Turkish Journal of Computer and Mathematics Education *Vol.12 No.6 (2021), 2483-2495*
Research Article

Scalable Trust Management model for Machine To Machine communication in Internet of Things using Fuzzy approach

Poonam Ninad Railkar[a], Dr. Parikshit Narendra Mahalle [b],Dr. Gitanjali Rahul Shinde [c]

[a] Research Scholar, [b]Head of Department of Computer Engineering & Professor, [c] Assistant Professor
[a,b,c] Smt. Kashibai Navale College of Engineering, SPPU,
[a]poonamrailkar@gmail.com, [b]aalborg.pnm@gmail.com, [c] gr83gita@gmail.com

Abstract: Revolution in Machine to Machine (M2M) Communication in Internet of Things (IoT) provides smart services in all verticals. These smart heterogeneous devices can be constraint or powerful devices that are generating sensitive information and introducing new challenges in security, privacy, and trust in devices to get and provide services in a distributed fashion. These challenges are overcome by providing scalable decentralized trust management for the access control system. Trust-based security models are more reliable over cryptographic security to identify and mitigate different inside threats by assessing the trust scores. This paper proposed Scalable Trust Management (STM) using a fuzzy approach and parameters like Experience, Recommendation, and device classification are used to calculate the crisp value of the trust score. While designing rule for trust score capacity of device is considered. The simulation of STM in NS2 ensures good performance and its result guarantees scalability and energy efficiency in the heterogeneous network

Keywords: Trust Management, Internet of Things, Machine To Machine communication, Fuzzy logic, Access Control

1. Introduction

Many new wireless technologies are invented to support smart applications. The adoption of Machine-to-Machine communication (M2M) or IoT devices and technologies has been increasing at a quicker rate. Different evaluations by different associations are released regarding the likely number of connected devices, varying from 24 billion to 50 billion connected devices. M2M is a great innovation for ubiquitous communication (Verma et al.,2016). A large number of smart devices communicate with each other automatically with or without human intervention. M2M supports a large number of applications like smart home, Smart e-health, etc (Chen et al.,2018). M2M is a subset of IoT. IoT has created its own universe in which smart things and smart devices communicate over a network and provide a variety of services to all human beings. While providing services, IoT is also facing measure challenges related to the security and privacy of data (Chen et al.,2018). Cryptography and authentication mechanisms can be used to provide security against various attacks. There is huge research is going on in the same context. Powerful authentication and a strong cryptography algorithm can help to reduce some security issues for IoT. These techniques and algorithms are used when nodes transfer the message between two nodes and we can say that these are the first step of defence against external attacks. But these algorithms and mechanisms are unable to defend against internal attacks. Internal attacks can bypass this authentication mechanism because the attacker is having all the credentials as he is one of the users of the system. To overcome these problems, there is need to work on the concept like trust management. IoT network is a dynamic network where multiple nodes joining and leaving the network dynamically (Chen et al.,2019). So, there is a need of an adaptable trust model where the dynamic trust of these devices should able to calculate.

Trust management is the most important concept as far as resource protection is concerned. The rule of trust management changes according to the context, for example, based on interactions and feedback we can build trust mechanisms. There are various computational and theoretical models that have been proposed in recent years. Now, most cloud service providers also integrate trust management features as services in their applications.

This paper is organized as follows. First, we provide the research, related work, and gap analysis that motivates the introduction of this model in Section 2. Then we provide the respective definitions of parameters that are considered in trust calculation, explain the main components of the proposed model and illustrate their interaction by providing the system architecture in Section 3. Section 4 discusses the results of the simulation. Section 5 concludes the paper and provides the future scope of the project.

2. Literature Survey

Formal trust management control mechanism based on architecture modeling of loT is introduced in (Gu et al.,2014). This work introduces IoT into three layers, Sensor Layer, Core Layer, and Application Layer. Final

decision-making is performed by the service requester according to the collected trust information as well as the requester's policy. Authors use a formal semantics-based and fuzzy set theory to realize trust mechanism, the result of which provides a general framework for the development of trust models of loT.

In (Gu et al.,2014) author implemented a Fuzzy Approach to Trust-Based Access Control (FTBAC) with the notion of trust levels for identity management. The result of this approach shows that the fuzzy approach for trust-based access control guarantees scalability and it is energy efficient. FTBAC framework for trust-based dynamic access control in distributed loT, support an increasing number of devices that do not affect the functioning and performance.

Nan Li (Li et al.,2019) introduced context-aware trust system for lightweight IoT devices to store feedback from contacts. Constant storage is required for that system, it does not store past behaviour to provide trustworthiness.

Ruan et al. (Ruan et al.,2016) introduces a general trust management framework aiming to help agents to evaluate their partners' trustworthiness.

System (Thirukkumaran & Muthukannan,2019) monitor the devices and gather the trust parameters like successful forward ratio (SFR), data integrity (DI), and energy consumption rate (ECR) and using fuzzy engine trust parameters are combined and overall trust value is calculated. Based on the trust value access control method is defined. They have used NS-2 to show simulation results and this TAACS-FL is scalable and energy-efficient.

