Received: December 22, 2016

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

ConTrust: A Trust Model to Enhance the Privacy in Internet of Things

Vera Suryani[1,2]* **Selo Sulistyo**[1] **Widyawan Widyawan**[1]

[1]*Department of Electrical Engineering & Information Technology, Universitas Gadjah Mada, Indonesia*
[2]*School of Computing, Telkom University, Indonesia*
* Corresponding author's Email: vera.s3te14@mail.ugm.ac.id

Abstract: The objects connected to the Internet of Things require security. Security can do a variety of forms, ranging from data encryption to trust management mechanism. Privacy aspects can be improved through the process of trust assessment. Here privacy is improved using Diffie-Hellman key distribution and trust assessment to ensure only trusted things can communicate in the IoT environment. This paper proposed new trust assessment model namely ConTrust. Inspired by the experience of everyday life, ConTrust uses two parameters for assessing trust value: current trust assessment and history-based reputation. History parameter is used in the formula of trust assessment in order to make a fair calculation based on its past object experiences. The formula also utilizes time parameter to improve the fluctuating values of reputation. Some simulations were conducted to evaluate ConTrust and showed that the time parameter is very important factors that influenced the stability of trust and reputation value.

Keywords: Internet of Things, Trust, Reputation, Trust assessment, ConTrust, Diffie-Hellman

1. Introduction

The Internet of Things paradigm brings new capability of Wireless Sensor Network (WSN) and mobile network into the next level. Sensors, objects now are connected to the Internet for easiness of data transmission of some applications: e-health, smart home, smart city, smart transportation, etc. IoT bridges the physical and virtual world using Internet connection.

IOT is a paradigm that enables sensors, people, or objects, which more commonly referred to "things", to be connected to the Internet. This means that things can be controlled from a distance for a particular purpose. In this paper, things will be called as objects for consistency purpose. Architecture is required to accommodate this characteristic. IOT architecture in general can be seen in Fig. 1, wherein the architecture consists of three layers: Perception, Network, and Application. Perception layer is the lowermost layer of the architecture, which mostly related to the physical aspects of objects or things in IOT, such as sensors, people, mobile or static devices. Aims to sense, to collect data, and to send these data to the upper layer called Network layer. Network layer functioned to forward the data obtained from the objects on the layer below it with technologies that lies on the network. Networks included in this layer can be composed of ad-hoc network elements, such as Zigbee, Bluetooth, Wi-Fi, etc., as well as elements of larger networks such as CDMA, GSM, 3G, 4G, etc. Once data are forwarded through the network layer, then they can be further processed into useful information in the Application layer. For example if the temperature sensor data received at Perception layer are passed through the network layer to the Application layer, these data can be transformed into meaningful information such as a value that will trigger the air conditioner to be turned on in smart home applications.

In smart transportation, where connected cars are equipped with Internet access, some interchangeable data from cars might help to save lives by sending data about bad weather or an accident ahead.

DOI: 10.22266/ijies2017.0630.04

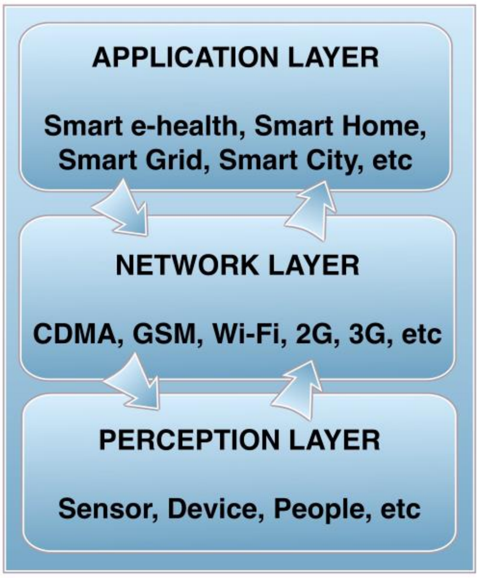
APPLICATION LAYER
Smart e-health, Smart Home, Smart Grid, Smart City, etc
NETWORK LAYER
CDMA, GSM, Wi-Fi, 2G, 3G, etc
PERCEPTION LAYER
Sensor, Device, People, etc

Figure.1 IoT architecture

Not only limited to important data such as car braking profile, accident info, traffic jam, but infotainment data can also be transferred to cars. One of the important factors that enable this technology is an Internet connection. The Internet connection is also the main element of Internet of Things or IoT. Because of Internet now objects, people, devices can be connected and controlled to make people's life easier.

