ISSN- 2350-0530(O) ISSN- 2394-3629(P)
Impact Factor: 2.035 (I2OR)

INTERNATIONAL JOURNAL OF RESEARCH – GRANTHAALAYAH
A knowledge Repository

Science

ENERGY AWARE SECURITY ALGORITHM DECISION METHOD FOR INTERNET OF THINGS USING SSL/TLS FOR WIRELESS NETWORK

Tae-Ho Cho *[1], Jin-Hee Chung [2]
[*1, 2] Department of Information and Communication Engineering, SungKyunKwan University, Republic of Korea

ABSTRACT

The Internet of Things (IoT) is an ever evolving infrastructure of physical objects and Internet-enabled devices and systems featuring IP addresses for connectivity. Physical objects consist of home appliances, electronic gadgets, machinery, healthcare items, wearable devices and anything that could be connected to the Internet. Each type of connection requires particular types of security service. Security algorithms in user devices are fixed by default and selected based on preferences. This limitation causes energy waste since a user might be using all services in an algorithm, even those the user does not need. In order to counter this problem, we propose an energy aware security service selection method that saves energy by selecting only particular types of security service required by a given connection. In this paper, we compared the energy consumption of each communication to provide integrity, authentication, and confidentiality in Secure Sockets Layer/Transport Layer Security (SSL/TLS) with our proposed method. The experimental results demonstrate the validity of our proposed method. Our proposed method saved 54.94% energy for integrity and 74.52% for authentication.

Keywords:
Internet of things; SSL/TLS; MQTT; security service; energy efficiency.

Cite This Article: Tae-Ho Cho and Jin-Hee Chung, "ENERGY AWARE SECURITY ALGORITHM DECISION METHOD FOR INTERNET OF THINGS USING SSL/TLS FOR WIRELESS NETWORK" International Journal of Research – Granthaalayah, Vol. 3, No. 12(2015): 1-8.

1. INTRODUCTION

The Internet of Things (IoT) is an infrastructure that uses the Internet to connect physical objects through IP addresses [1]. The increased data capacity, decreasing cost of broadband internet, and skyrocketing smartphone ownership are generating demand for IoT. The physical objects include refrigerators, ovens, washing machines, lamps, headphones, coffee makers, wearable electronics, and almost everything else that can be connected to the Internet (Fig. 1) [2]. Connectivity makes it possible for users to access and control physical objects from a distance [3]. The development

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
Impact Factor: 2.035 (I2OR)

of the IoT has accelerated recently. Many IoT devices have appeared, but most of these are still low energy and low performance to ensure a reasonable cost for the embedded devices. Thus, these devices usually use a lightweight messaging protocol: message queue telemetry transport (MQTT) [4].

However, MQTT transmits messages in plain text; therefore, we need to use SSL/TLS. The first step in a SSL/TLS handshake is selecting an algorithm which will be used throughout the communication between the two parties. SSL/TLS is a well-developed cryptographic protocol, but it does not consider residual energy or energy consumption of the devices. In wireless communication, there might be devices such as sensors that have very limited energy, and therefore we need to cater to this requirement. Since SSL/TLS is not energy aware it could unnecessarily drain the energy from IoT devices. One of the unique features of IoT devices is that they have their own unique requirements for exchanging data. For example, some devices are used for notification or advertisement, and these require integrity but not confidentiality. There are also some devices for individual purposes like handling personal medical data that require confidentiality and authentication. Therefore, based on the diverse purposes of communication in IoT, selecting security services (e.g., confidentiality, integrity, authentication, etc.) in the first step (i.e., the handshake) can help provide only the required service(s) and can therefore save energy by communicating efficiently.

