J Inf Process Syst, Vol.14, No.6, pp.1431~1437, December 2018
https://doi.org/10.3745/JIPS.03.0106

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Two-Phase Security Protection for the Internet of Things Object

Vera Suryani*,**, Selo Sulistyo**, and Widyawan Widyawan**

Abstract

Securing objects in the Internet of Things (IoT) is essential. Authentication model is one candidate to secure an object, but it is only limited to handle a specific type of attack such as Sybil attack. The authentication model cannot handle other types of attack such as trust-based attacks. This paper proposed two-phase security protection for objects in IoT. The proposed method combined authentication and statistical models. The results showed that the proposed method could handle other attacks in addition to Sybil attacks, such as bad-mouthing attack, good-mouthing attack, and ballot stuffing attack.

Keywords

Attacks, Authentication, Internet of Things, Security, Statistic

1. Introduction

Security in Internet of Things (IoT) is an interesting research area to be explored. Protecting object in IoT is a crucial issue considering that any misbehaving objects frequently attempt to make a malicious attack. Several methods of securing objects in IoT include encryption [1,2], authentication [3], and mathematical model [4]; each of which has its purpose. Authentication methods aim to filter valid and malicious objects. Meanwhile, encryption methods protect data from any spoofing activities launched by malicious objects. Mathematical models, meanwhile, are commonly used for trust assessment in IoT object security. It filters the trusted objects using a number of objective calculations to avoid malicious objects. Trust assessment is a part of trust management with the purpose of assessing other objects based on previous and current behaviors. This process is essential as objects in IoT are prone to be attacked, mainly to some trust-based attacks. Those attacks are: (1) an attack that gives a fake trust value to underrate an object (bad-mouthing attack), (2) an attack that gives a fake trust value to overrate an object (good-mouthing attack), and (3) an attack from malicious node that boosts the trust value of another bad node by providing good recommendations for collusion purpose (ballot-stuffing attack).

This study proposed two-phase security protection for objects in the IoT environment. This security protection used two methods: authentication and statistic, to ward off attacks related to trust value misuse. The paper is organized as follows: Section II describes the related works, Section III discusses

Manuscript received July 9, 2018; accepted July 20, 2018.
Corresponding Author: Vera Suryani (verasuryani@telkomuniversity.ac.id)
* School of Computing, Telkom University, Jawa Barat, Indonesia (verasuryani@telkomuniversity.ac.id)
**Dept. of Electrical Engineering and Information Technology, Universitas Gadjah Mada, Yogyakarta, Indonesia ({selo, widyawan}@ugm.ac.id)

the proposed method, Section IV explains the simulation result and discussion, and Section V summarizes the conclusion and future works.

2. Related Works

A study conducted by Khan and Herrmann [5] utilized a border router to detect the malicious attacks on IoT objects. Any object that passed through the border router could act as a trust evaluator for other objects. The trust evaluator used a threshold value to categorize whether the evaluated object was detected as an intruder or not. This method successfully exploited IDS mechanism, but it still required an objective justification to obtain an optimum threshold value for trust evaluator.

Meanwhile, Kim and Lee [6] proposed trust management in IoT using authentication and authorization methods based-on locally centralized. These methods were claimed to be capable of preventing any distributed denial-of-service (DDoS) attacks.

These aforementioned two studies maintained the security aspect by trust assessment. But none of these methods have been attempted to combine with the statistical model. This study, in turn, proposed two-phase security protection for objects in the IoT environment by utilizing authentication and statistical methods. Authentication method was used to handle the Sybil attack, and a statistical model was used to prevent a bad-mouthing attack, good-mouthing attack, ballot-stuffing attack, and on-off attack.

3. Proposed Scheme

The method proposed in this paper is the development of previous research, namely ConTrust framework [7], a security framework concerning the trust assessment for objects in IoT. If referring to the IoT layering scheme, then ConTrust is located between the application and network layers. It consists of a number of logical functions to assist objects in determining other trusted objects. Trust assessment conducted by the ConTrust model consists of current and past assessments to calculate the trust value of an object given by other objects. The past assessment used in ConTrust refers to the reputation value with a combination with the existing trust value as written in the following formula:

$$T(t) = (1-\propto).h_{ijl}^{nm}(t)+\propto.R(t) \quad (1)$$

where $T(t)$ is the total of trust value; α, weight parameter [0, 1]; $h_{ijl}^{nm}(t)$, existing trust value; and $R(t)$, reputation value.

