

Gateway based Trust Management System for Internet of Things

Madhura Apte¹; Supriya Kelkar²; Aishwarya Dorge³; Shilpa Deshpande⁴; Pooja Bomble⁵;
Anushka Dhamankar⁶

¹Department of Computer Engineering, Cummins College of Engineering for Women, Pune, India.
¹madhura.apte@cumminscollege.in

²Department of Computer Engineering, Cummins College of Engineering for Women, Pune, India.
²supriya.kelkar@cumminscollege.in

³Department of Computer Engineering, Cummins College of Engineering for Women, Pune, India.
³aishwarya.dorge@cumminscollege.in

⁴Department of Computer Engineering, Cummins College of Engineering for Women, Pune, India.
⁴shilpa.deshpande@cumminscollege.in

⁵Department of Computer Engineering, Cummins College of Engineering for Women, Pune, India.
⁵pooja.bomble@cumminscollege.in

⁶Department of Computer Engineering, Cummins College of Engineering for Women, Pune, India.
⁶anushka.dhamankar@cumminscollege.in

Abstract

Internet of Things (IoT) a growing phenomenon, refers to the seamless integration of things into the information network. The security in IoT is tampered because of the various attacks which happen due to resource constrained nature of the devices in the network. Thus, although IoT is evolving as an attractive next generation networking paradigm, it can be adopted only when the security issues are resolved. This implies that, in a dynamic and collaborative IoT environment, the devices need to be trustworthy. This paper proposes a gateway based trust management system and an algorithm for computation of trust for the devices. The system focuses on making the computations on the devices lightweight and the network robust. The proposed system is tested against various IoT attacks and results demonstrate that it can clearly identify the malicious device if any, in the IoT network.

Key-words: Attacks, Internet of Things (IoT), Security, Trust Computation, Trust Management.

1. Introduction

There is a lot of development in the field of Internet of Things (IoT). However, the devices in the IoT network are vulnerable which compromises the privacy of the device or of the user [1]. Today,

IoT systems have become more vulnerable for various types of attacks. This is due to the number of devices getting connected to IoT systems has been on rise. Being at the edge, IoT devices may become entry-point into the enterprise systems. These devices may become vulnerable as the security mechanisms are not well defined for many such devices. If these IoT devices are directly connected to the internet, they might be remotely controlled through the exploitation of vulnerabilities. Hence, before communication between IoT devices, trust need to be established [2].

This paper presents a gateway based trust management system for computing trust of the devices in IoT network. The system focuses on establishing trust between devices as well as between the device and a gateway. The trust is established between two devices by computing direct and indirect trust values. Direct trust is evaluated considering the Quality of Service [3] of the devices and indirect trust is the integrated recommendation trust value. It results into the lightweight trust computation because of the following two features of the proposed system for trust management. Firstly, whenever the direct trust of the device is not credible, then only indirect trust is computed. Secondly, direct and indirect trust values are calculated on the gateway rather than on the devices.

The remainder of the paper is organized as follows. Section II presents the earlier work done in the domain of trust in IoT. Section III depicts an architecture of the proposed system and presents an algorithm for gateway based trust management for IoT. Section IV presents experimental results for various test cases based on the simulation and hardware implementation. Section IV also includes the analysis of the proposed system. Section V summarizes the paper.

2. Related Work

Trust plays a significant role in implementing IoT [4]. Authors in [4] and [5] describe the various security concerns in the IoT environment and therefore the need for establishing trust between IoT devices. The approaches of trust evaluation for IoT systems, found in the literature, make use of various techniques like direct as well as recommendation and reputation based trust computation [6][7][1][2][8][9]. The approaches based on graphs [10], Machine Learning [11] and encryption [12] have also been suggested in literature. Trust management approaches for IoT environment in literature, take into consideration various domains such as healthcare [13][14], agriculture [15] and smart cities [16].

Authors in [4] describe the importance of governance in achieving the trust in IoT. They further specify security, privacy, identity management as trust related crucial factors in the IoT environment. Authors in [5] highlight that in IoT environment, IoT devices themselves may turn up to be adversaries

and hamper the security of IoT network. They further specify the need of trust mechanisms in IoT and indicate that gateway can act as significant resource for trust establishment.

For fog-based IoT systems, a context-aware trust using hybrid methodology and protocol for reputation management is presented by authors in [6]. In this work, to select a service provider as a credible entity, its recommendation is refereed and trustworthiness is calculated. Five trust related attacks namely, opportunistic service, badmouthing, self-promoting, discriminatory and ballot-stuffing are implemented to mitigate the attacks by malicious entities. Data aggregation scheme is used to address the scalability issue. However, the protocol is simulated to check its effectiveness. Authors in [7] proposed a lightweight methodology for the devices in the area of industrial IoT. These nodes cannot secure themselves during the data exchange among each other. LightTrust makes use of a centralized trust agent which generates and manages the trust certificates. Trust certificate is generated based on direct and indirect trust value evaluation. These certificates permit the devices to communicate with other devices for a certain amount of time without evaluation of trust values. This work claims to have time-driven trust management for better utilization of resource constraint devices in terms of computation and energy. However, protocol is implemented and evaluated with other work based on simulation.