In addition to the convenience offered by IoT, there are some issues related to security, privacy, trust [1]. Security aspects are needed in IoT since data collected from a sensor, people, or mobile device might have processed or mined through the Internet as unsecure channel. Privacy becomes complimentary requirement to enhance the security aspect in IoT. There are some big challenges correlated to privacy, one of them is how to choose trusted partner before data communication occurs instead of securing the data using encryption algorithm. Alternatively, we can use trust managements for seeking trusted partner. Trust managements are used to verify the security policies, and trust assessment is a tool to do this verification [2]. Using trust assessment for privacy enhancement has already been conducted by some researchers [3,4-5].

Recent studies have improved trust aspect using trust models. In [6], the model used cube structure for intersecting of three parameters: security (authorization), trust (reputation), privacy (respondent). However, there is no further explanation of the methods used for these three parameters. Yang Liu et.al [7] proposed a model to classify the user's trust using three level rank: high, medium, and low. The leveling system based on fuzzy mathematics for making a decision on authentication ranking. Meanwhile, M. Nitti [8] proposed trust model based on trustworthiness computation from friends experiences and opinions of a node in IoT environment. Trustworthiness value is calculated from centrality, intelligence, node's direct experience, and opinion. Other researchers Junqi Duan et.al did likewise on their research, which was also utilized trust and centrality degree (TC-BAC) to develop distributed trust mechanism in WSN [9]. The TC-BAC method allowing access to trusted objects using direct and indirect trust assessment. Furthermore, the object will be granted access using centrality degree.

Not only trust assessment that was used to model the trust, but the biological activity was also utilized to model the trust. Many of current research are inspired by the biological activities, and surprisingly many computing problems are solved using these biological models that already exist in nature. Take for an example; many researchers proposed trust models inspired by animal activities such as ant colony [10,11-12], evolutionary biology: inheritance, mutation, natural selection and recombination [13]. Also, some research associated with the bio-inspired area are developed by [14-15], where trust is modeled using genetic algorithms and bat-inspired routing. In addition to bio-inspired trust model, the trust also modeled using other existing algorithms on internets such as probability theory or game theory. Research utilizing probability theory for building the trust model, among others, performed by [16-17], while research on game theory-based was developed by [18].

From the research on trust models that have been described previously, their research mostly were not using time parameter in their trust algorithm. This paper proposes a trust algorithm which uses time parameter to protect the user's privacy for static and dynamic objects in IoT. The proposed model uses trust assessment based on object reputation and object's current activities rated from other objects in the same community. Also, the trust assessment here tries to improve the existing algorithm [9] by adding time parameter in the algorithm. The addition of this parameter is intended to prevent the reputation scoring which tends to stagnate at a certain value or increased without any apparent objectivities. Contribution expected from the addition of this parameter is a better trust assessment of reputation and current trust values.

The paper is organized as follows: Section II describes the proposed model, Section III describes the simulation, result, and discussion, and Section IV explains the conclusion and future works.

2. The Proposed Model: ConTrust

Based on the definition of IETF Internet Security Glossary privacy is defined as “The right of an entity (normally a person), acting on its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others” [19].

Privacy is one of the important parameters to improve security, which aims to preserve the private information so that one can feel comfortable to share his/her private information. Some methods can be used to improve privacy, such as authentication, encryption, and access restrictions. Trust as access restriction component plays an important role in enhancing the privacy. Using trust for limiting the communication among objects can prevent malicious objects from attempting to make such trust-based attacks. These attacks may give fake trust or reputation values of an object.

Trust is required for objects in the IOT environment to ensure secure data communication with a trusted object only. Objects in IoT have different characteristics compared to ordinary Internet objects. These IoT objects can dynamically join or leave communities at any time, which needs assessment to generate a precise trust recommendation.

ConTrust is a trust model consisting of current and past assessments. There are four main processes in the ConTrust: pre-processing, trust assessment, trust recommendation, and reputation updates. See Fig. 2 for details of ConTrust model.