The details of trust assessment from ConTrust model can be found in [8]. Trust value is vulnerable to be changed in which malicious objects can easily modify this value. To ensure the integrity of trust value against trust-based attacks, we have improved ConTrust model with two-phase security protection. The steps of detecting objects in attempting to launch some attacks in the proposed method include:

1. Group membership authentication using a Diffie-Hellman algorithm: The Diffie-Hellman algorithm is useful for authenticating a group containing many members of objects. If the number of objects varies, then the Diffie-Hellman algorithm can be adjusted in accordance with

those numbers.

2. Trust value deployment: This process can be conducted only for objects that have been authenticated using the Diffie-Hellman algorithm. The authenticated object can deploy trust values to other objects based on the equations in the ConTrust framework [8].
3. Ballot stuffing checking: The detection of ballot stuffing attack was carried out using specific graph theory. By limiting the allowed number of trust value given to an object, no object could flood the trust value of others.

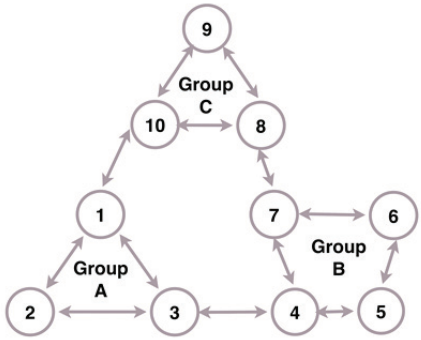

Fig. 1. Network topology illustrated by a graph.

As depicted in Fig. 1, the network topology is illustrated by a graph, which can be expressed as:

$$G = (V, E) \tag{2}$$

where V = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10} and E = {(1,2), (2,1), (1,3), (3,1), …, (9,10), (10,1)}.

V represents a set containing all objects in topology G, and E describes a set of connections between objects. The object can deploy and receive the trust value only from other directly connected neighbors. A group itself is illustrated in a sub-graph, as seen in Fig. 2.

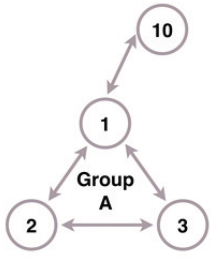

Fig. 2. Sub-graph of group A.

Eq. (3) is used to limit the number of allowed connections in a time range of t.

$$C_{max} = \frac{n^2 - n}{2} \tag{3}$$

with C_{max} is the total of possible edges in graph G, which represents the number of connections of all objects; n is the total members of V that represents the number of all objects in the network.

The allowed maximum number of connections can be determined using Eq. (3). This value was used as a reference to check the ballot-stuffing attack. Furthermore, an object could not give a trust value to other objects in the network that were higher than the value of C_{max}.

1. Bad or good mouthing attack detection: The attack detection process began by filtering a specific trust value considered unusual, combined with the limitation of the connection allowed in the specific period. The filtering process was conducted in the following steps:
   (a) Computing the average of all trust values stored in objects in the network

$$\overline{T} = \frac{1}{N}\sum_{i=1}^{N} T_i \tag{4}$$

   with $\overline{T}$ is average trust value and N is the number of objects in one network/group.
   (b) Subtracting the trust value of each object with the average value or $\overline{T}$ obtained from the previous step. Then, the variance was calculated using the following equation:

$$\sigma^2 = \frac{\sum_{i=1}^{N}(T_i - \overline{T})^2}{N-1} \tag{5}$$

$$\sigma = \sqrt{\frac{\sum_{i=1}^{N}(T_i - \overline{T})^2}{N-1}} \tag{6}$$

   with σ is standard deviation value.
   (c) The standard deviation was used to determine the threshold value, used to identify objects regarded as good or bad mouthing attacker.
   The maximum trust value (denoted as *G*), which was categorized as the good-mouthing attack threshold was:

$$G = \overline{T} + \sigma \tag{7}$$

Moreover, the minimum trust value (denoted as *B),* which was categorized as the bad-mouthing attack threshold was:

$$B = \overline{T} - \sigma \tag{8}$$

Once the value of G or B has been obtained, those values would be combined with the maximum connection allowed to an object to do the detection process of good or bad-mouthing attack. This value of the maximum connection would be dependent upon how many objects were directly connected to the object, and the equation used in this formula referred to Eq. (3).

