A Solution to Improve the Security of the Internet of Things Network with Lightweight Encryption Methods

Nguyen Van Tanh1, Ngo Quang Tri2, Nguyen Linh Giang3, Tien-Le Duy4

1,4 International School – Vietnam National University, 144 Xuan Thuy Str, Cau Giay Dist, Ha Noi
2,3 Hanoi University of Science and Technology, No. 1, Dai Co Viet Str, Hai Ba Trung Dist, Hanoi, Vietnam
*tanhnv@vnu.edu.vn

Abstract. Security is an important issue in the Internet of Things networks. Conventional security solutions do not have great value on the IoT network because of many special elements of this system. The article introduces new innovations in security solutions, building comprehensive security systems for the IoT network by combining multiple lightweight encryption methods, installed on layers, against attacks, exploit common basic information. The system is built to ensure the feasibility, confidentiality, efficiency, cost, and balance with the low energy system on the IoT network. This study is implemented on vulnerable layers of IoT, indicating the results after comparing and evaluating different experimental models and scenarios.

1. Introduction

The rapid development of application about Internet of Things (IoT) leads the rise of threat about information security and data secure with three basic characters including Confidentiality, Integrity and Availability. In the past, our research team also researched and improved the Overhearing mechanism as well as installed simulated experiments in Contiki Operating System and published in some papers [1] [2]. We also proposed the Comprehensive security solution including the improved DTLS and the Overhearing. We recognize that this solution is not perfect because the Confidentiality and Integrity of Information Security in the Sensors Environment is not protected. Therefore, we continued to research improved and integrating Quark Lightweight Cryptography to the proposed Comprehensive solution, so our new solution with the improved DTLS, improved Quark and Overhearing can protect all vulnerable components of IoT System. The process to research this Comprehensive solution also require deep theoretical research as well as careful experiment 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.

The study has 5 Sections: “Section 1: Introduction” introduces the basic overview of study; “Section 2: Comprehensive security solution with improved DTLS, Overhearing and Quark lightweight cryptography” describes the Comprehensive security solution; “Section 3: Simulation Experiments” describe process to design and content of experiments, “Section 4: Results of experiments” describes measuring criterions, result and it evaluation and “Section 5: Conclusion and future development” concludes the study and indicated future work.
2. Comprehensive security solution with improved DTLS, Overhearing and Quark lightweight cryptography

2.1 Introduction about comprehensive security solution with improved DTLS and Overhearing

a. Introduction about comprehensive security solution

Three basic characteristics of security and information safe are defined in CIA Security Triangle [4] concluded: Integrity, Availability and Confidentiality. Moreover, the extent Security 6-pointed star CIA [5] is indicated in Figure 1 with the addition of more 3 extend characteristics. In Figure 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:

![Figure 1. Indication of extend Security 6-pointed star CIA](image)

The IoT system will be absolutely 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 extend characteristics and it means all necessary characteristics of IoT System are in protection.

b. Comprehensive security solution with improved DTLS and Overhearing

DTLS was established by Netscape Communications [6] 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] 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 the combination between the DTLS and 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 [3]. However, the protection area of DTLS covers 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. Our team researched and select Quark Cryptographic as a final piece for the Comprehensive security solution.

2.2 Overhearing Combine Quark Lightweight Cryptography in Comprehensive Security Solution with DTLS and Overhearing

a. Comprehensive security solution with improved DTLS and Overhearing

Quark Lightweight Cryptography was developed by Jean-Philippe Aumasson with low resource consumption for the tiny-scale WSN [7]. Quark uses padded sponge construction which is developed by Guido Bertoni from STMicroelectronics [8], with 6 turns data is hashed by a hash function which the output of previous turn would be the input of the next. Figure 2 describes the padded sponge construction in Quark. It noted from Figure 2 that all blocks “Hash Function” represent only one hash function in the Quark but process data 6 turns.
Figure 2. Padded sponge construction in the Quark

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 bits. The larger the length is, the faster the cryptographic speed is, but the cryptography consumes more resource.

**b. 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. With the Quark Lightweight Cryptography, because this mission is protecting sensor nodes, so it is installed in Sensor Layer. Figure 3 describes installation location and target of each mechanism:

Figure 3. Location and Target of the Comprehensive Security Solution

From Figure 3, we recognize that DTLS, Overhearing and Quark are installed in all vulnerable components conclude Sensor Node, Sensor Environment and Gateway.