The approach proposed by [1] computes the trust of nodes in IoT networks based on the data rate and drop rate of packets in the network. The approach also takes into consideration different attacks in the IoT environment. Authors in [2] proposed a model to compute the trust values of various devices in IoT and to predict the trust for a specific amount of time. Yuan and Xiaoyong in [8] proposed a lightweight trust evaluation approach for IoT devices. It makes use of feedback from different sources in trust computation which results in the robustness for badmouthing attacks. HoliTrust [9] is a trust assessment mechanism meant for communication across the multiple domains in IoT.

In [10], authors propose a hybrid trust management framework using Probabilistic Neighbourhood Overlap (P-NO). P-NO is used for calculating trust between the nodes. This framework generates a social graph based on two types of social graphs namely, online social network of the IoT device owners and the social network of IoT-devices. The approach used in this work uses artificial intelligence of device and human intelligence for the trust management. However, this work provides simulation based analysis of proposed trust management framework. A framework is proposed by authors in [11], for trust evaluation of services in IoT based crowdsourcing environment. The approach makes use of a service, the owner and the device perspectives in evaluation of the trust. In this work, trust model based on Neural Networks is proposed. The approach has been evaluated for the accuracy in identifying the trustworthiness of IoT services. Authors in [12] proposed an algorithm for trust in

IoT based on encryption and authentication. It relies on lightweight trust evaluation which considers the sensors as anonymous.

Decision making based on trust for IoT systems, which are meant for health, is proposed in [13]. The algorithm takes into account risk category, reliability, and loss of probability of health as the major factors for assessment. Authors in [14] proposed an algorithm based on enhanced Dirichlet for trust assessment in IoT environment. The algorithm focuses on detection of IoT attacks as relevant to the healthcare applications based on IoT systems. Kaur and Tange in [15] evaluate the existing trust models and they proposed an algorithm for trust in IoT based on reputation and eigen values. Authors in [16] proposed a recommendation based technique for selection of devices in IoT systems, meant for smart cities. The technique makes use of dynamically generated black and white list for selection of trustworthy devices. The approach takes into account the relationship between the service providers of edge devices and the edge devices with respect to trust, along with the trust values between the smart devices. The qualitative validation of the proposed approach is performed using the game theory. However, the authors have used simulation to evaluate the performance of their model.

In summary, the above review of existing work implies that IoT environment is more vulnerable to various attacks and therefore security in IoT networks is a key concern. Security threats in IoT in turn lead to lack of trust in IoT environment. This indicates the continuous need of trust management approaches for IoT environment. The proposed gateway based trust management system for IoT takes into account direct and indirect assessment factors for evaluation of trust between the nodes. Gateway based centralized trust computation mechanism is meant to be robust. The proposed trust management system effectively detects the various IoT attacks based on the trust values and is also able to identify the malicious nodes.

3. Gateway based Trust Management System

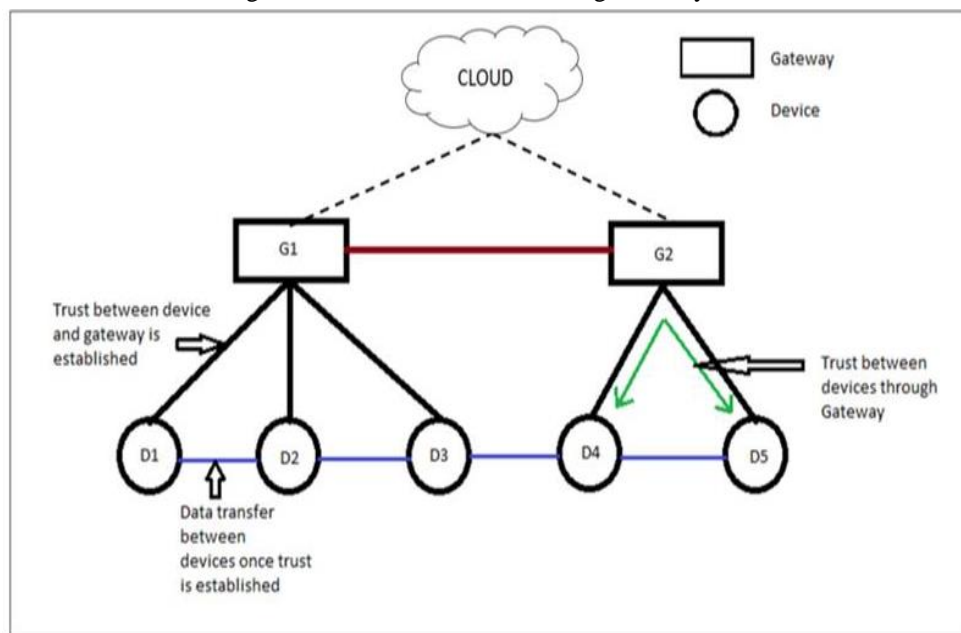
A. System Architecture

IoT devices such as smart sensors can be easily owned by malicious entities or be remotely controlled through exploitation of vulnerabilities. Hence to enable secure communication, we have proposed a gateway based trust management system. The layout of the proposed system is shown in Fig. 1. It shows a hierarchical structure consisting of IoT devices like smart sensors at the lowermost level and a gateway as the higher level. The gateway is responsible to calculate trust value of all the connected sensors and identify malicious nodes (sensors) under attack. Trust is established between

