COMPARATIVE ANALYSIS OF TRUST ESTABLISHMENT MODEL TO IDENTIFY MALICIOUS NODES IN SIOT

Anciline JeniferJ[1] and Piramu PreethikaSK[2]

[1]Department of Computer Science, Vels Institute of Science, Technology & Advanced Studies (VISTAS)

[2]Department of Computer Science, Vels Institute of Science, Technology & Advanced Studies (VISTAS)

ABSTRACT

Internet of Things enables the user to interact with devices which merges with Social Internet of Things (SIoT). SIoT is a new model that allows various attractive application and promote sharing of information. This can establish objects in an independent way based on the social relationship. The major issue is how to construct the trusted model and to understand how the objects interact with SIoT. In order to overcome these challenges, trust establishment model among these devices has been required before originating communication. This paper describes collaborative methods for calculating trust based on the trust evaluation system. The collaboration among the nodes can be established using encoded and decoded packets whereas the encoded packet transmission illustrates the collaboration. The each node of reliability based on the transaction factors can be assigned and their trust values can be calculated. This paper described comparison between proposed Cooperative Trust (CT) models which can be observed initially it achieves 79% trust value than the existing trust model. This framework provides more security and reliability for SIoT in order to identify the malicious nodes.

KEYWORDS

IoT devices, SIoT, security, malicious nodes, trust value, cooperation

1. INTRODUCTION

In today's digital era of Information Communication Technology (ICT), computers, mobile and other connecting devices are becoming ubiquitous in nature. According to a study, total number of connecting devices present in the globe exceeds multiple times the total population of humans making it more than 4 devices per person on the globe. By 2021, more than 20 billion devices will be connected to internet and communicate each other when required making it pervasive in nature [1]. This pervasive nature of the devices makes communication very obvious and hence these devices are known as Internet of Things (IoT) devices. The primitive nature of IoT devices is that they are anywhere, everywhere making communication and computation ubiquitous in the ICT domain. IoT network is the inter-networking of physical devices, smart devices, electronic appliances, automobile vehicles and other electronic devices having software, sensors, actuators, and network connectivity

D. Angeline, A. Arul et al.(Eds): ICICI-2021
pp. 47-55, 2021. IJCI – 2021 DOI:10.5121/ijci.2021.100206

which enable these components to collect and exchange data over a network. IoT devices are transforming our ICT spectrum completely. In communication over IoT, there is vulnerability in the messages being communicated among the devices because of the higher heterogeneity level. The vulnerability over IoT contains lack of integrity, reliability and trustworthiness of heterogeneous devices. IoT network uses diversified devices, multiple communication channels and lack of standards and enabling protocols result in multiple security threats. In a diversified distributed environment such as IoT network verification, approval, non-repudiation and access control are the significant to establish protective communication. These devices establish secure channel before beginning of the communication. Among the communication devices, these secure channels can be entrenched after establishing trust. Trust establishment is necessary to ensure that the vulnerabilities present in these devices should be resolved and ongoing communication is secure. These vulnerabilities are resolved by fulfilling security requirements by employing designated security mechanisms. Among these security concerns, privacy remains a challenge in IoT network as it solely depends on nature and characteristics of the devices. Once the communication can be started in the device due to heterogeneity has not controlled by security and privacy concerns among the communicating devices to establish the trust is one of the main reasons before starting of the communication. This method of establishing trust among the communicating devices is an aspect of Trust Management in IoT devices. Trust can also be established among the communicating devices by negotiating on certain aspects which is called Trust Negotiation. Trust Negotiation and Trust Establishment together comes under Trust Management. One of the approaches towards establishing trust among IoT devices is by treating these IoT devices as SIoT devices [2]. In SIoT, it is possible to distinguish people and objects from each other. It allows objects to protect their privacy from humans with their own social networks. There is billions of traffic in the IoT system as objects communicate in the network with other objects in an independent way and in this environment, it can lead to malicious behavior [3]. Management of trustworthiness plays an important role. Without this administration, the trusted network will not be available. There are many advantages that SIoT offers which are navigability, trustworthiness and scalability. The aim of this paper is to construct a comparison between trust evaluation models for SIoT based on the behavior of objects to develop security using trustworthiness management.