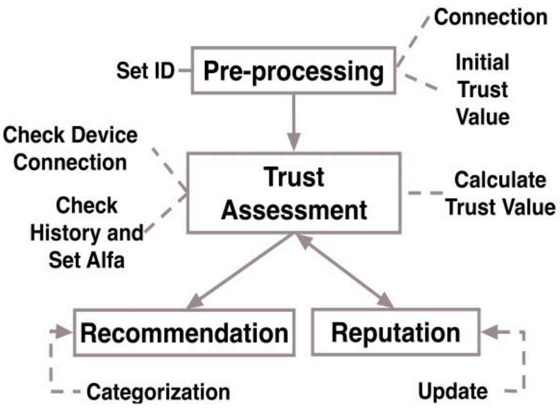

Figure.2 ConTrust model

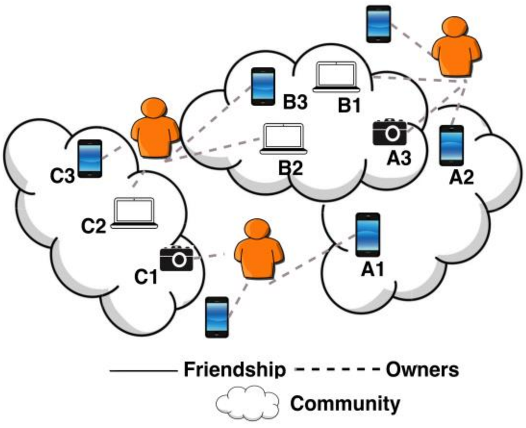

Figure.3 SioT

2.1. Pre-processing and Trust Assessment

The objects are modeled using SIoT [20] as shown in Fig. 3. Every user can have more than one object, and each object can join in a community according to its preference.

Each object has three initial matrixes, which contain connectivity information, trust value, and reputation value of other objects in the same community. The object is recognized from its ID which consisting of two components: user information and object number. Hence, the initial matrix of an object will look like:

$$M_c = \begin{bmatrix} a_{11} & \dots & a_{in} \\ \dots & \dots & \dots \\ a_{j1} & \dots & a_{jn} \end{bmatrix} \quad (1)$$

Connection matrix was given with a value of one if the objects are connected and filled with zero if they are not connected to each other. Rows of matrix describe the available networks, and the columns of matrix show the connected objects in each network. Thus the connection matrix of A1 becomes:

$$\begin{bmatrix} A1 & A2 & A3 & A4 \\ B1 & B2 & B3 & B4 \\ C1 & C2 & C3 & C4 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad (2)$$

Meanwhile, initial trust values for all objects were given by 0.8. Thus, the trust values matrix becomes:

$$\begin{bmatrix} A1 & A2 & A3 & A4 \\ B1 & B2 & B3 & B4 \\ C1 & C2 & C3 & C4 \end{bmatrix} = \begin{bmatrix} 0.8 & 0.8 & 0.8 & 0 \\ 0.8 & 0.8 & 0.8 & 0.8 \\ 0.8 & 0.8 & 0.8 & 0 \end{bmatrix} (3)$$

Every matrix is updated periodically. This periodic update is an important factor to identify active objects and who have left the community.

The assessment process considering two elements of trust: the past and current activities. Object history is the main component of trust computation. This component, known as α in Eq. (4), describes weighting method to be used in trust computation. Trust value used in this study ranging from the value of zero to one (0 to 1). Overall the trust value is calculated using Eq. (4).

$$T(t) = \propto . h_{ijl}^{nm}(t) + (1 - \propto). R(t) \tag{4}$$

Where:
$T(t)$ = total of trust value
$h_{ijl}^{nm}(t)$ = 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
$\propto$ = given weight of history function [0,1]

A function for calculating trust value for objects in the same community is expressed in Eq. (5). Meanwhile, Eq. (6) is used to calculate trust value of objects in a different community that might have communicated with the target object, and Eq. (7) is a function to calculate the average of trust value in the same and different community.

$$f_{ij}^{m}(t) = \frac{\frac{1}{N}\sum_{i=1,i\neq j}^{m} T_{[j]}(t) + T_{[j]}(t-1)}{2} \tag{5}$$

$$g_{jl}^{n}(t) = \frac{1}{N}\sum_{j=1,j\neq l}^{n} T_{[l]}\,(t) \tag{6}$$

$$h_{ijl}^{nm}(t) = \frac{f_{ij}^{m}(t) + \frac{1}{N}\sum_{a=1}^{b} g_{jl}^{n}(t)}{2} \tag{7}$$

Where:
$f_{ij}^{m}(t)$ = trust function of the object *i* to object *j* at time *t*
$g_{jl}^{n}(t)$ = trust function of the object *j* to object *l* at time *t*
$h_{ijl}^{nm}(t)$ = function to calculate the average of trust value in same and different community

Furthermore, *i* is an object which calculates trust value toward object *j*, while object *l* is another object in the different network which has already had communication experience to object *i* in past interaction.