two nodes (sensors) by computing final trust value using direct and indirect trust values. Direct trust is evaluated by making use of the Quality of Service of the devices and indirect trust [17] is the integrated recommendation trust value. Recommendation is taken from all the nodes [18] except the nodes which want to communicate.

Gateways communicate with the cloud at the backend where data approaching from the IoT devices is stored and processed. The main focus of this paper includes the trust computation between the devices and between the gateway and the device. Hence, the cloud related trust management is not considered further, in this paper. The proposed trust management system consists of three modules viz. Authentication, Trust computation and attack detection.

Fig. 1- Architecture of Trust Management System



Authentication module validates every device that attempts to communicate with the gateway. The unauthorized access by any of the devices is notified by the gateway. Trust computation module computes the final trust value of the device by making use of both the trust values namely direct and indirect. Attack detection includes the detection of Good Mouthing attack [14], Bad Mouthing attack [14][19], Newcomer attack [14][20] and On-Off attack [14][21]; by the gateway.

B. Algorithm for Trust Management System

The algorithm for trust management is comprised of two stages as described below.

Stage 1: Authentication Phase

In this stage, authentication and access to the devices is controlled by the gateway, as described in the below given steps.

1. Gateway maintains a list of Media Access Control (MAC) addresses of all the nodes connected to it.
2. If a new malicious node gets connected, the MAC address will be absent in the list. Hence unauthorized access is detected.
3. If a new entity is to be added in the network, its corresponding MAC address is required to be entered in the list maintained at the gateway.

Stage 2: Trust Computation between the Devices

In this stage, the final trust value of the device is calculated based on the direct and indirect trust values, as described by the below given steps and are as per [22].

1. Get the values of rate of successful and unsuccessful transactions.
2. Compute direct trust between node i and node j using Bayesian approach [22] as given by (1).

$$D_{ij} = (\alpha_{ij} + 1)/(\alpha_{ij} + \beta_{ij} + 2) \quad (1)$$

where D_{ij} is direct trust, α_{ij} and β_{ij} are rate of successful and unsuccessful transactions respectively.

3. Evaluate whether the direct trust is enough to decide the credibility of the node by comparing the value of direct trust with confidence threshold [22].
4. If the direct trust value is credible, then assign the value of direct trust D_{ij} to final trust T_{ij} [22].
5. If the direct trust value is not acceptable, then the final trust is computed by using trust values namely direct and indirect.
6. Indirect trust value of a node is calculated based on the entropy theory and feedbacks from other nodes [22]. Request for feedback for node j is broadcasted to the remaining nodes. Feedback is collected at the gateway. For example, consider node x to be the recommender node. Node x transmits its direct observation values $(\alpha_{xj}, \beta_{xj})$ of node j to node i . Then node

i calculates the indirect trust R_{ij}^x by combining its own values (α_{ix}, β_{ix}) of node x with the recommendation received from node x [22]. These steps of indirect trust calculation are described by the below given equations [22].

$$R^x \alpha_{ij} = 2 * \alpha_{ij} * \alpha_{xj} / (\beta_{ix} + 2 * (\alpha_{xj} + \beta_{xj} + 2) + (2 * \alpha_{ix})) \quad (2)$$

$$R^x \beta_{ij} = 2 * \alpha_{ix} * \beta_{xj} / (\beta_{ix} + 2) * (\alpha_{xj} + \beta_{xj} + 2) + (2 * \alpha_{ix}) \quad (3)$$

$$\begin{aligned} R_{ij}^x &= E[Beta(R^x \alpha_{ij} + 1, R^x \beta_{ij} + 1)] \\ &= (R^x \alpha_{ij} + 1) / (R^x \alpha_{ij} + R^x \beta_{ij} + 2) \end{aligned} \quad (4)$$

7. The final trust value is computed as shown by (5) below [22].

$$\left\{ \begin{array}{l} T_{ij} = D_{ij}, \gamma \geq \gamma_0 \\ T_{ij} = w_D * D_{ij} + w_R * R_{ij}, \text{ else} \end{array} \right. \quad (5)$$

Where γ is a confidence and γ_0 is a minimum confidence threshold. In (5), weights of trust values for direct and indirect methods are calculated based on the entropy values [22] as shown below.

