SECURITY IN THE INTERNET OF THINGS: TRUST AND REPUTATION EVALUATION MODEL

[1]Caroline Gurajena, [2]Khulumani Sibanda, [3]Edmore Chindenga
Department of Computer Science, University of Fort Hare, Alice, 5700, South Africa
[1]cgurajena@ufh.ac.za, [2]ksibanda@ufh.ac.za, [3]echindenga@ufh.ac.za

Abstract - Trust and reputation are vital in IoT because they enable entities to communicate or collaborate securely. Reputation minimizes uncertainty and risk. An entity's reputation is computed from recommendations obtained from all the entities that have interacted with the entity and this enables entities without prior experience to interact. This paper proposes a reputation model for the IoT environment based on fuzzy logic. Fuzzy logic was chosen because of its ability to handle imprecise and uncertain information. The fuzzy inference system takes in reputation properties and outputs the reputation value. The properties from multiple recommenders are combined into a single value before the values are fed into the fuzzy inference system. The results obtained from the model reveals that the model is effective in identifying malicious entities within IoT environments. The results imply that a reputation system can be used to support decision making in an IoT environment.

***Keywords*:** Internet of Things, Trustworthiness, Trust, Security, Privacy, Reputation model.

1 Introduction

The ensuing Data Revolution is seeing increasing amounts of data being generated from new data sources and devices, and also data being utilized in new and novel ways across the various sectors of society to support the achievement of sustainable development imperatives. We are moving into an era where everyone and every device embedded with sensors will be connected to the Internet of Things (IoT). IoT bridges the gap between the physical world and the digital world by connecting physical 'things' that are embedded with sensors to the Internet. Since its inception, the IoT has earned itself various definitions. For this paper we adopt the following definition by [Vermesan *et al.*, 2011]: IoT is a "*dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities, use intelligent interfaces and are seamlessly integrated into the information network*" [Vermesan *et al.*, 2011]. This definition encompasses serious challenges that are associated with IoT. Firstly, the issue of the global nature of the infrastructure means that numerous devices will be connected and new ones added at an astronomical rate. Secondly, the devices' self-configuring nature makes it possible to have malicious devices joining the network and pose security risks. Such security risks can take various forms, it can be communication risk, authentication risk, availability risk or integrity risk. Those risks are further compounded by the fact that it is imperative for these 'things' or devices to be "*discoverable, addressable and accessible*" [Leppänen and Riekki, 2012].

Such capabilities create smart devices that are capable of communicating and collaborating with each other. The smart devices are also able to collect and send data. This results in large amounts of data being collected for further analysis and utilization. IoT aims to equip the smart devices with some form of intelligence towards the goal of Intelligence Augmentation (IA) and Cognitive Augmentation (CA), where computing devices are able to support, enhance, and complement human intelligence in their everyday living. This makes trust and reputation an important part in making the smart devices intelligent and secure, and also of ensuring that the operation of these devices is geared towards the privacy of the users. Trust and reputation enable the devices to make intelligent decisions when collaborating or when sending data, this improves the quality and use of data in IoT.

Over the past ten years, many researchers have undertaken research in IoT. According to Konig, Hudert and Eymann (2010), the research that has been done can be categorized into two levels of abstraction: proposals of "*agents and intelligent services in conjunction with socio-economic mechanisms as crucial for the future of IoT… and simulation tools*". Such research has led to the identification of the challenges that need to be addressed to ensure the success of the IoT. According to [Leppänen and Riekki, 2012] the challenges in the IoT include "*addressing device heterogeneity, interoperability issues with different communication technologies, cooperation, coordination and scalability beyond current systems*". Cooperation challenges include security, trust and privacy challenges. Some of the security and trust challenges are caused by the presence of malicious and selfish entities within the network. In this research, an entity is any heterogeneous device that forms part of the IoT network. Such entities can be identified by trust and reputation models. This paper focuses on the design and development of a reputation model that is suitable for the IoT environment. Gutscher (2007) defined a reputation system as "*an*

approach to systematically evaluate opinions of online community members on various issues and their opinions on the trustworthiness of other community members" [Gutscher, 2007]. Reputation is an essential factor of human interaction and it is of paramount importance for systems that emulate human interaction such as systems that are provided in the IoT environment. In reputation systems, malicious behavior causes an entity to lose good reputation. Reputation can be computed from the accumulation of past experiences of either a single entity or from multiple entities.