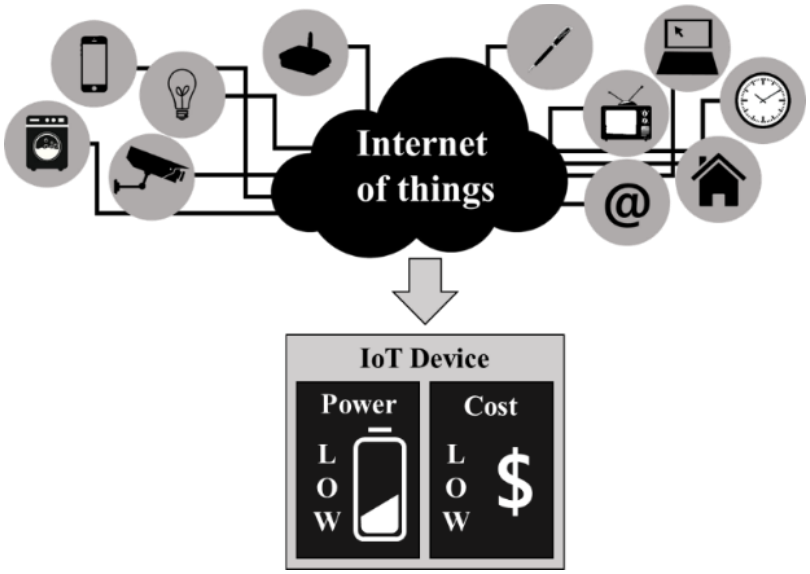

Figure 1: Internet of Things

The rest of this paper is organized as follows. In Section 2, we elaborate on the background of our proposal. We explain the proposed method in Section 3, and in Section 4 we provide the experimental results. The conclusion and future work are provided at the end of the paper.

2. BACKGROUND

This section presents the background of this paper. MQTT, security service, and SSL/TLS are discussed sequentially.

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
Impact Factor: 2.035 (I2OR)

2.1. MQTT

MQTT is a lightweight protocol accepted as a standard message protocol from OASIS (Organization for the Advancement of Structured Information Standard) [5].

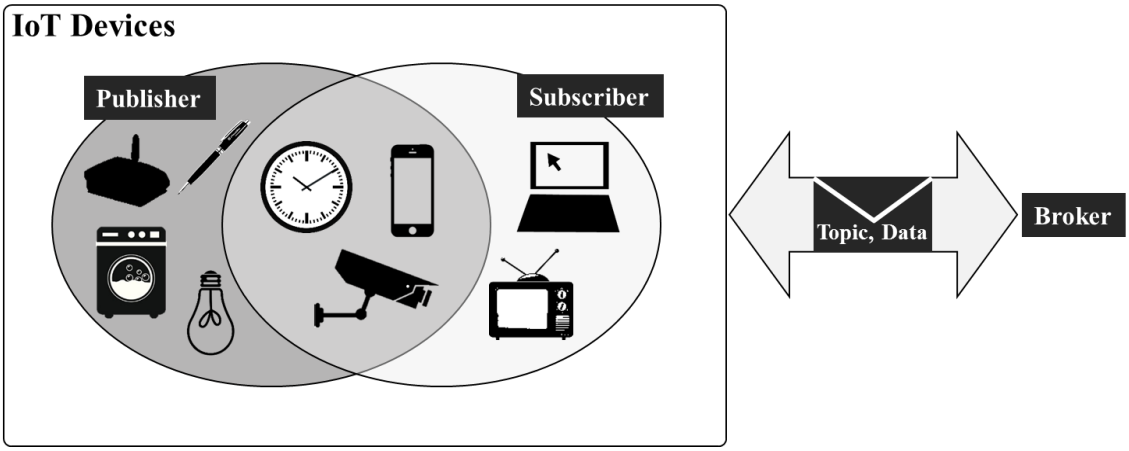

Figure 2: Messaging process of MQTT

The process of MQTT is shown in Fig. 2. MQTT distinguishes IoT devices as brokers, publishers and subscribers [6]. MQTT exchanges messages through brokers. Publisher devices publish messages with specific topics and send them to the broker. Subscribers subscribe to a topic, and they receive messages related to that topic. This protocol sends messages as plain text. Thus, it usually employs other security protocols like SSL/TLS. For example, Facebook messenger uses this protocol.

2.2. SECURITY SERVICES

As defined by ITU-T X.800, a security service is a service that ensures appropriate security for transmitting data or systems in protocol layers [7]. Also, the security service is a capability that provides more than one security requirement by following CNSS no. 4009 [8]. Thus, the security service provides security requirements to transfer data or protect systems. The security requirements are given below.