The organization of the paper is as follows: Section 2 describes the trust in SIoT, Section 3 describes survey based on trust based SIoT framework, Section 4 describes proposed CT model evaluation, Section 5 discusses the performance evaluation for calculating trust values with the comparison of proposed CT model and existing model, Section 6 ends with conclusion.

2. ROLE OF TRUST SOCIAL INTERNET OF THINGS

Trust in IoT communication plays an important role as the communication take place among multiple devices. Trust in human sociology refers to a degree of extent at which information can be shared explicitly without any constraint of privacy preservation. When initiating the communication, the degree of trust is much needed and the fulfillment of trust requirements is strictly associated among IoT devices of access control and identity management issues. In networking systems like SIoT, trust establishment model is an important characteristic. A human social relation is the general fundamental feature of trust which needs to be reviewed from trustor who gets correlated with the society while extending trust. There should be no neglect of social experiences, the subjective point of view of particular individuals, and society. This system also found out that in addition to the trustworthiness of a trustee, the tendency of the trustor and environmental factors like faults, threats and risks also contribute to the trust valuation as illustrated in Figure 1. This is evident due to trust only exists in

dangerous situations based on the trust which is vulnerable. In unique contexts, there are many meanings for trust that makes it difficult to construct a common notation of trust in computer science.

The trust model to adopt a generally accepted social science approach in order to define trust in the SIoT context, which considers trust as a belief that appears in various trust-related works [4].

Fig. 1. SIoT Environment based on trust

In computer science, a general concept of trust has been accepted as follows: In a trustee, the belief of trustor will achieve or provide trustor's expectation as trust goal for a certain period of time within a particular context is defined as trust. Trustors and trustees may be individuals, computers, systems, applications and services in the SIoT framework. The trust value may be absolute for instance 'probability' which measure as conviction for instance 'trust level'. The wide knowledge of trust goal to perform the action of trustee provides the trust for information. The objectives of the Trustor are intentionally considered for the trust target to contain specific criteria to perform well.

3. LITERATURE REVIEW

This focus on to build a reliable system based on the nature of devices provided by the SIoT users. They define their model into two type's namely subjective model and objective model [5]. The model is based on different type of relationship named as co-work object, parental object, co-location object, social object and ownership object relationship [6]. Proposed trust model uses recommendation, reputation and knowledge to calculate trust metric of every device. Their model measures both credibility namely, the trust value metrics of reputation and recommendation and knowledge properties based on trust value metrics of knowledge [7]. This paper proposes trust capabilities based on the trust management model that involve reference model of generic IoT for accomplishing trustworthiness management target. Moreover, the proposed Trust Information Management (TIM) platform is considered to involve trust information brokers, TIM system and trust agents aimed at providing stable interactions and trustworthy between individuals, physical things and virtual objects [8]. The middleware solution is providing an environment for enabling service composition and general set of services based on communication capabilities and abstraction of device functional designs are the major goals which may be identified [9]. The advantages of the proposed IoT framework are incorporating both smart object-based infrastructure and RFID which includes the implementation of an additional generic IoT architecture. The disadvantages are which does not have a solution based on flexibility, scalability and lower performance. SIoT network to manage in IoT