2.2. Recommendation

Trust value resulting from Eq. (4) will be used for object recommending, whether it is considered very trusted, trusted, untrusted, nor very untrusted. This categorization is described as follow:

$$T_j(t) = \begin{cases} Very\ trusted\ if\ 0.7 < h_{ijl}^{nm}(t) \leq 1 \\ Trusted\ \ if\ 0.5 < h_{ijl}^{nm}(t) \leq 0.7 \\ Untrusted\ if\ 0.3 < h_{ijl}^{nm}(t) \leq 0.5 \\ Very\ untrusted\ if\ h_{ijl}^{nm}(t) \leq 0.3 \end{cases} \tag{8}$$

Based on this recommendation value that generated from trust assessment before, an object may choose whether to perform data communication or not to the target object. The next step is giving the profile value of the target object based on communication satisfaction. This profile value becomes an input for deciding the reputation process of the target object.

2.3. Reputation

Reputation is used to determine the level of trust. It can be measured based on previous knowledge and current interactions among 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 objects in the IoT as a control system for selecting the services in the IoT. The value of reputation used in this study is inspired by everyday life, where trust value of a person can be gained from past experiences or history, and also can be obtained from other people appraisal.

In this ConTrust model, reputation value consists of history and reputation aspects. Weighting process is used to both of these aspects, which means that the reputation of the current object is affected by its previous history. The formula used in ConTrust actually is an improvement on the previous formula used in [21].

The formula used for calculating the history aspect can be seen in Eq. (9).

$$\beta = T(t) - T(t-1) \tag{9}$$

Where β = historical trust value of the object which is a reduction from the current trust value and the previous trust value β can be positive or negative value. If β is a positive value means that trust value is increasing, otherwise trust value is decreasing when β negative. This β value is used to determine the reputation formula. Hence, the reputation formula is defined as follows:

$$R(t) = \frac{h_{ijl}^{nm}(t)}{1+e^{-\beta t}} \tag{10}$$

where *R(t)* is indirect trust value produced from object's reputation in certain time periods.

2.4. Resistance to Trust Attacks

Some trust-related attacks might happen in IoT environment. These trust-related attacks usually correlated with giving fake recommendation from an object, such as:

a. Good-mouthing attacks: gives fake good recommendations of an object
b. Bad-mouthing attacks: gives fake bad recommendations of an object
c. Self-promoting attack: promote itself by giving good recommendation to boost its reputation

When an object tries to compute trust value using ConTrust model, this object has to ask other objects about trust value of target object. The process of asking involves the usage of Diffie-Hellman key distribution among trusted object in the same community. After finishing this process, the objects will exchange the trust value for trust computation purpose. Subsequently, reputation value will be produced at the end of the computation process.

Whitfield Diffie and Martin Hellman published Diffie-Hellman algorithm in 1976. Data needed in the algorithm are exchanged over a public network. The process performed by the algorithm is as follows [22]:

a. Necessary agreement between the two parties that communicate to choose large prime numbers suppose Alice and Bob select n and g, such that $g < n$
b. Alice generates random big integer x and sends A using Eq. (11) to Bob:

$$A = g^{x} mod\, n \tag{11}$$

c. Bob generates random big integer y and sends B using Eq. (12) to Alice:

$$B = g^{y} mod\, n \tag{12}$$

d. Alice computes K using Eq. (13) and sends its value to Bob:

$$K = B^{x} mod\, n \tag{13}$$

e. Bob computes K' using Eq. (14) and sends its value to Alice:

$$K' = A^{y}\ mod\ n \tag{14}$$

f. Both Alice and Bob will compare the value K and K'. If it has obtained that $K = K'$ then these values become symmetric keys between Bob and Alice.

3. Result and Discussion

We conducted some simulations to evaluate the formula of trust assessment that has been proposed. Using Matlab version 7.13 and topology as seen in Fig. 3, the simulations were run to investigate the effect of α parameter to the trust values and β paramater on reputation values. The initial trust and reputation values were set to 0.8. Performance evaluation of proposed algorithm ConTrust were achieved by comparing it to TC-BAC method, as well as without any trust method.