(Kang et al.,2014) proposed an interactive trust model (ITM) for communication between users and service providers. In developed model application trustworthiness (AT) is quantitatively evaluated based on the similarity. Results stated that market application, and helps users to select the most appropriate application from the market efficiently.

(Duan et al.,2014) proposed an energy-aware scheme using a trust-based game theory approach to manage overhead for adequate WSN security. The game-theoretic approach is applied to the trust derivation process to reduce the overhead of the process. Simulations exhibit that the proposed trust model provides significant improvement in security and efficiency levels in IoT. Table 1 gives a detailed Survey of which trust computation method and trust parameters are used in previous systems.

Table 1: Survey on trust parameters

Author	**Trust computation method**	**Trust Parameter**
(Mahalle et al.,2013)	Fuzzy approach	Experience, Knowledge and Recommendation
(Li et al.,2019)	Used Trust evaluation and reputation system, and uses direct and indirect observation	feedback from contacts
(Thirukkumaran & Muthukannan,2019)	Fuzzy logic	successful forward ratio (SFR), data integrity (DI) and energy consumption rate (ECR).
(Wang et al.,2020)	exponential smoothing and a Markov chain.	Dynamic trust model based on direct and indirect trust computation, trust prediction, success rate
Bernabe (Bernabe et al.,2016	Fuzzy trust computation	reputation, quality of service, security considerations and devices' social relationships.
(Gu et al.,2014)	Formal semantics-based Method and fuzzy set theory	Overhead, network price, local regulars, linkage condition, service efficiency, service risk, service history
(Ruan et al.,2016)	measurement theory. two metrics to measure trust: trustworthiness (m) and confidence (c).	quality of service, packet forwarding success rate, multiple environments, such as previous interactions, reputation, Human-to-human trust relationship, Device-to-device trust relationship, Human-to-device trust relationship

Alnasser (Alnasser & Sun ,2017)	Fuzzy logic	Direct trust, indirect trust, past trust, recommendation trust

3. Proposed Scalable Trust Management (STM) system using fuzzy approach

M2M communication is a subset of IoT. As we probably are aware fundamental prerequisite of IoT is, it ought to be scalable, so the combination of new devices is permitted to join the IoT network. To give or access services to these recently or old associated devices in the IoT network, an access control component is required. To give dynamic access control, scalable and dynamic trust computation is required. So, to satisfy this need, the proposed framework gives dynamic trust calculation of devices that are in the network.

In this proposed system all devices have Distributed Identifier (DID) which uniquely identify each device in the network. Each device is classified as Expedient devices, semi- Expedient devices or Non- Expedient devices using fuzzy approach. Fuzzy logic works like human decision. We used Mamdani-type fuzzy logic in the proposed system. This approach gives smooth output control despite wide verities of input which are vague and not clear (Ross,2004), (Guanrong & Tat,2001), (Bai & Wang, 2006). Fuzzification, fuzzy inference process, and defuzzification process involve in the fuzzy logic. Fuzzification transfer crisp input values to linguistic values. Fuzzy set uses linguistic values like 'Bad', 'Average', 'Good' and mapped with real values using membership function. In the defuzzification process, the result is converted into crisp value. The inference engine uses If-Else rules to compute fuzzy output functions. There are many ways for defuzzification, but in this system, Center of Gravity (COG) method has been used to get the crisp output value

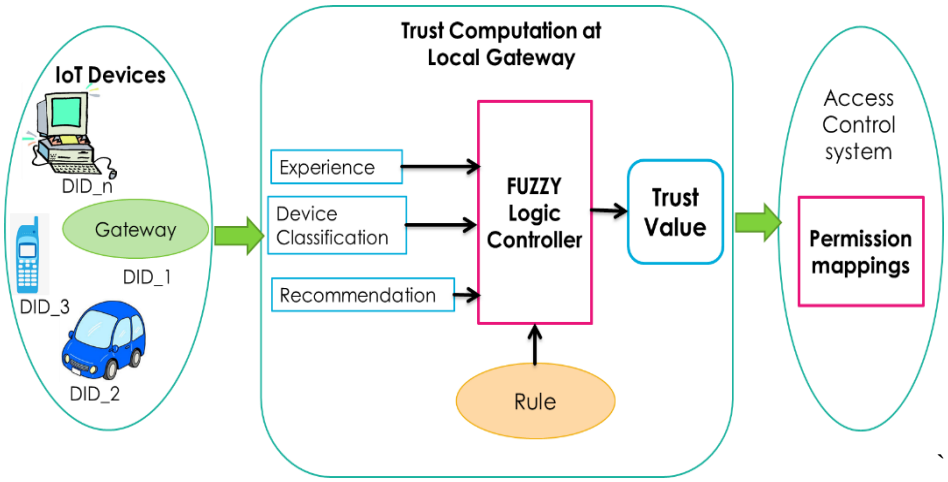

Figure 1: Architecture for Fuzzy base Trust Score calculation system for Access Control

Figure 1 shows the flow of the fuzzy-based trust score calculation system in M2M communication. Here the objective of this work is to research Scalable Trust Management (STM) model for M2M communication and gives trust score of every device to Access Control Framework for access control decision. How the access control framework will work isn't in the scope of this paper. The next version of this paper will give detail working of a distributed access control system using trust score.