- **Authentication**
- **Access control**
- **Data integrity**
- **Data confidentiality**
- **Non-repudiation**
- **Availability**

The mainly requirements are data integrity, data confidentiality, and availability.

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
Impact Factor: 2.035 (I2OR)

2.3. SSL/TLS

SSL/TLS is used for security communication between a client and a server. This security protocol is designed to protect data from eavesdropping or modification, which may arise due to vulnerabilities in the communication [9].

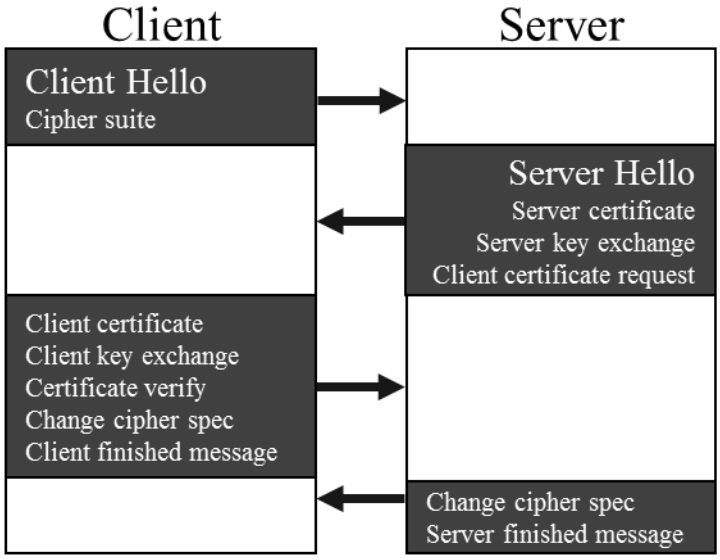

Figure 3: Handshake process of SSL/TLS

The handshake process of SSL/TLS is shown in Fig. 3. It is roughly composed of three steps. The first step is to select an algorithm to use in the session wherein the client sends a cipher suite, which is an encryption algorithm list, to the server. The server then chooses a supporting algorithm that it prefers. The second step is to exchange keys and authenticate each other. Finally, a session is started in the third step, and the two parties start communication using the algorithm selected in the first step.

3. PROPOSED METHOD

In this section, we describe the evaluation function we used in Section 3.1, and our proposed method is detailed in Section 3.2.

3.1. EVALUATION FUNCTION

In order to select an algorithm to use in the new session, the evaluation function in the proposed method uses three input factors: security service, residual energy and message length. Detailed explanations of the input factors are provided below.

- **Security service**: This value is used to indicate the purpose of the communication. Every communication has a purpose and required security services associated with that purpose. There is usually more than one required security service. However, in this experiment, we consider only one security service for each communication. The security service is selected at the initial step of the handshake in the proposed method. After the client

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
Impact Factor: 2.035 (I2OR)

selects a security service, this evaluation function selects an algorithm that provides the input security service.

- **Residual energy**: This value is used for saving energy and extending the battery life of IoT devices. It is a calculation of the percentage of residual energy. When the device has a low percentage of energy, this evaluation function selects the algorithm requiring the least energy among algorithms that providing the security service.
- **Message length**: This factor is also used for saving energy and extending the battery life. One of the most energy intensive factors is encrypting messages. Thus, consideration of the message length is important for minimizing energy usage.

We define an evaluation function based on these factors. The evaluation function is as follows:

$$f(x) = Security\ service_{Client\ selected} + \frac{Residual\ energy}{Message\ length} \qquad (1)$$

In Equation (1), x is a session, and f(x) is an algorithm used in the session.

