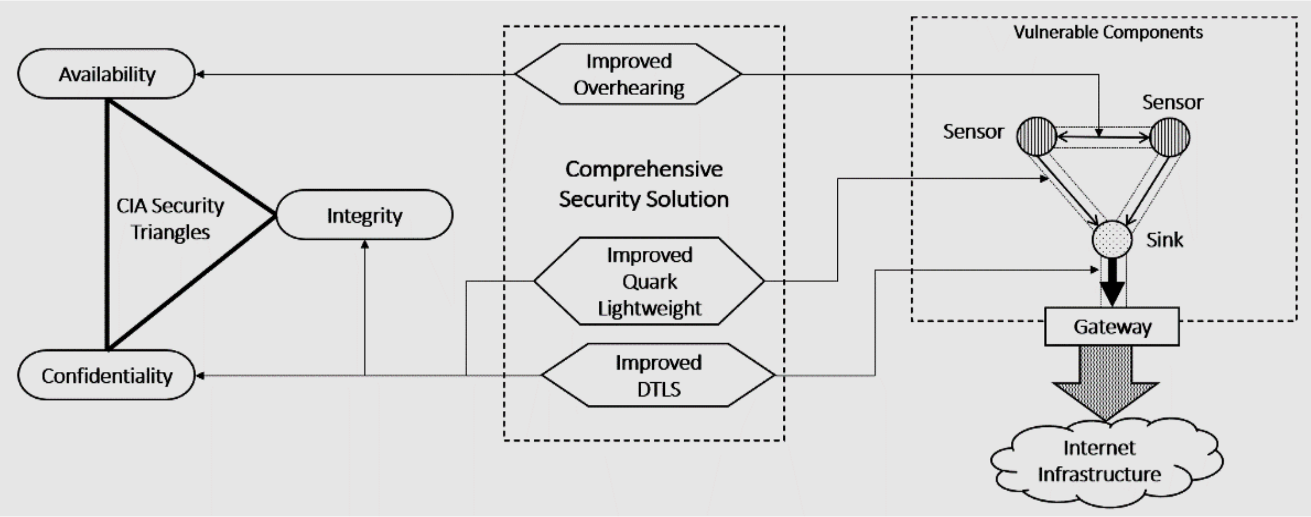


Fig.3. Location and Target of the Comprehensive Security Solution

From Fig 3, the Overhearing and Quark are installed in all vulnerable components conclude Sensor Node, Sensor Environment and Gateway. Firstly, these components have weak bandwidth, limited resource and weak back-up mechanism so the DoS Attack destroys the IoT Network easier than the Internet. Secondly, these components use IoT standards which lack effective security solutions in current world while the Internet Security is protected by strong security mechanisms such as TLS.

B3. Challenges of Combination between DTLS, Overhearing and Quark in IoT System

Similar to FAIR 2020 [5], the combination between Quark and this old security solution have some disadvantages. Firstly, like all security solutions, Quark Lightweight Cryptography, DTLS mechanisms and protocols must consume resource in operating and dominate resource of other IoT components, thus can cause the IoT activities are 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 content of all packets to secure as well as makes some difficulty for the hashing process of Quark.

IV. SIMULATION EXPERIMENTS

In this section, we describe the implementation of our proposal about the comprehensive security solution as well as design experiments to proof the efficiency of the solution. All implementation and experiments are in Contiki simulation because this simulation creates reliable experimental environment with minimum costs.

A. Implementation of Comprehensive Security Solution in Contiki Operating System

Our experiments are implemented in Contiki Operating System which is reliable operation system about IoT simulation. Our research team has a large amount of experience as well as necessary source code with this platform during the previous study.

A1. Combination between Improved DTLS Protocol and Overhearing Mechanism

In the previous published papers [1] [2] [5], our team researched and proposed the 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 simulate a DoS Attack by UDP Flood and Botnet in square grid WSN. In FAIR 2020, we have some improvement in file “tiny-dtls” to reduce energy consumption including reducing length of key and eliminating DoS Countermeasures. However, because of combining the Quark, the process for reducing length of key such as:

Decrease key length of Advanced Encryption Standard (AES) encryption: In FAIR 2020, the key length is decreased from 16 bits to 4 bits [5]. However, in this study, we continue to decrease to 2 bit to combine the Quark.

Decrease key length of Secure Hash Algorithm (SHA): We keep the improvement in FAIR 2020 which decrease the key length from 32 bits to 8 bits.

A2. Integrate improved Quark Lightweight Cryptography to the existed comprehensive security solution.

Similar to the DTLS, the Quark has a version in the Contiki OS and in was organized in folder “quark-master” [8]. 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 save 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 call “i-Quark” (improved Quark) which the length of input data block is 4 bit.

