Simulation of trust-based attacks in Internet of Things

Vera Suryani1,2,*, Selo Sulistyow3, and Widyawan Widyawan2

1School of Computing, Telkom University, Jl. Telekomunikasi no. 1, Bandung, Indonesia
2Department of Electrical Engineering and Information Technology, Universitas Gadjah Mada, Jl. Grafika No. 2, Sleman, Yogyakarta, Indonesia

Abstract. Security issue in Internet of Things (IoT) is one of the most important aspects to be resolved. Some attacks that occurred in Internet technology are also penetrated IoT. A trust-based security system is a promising solution in IoT as it is suitable for the characteristic of IoT which is distributed, decentralized control and on-off connections. Knowing the behaviors of the attacks might help up to understand of how we may prevent the attacks and plan to mitigate the attacks. In this paper, we simulated trust-based attacks in IoT environment by giving the fake reputation values of an object. For this purpose, we utilized ConTrust model, a trust-based security model. Matlab was used to simulate the attacks, and the simulation result showed that ConTrust model was outperformed on mitigating a trust-based attack. The attack was detected and resolved correctly.

1 Introduction

Internet of Things (IoT) is a new paradigm that is born and developed from Internet technology. The Internet here is used to connect the 'things', which are the IoT forming components. Things can be in the form of physical objects such as vehicles, sensors, cameras, and people. In this paper, the term 'things' are called as objects. Objects can be connected to communicate and interact with each other remotely via the internet. Various internet technologies can be used in IoT, ranging from Radio Frequency Identification (RFID) to large battery powered systems [1]. These technologies and connected objects can be used to form applications on smart cities, smart transportation, smart home, smart logistics, and other various applications.

In smart transportation, smart cameras can be used to monitor the density of the roadways, and sensors can be used to make it easier for car drivers to find the empty parking slots, also speed detecting sensors can be mounted at certain spots to monitor overrunning speed vehicles, reducing potential accidents that may occur. Meanwhile, in the smart homes, sensors are useful for lighting automation, home appliance automation: smart refrigerator, automatic room temperature setting, or automatic window cover in the case of the homeowner forgot to close the window when leaving home. With the IoT, many conveniences are offered in people’s everyday life.

However, behind the easiness offered by IoT, there is a security concern in IoT to be considered. Since the IoT was born from Internet technology, it causes various threats that might be appearing there, ranging from worm attacks to Distributed Denial of Service (DDoS). Preventive measures have been done before, from the physical aspects such as authentication models that are embedded in the chip of the sensor to the use of security framework that applies to all components in a system in IoT.

One possible method that can be used to improve security aspect in IoT is by utilizing the trust value among objects. Each object can assess the trust value of another object quantitatively, and the result of its assessment becomes a reference to determine whether the communication process will proceed or not. In our previous work, we have proposed ConTrust model [2] that used a mathematical model to compute the trust value of objects in the IoT environment. Preceded by the authentication process using the Diffie-Hellman algorithm, each object can calculate the trust value of another object independently or without involving a third party. The ConTrust model still requires proof to check how robust the model is against possible attacks, especially trust-based attacks. Being robust is essential for a security framework, especially concerning about attack resistance because the purpose of the framework is to protect the object from various possible vulnerabilities and attacks. In this paper, simulated trust-based attacks are performed to determine the robustness of the ConTrust model. The main contribution of the study is as follows. We outline that some security attacks might happen in the IoT network; one of them is a trust-based attack. We then present the alternative framework to prevent that attack, namely ConTrust model. Some simulations were made to find out the robustness of this model against trust-based attack. As a result, we discovered that this model was robust enough to prevent a trust-based attack.

This paper is organized as follows: Section II describes the related work specializing on security model in IoT, Section III describes the definition of security in...
IoT, including our previous work ConTrust model, Section IV reports simulation result and discussion, and Section V presents the conclusion and future works.

2 Related Works

Security on the Internet of Things (IoT) is a very open research area since the security is a fundamental aspect to be managed for any technologies. One component in IoT is an object, and this object has a dynamic character concerning of joining and leaving the network. This dynamic character is a challenge for security aspect.