This paper proposes a reputation system for the Internet of Things (IoT). The aim of the reputation model is to identify malicious and selfish entities in the network. This would encourage the entities to be cooperative and to share information in IoT. The contributions of this paper are as follows:

- It proposes a suitable model architecture for reputation computation in IoT.
- It develops a calculation method for computing recommendation weight based on fuzzy logic.
- It presents a multi-dimensional reputation evaluation method

The proposed reputation model offers local and global reputation computation, which is important for IoT environments. The rest of the paper is organized as follows. Section 2 gives a brief overview of reputation systems. Section 3 describes the proposed reputation model and section 4 details the evaluation of the proposed model.

2 Reputation Systems

Major Trust and reputation, although closely related, are different concepts. The main difference between trust and reputation is that trust aims to predict the future while reputation is a summary of the knowledge of the past behavior of a trustee. The trustee is the entity that is being trusted. Reputation shows the overall past behavior of the trustee obtained from all the entities that the trustee has transacted with; it doesn't indicate the trust value of a particular truster in the trustee. The truster is the trusting entity. Reputation can be used in determining the intentions of the trustee whenever the trustee is unknown to the truster. Security breaches cause entities to lose their reputation and this affects their interaction with other entities within the network. Even though they are different, trust and reputation share the following same characteristics [Wang and J Vassileva, 2003; Yu *et al.*, 2012]:

- Context-specific
- Dynamic
- Multi-dimensional
- Reflexive
- Asymmetric
- Incomplete transitive

Reputation models evaluate the credibility and the reliability of the entities based on past behavior. Reputation models use public reports in an attempt to determine the behavior of an entity. The reputation of an entity is based on the collected opinions of entities that have interacted with the entity. After the collection of information, the model then evaluates the reputation value based on the relevant information. Reputation can be computed based on a single thing or multiple things [Eder *et al.*, 2013].

There are different reputation systems that have been proposed over the years. Song *et al.*, (2005) proposed a reputation system that is based on fuzzy logic for P2P transactions [Song *et al.*, 2005]. The aim of the system was to assist strangers in P2P transactions to establish mutual trust. Another distributed P2P reputation system was proposed by [Kamvar, Schlosser and Garcia-Molina, 2003]. The reputation system is based on eigentrust. "*In EigenTrust, the global reputation of each peer **i** is given by the local trust values assigned to peer **i** by other peers, weighted by the global reputations of the assigning peers*" [Kamvar, Schlosser and Garcia-Molina, 2003]. The authors highlighted that a reputation system should be sensitive to malicious entities that work together in order to subvert the system. However, the proposed model does not take into consideration multiple properties of reputation.

Wang and Julita Vassileva, (2003) proposed a trust model for building reputation based on Bayesian network. The reputation was estimated based on download speed, file quality and file type. The problem with Bayesian networks is that the probability values used in the network are based on repeatable experiments which is not ideal for an IoT environment [Abdul-Rahman and Hailes, 2000]. This limitation can be addressed by using fuzzy logic. Fuzzy logic enables the model to deal with uncertain and imprecise information. Fuzzy reasoning enables the model to make approximate reasoning using imprecise and uncertain information.

Over the past few years there has been an increase on research that focused on using fuzzy logic to compute trust and reputation such as [Chen *et al.*, 2011; Javanmardi *et al.*, 2014; Bernal Bernabe, Hernandez Ramos and Skarmeta Gomez, 2016; Mhetre, Deshpande and Mahalle, 2016; Truong, Um and Lee, 2016]. These researchers found that fuzzy logic is computationally efficient in computing trust and reputation. The model proposed by

Mhetre, Deshpande and Mahalle (2016) focuses on trust computation. Truong, Um and Lee (2016) proposed a fuzzy-based trust model that used reputation, recommendation and knowledge of the trustee to compute trust for an IoT environment. However, although reputation was mentioned in the paper, its computation was not included. Bernabe, Ramos and Gomez (2016) proposed a trust-aware access control model based on fuzzy logic for the IoT environment which has reputation as one of the properties used in the access control model.

Chen *et al.*, (2011) proposed a fuzzybased reputation model for IoT as well. In the model proposed by Chen *et al.*, (2011), reputation is calculated based on package forwarding and this limits the model to WSN in IoT. In this paper, we are proposing a reputation model that can be used in different scenarios in IoT.

Another reputation base on fuzzy logic was proposed by Javanmardi *et al.*, (2014) for peer-to-peer grid networks. In the model proposed by Javanmardi *et al.*, (2014) the peers are organized into virtual organizations based on their similarities and each virtual organization has super cluster. Each super cluster has a trust agent that is responsible for computing trust. The limitation of the model by Javanmardi *et al.*, (2014) is that only Quality of Service (QoS) was used in computation and the reputation value is used to estimate trust. We are proposing a multi-value reputation computation model. The following section describes how the reputation model collects and analyses reputation information.