3.1. Simulation on Trust Values

Fig. 4, Fig. 5, and Fig. 6 depict the trust values affected by α parameter. Here α were set to $0.7 < \alpha \leq 1$, $0.5 < \alpha \leq 1$, $0.3 < \alpha \leq 0.7$. We can deduce from these figures that changing the α values will influence the stability level of the trust value. Moreover, the trust assessment without any trust method used its assessment tends to be more stable, although there is no guarantee that the stability rate will not change, as shown in Fig. 5. This is due to the trust assessment without any trust method tends to be subjective, which can lead to the fluctuation result of trust values. Meanwhile, the TC-BAC and ConTrust methods resulted in more varied trust value, with the same relative degree of stability. It is caused by α parameter which determines whether the trust assessment is focused to direct trust or reputation as indirect trust assessment. Both compared methods are focusing on direct trust assessment. The difference of trust value between ConTrust and TC-BAC was caused by the different calculation formula of indirect trust assessment. Details about indirect trust assessment or reputation formula are discussed in the next sub-section.

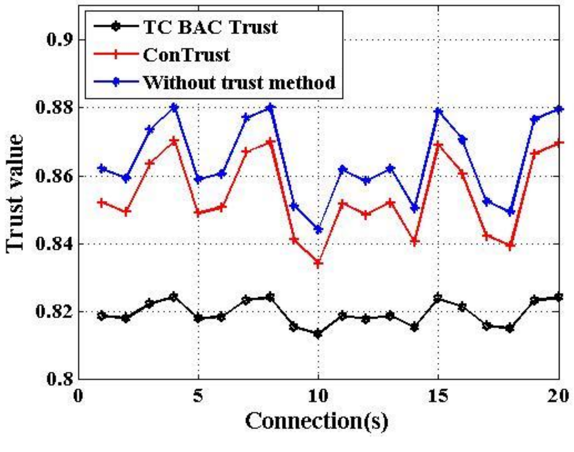

Figure.4 The effect of $0.7 < \alpha \leq 1$ parameter on trust value

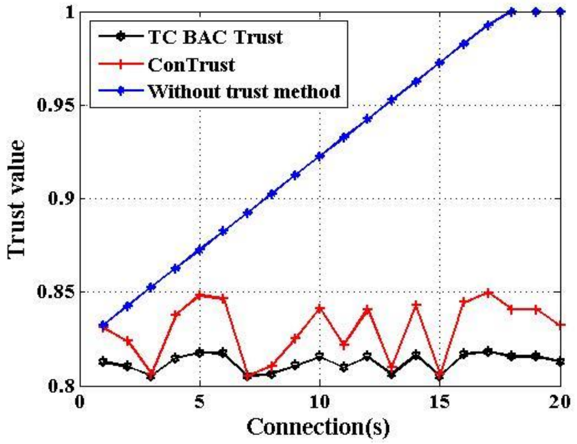

Figure.5 The effect of $0.5 < \alpha \leq 1$ parameter on reputation value

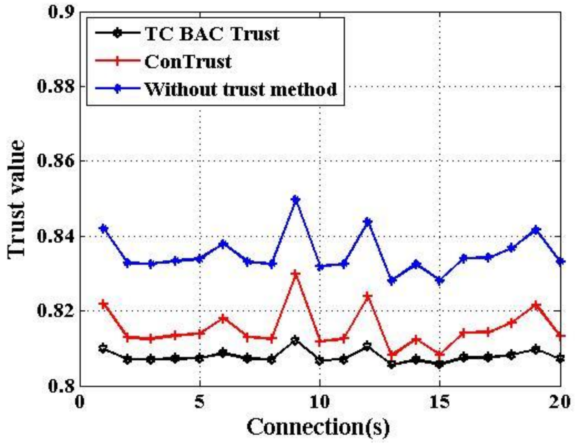

Figure.6 The effect of $0.5 < \alpha \leq 1$ parameter on reputation value

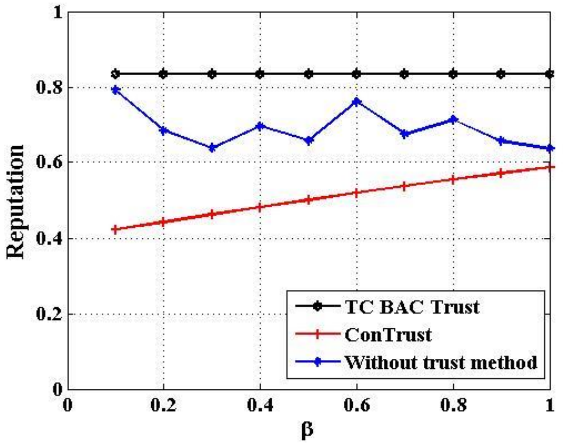

Figure.7 The effect of β parameter on reputation value

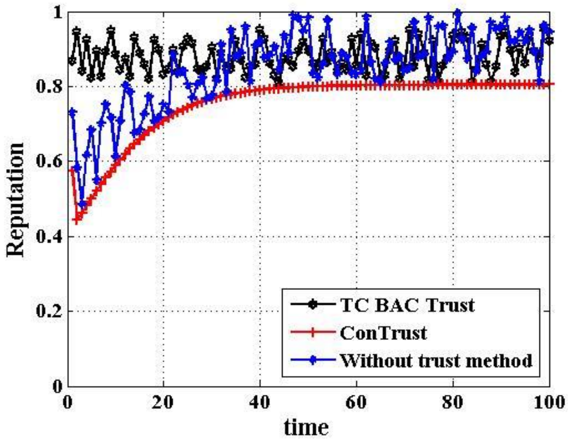

Figure.8 The effect of *time* parameter on reputation value

3.2. Simulation on Reputation Values

Reputation formula as described in Eq. (8), influenced by the historical value or β. The β parameter serves as stability controller for the reputation values, as depicted in Fig. 7. Moreover, the addition of the time parameter in ConTrust has made the reputation values were unchanged fluctuatively, which were not happening in TC-BAC and without any trust method. See Fig. 8 for more detail of comparison results. Factually, the reputation values will not suddenly increase, but changed slowly over time, unless the reputation values have counterfeited before. This time parameter effectively proved to address the problem of counterfeiting the reputation values.