architecture for the way of communication between several things in which the way of people handle social relationships as reference architecture. This paper addresses certain existing problems of IoT design and proposes SIoT-couched solutions which can be used to minimize architectural variability as requirements for potential IoT designs [10]. Gamini Joshi et al. has proposed the framework of cooperative trust management in accordance with data of encoding and decoding which assist in assessing IoT network trust using data normalization and evaluation. However, this proposed framework is highly cognizant and delivers quick decision making in nodes trustworthiness. Hence, the overhead has reduced by 61% in node 60 and the Packet Delivery Ratio (PDR) of non-malicious node gets increased with 40% in the node 30. Thus, the model is scalable with more node which is prompt to be realistic and reliable [11]. Chen et al. proposed trust evaluation which act as a major feature in network securing from annoying nodes [12]. Similarly, Atzori et al. has proposed various trust model related to fuzzy, game theory, neural network and Bayesian statistics whereas the limited work is done through trust [13]. Mart et al. has introduced direct observation using watchdog method for detecting the self-nodes. The trust correctness has been affected through direct observation and the watchdog method is utilizing the essential memory buffer which accumulates for additional storage in memory limited IoT devices [14]. Oliviero et al. has proposed a free routing path from malicious node but it is not secure while focusing only at trust dissemination [15]. Ren et al. has suggested trust evaluation with neighbor's advice but which influence the complexness [16]. Namal et al. has utilized the cloud in trust evalution for reducing the difficulties and advance the security. This proposed model is considered with Trust as a Service (TaaS) for providing availability and reliability over network [17]. The disadvantage faced in this method if any service gets interrupted. Hammi et al. has proposed a blockchain approach for designing the trust bubble which is identified that mechanism is not flexible to real-time applications as vendor intervention is frequently essential for basic process [18]. Duan et al. has proposed a game-theory method which utilized the cooperation idea over nodes but its consideration is lack of security and the outcome has resulted with network overhead [19].

4. METHODOLOGY

In SIoT, social network and IoT give a new paradigm to IoT devices and hence the IoT network becomes SIoT network which includes humans and IoT devices. In SIoT network, devices have their private social networks which offer persons to execute rules on these devices to prevent their security and privacy issues leading to secure communication after establishing trust. Companies such as eBay, Amazon and Google have utilized the benefits of social relationship models for providing reliable and secured services using the metrics of trust and reputation with reference to SIoT devices. In SIoT network, trustworthiness of IoT devices is measured using several trust management models. Social network mainly builds upon users having like own or business interests, events, experiences or real-life connections. Growth of SIoT is also depending upon communicating model of the IoT devices to approve a social approach. In SIoT network, the devices are accomplished for building social relationships with others. The interactions among devices can ensure in their social network. In SIoT network, IoT devices start communication with each other after establishing trust using a trust management model. In social network, users are connected through each other over social connections including contacts, acquaintance, friends, relatives etc. These connections need not ensure that the users know each other personally and having greater friendship affinity, trustworthiness, reputation etc. The SIoT technological development has created the path for various organization services in several domains. Moreover, this development may assist the attacker in disturbing the trustworthy and reputation of network services. Hence, there is an essential requirement for securing the SIoT network from the malicious nodes and create them with non-threatening. Thus, the CT framework has been

proposed for using the cooperative concept in securing the network from malicious nodes whereas the proposed CT mechanism is illustrated in figure 2.

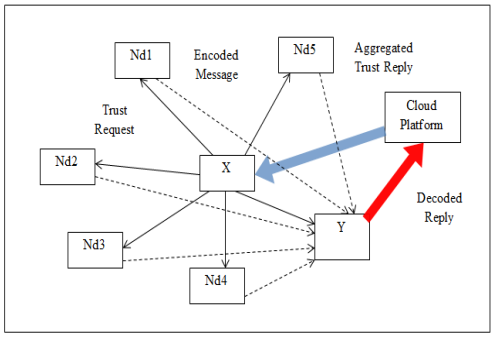

Fig. 2. Mechanism of proposed Cooperative Trust (CT) model

In order to determine the destination node (Y) is trustworthy, the source node (X) needs to send the request through its neighbor nodes such as Nd1, Nd2, Nd3, Nd4 and Nd5. These nodes have been utilized for forwarding the encoded and decoded packet to Y. Moreover, the process of this cooperative mechanism is illustrated below. The source node (X) have send the encoded packets to neighbor nodes which is then it is send to the respective Destination Node (Y). The send encoded packets are made to be decoded and reply is forwarded to the repository, then the respective node is determined to be Y. Therefore, the respective node Y is said to be cooperative else malicious or selfish. Thus, the aggregated trust reply from the repository is sent to node X that evaluate in decision making of X to determine the node Y is the trust node for communication.