3 Fuzzy-Based Reputation Model

In the proposed model, the reputation value of a trustee is a global value estimated by all the trusters that have interacted with the trustee. The proposed reputation system supports the following:

- handle the computation of the reputation of the same entity in different contexts.
- identify false or misleading feedback. The model does not assume that all feedback is honest.
- support decaying of old transactions.

Reputation is built from the overall behavior of the trustee. It is based on the context of the past behavior. This means an entity can have a different reputation for different contexts.

3.1 Model Architecture

After taking into consideration scalability of the reputation model and also resource-constrained entities in the IoT environment, we propose a distributed agent based hierarchical reputation model. This will enable the model to remain scalable while providing reputation related service to all the entities in the IoT environment. Taking into consideration all entities in the IoT, it surfaces that some of these entities are not capable of both computing and storing reputation information. In order to provide a reputation model that caters for all the 'things' in the network, we recommend the use of reputation agents. We propose that the reputation model be composed of distributed specialized reputation agents whose only purpose in the network is to manage reputation of entities in the network. The specialized reputation agents will create a reputation network amongst themselves. Since the model is distributed, it follows that the model uses a hierarchical decentralized model. Fig. 1 shows the proposed architecture of the reputation model. The model will be composed of two types of agents: root agents and reputation agents.

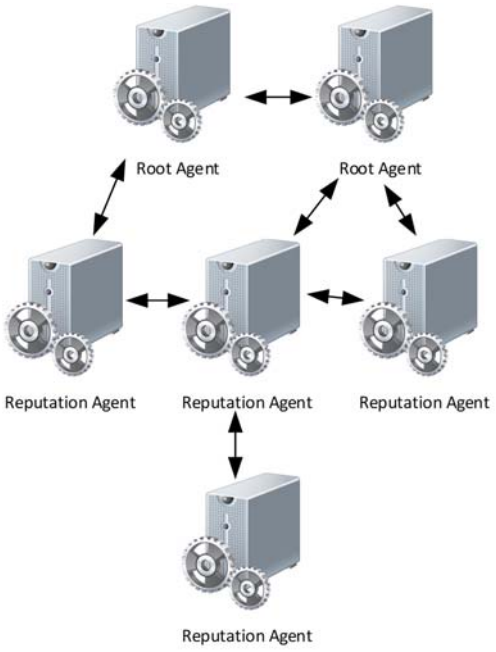

Fig. 1. Model Architecture

The root agents have the following responsibilities:

- Keep record of all reputation agents and other root agents in the network.
- Evaluation of reputation values of both reputation agents and root agents.
- Keep records of all the identities and resources of all the entities associated with each reputation agent in the network.

The root agents are not involved in any reputation computation for entities. They are responsible for calculating reputation values for reputation agents as well as for each other. This will eliminate malicious root agents. Reputation agents have the following roles:

- Keep records of all entities in their domain
- Keep reputation values of all entities in their domain as well as entities in other domains that have cooperated with any of the entities in their domain
- Evaluates reputation value upon request from an entity
- Keep records and reputation values of all reputation agents and root agents they are interested in
- Collect and analyze reputation data in their domain
- Validation of entities using the root agent
- Keep track of the resources that each of the entities in their domain has and provide ratings for them as per request of the truster.

Each reputation agent will keep a record of all entities that belong to its domain. The root agents will evaluate network activities to identify malicious reputation agents while reputation agent will be evaluating the network activities to identify malicious entities and reputation agents. Reputation estimates the trustworthiness of an entity based on the opinions of recommenders. In the proposed model the recommenders could be reputation agents or entities in the network who have communicated with the entity being recommended. An entity can query the reputation of another entity from its reputation agent.

3.2 Reputation Computation

The reputation agents store recommendation values for each context from each entity separately and update the value as the recommender provides new recommendation. When computing reputation value of an entity, a weight is assigned to each recommender. Reputation depends on the recommendations from other entities or reputation agents. Each recommendation is weighed according to the trust that the reputation agent has in the recommender. The sum of all the weights considered for each recommender in a single computation is equal to one. Reputation will be computed as follows:

- reputation values which are related to the defined context are collected
- a weight is applied to each reputation value based on its relevance and on the reputation trust value

Reputation is the accumulation of behavior of the entity based on all the transaction the entity has participated in. The recommendation provided for reputation computation is provided in the form of values of properties that were considered in the collaboration. The reputation agents keep these properties values separately and combines them when a reputation request is made. This enables the trusters to obtain personalized reputation values. When computing reputation from multiple entities, similar properties are combined into a single value using the following formula:

$$P_i^x = \frac{\sum_{j \in S} w_j t_{ji}}{\sum_{j \in S} w_j} \quad (1)$$

where P_i is the total value for property x of entity i, S is the set of all the entities that have interacted with entity i, t_{ji} is property value of i rated by j, w_j is the weight for entity j. The weight w_j for each recommender is computed using a Fuzzy Inference System (FIS) using the relevant properties selected by the trustee requesting for reputation. Fig. 2 show how w_j is computed.