Generally, an authentication scheme is used to secure the environment in IoT. Several authentication schemes can be applied such as centralization, semi-centralization, and decentralization. The centralization scheme usually involves a third party to handle the authentication processes; one is Certificate Authority (CA). The object should contact a trusted third party in order to be classified as an authenticated object. Some researchers already used this scheme to secure their system [3]. The advantage of centralization scheme is the energy savings from the computing side, yet the disadvantage is difficulties to choose a third party that can be considered reliable. The selection of responsible third parties becomes unnecessary in the decentralization scheme. In this scheme, each object may authenticate each other without involving a third party. However, behind the ease offered by this scheme, there is a relatively high computation cost, considering a load of authentication process calculation is charged to each object [4]. The decentralized scheme is then developed to a semi-decentralized scheme, from which one of the objects in the decentralization scheme is selected as coordinator to handle the authentication process. Local security handled by the local coordinator is considered better than one which involves a third party that might not necessarily be trusted.

Both decentralized and semi-centralized schemes rely on quantitative models to improve the security aspect, such as the trust value model. A study conducted by [5] utilized trust management into three phases of trust model: neighbor discovery, service request, and trust-based computation. The model was able to detect and mitigate on-off attack from malicious objects in the network.

Meanwhile, other researchers used distributed trust schemes and centrality degrees to obtain trust among objects [4]. The proposed model was named TC-BAC, using the trust calculation of objects in the network through direct and indirect trust calculations. Besides, this model also used access control in its architecture.

These previous studies can indeed mitigate some attacks, one of which is an on-off attack. However, their research has not been proven yet to cope against a trust-based attack. In this paper, we conducted some simulations to mitigate the trust-based attacks. The model used in this study was compared to another model, namely TC-BAC to find out whether the model used here is reliable enough to resist a trust-based attack as well as TC-BAC model.

3 Security in Internet of Things

Security in IoT becomes interesting and challenging issue because there are always two parties involved in it, the parties who try to defend the system with various prevention efforts, and those who try to attack the system or attackers. No security system is 100% secure, and there are only preventive efforts to stem attacks with various methods, algorithms, models, and security framework.

3.1 ConTrust Model

The model used in this paper is ConTrust Model [2]. In this model there are 4 processes that involve: pre-processing, calculating the value of trust, giving the value of trust, and recommendations. The topology used in ConTrust model is Social Internet of Things (SIoT) which proposed by [6].

3.1.1 Pre-processing Stage:

Objects are defined in matrix form, consisting of three independent default matrices that contain the object IDs, the initial trust values, and the initial recommendation values. These matrices can be filled with any values ranging from zero to one. The fulfillment of these values depends on the assumptions used in the simulation. If all objects are considered trustable then they can be assigned value of one. Otherwise, the value of zero means all objects are assumed not trustable.

3.1.2 Trust Assessment Stage:

For objects located in same network or intra network then the calculation of trust value is defined as follows:

$$f_{ij}^{m}(t) = \frac{1}{N} \sum_{t=1, t \neq m}^{m} T_{ij}(t) + T_{ij}(t-1)$$

And trust calculation for objects in a different network can be seen in equation (2).

$$g_{ji}^{n}(t) = \frac{1}{N} \sum_{t=1, t \neq m}^{m} T_{ji}(t)$$

$$h_{ij}^{nm}(t) = f_{ij}^{n}(t) + \frac{1}{N} \sum_{t=1}^{m} g_{ji}^{m}(t)$$

where:

$$f_{ij}^{m}(t) = \text{trust function of the object } i \text{ to object } j \text{ at time } t$$

$$g_{ji}^{n}(t) = \text{trust function of the object } j \text{ to object } i \text{ at time } t$$

$$h_{ij}^{nm}(t) = \text{function to calculate the average of trust value in the same and different community}$$
3.1.3 Trust Value Granting Stage:

The trust value used in the ConTrust model is ranging from zero to one. The minimum value of zero is identified as an object that is not trusted at all, and the maximum value of one is considered as a trustable object.

a. Total Trust Value calculation:

\[ T(t) = \alpha \cdot h_{ij}^{mn}(t) + (1 - \alpha) \cdot R(t) \quad (4) \]

where:

- \( T(t) \) = total of trust value
- \( h_{ij}^{mn}(t) \) = direct trust assessment of object \( i \) to object \( j \) at time \( t \), in the same community \( n \), and different community \( l \) to \( m \)
- \( R(t) \) = object reputation value
- \( \alpha \) = given weight of history function \([0,1]\)

b. Reputation Calculation. The equation for reputation value:

\[ R(t) = \frac{T(t)}{1 + e^{-\beta t}} \quad (5) \]

with

\[ \beta = T(t) - T(t-1) \quad (6) \]

where

- \( \beta \) = historical trust value of the object which is a reduction from the current trust value and the previous trust value
- \( R(t) \) is indirect trust value produced from object’s reputation in certain time periods

