International Journal of Electrical and Computer Engineering (IJECE)
Vol. 6, No. 5, October 2016, pp. 2396~2402
ISSN: 2088-8708, DOI: 10.11591/ijece.v6i5.9678

Trust-Based Privacy for Internet of Things

Vera Suryani, Selo Sulistyo, Widyawan
Department of Electrical Engineering & Information Technology, Universitas Gadjahmada, Yogyakarta, Indonesia

Article Info

Article history:

Received Dec 9, 2015
Revised Jun 27, 2016
Accepted Jul 15, 2016

Keyword:

Ant colony algorithm
IoT
Objects
Privacy
Trust

ABSTRACT

Internet of Things or widely known as IOT makes smart objects become active participants in the communication process between objects and their environment. IoT services that utilize Internet connection require solutions to a new problem: security and privacy. Smart objects and machine-to-machine communications in IOT now become interesting research, including that related to security. Privacy, which is a safe condition in which object is free from interference from other objects, is one of the important aspects in IOT. Privacy can be implemented using various ways for examples by applying encryption algorithms, restrictions on access to data or users, as well as implementing rules or specific policy. Trustable object selection is one technique to improve privacy. The process of selecting a trustable object can be done based on past activities or trust history of the object, also by applying a threshold value to determine whether an object is "trusted" or not. Some researchers have studied this approach. In this study, the selection processes of trustable objects are calculated using Modified Ant Colony algorithm. The simulation was performed and resulted in declining graphic trend but stabilized in certain trust value.

Corresponding Author:

Vera Suryani,
Department of Electrical Engineering & Information Technology,
Universitas Gadjahmada,
Jl Grafika No 2, Sleman, Yogyakarta, Indonesia.
Email: vera.s3te14@mail.ugm.ac.id

1. INTRODUCTION

The concept of the Internet of Things (IOT) lab was first developed by Auto-ID Center at MIT in 1998. The objects, persons, or things are identified with a visual representation on the Internet [1]. Information Technology (IT) infrastructure will be needed (such as computers and telecommunication networks) for data exchanging among objects or things in the IOT.

In agreement with the definition of "things", the IOT communication can take place between the objects and the object to humans. The objects that may consist of sensors can be numerous, can be either static or mobile, and everywhere distributed. Many applications can be applied in IoT, such as real-time medical monitoring, intelligent transportation system, intelligent appliance and intelligent agriculture. Another application that is not less important to develop in the IOT is a smart grid, where the estuary end of the existing research in this area is human energy saving for smart appliances. Sensors technologies take an important role in some IoT applications. For example, for monitoring environmental conditions purposes required many sensors; such as humidity sensors, temperature sensors, and other sensors. Sensors are also needed in e-health; for example, is a blood pressure sensor (sphygmomanometer), sensor heart rate (ECG), sensor muscle (EMG), and accelerometer [2]. These sensors or objects should be connected to a public network or communicate wirelessly with other objects [3]. This condition makes objects become vulnerable to attack [4]. Access control plays an important role here, to classify anyone who is allowed to communicate or exchange data.

Data needs a safe and reliable means to be sent between objects because objects are vulnerable to being attacked [5]. Aspects of privacy, confidentiality, authenticity and integrity in the IOT are among parameters that can be used as security performance in exchange of such data. Many ways can be used to implement privacy [6], either centralized or distributed. The use of key distribution is one centralized way to improve privacy; both symmetric and asymmetric key distributions. While giving the value of trust or scoring has a different way to improve privacy, and this way use distributed way instead of centralized one. Objects that are potential to act some attacks or have carried out the attack will be given a very low score of trust value, causing other objects to reconsider their decision on making the connection to these objects. Likewise, an object that was never carried out an attack and has a good track record will be given the value of high trust. Trust metric calculations become an important issue to be resolved in the IOT because the numbers of connected objects are dynamically changed or they can move to different networks freely. To make data exchange between objects can be done safely it requires appropriate recommendations.

Objects with many experiences of visiting some networks causing many recommendations can be given to the object. In other words, hierarchical trust scoring is needed to make an accurate trust scoring. For example, trust scoring can be found on the friend's recommendation in social networks such as Facebook and Linked In. In IOT, this calculation is useful for provisioning recommendations among objects to exchange data securely.