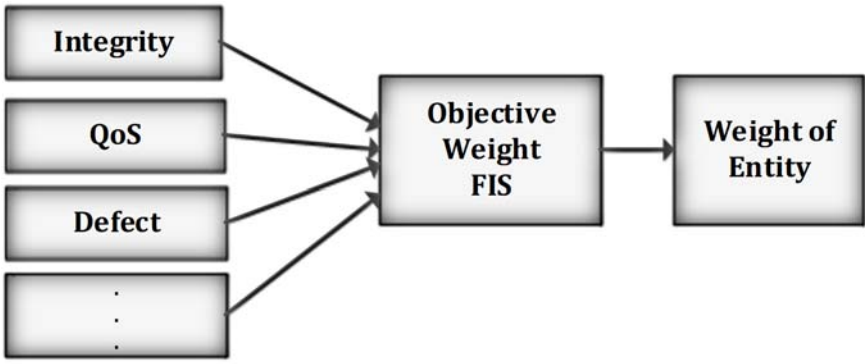

Fig. 2. w_j Computation

There are two types of FIS which are the Mamdani and the Sugeno. The Sugeno systems is well suited for the IoT reputation model because it is "*more compact and computationally efficient than the Mamdani*" [The Mathwork Inc, 2017]. Therefore, FIS systems proposed in this paper used the Sugeno. The membership function of the Sugeno is a singleton which is an exact value; this shortens the process time of the fuzzy inference [Negnevitsky, 2005].

3.2.1 FIS for recommender weight computation

The FIS for computing the weight of entities takes in the values of the properties and outputs the weight of the recommender. The FIS processes the information as follows:

- Define the fuzzy sets
- Determine the degree to which the input values belong to the fuzzy sets
- Apply the fuzzy rules to the input data
- Evaluate the results

The proposed reputation used multiple properties to compute reputation. The properties used include:

- Competence
- Availability
- QoS
- Reliability
- Motive
- Reciprocity
- Incentive
- Defect

The universe of discourse for the properties is $[-1, 1]$. The linguistic variables for the properties are: *very low*, *low*, *medium*, *high* and *very high*. The membership functions for the fuzzy variable are trapezoidal. Trapezoidal membership functions were chosen because they are computationally efficient. Fig. 3 shows the membership function for Quality of Service (QoS).

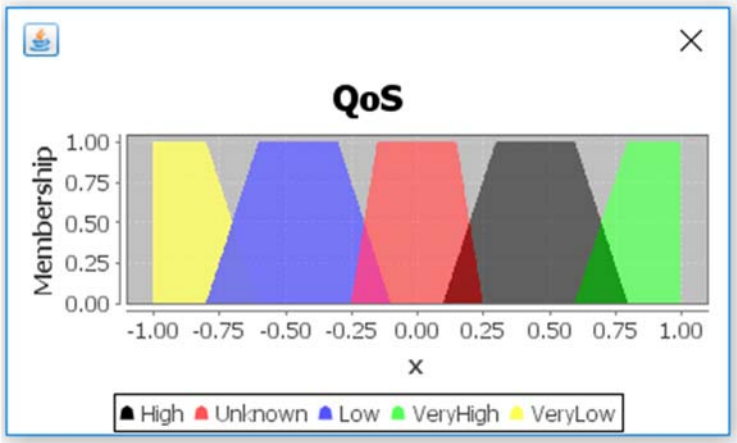

Fig. 3. Membership functions

The membership functions define the linguistic variables. Table 1 lists the ranges for the linguistic variables.