Meanwhile, as resistance against the good and bad mouthing attacks, ConTrust can detect attacks aforementioned thanks to the Diffie-Hellman authentication. All connected objects that plan to do trust assessment will be pre-filtered by the Diffie-Hellman authentication, so that if there is a new object that has not been authenticated before can not send fake trust and reputation values.

However, this method still needs to be improved since the authentication process itself is not sufficient enough to strengthen the privacy. Improvement in security model for automatic trust-based attacks detection is next research challenge to be resolved.

4. Conclusion

In this paper, we proposed a trust assessment and analyzed its feasibilities by some simulations. This trust assessment including parameters based on current trust assessment and object past experiences rating to other objects or called as reputation value. Proposed algorithm ConTrust uses time parameter instead of the historical parameter in its formula for trust assessment. These parameters are an improvement from TC-BAC method. The influence of both parameters as seen from simulation results lies in the stability of the trust values. The stability of the trust value is required to detect the forgery reputation scoring. Trust values of ConTrust found more stable than the TC-BAC and without any trust methods.

Future research can be developed to ConTrust algorithm is deploying more security aspect to make ConTrust more resistant to some attacks, especially trust-based attacks. The importance of this development is to improve the privacy rather than through trust calculation and rely on Diffie-Hellman key distribution only. We also plan to extend the proposed method by designing security framework, which contain novel election algorithm for ConTrust manager.

Acknowledgments

This research was funded by PPI (Penyiapan Publikasi Internasional) 2016, Universitas Gadjah Mada. This research was also partially supported by Ministry of Research, Technology, and Higher Education, Indonesia under the PUPT grant (751/UN1-P.III/LT/DIT-LIT/2016). We would also like to thank Laboratory of Sistem Elektronis for permitting us to use the laboratory facilities.

References

[1] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, Privacy and Trust in Internet of Things: The Road Ahead", *Computer Networks*, Vol.76, pp.146–164, 2015.

[2] M. Blaze, J. Ioannidis, and A. D. Keromytis, "Experience with the KeyNote Trust Management System: Applications and Future Directions", *Trust Management*, Vol.2692, pp.284–300, 2003.

[3] X. Wang, W. Cheng, P. Mohapatra, and T. Abdelzaher, "ARTSense: Anonymous Reputation and Trust in Participatory Sensing", *Proceedings of IEEE INFOCOM*, Turin, Italy, pp.2517–2525, 2013.