$$H(D_{ij}) = -D_{ij} \log_2 D_{ij} - (1 - D_{ij}) \log_2 (1 - D_{ij}) \quad (6)$$

$$H(R_{ij}) = -R_{ij} \log_2 R_{ij} - (1 - R_{ij}) \log_2 (1 - R_{ij}) \quad (7)$$

$$w_D = \frac{1 - \frac{H(D_{ij})}{\log_2 D_{ij}}}{\left(1 - \frac{H(D_{ij})}{\log_2 D_{ij}}\right) + \left(1 - \frac{H(R_{ij})}{\log_2 R_{ij}}\right)} \quad (8)$$

$$w_R = \frac{1 - \frac{H(R_{ij})}{\log_2 R_{ij}}}{\left(1 - \frac{H(D_{ij})}{\log_2 D_{ij}}\right) + \left(1 - \frac{H(R_{ij})}{\log_2 R_{ij}}\right)} \quad (9)$$

Where $H(D_{ij})$ and $H(R_{ij})$ are entropy values of direct and indirect trust values respectively.

Here w_D and w_R are the entropy based weights.

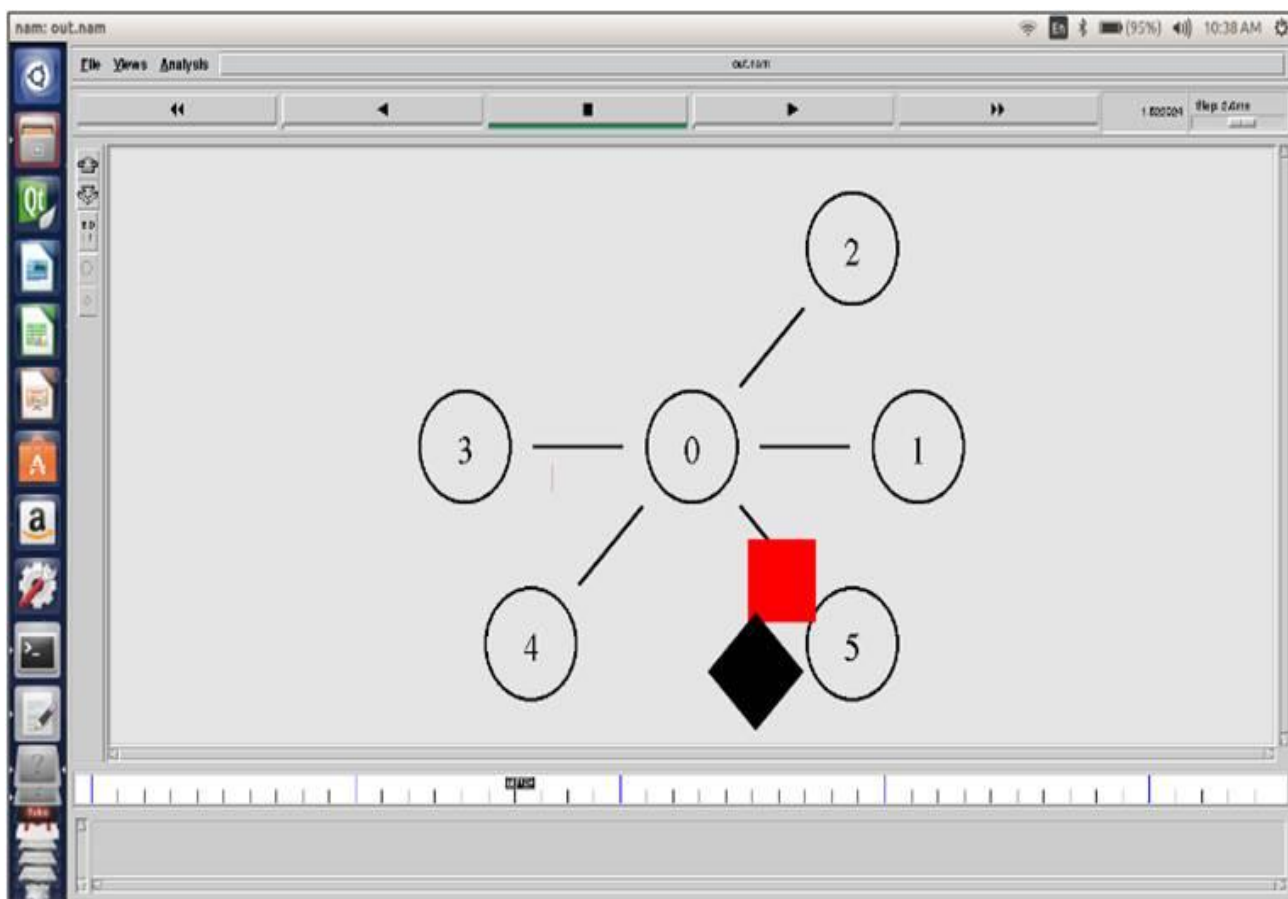
4. Results and Discussions

The system for trust computation is simulated using Network Simulator-2 (NS2). The system is then implemented on hardware using Raspberry Pi development boards, consisting of four nodes and one gateway device connected using wired Local Area Network (LAN). The system is also tested against various attacks which include Good mouthing attack, Bad mouthing attack, Newcomer attack and On-Off attack.