Table 1. Ranges for the membership functions

Linguistic Variable	*Range*
Very High	(0.6, 1)
High	(0.1, 0.8)
Unknown	(-0.25, 0.25)
Low	(-0.8, -0.1)
Very Low	(-1, -0.6)

The properties used in computing reputation will depend on the requirements of the reputation requestor. After determining the fuzzy sets to which the input sets belong, fuzzy rules are applied to the input data. In the FIS, the set of rules defines how the weight information is combined and how the weight is computed. Fig. 4 shows some of the rules that were used in computing the weight of the recommender.

```
RULE 1 : IF QoS IS Low OR QoS IS VeryLow THEN weight IS Low;
RULE 2 : IF QoS IS VeryHigh OR trustworthiness IS High THEN weight IS High;
RULE 3 : IF QoS IS Unknown THEN weight IS Low;
RULE 4 : IF trustworthiness IS VeryLow THEN weight IS Low;
RULE 5 : IF trustworthiness IS High THEN weight IS High;
RULE 6 : IF reliability IS Unknown THEN weight IS Low;
RULE 7 : IF integrity IS High OR QoS IS VeryHigh THEN weight IS High;
```

Fig. 4. Rules for weight computation

The evaluation of the rules produces the output, which in this case is the weight. The process of evaluating the results is known as the defuzzification process. The weight of the recommender is output as a real number in the range (0,1). Fig. 5 shows the membership functions for the weight.

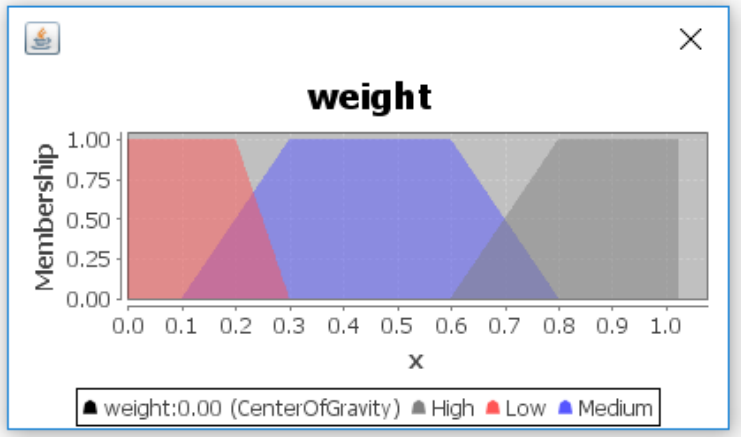

Fig. 5. Membership function for weight

The linguistic variables for the weight are *low*, *medium* and *high*. In defuzzification process, the fuzzy output is mapped into crisp variables using membership functions. The Center of Gravity (CoG) method was used in the defuzzification process. The CoG methods outputs a crisp value that is based on the fuzzy set's center of gravity. This is done by dividing the total area of membership functions. The defuzzified value is obtained by finding the summation of the area and the CoG of each sub-area.

3.2.2 Fuzzy component for reputation computation

The FIS for reputation computation takes in reputation properties as input and outputs the reputation value. The reputation value obtained from the reputation system may be used together with personal reputation values. This will enable entities to make more reliable decisions. Trust relationships can be easily created from reputation. The proposed model can be used to create relationships among entities in the IoT environment.

Fuzzy logic enables multiple properties to be combined into a single reputation value. The properties are fed into the FIS as real numbers in the range (-1, 1). Fig. 6 shows FIS for reputation computation.