Metaheuristic methods such as Genetic Algorithm, Ant Colony, Harmony Search, Particle Swarm Optimization, can be used to assess trust metric [7]-[9] objectively, instead of subjectively [10],[11]. But not many of these studies have solved the problems of trust metrics for dynamical and hierarchical objects. Metaheuristic method will be used in this study for scoring or assessing trust metric for dynamic and mobile objects in IoT. The usage of this method for trust metrics calculation is expected to be a contribution to the privacy aspects of IoT.

The paper is organized as follows: Section II describes the definition of trust and privacy in IoT and also Ant Colony algorithm, Section III describes the simulation environment, Section IV explains the result of simulation and its analysis, and finally Section V concludes the conclusions.

2. PRIVACY AND TRUST IN THE INTERNET OF THINGS

An object can be represented digitally, and when it is connected to the Internet, then it can be accessed and controlled from anywhere. Some applications take benefit of these kinds of objects: Intelligent Transportation System (ITS) where communication occurs between vehicles (V2V) or between Vehicle and Infrastructure (V2I), health monitoring in telemedicine where attached sensors can be remotely monitored, and general machine-to-machine communications. Prior to the communication establishment, an object can choose other objects that are trustable or not.

2.1. Privacy

IETF Internet Security Glossary defines privacy as "the right of an entity (usually a person), acting on their own behalf, to determine the extent to which it will interact with its environment, including the extent to which the entity is willing to share information about themselves with others" [12]. Based on this definition, privacy can be applied in [6]:

a. Devices
   Devices in IOT are any type of devices that is connected to The Internet, including sensors, actuators, cameras and any others networked devices. If the devices are manipulated for specific purposes, then the data transmission may become unsafe.
b. Communication
   Data encryption can be done to ensure confidentiality during the transmission process takes place. For this various encryption algorithms can be applied.
c. Storage
   Access control is one of the mechanisms to monitor who is allowed to access the database. Encryption of data is useful enough to cope with the intrusion of the database.
d. Processing
   The data must be ensured a safe process so other can not misuse the data. Digital Right Management (DRM) is a method that can be used here.

In general, the privacy aspect is closely linked to the level of confidence or trust. The higher the levels of trust to an object, the higher the level of privacy of the object. A high degree of privacy can be described as the guidance for an object to choose which objects it will communicate with, by supporting data in the form of reputation and trust metrics of the candidate objects.

2.2. Trust Calculation

Trust is a concept related to the belief and expectations of reliability, integrity, security, as well as the ability of an entity [13]. Trust becomes an important thing that should be implemented in IOT because its usefulness to secure the communication between objects; for example helping the objects to choose another trustable object during the communication [14]. Meanwhile, reputation is used to determine the level of trust, and it can be measured based on prior knowledge of the interaction with others objects and based on the experiences of other objects. Reputation can also be used as a parameter for assessing the level of trust of an object. Dynamic trust mechanism is useful for the object as a control for selecting the application services in the IOT. Characteristic of trust as described in [8],[15]:

a. Asymmetric and subjective
b. Dependent or has a particular context
c. Dynamic; which means that its value might increase, decrease, or remain stable

Trust is intransitive, for example if A trusts B and B trusts C, then A is not necessarily to trust C. But B can provide a recommendation of C reputation that might be beneficial for A in taking a decision whether to trust C or not.

A sociologist Diego Gambetta defines trust as follows:

> *"... trust is a certain degree of probability that is owned by someone or something (subjectively) to perform an action, to monitor the actions (although not directly) and can influence the actions of a person or thing"* [16].

This definition, when to be applied to the computer science, will lead to the trust modeling, trust management, and quantitative decision-making. Trust modeling related to the aspects of computational representation of the trust value, while trust management is a collection of evidence and risk assessment for decision-making [15]. The trust value is usually written in the number or label, and can be in binary, discrete or continuous forms. For example in the form of binary representation of the number 1 indicates "trustable" and 0 indicates "un-trustable".

To calculate the trust value we apply Modified Ant Colony Algorithm. The algorithm is suitable for trust calculations because of its method which involving prior knowledge, the trail of other ants left on a track that has been passed. This prior knowledge involves the calculation of the trust values that have been saved from previous interactions, either directly or indirectly. Similarities way of working is the reason for the development of Ant Colony algorithm for trust metrics calculation. Some modifications of Ant Colony algorithm are made in our trust metrics calculation. This modification briefly made for the pheromone deposit or trust value deposit as seen in Eq. (4), (5) and (6). The following subsections explain the overall process of the proposed trust assessment method.