3.2. PROPOSED METHOD

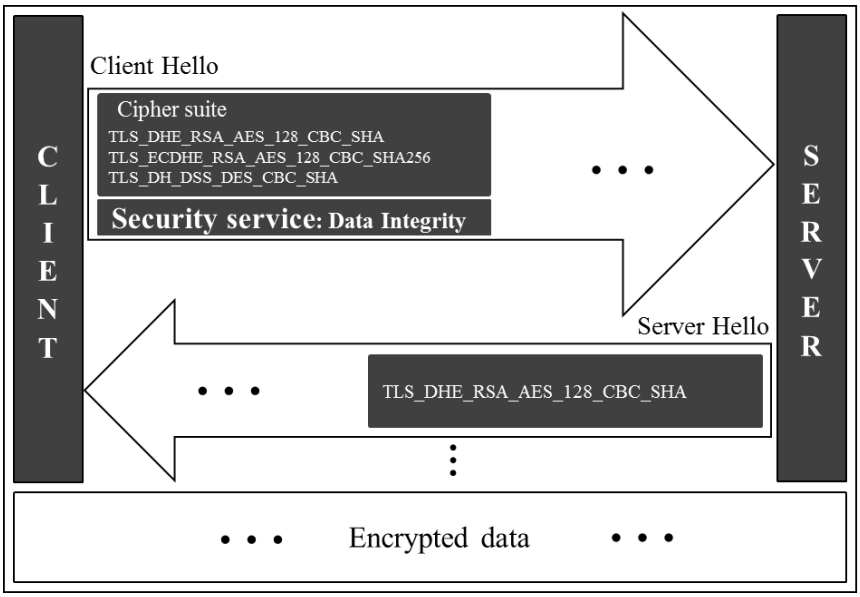

Figure 4: Proposed handshake process

In SSL/TLS, the client and server exchange their supporting algorithm list (cipher suite) in the first step (handshake) as shown in Fig. 4. However, in our proposed method, the required security service is sent simultaneously. After the server receives the hello from the client, the server selects the most efficient algorithm for this communication using the evaluation function in the common supported algorithms. This proposed method maintains the security level of the SSL/TLS using algorithms supported by SSL/TLS and spends energy efficiently to extend the lifetimes of IoT devices.

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
Impact Factor: 2.035 (I2OR)

4. EXPERIMENTAL RESULTS

This section provides the experimental results. The initial parameters are discussed in Section 4.1, and the specific results are presented in Section 4.2.

4.1. INITIAL PARAMETERS

Table 1 provides definitions of the initial parameters used in this experiment. Each experiment is run 100 times for each security service. There are many different kinds of security services. However, we deal with only three items of interest: data integrity, confidentiality and authentication. Moreover, the residual energy of a device and length of the message is generated randomly in every experiment.

Table 1: The initial parameters

Parameter	Value
The number of experiments	100
Experimental security service	Integrity, confidentiality, authentication
Residual energy	Random
Length of the message	Random

The selected algorithm consisted of protocols including key exchange, encryption, MAC and authentication. In order to calculate the energy consumption of each protocol in an algorithm, we used data from other experiments [10, 11].

4.2. RESULTS

Experimental results were obtained to demonstrate the energy effectiveness of the proposed method as compared to SSL/TLS. The following figures provide the energy consumption of SSL/TLS and the proposed method.