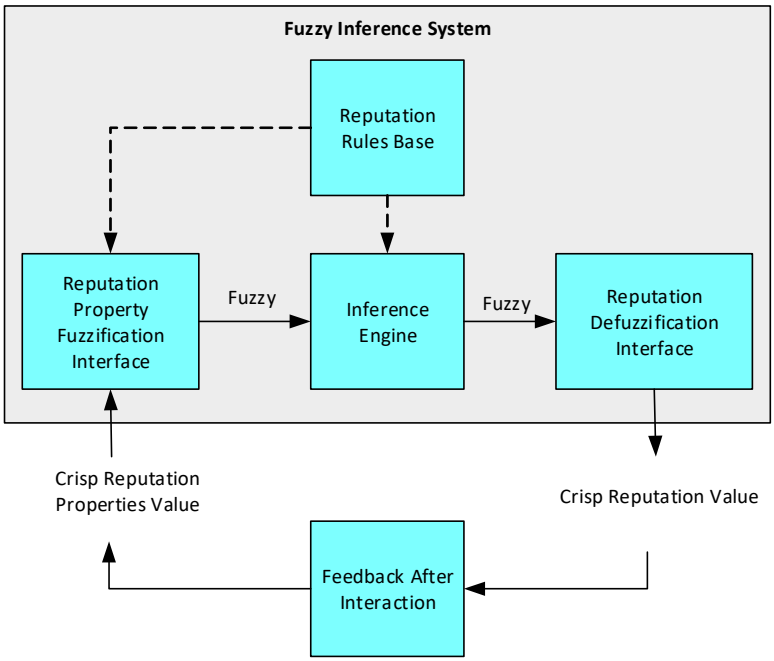

Fig. 6. Fuzzy Inference System

The crisp values are fuzzified against the linguistic fuzzy sets. This process is followed by rule evaluation. Fig. 7 shows a summary of some of the rules used in reputation computation.

```
RULE 10 : IF reliability IS Unknown THEN reputation IS Low;
RULE 11 : IF reliability IS High AND QoS IS VeryHigh THEN reputation IS VeryHigh;
RULE 12 : IF security IS VeryLow OR dependability IS Low THEN reputation IS Low;
RULE 13 : IF security IS Unknown THEN reputation IS VeryLow;
RULE 14 : IF integrity IS VeryHigh AND security IS High THEN reputation IS VeryHigh;
RULE 15 : IF defect IS High AND cooperative IS Low THEN reputation IS Low;
```

Fig. 7. Rules for reputation computation

As mentioned earlier, defuzzification it the last process. The linguistic variables for reputation are: *very low, low, unknown, high and very high*. The universe of discourse for the variables is $[-1, 1]$. The ranges of the membership functions are the same as the ones shown in Table 1. Fig. 8 shows membership functions for reputation computation.

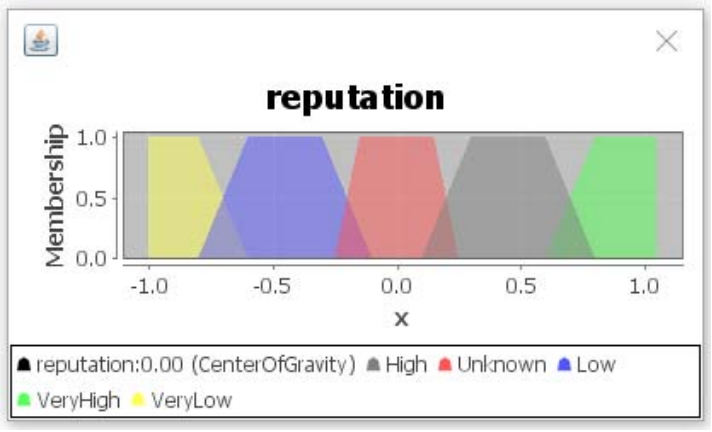

Fig. 8. Membership functions for Reputation

Reputation is a type of a recommender system where each entity in the system is a recommender after each transaction. A reputation system allows entities to share trust information with each other. The entities can specify the properties that they need to be considered when computing reputation. Reciprocity is one of the important properties in reputation which should be taken into consideration when computing reputation values. However, malicious entities might try to use reciprocity to boost each other's reputation and this needs to be prevented by the model. The proposed reputation model attempts to prevent this attack by taking note of abnormally high number of transactions between entities.

4 Model Evaluation

The model was evaluated in a simulated environment. The simulation environment was implemented using Java. We assumed that each entity has a unique identification and it cannot change its identification for testing purposes. The agents were created using the Java Agent DEvelopmnet framework (JADE). The FIS was created using the opensource jFuzzyLogic library which was created by Cingolani and Alcalá-Fdez (2013). The JFuzzyLogic enables the easy development of the FIS in Java. The jFuzzyLogic library uses the Fuzzy Control Language (FCL) to create the FCL file. FCL is a Fuzzy Control Programming Language defined in the International Electrotechnical Commission (IEC) 61131 part 7 [IEC 61131, 2000]. The jFuzzyLogic library also supports the execution of the FCL file. The input values to the FIS are crisp values. In the reputation model, the reputation properties are the crisp values

4.1.1 Environment Description

The simulation was carried out on a PC machine with 8GB of RAM and an i7 processor with 2.60 GHz. The environment consisted of honest entities, malicious entities, and selfish entities. Table 2 shows the parameters of the simulation of the IoT network. An average of 1200 transactions were carried out among the simulated devices.

Table 2. Simulation Parameters

Entities	
Number of Entities	200
Entities with computational ability	110
Malicious Entities	25
Selfish Entities	25
Agents	
Root Agents	4
Trust Agents	15
Malicious trust agents	3
Simulation Details	
Total Simulation Runs	9
Average Total Transactions Per Run	1200

Selfish entities are entities that are not willing to cooperate with other entities in the network. In the simulated environment, malicious entities carried out denial of service attacks and provided false recommendations. The false recommendations include bad mouthing and good mouthing. Malicious entities also try to promote themselves by sometimes behaving like good entities.

4.1.2 Simulation Results

All entities begun with a reputation value of zero. The reputation agents keep track of the reputation of all the entities. Of all the entities in the simulation environment, 25% were not honest. The first tests performed evaluated the performance of the environment with and without the reputation model. Fig. 9 shows the evaluation results of the tests.