2.2.1. Pre-processing

Objects are defined in the form of matrices: one containing the trust value and other containing the connection among objects. Default trust value for all objects is 0.5 by considering that all new objects have the same probability of trust value.

2.2.2. Trust Value Calculation Process

a. An object can moving from one network to other networks and can be connected to a number of objects. Before the connection to a target object, a trust assessment is done. If the target object is located in the same network or intra-network, then the trust value calculation is performed as follows:

$$f_{ij}^{m}(t) = \frac{\frac{1}{N}\sum_{j=1,i\neq j}^{m} T_{[j]}(t) + T_{[j]}(t-1)}{2} \quad (1)$$

where $\forall\, i, j, m \in [1, n]$

b. If the target object is located and connected to different network or inter-network.
When other networks exist more than one object that ever communicate with the target object or object *j*, the most trustful object will be chosen using maximal value of $f_{ij}^{n}(t)$.Trust value calculation in different network is written as follows:

$$g_{lj}^{m}(t) = \frac{1}{N}\sum_{l=1,l\neq m}^{m} T_{[l]}(t) \quad (2)$$

where $\forall j, l, m \in [1, n]$

c. The equation for all Intra and internetworks:

$$h_{ijl}^{nm}(t) = \frac{f_{ij}^{n}(t) + \frac{1}{N}\sum_{x=1}^{y} g_{lj}^{m}(t)}{2} \quad (3)$$

where $\forall i, j, l, n, m, x, y \in [1, n]$

d. Pheromone deposit or trust value deposit:

$$\tau_{ij}(t) = \tau_{ij}(t-1) + \Delta\tau_{ij}(t) + r_j \quad (4)$$

$$r_j = \frac{\sum_{l=1}^{m} k_{ij}}{N_j} \quad (5)$$

e. Pheromone evaporation or trust value reduction:

$$\tau_{ij}(t) = (1-\rho)\tau_{ij}(t-1) + r_j \quad (6)$$

3. SIMULATION AND RESULTS

To demonstrate the idea we have implemented the proposed modified algorithm on MATLAB version 7.13 and using a simple topology as shown in Figure 1. The topology used in the simulation consists of three networks where each network has three members of objects.

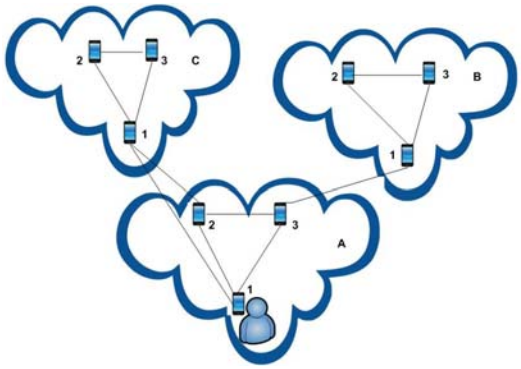


Figure 1. Network Topology

Based on topology showed in Figure 1, a simulation was performed using a scenario as follows. An object A1 want to connect to object B1. So A1 calculates the trust value towards object B1. The trust value calculations undertaken from object A1 are as follow:

a. Pre-processing

The connection matrix and initial trust value matrix were initialized in this step. Connection matrix was filled up with a value of '1' if the object was connected, and value of '0' for vice versa. Rows of the matrix describe the available networks, and columns of the matrix show objects that are connected to each network. Thus the connection matrix from A1 point of view will be:

$$\begin{bmatrix} A1 & A2 & A3 \\ B1 & B2 & B3 \\ C1 & C2 & C3 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

Default trust value for all objects in the beginning is 0.5. So the content of trust matrix from A1 point of view will be:

$$\begin{bmatrix} A1 & A2 & A3 \\ B1 & B2 & B3 \\ C1 & C2 & C3 \end{bmatrix} \rightarrow \begin{bmatrix} 0.5 & 0.5 & 0.5 \\ 0.5 & 0.5 & 0.5 \\ 0.5 & 0.5 & 0.5 \end{bmatrix}$$

b. Trust Value Calculation Process

Based on equation (1), object A1 tried to find out whether object B4 is located on the same network with object A1 or not. If object B1 is situated in the same network with object A1, then object A1 will calculate the trust value of object B1 using equation (1). However, if it turns that object B1 is not located in the same network with the object A1, and then object A1 will ask others objects in the network that connected with object B1. From the topology in Figure1, object A3 is connected to object B1. Furthermore, object A1 will give weight to object A3 based on previous historical trusts value of object A3. If object A3 is a trustable object, then object A1 will give a weight of 0.8, or give a weight of 0.3 otherwise. Object A3 investigates all connected objects that have a history of trust towards B1. Trust value of objects which located in the same network with object B1 will be calculated using equation (2), and added altogether with other objects located in different networks using equation (3).