This paper considered the following parameters for trust calculation:

(1) Experience

(2) Recommendation

(3) Device classification

Detailed explanations of calculation of each parameter are as follows:

(1) Experience (E):

Trust of device A to device B is based on the track record of interactions V_k, where k varies from integers 1 to n. If the interaction is successful then V_k value is +1, in case of failure it is -1. For the current time t_i,

$$Ex_i = \frac{\sum_{k=1}^{n} v_k}{\sum_{k=1}^{n} |v_k|} \qquad (3.1)$$

Where Ex_i is experience calculated in equation (3.1), and it is calculated for that particular time t_i.

$$E = \sum_{i=0}^{n} Ex_i * g_i \quad (3.2)$$

E is actual experience of that device calculated using equation (3.2) by considering its previous experience Ex_i. g_i is weight assign for every experience which is decreasing as it becomes an old experience. To calculate g_i equation (3.3) is considered.

$$\sum_{i=1}^{n} g_i = \sum_{i=1}^{n} \frac{m_i * x}{n} = 1 \quad (3.3)$$

Where, n is a number of past experiences and m_i =i, ∀ i. And i is considered from 1 to n. When the device enters first time in IoT network it has neutral experience considered value 0, as it does not have any past experience.

(2) Recommendation (R):

R can be obtained by the summation of R values from 'n' number of devices about trustee B by device A.

$$R = \frac{\sum_{i=1}^{n} w_i(r)_i}{\sum_{i=1}^{n} (r)_i} \quad (3.4)$$

Where n is a number of devices. w_i is the weight assigned by device A to i^{th} device. r_i is the recommendation given by i^{th} device for device B. $r \in [-1,1]$. $w_i \in [0,1]$

(3) Device classification (D):

Devices classified in three categories:

i) Expedient Device

ii) Semi-Expedient Device

iii) Non-Expedient Device

Parameters for device classification

- Device-Proximity (DP) = {Excessive, Moderate, Shallow};
- Environment (Ev) = {WLAN, WiMAX, 3G/4G};
- Device Type (Dt) = {WSN, IP, RFID};
- RSSI (Rs) = {High, Medium, Low};
- Battery (Bt) = {Battery-operated, low-battery, no-battery}

E.g., For Expedient Device:

{Dp, Ev, Dt, Rs, Bt}={Excessive, 3G/4G, IP, High, Battery-operated}

Main aim to consider device classification as a parameter is its capacity. Every device has a different capacity to process data. So, trust is calculated proportionally to the device's capacity. Accordingly, rules are written for the fuzzy inference process.

To classify devices as well as to calculate trust we utilized the Mamdani-type (Bai & Wang, 2006) fuzzy rule based model. Two independent fuzzy logic applied, one for classification of devices and the second time for overall calculation of Trust score of devices, which uses vague and imprecise values of Dp, Ev, Dt, Bt, Rs for device classification and T_D, T_E, T_R for trust score of devices. Table 2 represents Linguistic values of Device-Proximity, Environment, Device Type, RSSI, Battery for device classification and Table 3 represents Linguistic values of Device classification, Experience, and Recommendation for trust score. Figures 2,3, 4, 5, 6, 7, 8 and 9 represents the membership function of Device-Proximity, Environment, Device Type, RSSI, Battery, Device classification, Experience, and Recommendation individually.

Table 2 Linguistic values of T_D,T_E, T_I,T_R

Dp	Ev	Dt	Rs	Bt	Crisp Range	Fuzzy Numbers
Shallow	3G/4G	RFID	Low	Low-Battery	Below -0.2	-1, -1, -0.6, -0.2
Moderate	WiMAX	IP	Medium	Battery-operated	-0.2 to 0.6	-0.4, -0.2, 0.2, 0.6
Excessive	WLAN	WSN	High	AC power	Above 0.6	0.2, 0.6, 1, 1

Table 3 Linguistic values of T_D,T_E, T_I,T_R

T_D	T_E	T_R	Crisp Range	Fuzzy Numbers
Non-Expedient	Bad	Negative	Below -0.2	-1, -1, -0.6, -0.2
Semi-Expedient	Average	Neutral	-0.2 to 0.6	-0.4, -0.2, 0.2, 0.6
Expedient	Good	High	Above 0.6	0.2, 0.6, 1, 1

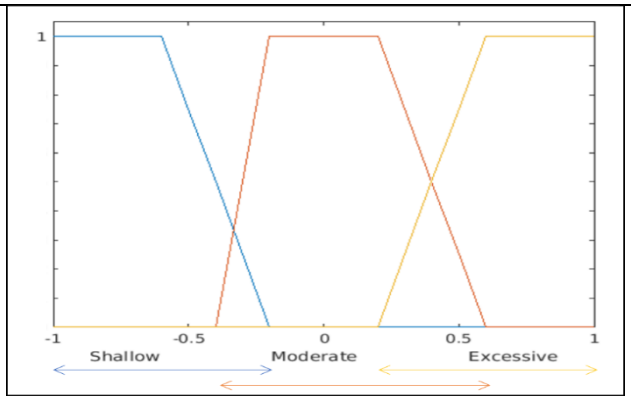

Figure 2: Membership function for Device-Proximity (Dp)