3.1.4 Recommendation Stage:

After the calculation of the total trust value, then the resulting value categorized as follows:

\[ K = \begin{cases} 
  \text{very trustable} & \text{if } 0.7 \leq T(t) \leq 1 \\
  \text{trustable} & \text{if } 0.5 < T(t) < 0.7 \\
  \text{untrustable} & \text{if } 0.3 < T(t) < 0.5 \\
  \text{very untrustable} & \text{if } 0 < T(t) < 0.3
\end{cases} \quad (7) \]

The recommendation value is useful for assessing the trust level of an object. It is also useful for deciding whether the data communication process to proceed or not.

3.2 Trust-based Attack

Attacks may occur among objects in IoT, especially those relating to trust. The types of attacks on fake trust scores [7] include:

- Good-mouthing attacks: gives a false trust value of an object, that is exaggerated value
- Bad-mouthing attacks: gives a false trust value of an object, that is to vilify an object
- Ballot-stuffing attacks: provides a congregation false trust value of an object

In the ConTrust model, these attacks are prevented through an authentication process between objects that is performed before the trust value is calculated. Thus only authenticated objects can perform trust value calculations. The authentication process used in the ConTrust model is Diffie-Hellman key distribution [8].

4 Simulation and Discussion

In this section, we give simulation result of trust-based attack as an output of ConTrust model usage. The simulation was conducted using MatLab tool considering the ConTrust model as a mathematical model. We compared our work with TC-BAC method, as well as without any trust method to fulfill the performance evaluation. The scenario given was to deploy false reputation values randomly to an object, in which these fake values would imply the trust values.

Figure 1 depicted the normal distribution of reputation value when there was no such attack happened in the simulation. As can be seen in Figure 1, reputation values in ConTrust model remained stable compared to TC-BAC and without any trust method. It means that ConTrust model was proven to be a stable trust assessment model.

![Fig 1. Normal distribution of reputation value](image1)

![Fig 2. Distribution of reputation value affected by good mouthing attack](image2)
Meanwhile, after a good mouthing attack simulation was conducted, it appears that the ConTrust model experiences a fluctuation of the trust value up to a certain time, and becomes stable again afterwards, as shown in Figure 2. The same result occurs for the type of bad mouthing attack simulation, it becomes stable again after fluctuating for a while, as shown in Figure 3. The simulation results of both good and bad mouthing attack are shown in Figure 2 and 3, respectively. ConTrust model was able to detect and dampened fluctuations of trust value that was changing because of the attack. This was due to the negative feedback mechanism as written in Eq. 5, where the current reputation value was influenced by previous input value. The changing of input value is expressed in Eq. 6, which can be analogous to the history parameter used in the ConTrust model.

5 Conclusion and Future Works

Our work presents simulations of trust-based attack that had been solved using ConTrust model, TC-BAC and without any trust assessment method. From simulation results, we can conclude that ConTrust model was proven to be a stable model compared to two other methods mentioned previously. However, ConTrust model still needs to be developed further in order to handle other attacks apart from trust-based attack. Authentication provided by Diffie-Hellman key distribution or a statistical approach could be deployed to mitigate some attacks that might be launched by attackers.

References

1. S. Chakrabarty, D. W. Engels. 13th IEEE Annual Consumer Communications & Networking Conference (CCNC) (2016)
2. V. Suryani, S. Sulistyo, W. Widyawan. Int. J. Intell. Eng. Syst., 10, 3 (2017)
3. X. Zou, Y. S. Dai, Y. Pan. Trust and Security In Collaborative Computing (World Scientific, Singapore, 2008)
4. J. Duan, D. Gao, C. H. Foh, H. Zhang. Ad Hoc Networks. 11, 8 (2013)
5. C. V. L. Mendoza, J. H. Kleinschmidt. Int. J. Distrib. Sens. Networks. 2015 (2015)
6. L. Atzori, A. Iera, G. Morabito. IEEE Commun. Lett. 15, 11(2011)
7. F. Bao, I.-R. Chen, J. Guo. 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS) (2013)
8. E. Rescorla. RFC 2631: Diffie-Hellman Key Agreement Method. (RTFN, Virginia, 1999)