c. Trust Value Scoring Process

The scoring process of trust value will lead to 2 results; whether another object is trustable enough or not. Reputation is another parameter that can be used to determine a trustable object. Weighting the reputation can be done using a range of value 0 to 1, and set a threshold value for determining the limit of a trustable object. A particular constant value was used in this simulation; a trustable object was given a value of 0.8, and a un-trustable object was given a value of 0.3. The process of trust value scoring in this simulation was performed using pheromone deposit equation as described in equation (4). Moreover, granting a reputation was done using equation (5).

The trust value can be reduced or increased over time, depending on the reputation of the object. The process of trust value reduction was done using equation (6).

The simulation was aimed for calculating the trust value, and it was done serially and randomly in 100 times. Initial trust value for every object was set of 0.5, and this value can be changed according to the number of objects that provide an assessment of the amount of trust towards object B1. Figure 2 shows the results of the trust value of object B1.

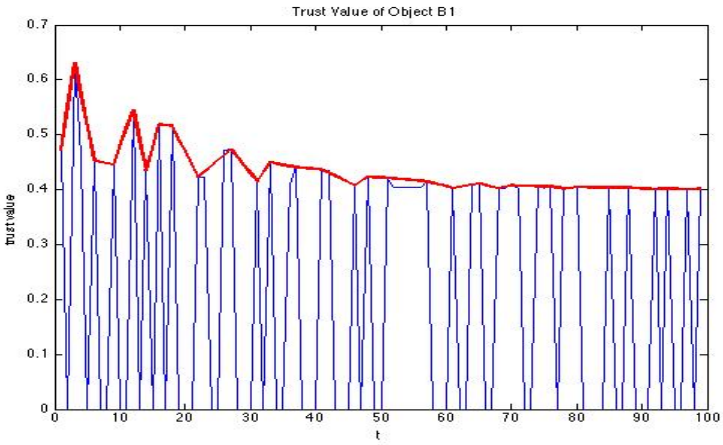


Figure 2. Trust Value of Object B1

Trend chart from Figure 3 displays the reducing trend of pheromone value, in which some point will stable in a certain value. This reducing trust value is caused by evaporation process when there is no connections happened during simulation. Reputation value also contributing to the decreasing of the trust value, where the values of reputation wane when there are no trust assessments done for some objects. Weighting process in the scoring reputation gives a significant influence in determining of this value. Selecting the appropriate method for scoring reputation can make the improvement.

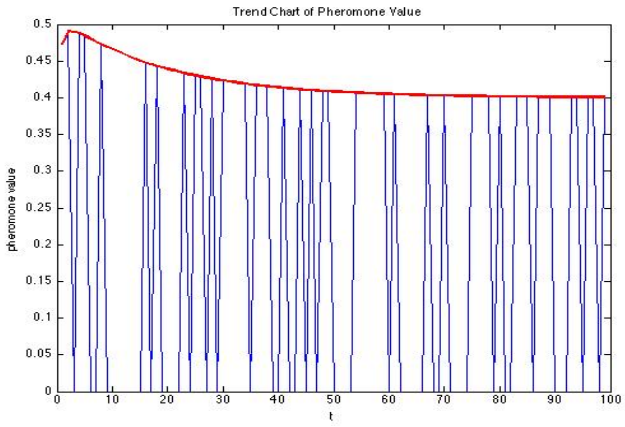


Figure 3. Trend Chart of Pheromone Value

Another trust assessment research, which was inspired by ant colony, was also done by [8]. Using different reputation and trust formula as well as selected performance parameters, research in this area are very potential to be developed.

4. CONCLUSION

Security aspects play an important role in Internet of Things. Some applications such as ITS, e-health, fleet management, smart metering, home automation might require security implementation to secure the data transferred and to improve privacy. In this paper, a modification of Ant Colony algorithm was proposed for scoring trust value of objects in Internet of Things. The simulation shows that adding a parameter namely reputation needs an appropriate weighting method so that the trust values will be scored fairly for all objects, regarding their previous activities during the communication process. Improvements on security model for trust value scoring will be a good alternative solution in future works, especially the one, which has better resistance against attacks.