The proposed CT model assist in evaluating the trust value has been modeled as triplet μ = (M, N, Q)

'i' node represents evaluating node for encoding the packets

'j' node represents evaluated node for decoding the packets

Where M = {Nd1, Nd2, Nd3, Nd4..Nd_m } is the set of neighbor nodes of node j,

N = {n1, n2, n3…n_n } is the set of positive reports received for evaluated node j from neighbor nodes.

Q = {q1, q2, q3…q_q} is the set of negative reports received for evaluated node j from neighbor nodes,

x (M) = x(N) + x(Q) ……(1)

Trust value of evaluated node at time instant t is given as

$$\overline{TV_t} = \overline{\sum_{y=1}^{n} N_y} + \overline{\sum_{z=1}^{q} Q_z} \quad \text{……..….(2)}$$

Then the TV represents trust value is normalized (range 0 to 1) and decision is taken accordingly,

$$\text{Normalized } \overline{TV_t} = \frac{TV_t - \min(TV)}{\max(TV) - \min(TV)} \quad \text{……..……(3)}$$

Algorithm for cooperative trust mechanism model:
Step:1 Start with evaluating trust of node 'j' is ready for node 'i'
Step:2 Then node I sends trust request to all the neighboring nodes of j
Step:3 All the neighboring node will send the encoded packet to node 'j'
Step:4 Node j decodes the packet and generate the report Rm=1 if decoded is successful else Rm = -1 if not packet sent to repository for aggregation.

Step:5 The above step2, step3 and step4 can aggregated data which is normalized and the trust value is evaluated

Step:6 If the trust value is above the threshold, the evaluated node is trusted and the communication is smooth otherwise risky communication.

5. PERFORMANCE EVALUATION

Performance indices are used to measure the success of the system. Our model uses the following parameters as the performance indicator. The proposed approach can be evaluated in computing devices trust by the Contiki-2.7 Cooja simulator. Moreover, this research has implemented with RPL-UDP for determining an accurate network traffic flow and by considering some malicious nodes have interrupted the traffic of the network that usually troublesome the trustworthiness. Thus, the range value of trust is from 0 to 1 in which the "0" represent the minimum value and "1" represent the maximum value but the default value is the minimum value. Table 1 has illustrated the simulation parameter used for evaluation.

TABLE 1: Mechanism of proposed Cooperative Trust (CT) model

Parameter	**Value**
Simulation time	Max 300 sec
Number of nodes(neighboring)	Max 60
Number of malicious nodes	Max 40
Communication range	50m
Protocol	RPL-UDP
Initial trust value	1.5

Trust Value – The mutual relationship among the two nodes is trust whereas the communication type is generally decided based on the calculated trust value as per equation (3) which is illustrated in Table 2.

TABLE 2: Type of communication

Value of Normalized Trust	**Trust Type**	**Communication Type**
0-0.50	Untrusted	Hazard communication
0.51-0.70	Medium trust	Risky communication
0.71-1.00	High trust	Trusted communication

The above mechanism is repeated for every node and nature of communication between trustor and trustee is established.

6. COMPARATIVE ANALYSIS OF THE PROPOSED MODEL BASED ON TRUST VALUES

There are several models that have been proposed in the trust domain such as Trust-Doe approach [20], Belief-based Trust Evaluation Mechanism (BTEM) approach [21] so on. During the analysis of Trust-Doe approach, malicious node present in the network can be detected but lack in accuracy detection which is limited only for collusion attack. In other hand, the BTEM approach is implemented and outperforms better than Trust-Doe approach. Thus, the BTEM has improved the network trust and handling capacity with various attack types namely DoS, bad-mouthing etc. It has detected based on the value of malicious path and its node. The highest value of path or node can be considered as trustworthy path or node whereas lowest value can be considered as untrusted path or node. The difference of trustworthy and untrusted path will be measured as follows. In the experimental results, the proposed model illustrates in table.3 achieves highest trust value evaluation for each transaction based on varying the malicious nodes, therefore security is considerably better for SIoT framework.