3. Simulation Experiments

3.1 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 have a large amount of experience as well as necessary source code with this platform during the previous study [1][2][3].

a. Combination between improved DTLS Protocol and Overhearing mechanism

In the previous published papers [1][2][3], our team researched and proposed the Overhearing including detection of Bots by “Singularity point by 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. The combination between Quark and this old security solution has some disadvantages. Firstly, like all security solutions, Quark Lightweight Cryptography, DTLS mechanism and Overhearing protocol must consume resource in operating and dominate resource of other IoT components, thus can cause all IoT activities are delayed. Secondly,
Lightweight Quark and DTLS Protocol also changes data and information in IoT operation. In fact, in old security solution, we have some improvements 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 must be re-designed such as, firstly, decrease key length of Advanced Encryption Standard (AES) encryption: the key length is decreased from 16 bits to 2 bits and, secondly, decrease key length of Secure Hash Algorithm (SHA) from 32 bits to 8 bits.

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

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 such as, firstly, 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 bits and, secondly, 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. 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.

3.2 Design and installation the simulation and experiment

a. Design schedule of experiments

We simulate our solution in Contiki-OS. The validation of the fact whether the DTLS and the Quark prevented the Overhearing activities in suffering DoS Attack by Botnet and UDP Flood is extremely necessary, although its encryption is independent with the Overhearing. We designed 4 test cases of simulation:

1) Test case 1 (TC 1): Normal transmission, no Overhearing, no DTLS and Quark.
2) Test case 2 (TC 2): Normal transmission, installing Overhearing, installing DTLS and Quark.
3) Test case 3 (TC 3): Overload transmission, no Overhearing, no DTLS and Quark.
4) Test case 4 (TC 4): Overload transmission, installing Overhearing, installing DTLS and Quark.

It is total the comprehensive security solution.

From four of these Test cases, the mutual comparison between test cases becomes simple.

b. 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 enhancing of the flexibility in routing.

![Figure 4. Topology of IoT Network in simulation Test cases.](image-url)

In Figure 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 Client nodes. A node can transmit directly to all its side-by-side nodes in vertical, horizontal and 2 diagonal lines. In Figure 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. In experiments, the Sensor
nodes must send data message to a Sink node with fixed frequency. Total time-length in each testcase
is 5 minutes.

4. Results

4.1 Measurement criterions
Three measuring criterions concludes Packet Delivery Ratio, Latency and Energy Consumption.

a. 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:

\[ PDR = \frac{R}{S} \times 100 \]  

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.

b. 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:

\[ \text{Latency} = \frac{\sum_{i=1}^{n} (T(R)_i - T(S)_i)}{n} \]  

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.

c.) Energy consumption
Energy Consumption is the abstract criterion represent 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 and total time of simulation. However, Source forge proposed the
Formula (3) to calculate energy consumption measured by (mJ) from the abstract value [9].

\[ E = (T_x \times 1.95 + R_x \times 21.8 + CPU \times 1.8 + LPM \times 0.545) \times \frac{3}{32768} \]  

In Formula (3), T_x is the rate between time a node uses to send packets and total simulation time while
R_x is the rate between time a node uses to receive packets and total simulation time. CPU is energy
consumption of CPU for simulation 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
a. Table of results
In total WSN, we will measure three criterions and take the average value of all nodes in WSN
from TC1 to TC4. Result is indicated in Table 1.

| Condition         | Overhearing, DTLS and Quark | PDR (%) | Latency (ms) | Energy (mJ) |
|-------------------|-----------------------------|---------|--------------|-------------|
| TC1               | Normal transmission        | No installed | 99.17 | 574.59 | 158.29 |
| TC2               | Installed                  | 95.92 | 603.34 | 294.83 |
b. Evaluation of results

This are some evaluations from results of experiments indicated in Table 1:

1) In normal the 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.

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

From this above evaluation, we can conclude all experiments simulating comprehensive security solution complete all tasks.

5. Conclusion and Future Development

From this paper, 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 included 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. The results proved the stable operation of WSN with installing this comprehensive security solution and suffering a simulated DoS Attack. In the future, we will continue the idea which deploy this comprehensive security solution in real IoT System with Arduino devices and integrating and combining more security solutions to provide the strong protection level such as Blockchain mechanism. Our target of proposed simulations will be effectiveness, reliability, adequate costs, and minimum resource consumption.

Acknowledgements

Our team sends the gratefulness to tutors and the colleagues for providing adequate support about infrastructure and advice during the researching 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. This paper supported by Cortek Co.,ltd in KC01.15 project.

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 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] 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.

[4] 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

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

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

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

[8] 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

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