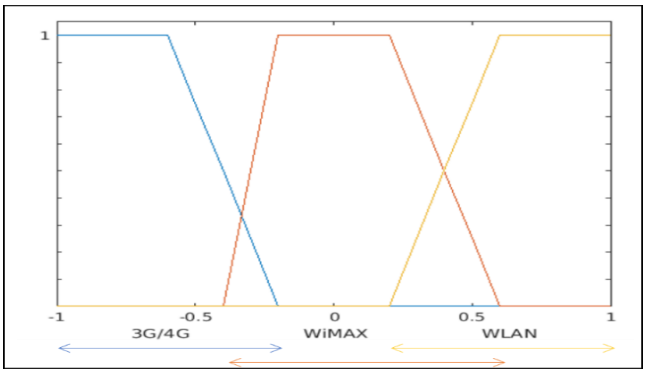

Figure 3: Membership function for Environment (Ev)

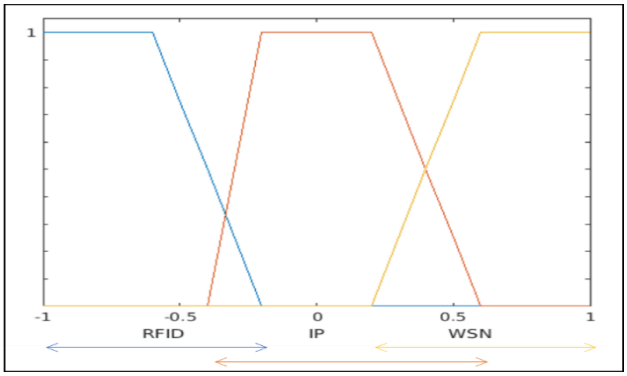

Figure 4: Membership function for Device Type (Dt)

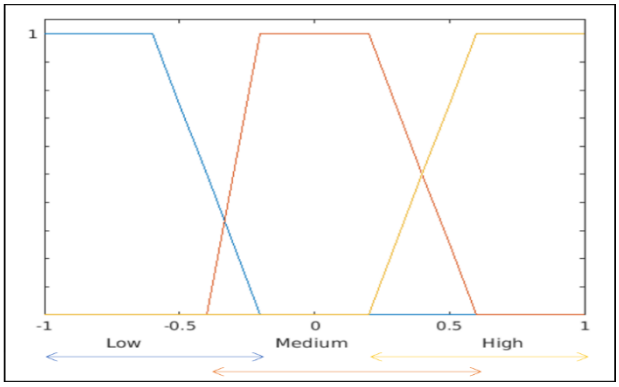

Figure 5: Membership function for RSSI (Rs)

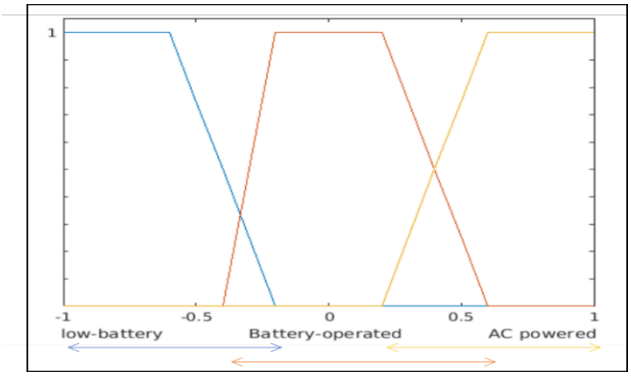

Figure 6: Membership function for Battery (Bt)

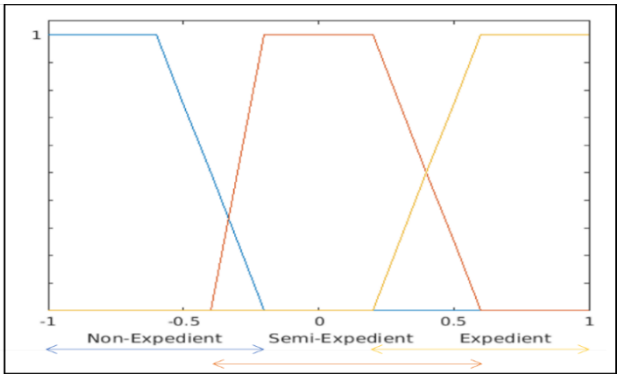

Figure 7: Membership function for Device classification (D)

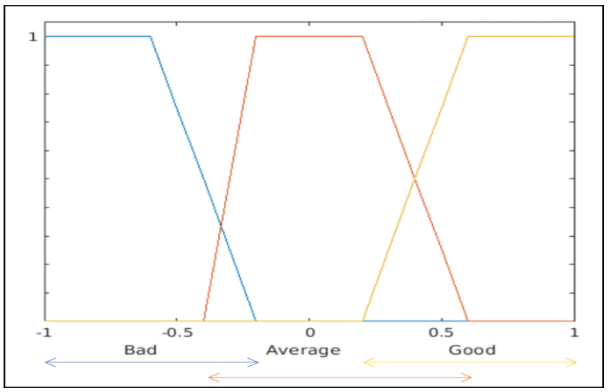

Figure 8: Membership function for Experience (E)