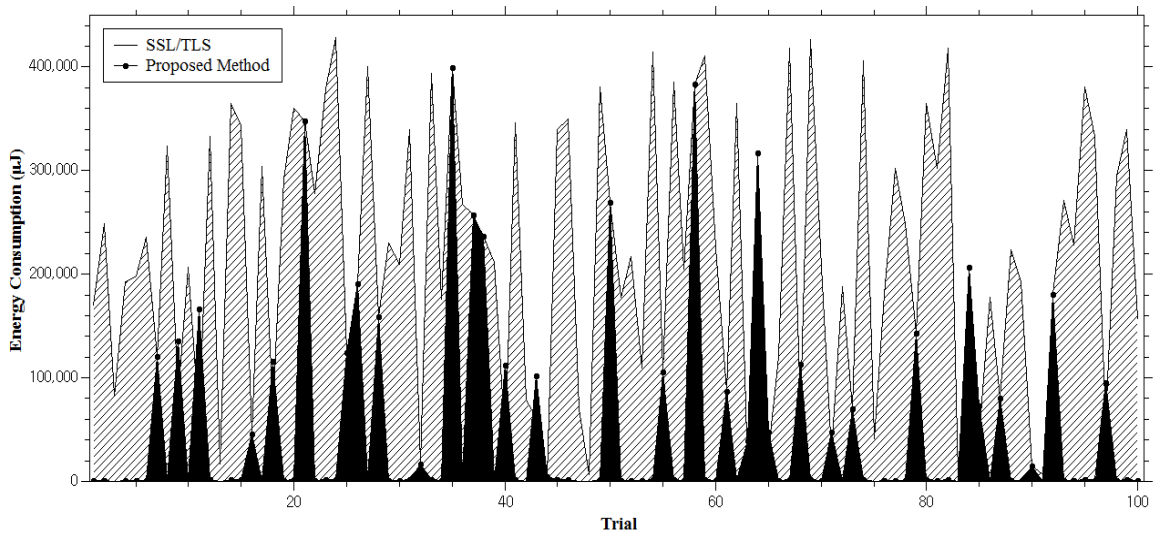

Figure 5: Results of data integrity testing

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
Impact Factor: 2.035 (I2OR)

When the required security service is data integrity, 54.94% of the energy is saved as shown in Fig. 5.

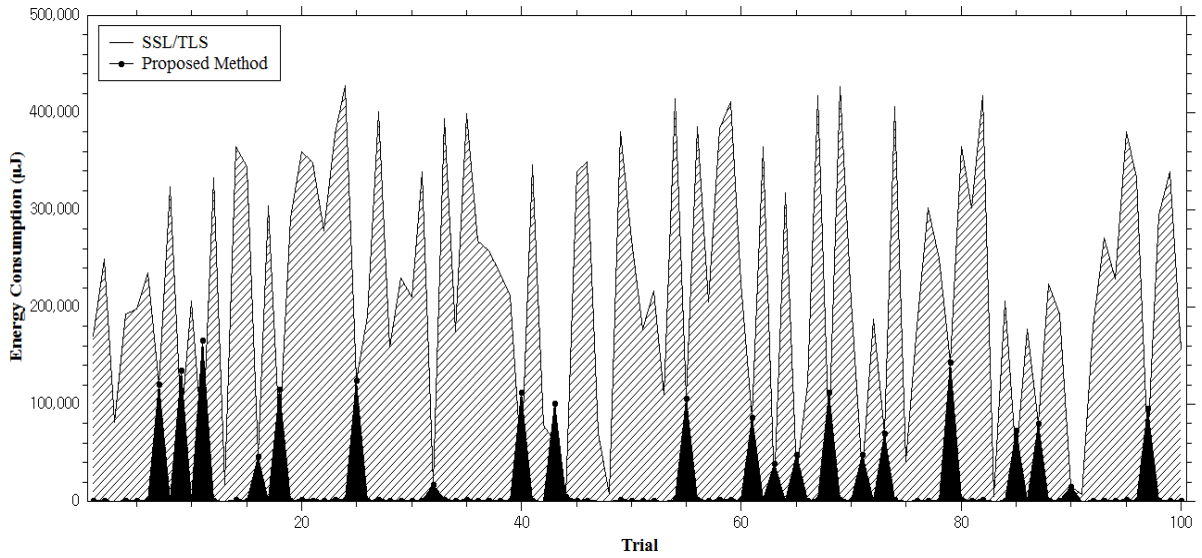

Figure 6: Result of authentication

When the required security service is authentication a 74.52% energy savings is observed as shown in Fig. 6.