[4] Z. Erkin, T. Veugen, and R. L. Lagendijk, "Generating Private Recommendations in A Social Trust Network", In: *Proc. of 2011 International Conf. on Computational Aspect of Social Networks*, Salamanca, Spain, pp.82–87, 2011.

[5] X. Wang, W. Cheng, P. Mohapatra, and T. Abdelzaher, "Enabling Reputation and Trust in Privacy-Preserving Mobile Sensing", *IEEE Transaction on Mobile Computing*, Vol.13, No.12, pp.2777–2790, 2014.

[6] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, "Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)", *Communication on Computing and Information Science (CCIS)*, Vol.89, pp.420–429, 2010.

[7] Y. Liu, Z. Chen, F. Xia, X. Lv, and F. Bu, "A Trust Model Based on Service Classification in Mobile Services", In: *Green Computing and Communication (GreenCom), 2010 IEEE/ACM International Conf. on Cyber, Physical, and Social Computing*, Hangzhou, China, pp.1–5, 2010.

[8] M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito, "A Subjective Model for Trustworthiness Evaluation in the Social Internet of Things", In: *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Sydney, Australia, pp.18–23, 2012.

[9] J. Duan, D. Gao, C. H. Foh, and H. Zhang, "TC-BAC: A Trust and Centrality Degree based Access Control Model in Wireless Sensor Networks", *Ad Hoc Networks*, Vol.11, No.8, pp.2675–2692, 2013.

[10] P. Bedi and R. Sharma, "Trust based Recommender System using Ant Colony for Trust Computation", *Expert System with Application*, Vol.39, No.1, pp.1183–1190, 2012.

[11] M. Zhang, R. Zheng, Q. Wu, W. Wei, X. Bai, and H. Zhao, "B-iTRS : A Bio-Inspired Trusted Routing Scheme for Wireless Sensor Networks", *Journal of Sensors*, Vol.2015, 2015.

[12] F.S. Gohari, H. Haghighi, and F.S. Aliee, "A Semantic-enhanced Trust based Recommender System using Ant Colony Optimization", *Applied Intelligent Journal*, Vol.46, No.150, pp.1–37, 2016.

[13] S. Zafar and M. K. Soni, "Trust based QOS Protocol (TBQP) using Meta-heuristic Genetic Algorithm for Optimizing and Securing MANET", In: *Proc. of 2014 International Conf. on Reliability, Optimization and Information Technology*, Delhi, India, pp.173–177, 2014.

[14] K. Jayabharathi, V. Ranganathan, and R. Kishore, "An Efficient Trust Based Bat-Inspired Routing (TBIR) Protocol for MANET", *International Journal of Advance Engineering Technology*, Vol.7, No.2, pp.721-730, 2016.

[15] U. E. Tahta, S. Sen, and A. B. Can, "GenTrust: A Genetic Trust Management Model for Peer-to-peer Systems", *Applied Soft Computing Journal*, Vol.34, pp.693–704, 2015.

[16] Z. Taghikhaki, N. Meratnia, and P. J. M. Havinga, "A Trust-based Probabilistic Coverage Algorithm for Wireless Sensor Networks", *Procedia Computer Science*, Vol.21, pp.455–464, 2013.

[17] Y. Wang, G. Yin, Z. Cai, Y. Dong, and H. Dong, “A Trust-based Probabilistic Recommendation Model for Social Networks”, *Journal of Network and Computer Application*, Vol.55, pp.59–67, 2015.

[18] B. Aziz, P. Fremantle, R. Wei, and A. Arenas, “A Utility-based Reputation Model for the Internet of Things”, *IFIP Advance in Information and Communication Technology*, Vol.471, pp.261–275, 2016.

[19] R. Shirey, “RFC 2828: Internet Security Glosary”, GTE/BBN Technologies, Internet Society, 2000.

[20] L. Atzori, A. Iera, and G. Morabito, “SIoT: Giving A Social Structure to The Internet of Things”, *IEEE Communication Letter,* Vol.15, No.11, pp.1193–1195, 2011.

[21] V. Suryani, S. Sulistyo, and Widyawan, “Trust-Based Privacy for Internet of Things”, *International Journal of Electrical and Computer Engineering*, Vol.6, No.5, 2016.

[22] E. Rescorla, “RFC 2631: Diffie-Hellman Key Agreement Method”, RTFM Inc., Internet Society, 1999.