TABLE 3: Communication Nodes Vs Trust Values

Communication Nodes	**Percentage of Trust Values**	
	Proposed cooperative trust model (%)	Existing system of BTEM (%)
10	40	28
20	52	40
30	58	40
40	78	32

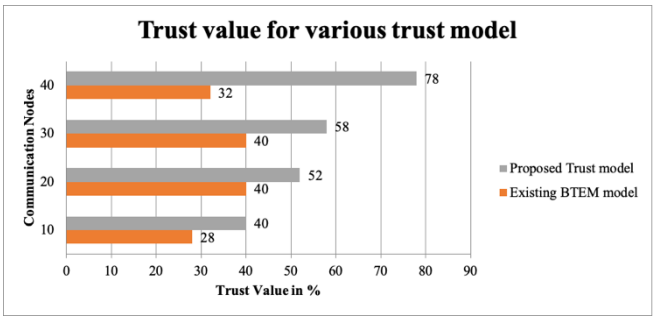

Fig. 3. Comparative analysis of trust values based on communication nodes

Figure.3 has illustrated the percentage of trust value for the models with comparative analysis based on 40 communication nodes presents in the network. The figure 3 shown the network trust value related to presence of varying malicious node percentage. The trust value for proposed trust model is high for all communication nodes whereas the trust value gets increased based on the incremental of communication node. The node of 20 and 30 consists of same trust value percentage of 40% in

existing model but the value of proposed trust model percentage is 52% and 58%. Finally, the communication node of 40 with the trust value of 32% in existing BTEM and for proposed trust model is 78%. Thus, the reliability and accuracy of proposed more is comparatively higher in proposed trust model than BTEM model.

7. CONCLUSION

In this study, present a model for calculating Trust evaluating model for IoT devices in SIoT network. In SIoT network, devices have their individual social networks which offer persons to execute rules on these devices to prevent their security and privacy issues. It also leads to secure communication after establishing trust, where trustworthiness of IoT devices are measured using reputation and trust metrics with reference to the devices. Our model is lightweight and deterministic in nature. This paper has introduced a comparative study of proposed CT model with existing model in accordance with data of both encoding and decoding which assist in assessing SIoT network trust by normalizing and evaluation of data. Moreover, the higher trust value present in the communication node is considered to be an accurate and better trusted path in the network whereas the lowest trust value present in the communication node is determined as an untrusted path of the network that may contain malicious nodes. Hence the proposed cooperative trust model provides highly secure than the existing framework. This performance can be increased and more appropriate in social network such as Facebook, LinkedIn, Twitter, Instagram etc. In future introduce a new method of encoding and decoding methods like Viterbi decoder will suited for SIoT.

REFERENCES

[1] Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated [Internet]. [cited 2016 Aug 18]. Available from: https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devicesby-2020-is-outdated.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] Chanchal Sharma, M. Afshar Alam and Aqeel Khalique, “A Novel Trust Establishment Model in SIoT Network based on Sociological Aspects of Users in Social Networking Services”, Indian Journal of Science and Technology, Vol 12(17), DOI: 10.17485/ijst/2019/v12i17/143128, May 2019.

[3] Priyadharshini.P and Ramya.J, “Security Improvement in Social IOT”, International Journal of Advanced Research in Education & Technology, Vol. 3, Issue 2, 2016.R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[4] Schoorman, F.D.; Mayer, R.C.; Davis, J.H. An integrative model of organizational trust: Past, present, and future. Acad. Manag. Rev. 2007, 32, 344–354.

[5] Nguyen Binh Truong , Hyunwoo Lee , Bob Askwith and Gyu Myoung Lee, “Toward a Trust Evaluation Mechanism in the Social Internet of Things”, Sensors 2017, 17, 1346; doi:10.3390/s17061346.

[6] Nitti M, Girau R, Atzori L, “Trustworthiness management in the social Internet of Things”, IEEE Transactions on Knowledge and Data Engineering, 2014, 26:1253–66. https://doi.org/10.1109/TKDE.2013.105.