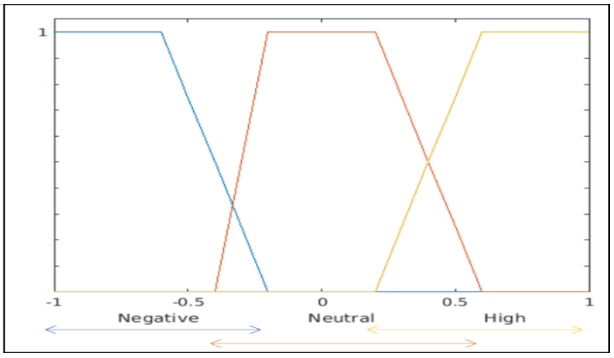

Figure 9: Membership function for Recommendation (R)

The fuzzy rule is going to apply as per table 4 and table 5 for device classification and Trust calculation respectively. The Mamdani scheme is a type of fuzzy relational model where each rule is represented by an If-Then relationship. The **IF-THEN** rules are used to formulate the conditional statements that are required by fuzzy logic. There can be multiple **IF-THEN** rules. For device classification there are 5 attributes and 3 linguistic values each, so 3^5 i.e., 243 rules are possible out of these few rules are shown in table 4. For trust score 3^3 i.e., 27 rules are possible there are 3 attributes and 3 linguistic values, few of them are shown in table 3.5.

Table 4 Fuzzy rule set for device classification (few of them)

Rule	If Dp	and Ev	and Dt	and Rs	and Bt	Then Device
1	Excessive	3G/4G	IP	High	AC powered	Expedient
2	Moderate	WLAN,	IP	Medium	Battery-operated	Expedient
3	Shallow	WiMAX	WSN,	Medium	Battery-operated	Semi-Expedient
4	Shallow	WiMAX	RFID	Low	low-battery	Non-Expedient

Rule	If D	and E	and R	Then Trust
1	Non-Expedient	Good	Negative	High
2	Semi-Expedient	Good	Negative	Medium
3	Expedient	Good	Negative	Low
4	Non-Expedient	Average	Neutral	Low
5	Semi-Expedient	Good	High	Medium
6	Expedient	Good	High	High
7	Non-Expedient	Bad	Neutral	Medium
8	Semi-Expedient	Average	High	High
9	Expedient	Bad	Neutral	Low

Table 5 Fuzzy rule set for trust score (few of them)

We have defined linguistic value for the output variables Device classification and trust in table 6 and 7 respectively.

Table 6 Linguistic value of output Device classification

Linguistic Trust	Range	Fuzzy numbers
Non-Expedient	Below -0.2	-1, -1, -0.6, -0.2
Semi-Expedient	-0.2 to 0.6	-0.4, -0.2, 0.2, 0.6
Expedient	Above 0.6	0.2, 0.6, 1, 1

Table 7 Linguistic value of output Trust

Linguistic Trust	Range	Fuzzy numbers
Low	Below -0.2	-1, -1, -0.6, -0.2
Medium	-0.2 to 0.6	-0.4, -0.2, 0.2, 0.6
High	Above 0.6	0.2, 0.6, 1, 1

To transform a fuzzy set, or a collection of subsets into a crisp value defuzzification takes place. Crisp value of Trust and device classification are calculated using the following formulae (3.5) which is called Center-of-Gravity (Bai & Wang, 2006),

$$COG(A) = \frac{\sum_{q=1}^{Nq} \mu_A(x).x}{\sum_{q=1}^{Nq} \mu_A(x)} \quad (3.5)$$

So this final crisp trust output will be pass to access control system for decision making of access permission.

4. Performance evaluation

Performance evaluation of the STM system is performed using Network Simulator (NS2). ns-allinone-2.34 package tool has used to evaluate STM protocol. Considered simulation parameters are mentioned in table 8.

Table 8 Considered Simulation parameter

Simulation Network Area	500m x 500m
Number of nodes	100 to 300
Total Simulation Time	1000s
Value of Initial Energy	100J
Transmission Power	0.06mW
Receiving Power	0.03mW
Application start time	35s
Application stop time	190s
Number of Attackers	3,6,9,12,15
Packet Size	64 bytes
Data Interval	0.1s

Performance metrics:

STM system evaluates against TAACS-FL (Thirukkumaran & Muthukannan,2019) system and without trust calculation. Following are performance metrics evaluations are done by varying the total number of nodes from 100 to 300.

(1) Packet Delivery Ratio:

Packet Delivery Ratio is a ratio of the number of packets received out of the number of packets sent. STM protocol proves that PDR is better than other similar systems. Simulation of PDR is shown in figure 10.