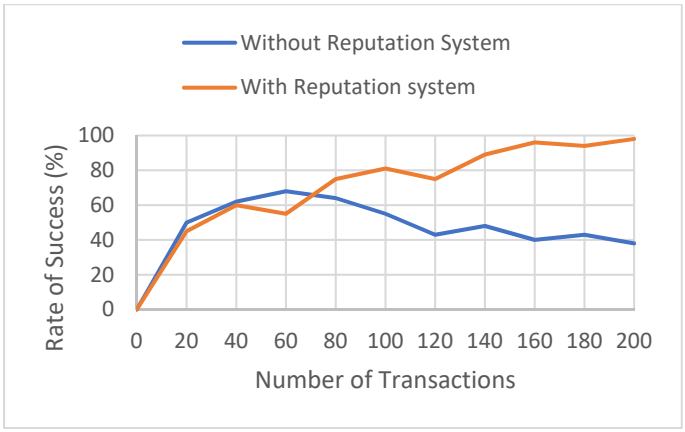

Fig. 9. Performance of environment

The results show that the rate of successful transactions continues to decrease when the reputation is not included. The fluctuation of the values when the model was included can be attributed to the oscillating behavior of malicious entities. Reputation evaluation error was also tested. Fig. 10 shows the error that occurred when computing reputation values over 200 transactions. As expected, the error continued to decrease as the number of transactions increases. The decrease is mainly because malicious entities are accurately identified as the number of transactions increases.

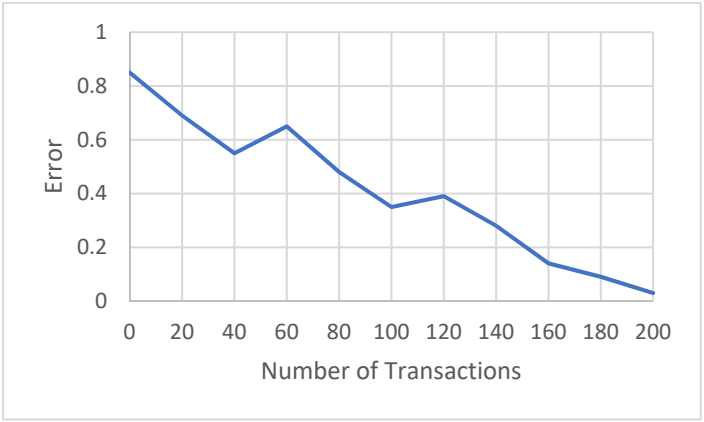

Fig. 10. Reputation computation error

The convergence of the reputation values among reputation agents were also taken into consideration during testing. The reputation values were considered to have converged if all the reputation agents had values that falls in the same linguistic variable for the same entity. Fig. 11 shows the convergence graph over 200 transactions. The initial drop of the convergence can be attributed to both computation error and oscillating behavior of malicious entities.

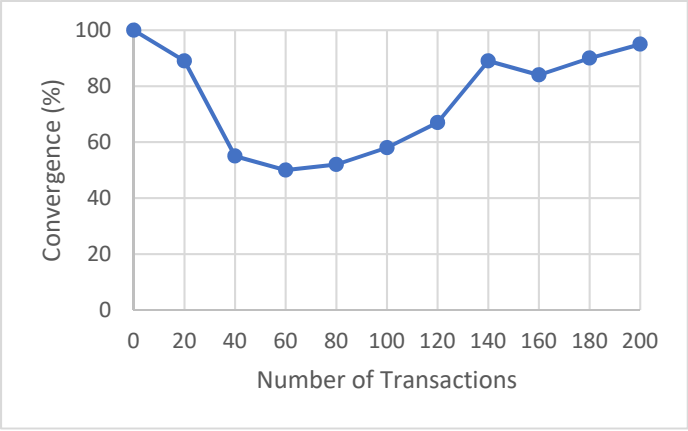

Fig. 11. Reputation convergence percentage

All the results from the simulation shows that the proposed model can effectively identify malicious entities in the simulated environment.

5 CONCLUSION

Reputation is important when determining trust in a social environment. This paper is part of an ongoing research to design a scalable trust model that can be utilized for IoT. The paper proposed a reputation model that utilizes fuzzy-logic for the computation of reputation scores. In order to cater for entities without computational capability, the proposed model is agent-based and is a hybrid of a centralized and distributed model.

The results from the testing of the model show that the model is able to deal with different types of behaviors and it is able identify malicious entities. The results prove that a reputation model can be used to support decision making in the context of collaboration among entities within an IoT environment. During the testing of the model, both malicious and selfish entities were identified as malicious. More work still needs to be done on the model to enable it to differentiate between selfish and malicious entities. As part of the future work, we propose to integrate this model into a trust model. We also propose the addition of policies to the model that can be used to specify how reputation can be used as part of trust computation. The proposed model still needs to be tested in a real IoT environment.