A. Simulation of Denial of Service (DoS) Attack

The Fig. 2 depicts a simulation of Denial of Service (DoS) attack using NS2. Here, Node 3 being the malicious node attacks Node 5. So, Node 5 has spent resources on consuming the Node 3's data and fails to serve the legitimate data.

Fig. 2 - Simulation of DoS Attack



B. Good and Bad Mouting Attack

Fig. 3 represents the Gateway node's output. The initial trust matrix represents historic trust values that gateway maintains. Positive transaction matrices are the number of successful transactions between corresponding nodes whereas negative transaction matrices are the number of unsuccessful transactions between corresponding nodes. Node 0 establishes connection with Node 1. Since the initial trust value is less than the confidence threshold, indirect trust values are requested.

Fig. 3 - Gateway Node Output

```
pi@raspberrypi: ~/Desktop/IOT $ python3 NewcomerGoodBadMouthing.py
Initial Trust Matrix
[[ 0.7  0.3  0.3  0.7  0.3]
 [ 0.3  0.3  0.3  0.7  0.3]
 [ 0.3  0.3  0.3  0.3  0.7]
 [ 0.7  0.3  0.7  0.3  0.3]
 [ 0.7  0.3  0.3  0.3  0.7]]

Positive Transaction Matrix
[[ 0.  0.  0.  0.  1.]
 [ 0.  0.  1.  0.  1.]
 [ 0.  1.  0.  0.  0.]
 [ 0.  0.  0.  0.  2.]
 [ 1.  1.  0.  2.  0.]]

Negative Transaction Matrix
[[ 0.  0.  0.  0.  0.]
 [ 0.  0.  0.  0.  0.]
 [ 0.  0.  0.  0.  0.]
 [ 2.  0.  0.  0.  0.]
 [ 0.  0.  0.  0.  0.]]

Positive Transaction Matrix
[[ 0.  0.  1.  1.  1.]
 [ 0.  0.  1.  0.  1.]
 [ 1.  1.  0.  0.  0.]
 [ 1.  0.  0.  0.  2.]
 [ 1.  1.  0.  2.  0.]]

Negative Transaction Matrix
[[ 0.  0.  0.  0.  0.]
 [ 0.  0.  0.  0.  0.]
 [ 0.  0.  0.  0.  0.]
 [ 2.  0.  0.  0.  0.]
 [ 0.  0.  0.  2.  0.]]

Ready to receive indirect trust values from nodes

Connection from MAC: b8:27:eb:27:f6:f1
Connection from IP: 169.254.78.116
Trust value for source: 0.26
Trust value for destination: 0.92

Connection from MAC: b8:27:eb:84:d7:b1
Connection from IP: 169.254.77.218
Trust value for source: 0.27
Trust value for destination: 0.03
```

Fig. 4 shows that indirect trust matrix is used to detect the good and bad mouthing attacks. If trust value is greater than positive threshold (0.7), then node is under good mouthing attack and if trust value is lesser than negative threshold (0.3), then node is under bad mouthing attack.

Fig. 4 - Simulation of Good and Bad Mouthing Attack

```

File Edit Tabs Help
Indirect Trust Matrix:
[[ 0.35 0.27 0.03 0.55 0.321]
 [ 0.27 0.5 0.5 0.26 0.41 ]
 [ 0.03 0.5 0.5 0.92 0.72 ]
 [ 0.31 0.26 0.92 0.53 0.68 ]
 [ 0.36 0.41 0.72 0.57 0.59 ]]

Indirect Trust Matrix:
[[ 0.35 0.27 0.03 0.55 0.321]
 [ 0.27 0.5 0.5 0.26 0.41 ]
 [ 0.03 0.5 0.5 0.92 0.72 ]
 [ 0.31 0.26 0.92 0.53 0.68 ]
 [ 0.36 0.41 0.72 0.57 0.59 ]]

Bad mouthing Malicious node is : 0
Bad mouthing attack is on node: 1

Bad mouthing Malicious node is : 0
Bad mouthing attack is on node: 2

Bad mouthing Malicious node is : 3
Bad mouthing attack is on node: 1

Good mouthing Malicious node is : 3
Good mouthing attack is on node: 2

Good mouthing Malicious node is : 4
Good mouthing attack is on node: 2

Positive Transaction Matrix
[[ 0. 0. 1. 1. 1.]
 [ 0. 0. 1. 0. 1.]
 [ 1. 1. 0. 0. 0.]
 [ 1. 0. 0. 0. 2.]
 [ 1. 1. 0. 2. 0.]]

Negative Transaction Matrix
[[ 0. 0. 0. 0. 0.]
 [ 0. 0. 0. 0. 0.]
 [ 0. 0. 0. 0. 0.]
 [ 2. 0. 0. 0. 0.]
 [ 0. 0. 0. 2. 0.]]
    
```

Fig. 5 represents the recommendation trust values for the nodes in communication.