ACKNOWLEDGMENT

This research was partially supported by Ministry of Research, Technology, and Higher Education, Indonesia under the PUPT grant (751/UN1-P.III/LT/DIT-LIT/2016).

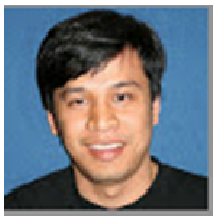
REFERENCES

[1] R. H. Weber, "Internet of Things – New security and privacy challenges," *Computer Law and Security Review*, vol/issue: 26(1), pp. 23–30, 2010.
[2] H. S. Kim and J. S. Seo, "A Daily Activity Monitoring System for Internet of Things-Assisted Living in Home Area Networks," *International Journal of Electrical and Computer Engineering*, vol/issue: 6(1), pp.399–405, 2016.
[3] S. Tozlu, *et al.*, "Wi-Fi enabled sensors for internet of things: A practical approach," *IEEE Communication Magazine*, vol/issue: 50(6), pp. 134–143, 2012.
[4] J. Pescatore, "Securing the ' Internet of Things ' Survey", Report, SANS Institute, 2014.
[5] J. M. S. Koppula, "Secure Digital Signature Scheme Based on Elliptic Curves for Internet of Things," *International Journal of Electrical and Computer Engineering*, vol/issue: 6(3), 2016.
[6] Y. Cheng, *et al.*, "Privacy in machine-to-machine communications A state-of-the-art survey," in *2012 IEEE International Conference on Communication Systems, ICCS 2012*, pp. 75–79, 2012.
[7] D. Chen, *et al.*, "TRM-IoT: A trust management model based on fuzzy reputation for internet of things," *Computer Science and Information System*, vol/issue: 8(4), pp. 1207–1228, 2011.
[8] P. Bedi and R. Sharma, "Trust based recommender system using ant colony for trust computation," *Expert System with Application*, vol/issue: 39(1), pp. 1183–1190, 2012.
[9] S. Zafar and M. K. Soni, "Trust based QOS protocol(TBQP) using meta-heuristic genetic algorithm for optimizing and securing MANET," *ICROIT 2014 - Proc. 2014 International Conference on Reliability, Optimization, and Information Technology*, pp. 173–177, 2014.
[10] M. Nitti, *et al.*, "A subjective model for trustworthiness evaluation in the social Internet of Things," *IEEE International Symposium on Personal, Indoor, and Mobile Radio Communication PIMRC*, pp. 18–23, 2012.
[11] Z. Chen, *et al.*, "Fuzzy Theory for the P2P Subject Trust Evaluation Model," *International Journal of Advancement in Computing Technology.*, vol/issue: 4(8), pp. 67–74, 2012.

[12] RFC 2828, "Internet Security Glosary."
[13] Z. Yan and P. Zhang, "A Survey on Trust Management for Internet of Things," 2014.
[14] R. Roman, *et al.*, "Securing the Internet of things," *IEEE Computer Society.*, vol/issue: 44(9), pp. 51–58, 2011.
[15] S. Ries, *et al.*, "A Classification of Trust Systems," *Move to Meaningful Internet System 2006*, pp. 894–903, 2006.
[16] D. Gambetta, "Trust: Making and Breaking Cooperative Relations," 2000.

BIOGRAPHIES OF AUTHORS

Vera Suryani received Master degree ini Information Techology from Institut Teknologi Bandung, Indonesia in 2009. She joined as a Lecturer in the School of Computing and Informatics, Telkom University, in 2003. She is currently member of Sistem Elektronis laboratory at Universitas Gadjah Mada. Her research interests include wireless sensor network, distributed system, and Internet of Things. Currently she is working for Ph.D program at Departement of Electrical Engineering & Information Technology, Universitas Gadjah Mada, Indonesia.



Selo Sulistyo is an associate professor in Information and Communication Technology at the Department of Electrical Engineering and Information Technology. He is also Head of Sistem Electronis laboratory at Universitas Gadjah Mada. His research interests including Software Modeling, Mobile application development and Security for the Internet of Things and connected objects.

Widyawan is an assistant professor in Information and Communication Technology at the Department of Electrical Engineering and Information Technology Universitas Gadjah Mada. He is also Director of Center of System and Information Resource at Universitas Gadjah Mada. His research interests including pervasive computing, computer security, ubiquitous computing, and wireless system.