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

With the second improvement which decrease number of hashed turn, 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 length of input data block, it is more complicated than the second one because it require to create new data structure “IQUARK” representing i-quark and attach it into the Quark functions with the role of Quark type (similar to “UQUARK” representing u-Quark, “DQUARK” representing d-Quark and “TQUARK” representing t-Quark). All change in source code is implemented in file “quark.h”. This source code in below rectangle create 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     4
/* Add this code */
This source code in below rectangle attaches it into the
Quark functions:
// #define   QUARK   FAMILY{&uquark,   &tquark,
&dquark, &iquark  }
/* Add this code */
#define QUARK_FAMILY{&uquark, &tquark, &dquark
}
/* Add this code */
#endif
```

It is noted that removed code lines is shown in these above rectangles but is deactivated by prefix "//" while the added code lines is surrounded by 2 deactivated code lines /* Add this code */ at the top and bottom.

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

B. Design and Installation of the Simulation and Experiment

B1. Design Schedule of Experiments

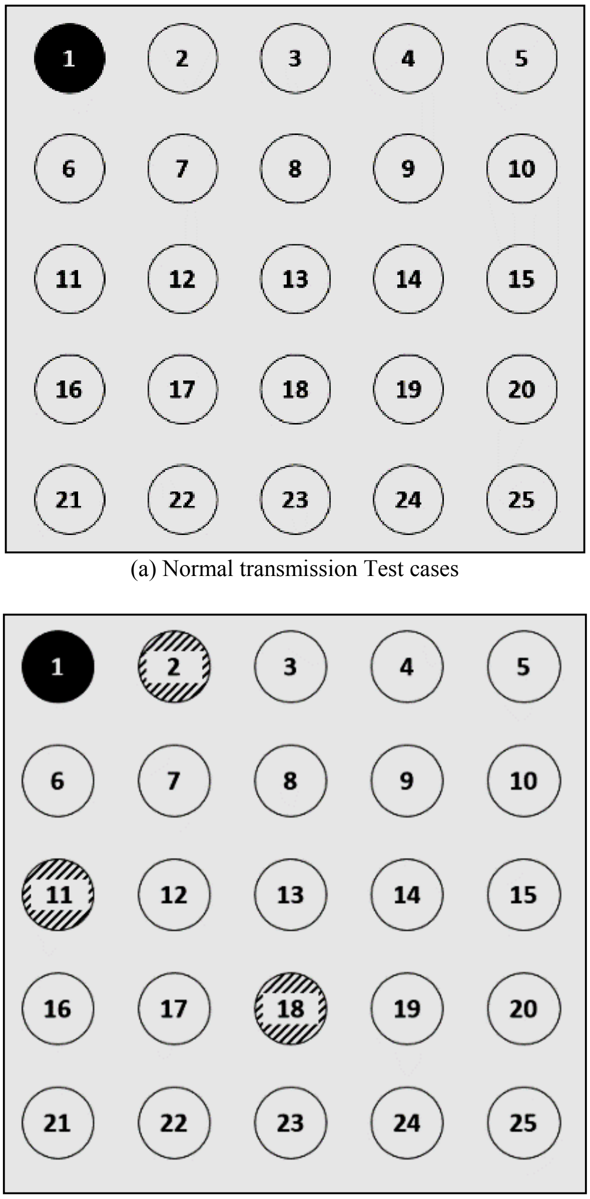
As the above mention, the target of this study is proving the realizability, the effectiveness and the optimization in combination between DTLS, Quark and Overhearing in the IoT System in a comprehensive security structure for IoT, thus, we simulate our combining solution in Contiki-OS. Source code "tiny-dtls" and "quark-master" is adequate to 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 with the Overhearing. We designed 4 simulation test cases with 2 of them run in normal transmission and the rest runs in overload transmission for simulating a DoS Attack.

- Test case 1 (TC 1): Normal transmission, no Overhearing, no DTLS and Quark.
- Test case 2 (TC 2): Normal transmission, installing Overhearing, installing DTLS and Quark.
- Test case 3 (TC 3): Overload transmission, no Overhearing, no DTLS and Quark.
- Test case 4 (TC 4): Overload transmission, installing Overhearing, installing DTLS and Quark. It is totally the comprehensive security solution.

From these 4 Test cases, it is easy to mutually compare the test cases.

B2. Topology of Simulation

The IoT Network use the grid topology which is extremely popular in IoT Systems because of increasing the number of neighbor of each node and thus increasing of the flexibility in routing. Fig 4 described the topology of simulation in 2 transmission conditions including Normal and Overload.



(a) Normal transmission Test cases

(b) Overload transmission Test cases

Fig.4. Topology of IoT Network in simulation Test cases.

In Fig 4a and 4b, nodes with black background color and white character color are Server nodes while nodes with white background color and black character color are the Client nodes. Similar to FAIR 2020, a node can be transmit directly to all its side by side nodes in vertical, horizontal and 2 diagonal lines [5]. In Fig 4b, there are 3 Bot nodes with dark-upward-diagonal background pattern which launch DoS Attack by sending large amount of UDP Packets to dominate the resource of Server. The location of Bot is various insure the DoS Attack effects all IoT Network. In experiments, the Sensor nodes must send data message to a Sink node with fixed frequency. Total time in each testcase is 5 minutes.

V. RESULTS OF EXPERIMENTS

In this chapter, we describe some criterions for measuring the performance of simulated experiments. After the indication of the result, we evaluate this result and relate it to the target of experiments as well as aim of this study.

A. Measurement Criterions

Three measuring criterions conclude Packet Delivery Ratio, Latency and Energy Consumption.

A1. Packet Delivery Ratio

Packet Delivery Ratio (PDR) is 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 Formula (1), S is the number of packets the calculating node sent while R is the number of packets the other nodes received from calculating node.

A2. Latency

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

$$Latency = \frac{\sum_{i=1}^{n}(t(R)_i - t(S)_i)}{n} \qquad (2)$$

In Formula (2), n is 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.

A3. Energy Consumption

Energy Consumption is the abstract criterion represents to which amount of energy is 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 total time of simulation. However, Sourceforge proposed the Formula (3) to calculate energy consumption measured by mile Joule (mJ) from the abstract value [7].