Fig. 5 - Recommendation Trust Values

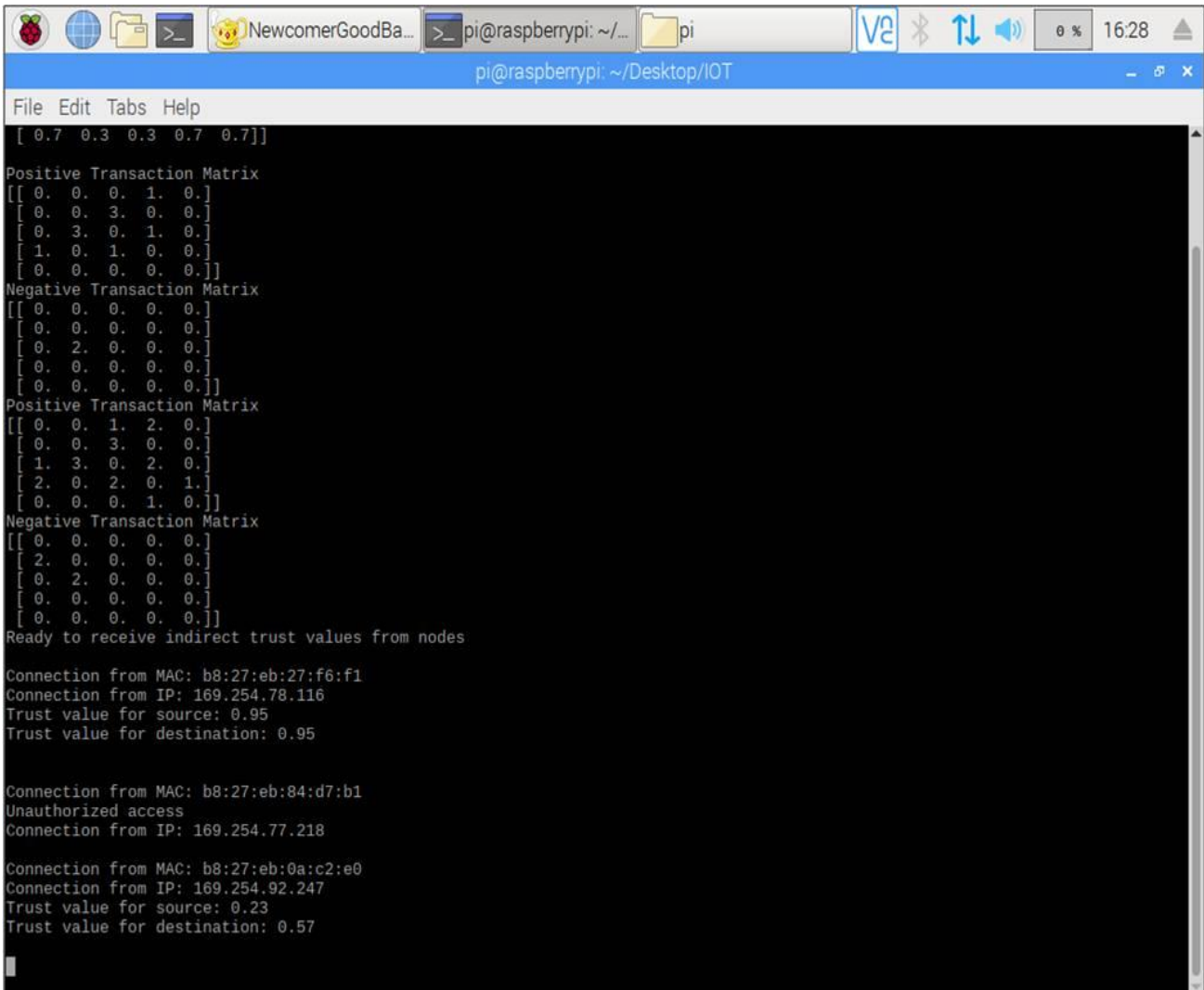
```

pi@raspberrypi: ~/... Client.p
pi@raspberrypi:~/Desktop/IOT $ python Client.py
Recommending trust value for source: 0.27
Recommending trust value for destination: 0.03
pi@raspberrypi:~/Desktop/IOT $
    
```

C. Newcomer Attack

Fig. 6 depicts the output of the Newcomer attack. Gateway has a list of MAC addresses of all the nodes present in the network. If any unauthorized node enters into the network, gateway recognizes it and further operations are denied for that node.