[7] B.Truong, N., Um, T.W., Lee, G.M, “A reputation and knowledge based trust service platform for trustworthy social Internet of Things”, 2016, Available from: https://www.semanticscholar.org/paper/A-Reputationand- Knowledge-Based-Trust-Service-for-Truong/6960e85 5b20262c49d492b32d31f0fd6c20a46f5.

[8] Tai-Won Um , Eunhee Lee , Gyu Myoung Lee and Yongik Yoon, “Design and Implementation of a Trust Information Management Platform for Social Internet of Things Environments” , Sensors 2019, 19, 4707; doi:10.3390/s19214707.

[9] E. A. K. amd, N. D. Tselikas, and A. C. Boucouvalas, “Integrating RFIDs and smart objects into a unified Internet of things architecture,”Adv. Internet Things, vol. 1, no. 1, pp. 5–12, 2011.

[10] [10] David Goad and Uri Gal, “IoT Design Challenges and the Social IoT Solution” , Twenty-third Americas Conference on Information Systems, Boston, 2017.
[11] Gamini Joshi, Vidushi Sharma, “ A Cooperative Approach for Implementation of Trust for IoT Networks” , International Journal of Advanced Science and Technology Vol. 29, No. 03, 2020, pp. 9228 – 9237.
[12] Al-Hamadi, H., Chen, I.R., “Trust-Based Decision Making for Health IoT Systems”, IEEE Internet of Things Journal. 4, 1408–1419 , 2017. https://doi.org/10.1109/JIOT.2017.2736446.
[13] Atzori, L., Iera, A., Morabito, G., Nitti, M, “The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization”, Computer Networks. 56, 3594–3608 , 2012. https://doi.org/10.1016/j.comnet.2012.07.010.
[14] Marti, S., Giuli, T.J., Lai, K., Baker, M, “Mitigating routing misbehavior in mobile ad hoc networks”, In: Proceedings of the 6th annual international conference on Mobile computing and networking - MobiCom ’00. pp. 255–265. ACM Press, New York, New York, USA, 2000. https://doi.org/10.1145/345910.345955.
[15] Oliviero, F., Romano, S. Pietro, “A Reputation-Based Metric for Secure Routing in Wireless Mesh Networks”, In: IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference. pp. 1–5. IEEE, 2008. https://doi.org/10.1109/GLOCOM.2008.ECP.374.
[16] Ren, Y., Boukerche, A, “Performance Analysis of Trust-Based Node Evaluation Schemes in Wireless and Mobile Ad Hoc Networks”, In: 2009 IEEE International Conference on Communications. pp. 1–5. IEEE, 2009. https://doi.org/10.1109/icc.2009.5305933.
[17] Namal, S., Gamaarachchi, H., MyoungLee, G., Um, T.-W, “Autonomic trust management in cloud-based and highly dynamic IoT applications”, In: 2015 ITU Kaleidoscope: Trust in the Information Society (K-2015). pp. 1–8. IEEE, 2015. https://doi.org/10.1109/Kaleidoscope.2015.7383635.
[18] Hammi, M.T., Hammi, B., Bellot, P., Serhrouchni, A, “Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. Computers & Security”, vol-78, pp-126–142, 2018. https://doi.org/10.1016/j.cose.2018.06.004.
[19] Duan, J., Gao, D., Yang, D., Foh, C.H., Chen, H.-H, “An Energy-Aware Trust Derivation Scheme With Game Theoretic Approach in Wireless Sensor Networks for IoT Applications”, IEEE Internet of Things Journal. Vol-1, pp-58–69, 2014. https://doi.org/10.1109/JIOT.2014.2314132.
[20] Nie Shuzhi, “A novel trust model of dynamic optimization based on entropy”[Journal]. - [s.l.] : Springer Nature, 2017.
[21] Raja Waseem Anwar Anazida Zainal ,Fatma Outay, “BTEM: Belief based trust evaluation mechanism for Wireless Sensor”, [Journal] // Future Generation Computer Systems. - 2019.