$$E = (Tx\ x\ 19.5 + Rx\ x\ 21.8 + CPU\ x\ 1.8 + LPM\ x\ 0.545)\ x\ \frac{3}{32768} \qquad (3)$$

In Formula (3), Tx is the rate between time a node uses to send packets and total simulation time while Rx is the rate between time a node uses to receive packets and total simulation time. CPU is energy consumption of CPU for simulation (different kind 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.

B. Results and Evaluation

B1. Table of Results

In total WSN, we measured three criterions and take the average value of all nodes in WSN from TC1 to TC4. Table I indicates the results of experiments.

TABLE I. RESULTS OF EXPERIMENTS

	Condition	Overhearing, DTLS and Quark	PDR (%)	Latency (ms)	Energy (mJ)
TC1	Normal transmission	No installed	98.43	613.14	147.92
TC2		Installed	95.04	692.11	231.84
TC3	Overload transmission under DoS Attack	No installed	16.67	51064.53	1000.02
TC4		Installed	94.98	801.18	332.17

B2. Evaluation of Results

The evaluations of the results of experiments are as shown in Table I.

In normal deployment of comprehensive security solution combining Quark, DTLS and Overhearing decreased the performance of WSN, especially, the energy consumption increased a large amount in a small period. The reason of this decrease is the operation of both 3 security mechanisms also consume resource of WSN. However, the decrease completely did not delay the operation of WSN, the PDR and Latency was still above threshold for stable transmission.

In overload transmission from a simulated DoS Attack, the Overhearing detected this attack early restricted its consequence. All criterions of WSN in spite of decreasing but still above threshold for stable transmission. It also proved the operation of Quark does not eliminate the efficiency of the Overhearing.

The DTLS and the Overhearing was 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 out improvement. The experiment simulating comprehensive security solution completes all tasks.

VI. CONCLUSION AND FUTURE DEVELOPMENT

From this paper, we classified all risks at Security and Information Safety in IoT System by 3 information security characteristics including Confidentiality, Integrity and Availability. In addition, we indicated all components which is vulnerable about security including Gateway and Sensors Environment. With each security characteristic and each component, we proposed independent security solutions such as DTLS Protocol preventing sniffing and spoofing Attack in Gateway, the Quark Lightweight Cryptography preventing these Attacks in Sensors Environment and Overhearing mechanism preventing DoS Attack in Sensors Environment. In this article, we design a comprehensive security solution combine the DTLS, the Quark and the Overhearing to provide the full protection to the vulnerable components of IoT network. The efficiency of our proposal was proofed by measuring performance of simulated experiments in Contiki platform. In our future research, we will continue work on ideas from FAIR 2020 which deploy this comprehensive security solution in real IoT System with Arduino devices and integrating and combining more security solutions to provide a strong protection level such as Blockchain mechanism [5]. Our targets for the proposed simulations will be effectiveness, reliability, adequate costs and minimum resource consumption.

ACKNOWLEDGMENT

We wish to express our gratitude to tutors and colleagues for providing excellent support in infrastructure and advice during the research process, in particular staff at the Bach Khoa Cipher Security Center and other faculties in the School of Information Communication Technology, Hanoi University of Science and Technology as well as Vietnam National University. This research is funded by Hanoi Department of Science and Technology under the project 01C-02/01-2019-3.

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

[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 detectinng 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] T Dierks, E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246”, Proposed Standard, Internet Engineering Task Force, 8/2008.

[5] 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.

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

[7] Mohammad Abdellatif, “Power Consumption”, Contiki Developer, 2017

[8] Jean-Philippe Aumasson, Luca Henzen, Willi Meier, Marıa Naya-Plasencia, “Quark: a lightweight hash”, Nagravision S. A., Cheseaux, Switzerland, 2010

[9] 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.