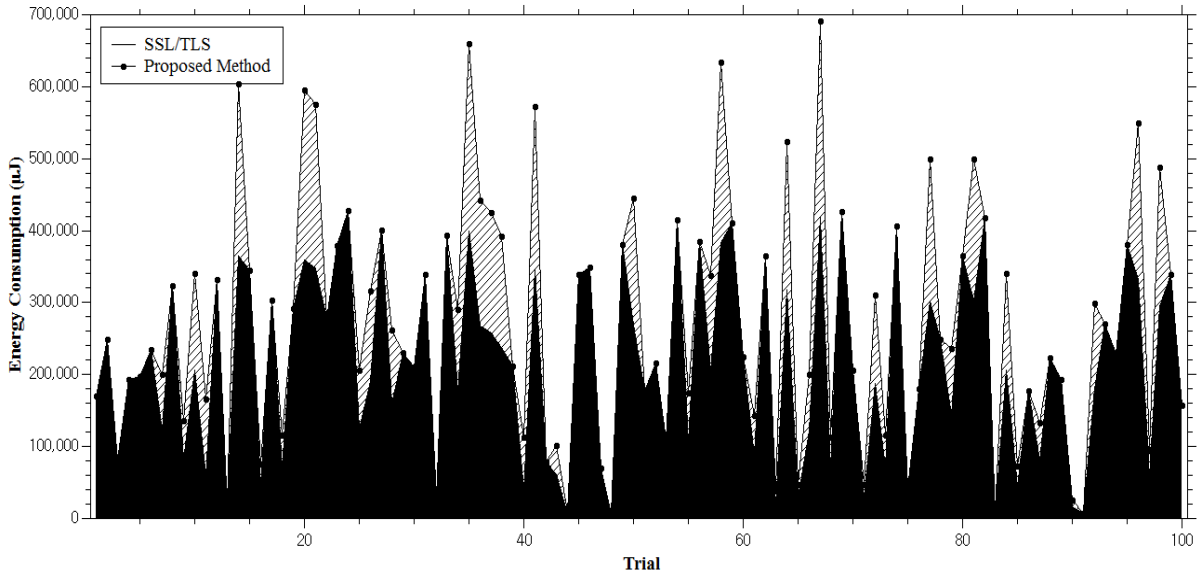

Figure 7: Result of confidentiality

However, as shown in Figure 7, our method does not perform well in the case where confidentiality is selected as 33.14% more energy is required.

ISSN- 2350-0530(O) ISSN- 2394-3629(P)
Impact Factor: 2.035 (I2OR)

5. CONCLUSION AND FUTURE WORKS

In order to select a more energy efficient security algorithm in the first step of the handshake process, we consider the following factors related to a client-selected security service: residual energy and length of the message. We observe that a significant amount of energy can be saved in most cases. However, our proposed method may not be energy efficient in some cases. By using our security service selection method in cases of integrity and authentication, a user can save a significant amount of energy. In order to further improve our method, we plan to investigate the data confidentiality case and improve it.

6. ACKNOWLEDGEMENTS

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. NRF-2015R1D1A1A01059484).

7. *REFERENCES*

[1] K. Zhao and L. Ge, "A survey on the internet of things security," in Computational Intelligence and Security (CIS), 2013 9th International Conference On, 2013, pp. 663-667.

[2] L. Atzori, A. Iera and G. Morabito, "The internet of things: A survey," Computer Networks, vol. 54, pp. 2787-2805, 2010.

[3] I. Ishaq, D. Carels, G. K. Teklemariam, J. Hoebeke, F. V. d. Abeele, E. D. Poorter, I. Moerman and P. Demeester, "IETF standardization in the field of the internet of things (IoT): a survey," Journal of Sensor and Actuator Networks, vol. 2, pp. 235-287, 2013.

[4] S. Bandyopadhyay and A. Bhattacharyya, "Lightweight internet protocols for web enablement of sensors using constrained gateway devices," in Computing, Networking and Communications (ICNC), 2013 International Conference On, 2013, pp. 334-340.

[5] A. Banks and R. Gupta, "MQTT Version 3.1. 1," OASIS Standard, 2014.

[6] U. Hunkeler, H. L. Truong and A. Stanford-Clark, "MQTT-S—A publish/subscribe protocol for wireless sensor networks," in Communication Systems Software and Middleware and Workshops, 2008. Comsware 2008. 3rd International Conference On, 2008, pp. 791-798.

[7] ITU-T, "X.800 Recommendation," 1991.

[8] CNSS, "Instruction No.4009," 26 April, 2010.

[9] E. Rescorla, SSL and TLS: Designing and Building Secure Systems. Addison-Wesley Reading, 2001.

[10] N. R. Potlapally, S. Ravi, A. Raghunathan and N. K. Jha, "Analyzing the energy consumption of security protocols," in Proceedings of the 2003 International Symposium on Low Power Electronics and Design, 2003, pp. 30-35.

[11] R. Karri and P. Mishra, "Minimizing energy consumption of secure wireless session with QoS constraints," in Communications, 2002. ICC 2002. IEEE International Conference On, 2002, pp. 2053-2057.