Fig. 6 - Simulation of Newcomer Attack



```
pi@raspberrypi: ~/Desktop/IOT
File Edit Tabs Help
[ 0.7 0.3 0.3 0.7 0.7]
Positive Transaction Matrix
[[ 0. 0. 0. 1. 0.]
 [ 0. 0. 3. 0. 0.]
 [ 0. 3. 0. 1. 0.]
 [ 1. 0. 1. 0. 0.]
 [ 0. 0. 0. 0. 0.]]
Negative Transaction Matrix
[[ 0. 0. 0. 0. 0.]
 [ 0. 0. 0. 0. 0.]
 [ 0. 2. 0. 0. 0.]
 [ 0. 0. 0. 0. 0.]
 [ 0. 0. 0. 0. 0.]]
Positive Transaction Matrix
[[ 0. 0. 1. 2. 0.]
 [ 0. 0. 3. 0. 0.]
 [ 1. 3. 0. 2. 0.]
 [ 2. 0. 2. 0. 1.]
 [ 0. 0. 0. 1. 0.]]
Negative Transaction Matrix
[[ 0. 0. 0. 0. 0.]
 [ 2. 0. 0. 0. 0.]
 [ 0. 2. 0. 0. 0.]
 [ 0. 0. 0. 0. 0.]
 [ 0. 0. 0. 0. 0.]]
Ready to receive indirect trust values from nodes

Connection from MAC: b8:27:eb:27:f6:f1
Connection from IP: 169.254.78.116
Trust value for source: 0.95
Trust value for destination: 0.95

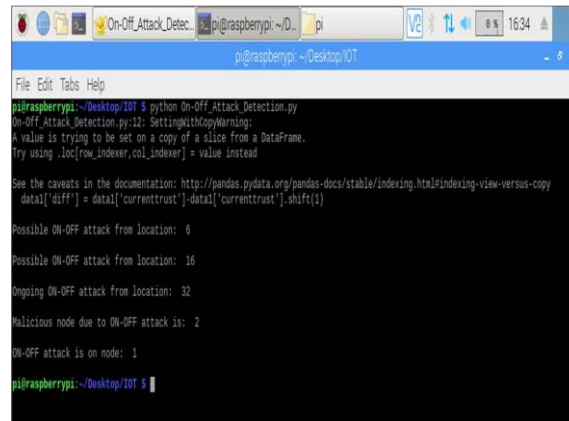
Connection from MAC: b8:27:eb:84:d7:b1
Unauthorized access
Connection from IP: 169.254.77.218

Connection from MAC: b8:27:eb:0a:c2:e0
Connection from IP: 169.254.92.247
Trust value for source: 0.23
Trust value for destination: 0.57
```

D. On-Off Attack

Fig. 7 depicts the on-off attack detection. Node 1 is under on-off attack by Node 2 following the pattern of behaving well and bad according to the situations.

Fig. 7 - Simulation of On-Off Attack



```
pi@raspberrypi:~/Desktop/10T
File Edit Tabs Help
pi@raspberrypi:~/Desktop/10T $ python On-Off_Attack_Detection.py
On-Off_Attack_Detection.py:12: SettingWithCopyWarning:
A value is trying to be set on a copy of a slice from a DataFrame.
Try using .loc[row_indexer,col_indexer] = value instead

See the caveats in the documentation: http://pandas.pydata.org/pandas-docs/stable/indexing.html#indexing-view-versus-copy
data['diff'] = data['currenttrust'] - data['currenttrust'].shift(1)

Possible ON-OFF attack from location: 6

Possible ON-OFF attack from location: 16

Ongoing ON-OFF attack from location: 32

Malicious node due to ON-OFF attack is: 2

ON-OFF attack is on node: 1

pi@raspberrypi:~/Desktop/10T $
```

E. Analysis of the Proposed Work and Comparison with the Earlier Work of [14]

The proposed system takes into consideration both direct and indirect trust. The proposed system is more secure compared to peer to peer system as the trust is evaluated at the centralized gateway device.

The proposed system consists of resource-rich centralized gateway for the computation of trust, thus enabling the system to have resource-constrained nodes (edge devices). This makes the computations extremely lightweight at the nodes (edge devices). However, the proposed system may have a single-point of failure since trust computation is performed at the gateway device.

The proposed algorithm is evaluated for its performance. The performance is found to be good as the trust computation time is 0.15 seconds for the prototype implementation consisting of four nodes and one gateway device. Also, the computational complexity of the proposed algorithm is found to be $O(n^2)$ which is fairly good. Our proposed system is also scalable as the system is based on wired LAN.

The trust computation method mentioned in [14] is implemented using network simulator. However, our proposed algorithm is implemented using IoT development boards and the results are discussed above, in the earlier part of this section. Our proposed system uses gateway based architecture, whereas this architecture is not used in the trust management system in [14].

5. Conclusion

This work has proposed a gateway based trust management system for computing trust of the devices in IoT network. The system ensures and enhances the protection of smart IoT devices in the network against IoT attacks. The trust computation takes into consideration direct as well as indirect trust according to their randomness. The system makes use of lightweight trust evaluation mechanism

and it considers hierarchy of the devices. The proposed trust management system effectively detects the various IoT attacks viz. Good Mouthing attack, Bad Mouthing attack, Newcomer attack and On-Off attack; based on the trust values and is also able to identify the malicious nodes.

In future, the system can be extended to include trust establishment between the gateways. Higher level in the hierarchy which is cloud, may be added for computing trust in IoT network. Real time data from sensors may also be considered in trust computation. The system can also be tested against other attacks like Sybil attack for more robustness.