References

[1] Abdul-Rahman, A. and Hailes, S. (2000) 'Supporting trust in virtual communities', in 33th Hawaii International Conference on System Sciences, Hawaii, USA.
[2] Bernal Bernabe, J., Hernandez Ramos, J. L. and Skarmeta Gomez, A. F. (2016) 'TACIoT: multidimensional trust-aware access control system for the Internet of Things', Soft Computing, 20(5), pp. 1763–1779. doi: 10.1007/s00500-015-1705-6.
[3] Chen, D. et al. (2011) 'TRM-IoT: A trust management model based on fuzzy reputation for internet of things', Computer Science and Information Systems, 8(4), pp. 1207–1228. doi: 10.2298/CSIS110303056C.
[4] Cingolani, P. and Alcalá-Fdez, J. (2013) 'jFuzzyLogic: A Java Library to Design Fuzzy Logic Controllers According to the Standard for Fuzzy Control Programming', International Journal of Computational Intelligence Systems, 6(SUPPL1), pp. 61–75. doi: 10.1080/18756891.2013.818190.
[5] Eder, T. et al. (2013) 'Trust and Reputation in the Internet of Things'.
[6] Gutscher, A. (2007) 'A Trust Model for an Open , Decentralized Reputation System', in Etalle, S. and Marsh, S. (eds) Joint iTrust and PST Conferences on Privacy Trust Management and Security, IFIPTM 2007. Moncton, New Brunswick, pp. 285–300.
[7] IEC 61131 (2000) International Electrotechnical Commission Technical Committee Industrial Process Measurement and Control. IEC 61131 - Programmable Controllers - Part 7: Fuzzy Control Programming.
[8] Javanmardi, S. et al. (2014) 'FR TRUST: A Fuzzy Reputation Based Model for Trust Management in Semantic P2P Grids', International Journal of Grid and Utility Computing, pp. 1–11. doi: 10.1504/IJGUC.2015.066397.
[9] Kamvar, S. D., Schlosser, M. T. and Garcia-Molina, H. (2003) 'The Eigentrust algorithm for reputation management in P2P networks', in 12th International Conference on World Wide Web (WWW), pp. 640–651. doi: 10.1145/775240.775242.
[10] Konig, S., Hudert, S. and Eymann, T. (2010) 'Socio-Economic Mechanisms to Coordinate the Internet of Services : The Simulation Environment SimIS', Journal of Artificial Societies and Social Simulation, 13(2).
[11] Leppänen, T. and Riekki, J. (2012) A lightweight agent-based architecture for the Internet of Things. Finland.
[12] Mhetre, N. A., Deshpande, A. V. and Mahalle, P. N. (2016) 'Trust Management Model based on Fuzzy Approach for Ubiquitous Computing', International Journal of Ambient Computing and Intelligence, 7(2), pp. 33–46. doi: 10.4018/IJACI.2016070102.
[13] Negnevitsky, M. (2005) Artificial Intelligence. Second Edi. Harlow, England: Pearson Education Limited. Available at: www.pearsoned.co.uk.
[14] Song, S. et al. (2005) 'Trusted P2P Transactions with Fuzzy Reputation Aggregation', IEEE Internet Computing, (December), pp. 24–34.
[15] The Mathwork Inc (2017) Fuzzy Logic Toolbox TM User ' s Guide.
[16] Truong, N. B., Um, T.-W. and Lee, G. M. (2016) 'A reputation and knowledge based trust service platform for trustworthy', in In Proceedings of the 19th International Conference on Innovations in Clouds, pp. 104–111.
[17] Vermesan, O. et al. (2011) Internet of Things Strategic Research Roadmap.
[18] Wang, Y. and Vassileva, J (2003) 'Bayesian Network-Based Trust Model in Peer-to-Peer Networks', in The Sixth International Workshop on Trust, Privacy, Deception and Fraud in Agent Systems, 200, pp. 23–34.
[19] Wang, Y. and Vassileva, Julita (2003) 'Trust and Reputation Model in Peer-to-Peer Networks', Peer-to-Peer Computing, 2003.(P2P 2003). Proceedings. Third International Conference on, (September), pp. 150–157. doi: 10.1109/PTP.2003.1231515.
[20] Yu, Y. et al. (2012) 'Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures', Journal of Network and Computer Applications. Elsevier, 35(3), pp. 867–880. doi: 10.1016/j.jnca.2011.03.005.