2. Attack mitigation: If an object has been detected as an attacker launching a bad-mouthing attack or good-mouthing attack or ballot-stuffing attack, then the object would be given a score that banned it from giving trust value to others for a specific period. Moreover, the reputation value of an object identified as an attacker was reduced as a punishment to the object.

4. Performance Analysis

We conducted some simulations to evaluate the proposed method. The simulations were performed using MATLAB with R2015b version. The evaluation goal was to observe the robustness of the

proposed method, where it was identified by the parameters of computation cost and security requirements. The scenario used in the simulation was to place a malicious object in a group to give some fake trust values to other trusted objects in the same group. The given trust value was varied in which the one below the threshold value was to find out whether the proposed method was capable of detecting bad-mouthing attacks. Another above the threshold was to detect good-mouthing attacks, and the combination of those two values was to consecutively send to detect ballot-stuffing attack.

The authentication process was the first process without any effect on the trust value, but it affected the security against the Sybil attack. Authentication executed to an object before trust value deployment was suitable to filter an object that tried to use a fake ID to be a member of a group or network. The Diffie-Hellman group authentication applied in this scheme did not use object ID, but private and public keys in the authentication process.

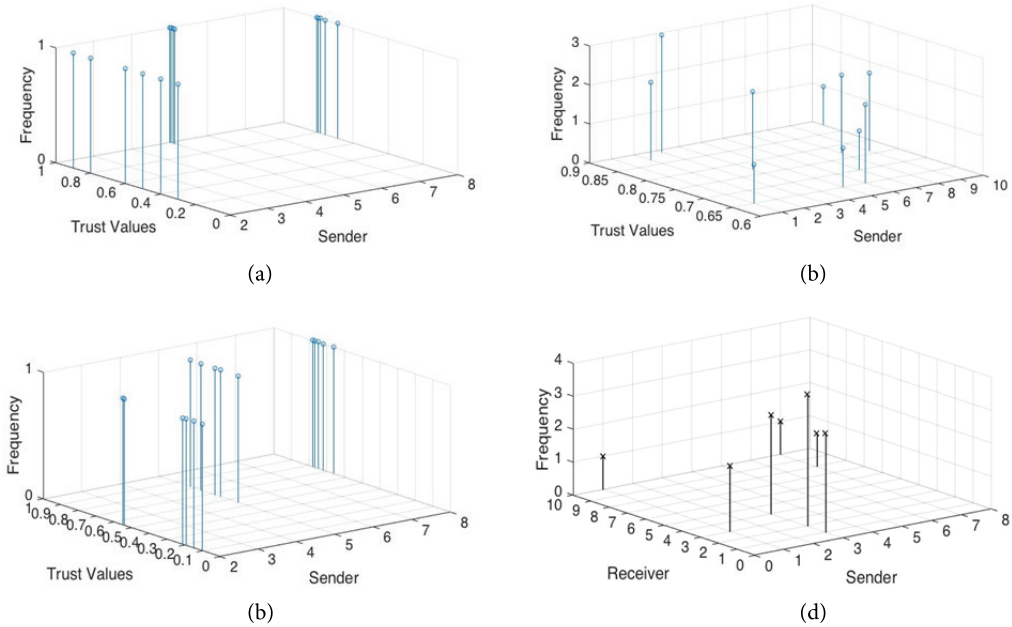

Fig. 3. Attacks result simulation. (a) Normal condition without an attack, (b) bad-mouthing attack, (c) good mouthing attack, and (d) ballot-stuffing attack.

The trust value was more affected by the second security phase—a statistical model based on a standardized deviation value. The threshold values of bad-mouthing attack or good-mouthing attack were taken after several periods (t) to obtain an optimum threshold value. Fig. 3(a) depicts the number of connections for each object that did not exceed the maximum number allowed, as described as the G or B threshold. If the condition remained like this, then there would be no trust-based attack launched in the group.

Fig. 3(b) depicts that object number two sent some values below the allowed B value. The amount of connection also exceeded the allowable amount. This number indicated that object number two had performed a bad-mouthing attack. In the meantime, the evidence of a good-mouthing attack was detected when object number 4 gave some values that exceeded the limit of G threshold value, along with the exceeding amount of the allowed connection limits as well. See Fig. 3(c) for more detail depiction.