References

- K.N. Qureshi, A. Iftikhar, S. N. Bhatti, F. Piccialli, F. Giampaolo, and G. Jeon, Trust management and evaluation for edge intelligence in the Internet of Things, *Eng. Appl. Artif. Intell.*, vol. 94, Sep. 2020, Art. no. 103756.
- Wang, Eric Ke, Chien-Ming Chen, Dongning Zhao, Wai Hung Ip, and Kai Leung Yung, "A dynamic trust model in internet of things." *Soft Computing* 24, no. 8 (2020): 5773-5782.
- Deshpande, Shilpa, and Rajesh Ingle, "Trust assessment in cloud environment: Taxonomy and analysis." In *International Conference on Computing, Analytics and Security Trends (CAST)*, pp. 627-631. IEEE, 2016.
- R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things", *IEEE Computer*, 44, 51-58, 2011.
- Román-Castro, Rodrigo, Javier López, and Stefanos Gritzalis. "Evolution and trends in IoT security." *IEEE Computer*, vol. 51, no. 7 (2018): pp.16-25.
- Jabeen, Farhana, Zara Hamid, Zobia Rehman, and Abid Khan. "Adaptive and survivable trust management for Internet of Things systems." *IET Information Security* (2021).
- Din, Ikram Ud, Aniqah Bano, Kamran Ahmad Awan, Ahmad Almogren, Ayman Altameem, and Mohsen Guizani. "LightTrust: Lightweight Trust Management for Edge Devices in Industrial Internet of Things." *IEEE Internet of Things Journal* (2021).
- Yuan, Jie, and Xiaoyong Li. "A reliable and lightweight trust computing mechanism for IoT edge devices based on multi-source feedback information fusion." *IEEE Access* 6 (2018): pp. 23626-23638.
- Awan, Kamran Ahmad, Ikram Ud Din, Mahdi Zareei, Muhammad Talha, Mohsen Guizani, and Sultan Ullah Jadoon. "Holitrust-a holistic cross-domain trust management mechanism for service-centric Internet of Things." *IEEE Access* 7 (2019): pp. 52191-52201.
- Narang, Nishit, and Subrat Kar. "A hybrid trust management framework for a multi-service social IoT network." *Computer Communications* 171 (2021): 61-79.
- Ba-hutair, Mohammed Nasser, Athman Bouguettaya, and Azadeh Ghari Neiat. "Multi-Perspective Trust Management Framework for Crowdsourced IoT Services." *IEEE Transactions on Services Computing* (2021).
- Jebri, Sarra, Mohamed Abid, and Ammar Bouallegue. "LTAMA-algorithm: light and trust anonymous mutual authentication algorithm for IoT." In *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, pp. 1-5. IEEE, 2018.

Al-Hamadi, Hamid, and Ray Chen. "Trust-based decision making for health IoT systems." *IEEE Internet of Things Journal* 4, no. 5 (2017): pp.1408-1419.

Malhotra, Mansi, Mehak Ganjoo, Shreya Kulkarni, Sneha Paranjape, and Supriya Kelkar, "Mitigating Iot Attacks In Smart Medical Networks Using Enhanced Dirichlet Based Algorithm For Trust Management System." In *2020 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, pp. 1-6. IEEE, 2020.

Kaur, Bipjeet, and Henrik Tange. "Heuristic trust in iot." In *Proceedings of the Fifth International Conference on Wireless Communications, Vehicular Technology, Information Theory, Aerospace & amp.* 2015.

Wang, Bo, Mingchu Li, Xing Jin, and Cheng Guo. "A reliable IoT edge computing trust management mechanism for smart cities." *IEEE Access* 8 (2020): 46373-46399.

Parhizkar, Elham, Mohammad Hossein Nikravan, and Sandra Zilles, "Indirect Trust is Simple to Establish." In *IJCAI*, pp. 3216-3222. 2019.

Kelkar, Supriya, and Raj Kamal, "Adaptive fault diagnosis algorithm for controller area network." *IEEE transactions on Industrial Electronics* 61, no. 10 (2014): 5527-5537.

Reddy, Vijender Busi, Atul Negi, S. Venkataraman, and V. Raghu Venkataraman, "A similarity based trust model to mitigate badmouthing attacks in Internet of Things (IoT)." In *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, pp. 278-282. IEEE, 2019.

Ramanathan, Anusha. "A multi-level trust management scheme for the Internet of Things", University of Nevada, Las Vegas, 2015.

Caminha, Jean, Angelo Perkusich, and Mirko Perkusich. "A smart middleware to detect on-off trust attacks in the Internet of Things." In *2018 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1-2. IEEE, 2018.

Che, Shenyun, Renjian Feng, Xuan Liang, and Xiao Wang, "A lightweight trust management based on Bayesian and Entropy for wireless sensor networks." *Security and Communication Networks* 8, no. 2 (2015): 168-175.