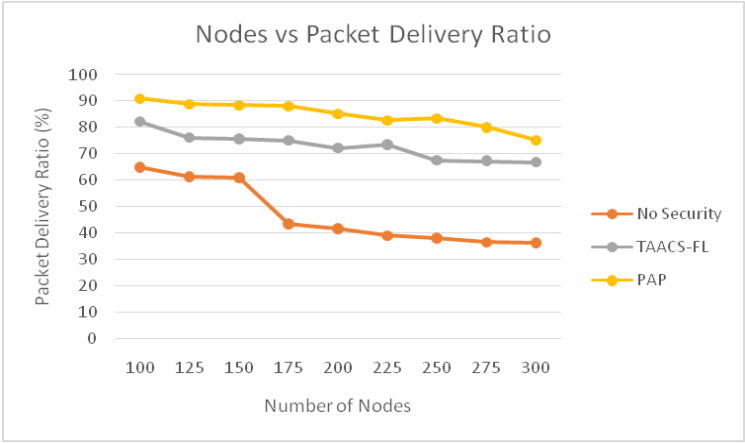

Figure 10: Packet Delivery Ratio

(2) Throughput:

Here throughput is calculated as how many numbers of bits are transferred in seconds (bits/sec). The simulation result of throughput is shown in figure 11.

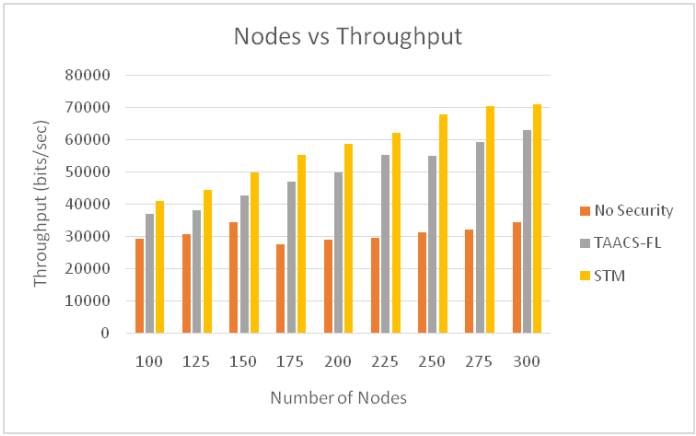

Figure 11: Throughput

(3) Delay:

Delay is the time required to reach a destination. It should be small for better performance. The simulation result of Delay is shown in figure 12

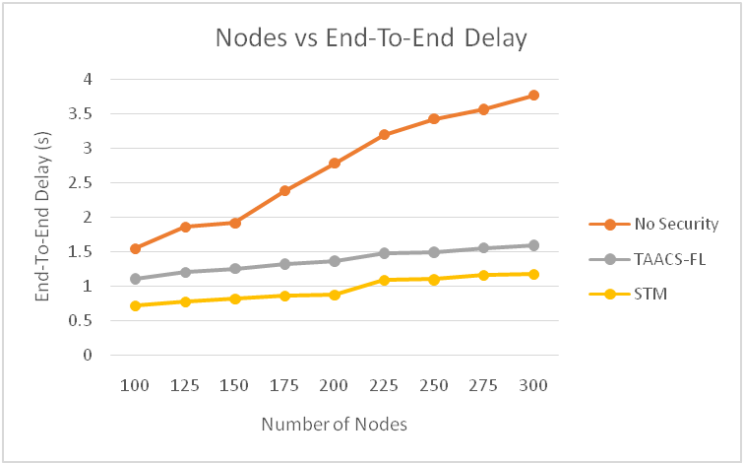

Figure 12: Delay

(4) Energy Consumption:

Energy is required while transferring and receiving data packets. This should be less for better performance. The simulation result of Energy Consumption is shown in figure 13.

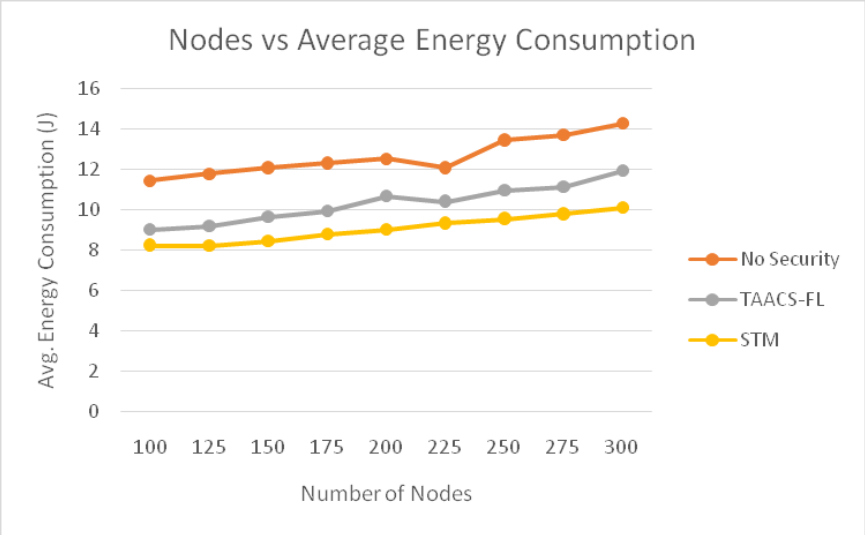

Figure 13: Energy Consumption

Performance evaluation by varying number of attackers:

For protocol analysis basically, we have considered replay attack, Man in Middle attack, and DoS attack by varying a number of attacks. We have considered a number of nodes are 100 and the data packet is 0.1 seconds. Simulation result of Attackers vs Packet Delivery Ratio, Throughput, End-To-End Delay and Average Energy Consumption are shown in following figure 14, 15, 16, and 17 respectively

(1) Attackers vs Packet Delivery Ratio:

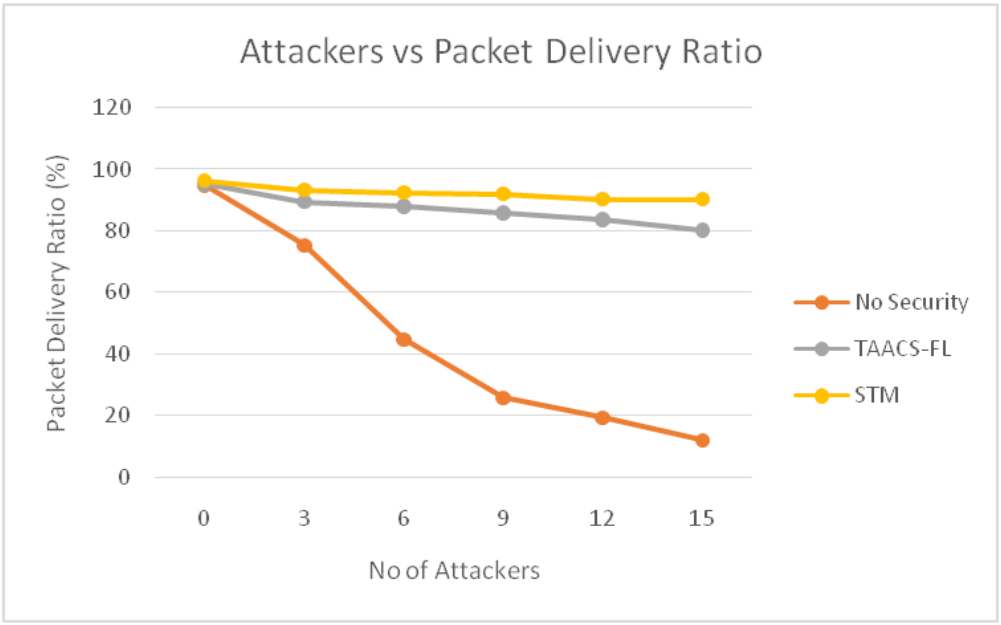

Figure 14: Attackers vs Packet Delivery Ratio

(2)Attackers vs Throughput:

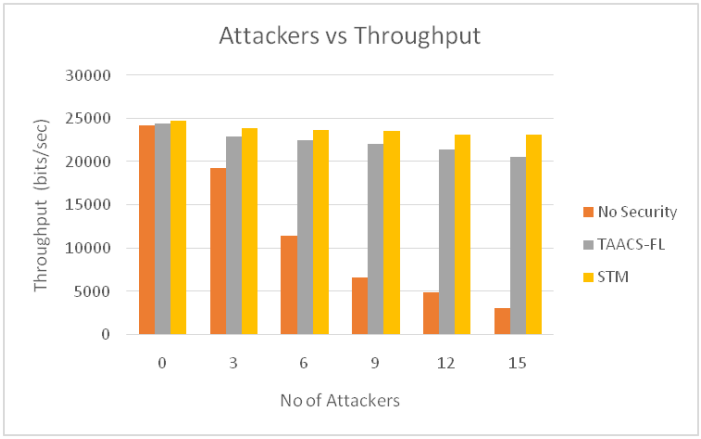

Figure 15: Attackers vs Throughput

(3)Attackers vs End-To-End Delay

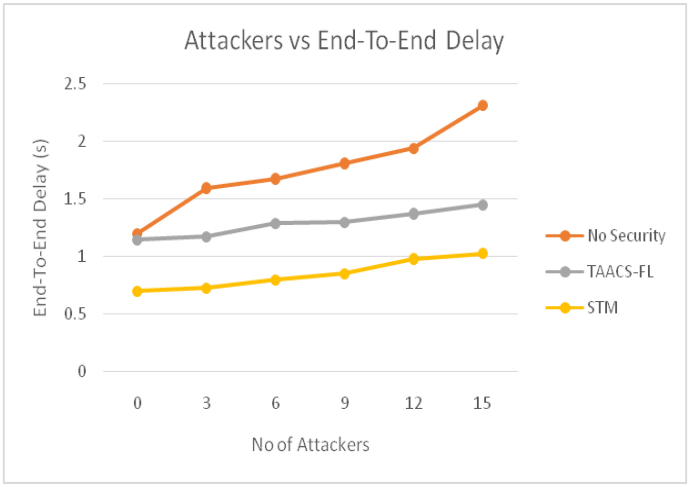

Figure 16: Attackers vs End-To-End Delay

(4). Attackers vs Average Energy Consumption

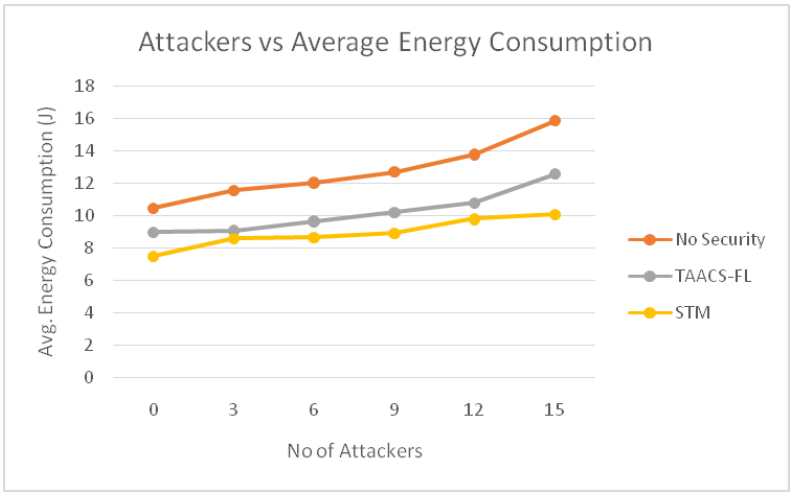

Figure 17: Attackers vs Average Energy Consumption

5. Conclusions and future work

In distributed environment for M2M communication to get and provide services, security, and privacy is the main concern. This paper proposed a scalable trust management system using a fuzzy approach. To calculate the trust of the device, linguistic values of input parameters, device classification, experience, and recommendation are used. This system returns the trust score of devices that want to access or provide service. The simulation result of the STM scheme shows that it is scalable, even the number of devices increases, it improves throughput, packet Delivery Ratio. In addition to it, energy Consumption, as well as delay, is also less as compared to other systems. The future plan is to implement it in a real-time heterogeneous distributed IoT environment and incorporate this trust score in the access control scheme

References

1. Alnasser, A., & Sun, H. (2017). A fuzzy logic trust model for secure routing in smart grid networks. *IEEE access*, *5*, 17896-17903.

2. Bai, Y., & Wang, D. (2006). Fundamentals of fuzzy logic control—fuzzy sets, fuzzy rules and defuzzifications. In *Advanced fuzzy logic technologies in industrial applications* (pp. 17-36). Springer, London.

3. Bernabe, J. B., Ramos, J. L. H., & Gomez, A. F. S. (2016). TACIoT: multidimensional trust-aware access control system for the Internet of Things. *Soft Computing*, *20*(5), 1763-1779.

4. Chen, J., Tian, Z., Cui, X., Yin, L., & Wang, X. (2019). Trust architecture and reputation evaluation for internet of things. *Journal of Ambient Intelligence and Humanized Computing*, *10*(8), 3099-3107.

5. Din, I. U., Guizani, M., Kim, B. S., Hassan, S., & Khan, M. K. (2018). Trust management techniques for the Internet of Things: A survey. *IEEE Access*, *7*, 29763-29787.

6. Duan, J., Gao, D., Yang, D., Foh, C. H., & Chen, H. H. (2014). An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications. *IEEE Internet of Things Journal*, *1*(1), 58-69.

7. Gu, L., Wang, J., & Sun, B. (2014). Trust management mechanism for Internet of Things. *China Communications*, *11*(2), 148-156.

8. Guanrong, C., & Tat, P. T. (2001). Fuzzy sets, fuzzy logic, and fuzzy control systems. CRC Press LLC, ISBN 0-8493-1658-8, (2001).

9. Kang, K., Pang, Z., Da Xu, L., Ma, L., & Wang, C. (2014). An interactive trust model for application market of the internet of things. *IEEE Transactions on Industrial Informatics*, *10*(2), 1516-1526.

10. Li, N., Varadharajan, V., & Nepal, S. (2019, July). Context-aware trust management system for IoT applications with multiple domains. In *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)* (pp. 1138-1148). IEEE.

11. Mahalle, P. N., Thakre, P. A., Prasad, N. R., & Prasad, R. (2013, June). A fuzzy approach to trust based access control in internet of things. In *Wireless VITAE 2013* (pp. 1-5). IEEE.

12. Ross, T. J. (2004). *Fuzzy logic with engineering applications* (Vol. 2). New York: Wiley.

13. Ruan, Y., Durresi, A., & Alfantoukh, L. (2016, March). Trust management framework for internet of things. In *2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)* (pp. 1013-1019). IEEE.

14. Thirukkumaran, R., & Muthukannan, P. (2019). TAACS-FL: trust aware access control system using fuzzy logic for internet of things. *International Journal of Internet Technology and Secured Transactions*, *9*(1-2), 201-220.

15. Verma, P. K., Verma, R., Prakash, A., Agrawal, A., Naik, K., Tripathi, R., ... & Abogharaf, A. (2016). Machine-to-Machine (M2M) communications: A survey. *Journal of Network and Computer Applications*, *66*, 83-105.

16. Wang, E. K., Chen, C. M., Zhao, D., Ip, W. H., & Yung, K. L. (2020). A dynamic trust model in internet of things. *Soft Computing*, *24*(8), 5773-5782.