Furthermore, Fig. 3(d) displays the detection of ballot-stuffing attack using maximum connection allowed for all objects. Object number three deployed the trust values to other directly connected objects, and the number of connection was over to the allowed C_{max} number, namely 9. This value was obtained from the number of other connected objects of objects number three, namely three directly connected objects. The total connections made by object number three were 10, so the object number three was detected for launching the ballot-stuffing attack.

Once the objects were detected to give some values in the category of bad-mouthing attack, good-mouthing attack, and ballot stuffing attack, then those objects would be banned in terms of deploying the value of trust to other objects within a certain period. In this case, this punishment was given to object number two, three, and four.

In addition, the time required to simulate the proposed method was 0.229 seconds. This value referred to the processing time for all functions run during the simulation. Thus, the total simulation time needed for running the proposed method was dependent upon the speed of inputting the data of public key, private key, and trust values for other objects.

5. Conclusion

Various security methods nowadays can be implemented to secure objects in IoT. This paper utilized a combination of two existing methods: authentication and statistical method to enhance the security aspects of the IoT environment. It also applied graph theory to detect some trust-based attacks by limiting the number of edges allowed in a single graph.

The contribution of this paper is to provide an alternative solution for detecting trust-based attacks on IoT objects. Even though not all attacks could be covered, the proposed method could handle various types of attacks: bad-mouthing attack, good-mouthing attack, and ballot stuffing attack. The additional security features that are more resistant to other previously mentioned attacks are a challenge in the future work. Some mitigating efforts to overcome other attacks are also planned to be conducted later.

References

[1] J. D. Bokefode, A. S. Bhise, P. A. Satarkar, and D. G. Modani, "Developing a secure cloud storage system for storing IoT data by applying role based encryption," *Procedia Computer Science*, vol. 89, pp. 43-50, 2016.

[2] Y. Mao, J. Li, M. R. Chen, J. Liu, C. Xie, and Y. Zhan, "Fully secure fuzzy identity-based encryption for secure IoT communications," *Computer Standards and Interfaces*, vol. 44, pp. 117-121, 2016.

[3] F. Wu, L. Xu, S. Kumari, and X. Li, "A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security," *Journal of Ambient Intelligence and Humanized Computing*, vol. 8, no. 1, pp. 101-116, 2017.

[4] I. R. Chen, F. Bao, and J. Guo, "Trust-based service management for social internet of things systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 6, pp. 684-696, 2016.

[5] Z. A. Khan and P. Herrmann, "A trust based distributed intrusion detection mechanism for Internet of Things," in *Proceedings of IEEE 31st International Conference on Advanced Information Networking and Applications*, Taipei, Taiwan, 2017, pp. 1169-1176.

[6] H. Kim and E. A. Lee, "Authentication and authorization for the Internet of Things," IT Professional, vol. 19, no. 5, pp. 27-33, 2017.
[7] V. Suryani, S. Sulistyo, and W. Widyawan, "Internet of Things (IoT) framework for granting trust among objects," *Journal of Information Processing Systems*, vol. 13, no. 6, pp. 1613-1627, 2017.
[8] V. Suryani, S. Sulistyo, and W. Widyawan, "ConTrust : a trust model to enhance the privacy in Internet of Things," *International Journal of Intelligent Engineering and Systems*, vol. 10, no. 3, pp. 30-37, 2017.

Vera Suryani https://orcid.org/0000-0002-2073-1447

She is a Ph.D. candidate at Department of Electrical Engineering & Information Technology, Universitas Gadjah Mada, Indonesia. She was a lecturer in the School of Computing and Informatics, Telkom University, in 2003. Her research interests include security, distributed system, and the Internet of Things.

Selo Sulistyo https://orcid.org/0000-0002-0427-6421

He is an associate professor in Information and Communication Technology at the Department of Electrical Engineering and Information Technology Universitas Gadjah Mada, Indonesia. His research interests include intelligent transportation system, software modeling, mobile application development and security for the IoT.

Widyawan Widyawan https://orcid.org/0000-0002-0340-1198

He is an assistant professor in Information and Communication Technology at the Department of Electrical Engineering and Information Technology, Universitas Gadjah Mada, Indonesia. His research interests include wireless sensors network, machine learning, location technology, and ubiquitous computing.