J. Sustain. Wireless Syst.
Vol.02/ No. 2
Pages: 84-91
http://irojournals.com/irosws/
DOI: https://doi.org/10.36548/jsws.2020.2.004

Edge Computing through Virtual Force for Detecting Trustworthy Values

Dr.R.Dhaya,
Department of Computer Science,
Sarat Abida Campus -King Khalid University,
KSA,
dhayavel2005@gmail.com

Dr.R.Kanthavel,
Department of Computer Engineering,
King Khalid University,
Abha,
KSA
kanthavel2005@gmail.com

Abstract: As the advancement of IoT (Internet of Things) and other emerging mobile application continues, it is an accepted fact that Edge Computing paradigm is considered to be the best fit in terms of fulfilling the resource requirements. Moreover, it is a fact that the data collected by the sensor networks serves as the base for the IoT applications as well as the systems. However, due to advancement in cybercrimes, there is a possibility that the data collected through the sensor networks are vulnerable to attacks which may result in serious consequences. The proposed work focuses on a new model which is used to gather trustworthy data using edge computing in IoT. In order to get the accurately quantified trust values, the sensor nodes are analyzed and found from different dimensions. Moreover, with the help of trust value obtained, it is possible to find the best mobility path which carries the highest value of trust. This data is gathered from the sensors with the help of mobile edge data collector. This analysis shows that for a trustworthy data collection model of IoT, there is noticeable improvement in terms of energy conservation and system security, thereby improving the performance of the system.

Keywords: Internet of Things, Edge Computing, Quantified trust values, Sensor Nodes

1.Introduction

The exuberant advancement in Mobile applications and Internet of Things (IoT) has increasingly stringent requirement for the Wireless Sensor Networks (WSNs) and cloud infrastructure which includes data trustworthiness, low power consumption, ultra-low latency and system security [1]. This growing demand requires highly localized services which are near the user on the network edge. It has given rise to Mobile Edge Computing (MEC) that serves to integrate applications, storage, computing and network on an open platform which has the capability to give edge intelligence services based on edge of network, close to the data source [2]. In general, the data that is gathered by the wireless sensor networks are the base for IoT applications and system. However, the drawback is that this data is untrustworthy without the right security measures [3] [4]. These sensor networks are employed in harsh environments and unattended areas to do many important tasks in many areas like emergency responses, intrusion detection, medical monitoring, smart cities and battlefield surveillance [5]. Because of this the possibility of attack on the underlying sensor network is very high as a result of which the data gathered through these sensors might be misleading or invalid. The worst part of the scenario is that only 49% or less data is trustworthy and valid [6] [7].

Since the data collected through these sensor networks are untrustworthy and problematic, application and data protection of the upper layer is not possible. Hence it is necessary to protect the network by means a security which serves to protect the resources as well as the system from all types of attacks. The attacks faced by WSNs can be categorised into two namely external attack and internal attack. A details study on these attacks by [8] shows that more than the external attacks, internal attacks are known to be more harmful. Also, the security measures for the external for routing protocols and cryptographic. One effective method which is also lightweight is trust evaluation which is used to address malicious nodes [9]. Moreover, it forms a crucial part of the security system. There are may theories on data acquisition in the recent years that are focussed on the mobile data collector which is the common node at the bottom which has limited communication capacity, storage capacity and computing power, but the energy consumption is very high [11]. Moreover, when this node traverses all the other nodes during the data gathering process, it will not only increase the energy consumption and delay, but will further result in the collection of malicious data at a large scale. To address this issue, we propose the methodology of virtual force mapped by trust value (VFDC) for gathering trustworthy data. This proposed methodology will take into consideration the factors that are essential to secure trustworthiness of sensor nodes. Based on the evaluation of trust in many aspects, this virtual force will enable mapping of the trust values in order to build a reliable path of communication. Also, trustworthy data can be gathered through the mobile data collector in the form of edge node.

2. Problem Formulation

In a typical node which is connected to Internet of Things, there are said to be many base station nodes and m sensor nodes which are of the dimensional plane LxL. A clustering protocol is used to cluster all the nodes where the network is established which is inclusive of s cluster head nodes which is found to be based on $m \gg s$. Moreover, in the edge network system, there are two basic types of nodes used namely malicious nodes and trustworthy nodes. Based on the behavior information gathered, the cluster head nodes analyze the trust of trustworthy node. Trustworthy data is collected from the trustworthy nodes and the subsequent trustworthy values are also updated accordingly. The network structure comprises of many clusters and each cluster head is used to find the value of trust in the node based on its characteristics and behavior. Accordingly, the untrustworthy nodes and the trustworthy nodes are divided within the cluster. The edge mobile node is assigned the task of gathering data from the clusters [10].

Depending on the trust value, the trustworthiness is determined and the one with higher value is assigned to be the cluster head node. Randomization of the initial path is accomplished but they are designed to pass through almost all the head nodes [12-13], in the direction where the mobile edge nodes travel and gather data. The path of simulation is similar to that of a soft magnetic rope such that the untrustworthy nodes are repelled while the trustworthy ones are attracted. Accordingly the resultant force of interaction between the repulsive force and the attractive force will direct the path of travel towards the area which has better trust value. This is also the area which is not near the untrustworthy area and the efficiency of trustworthy data collection is improved significantly by decreasing the distance. That is, the mobile edge nodes are granted quick entrance to the cluster head of trustworthy nodes and it simultaneously reduces the nodes' usage of energy.

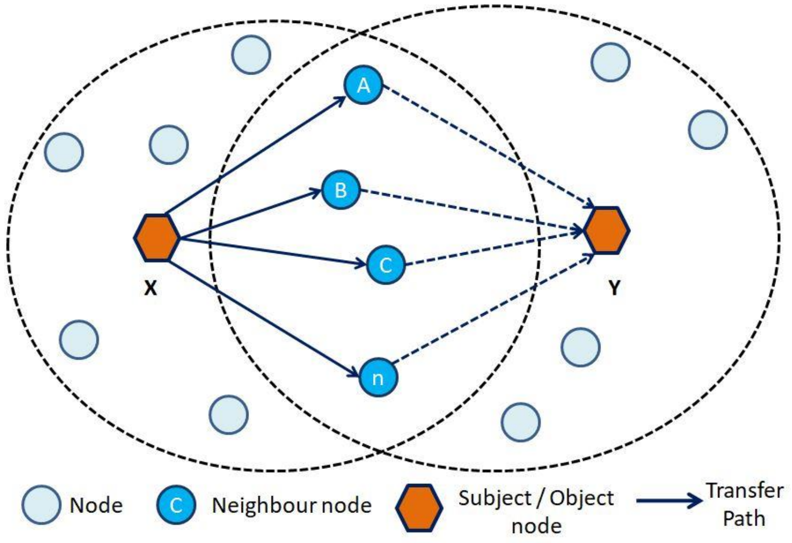

Fig.1. Indirect trust delivery

3. Sensor Network Methodology

If there are n randomly deployed sensor nodes in a network, then data collection from the nodes will be an important application in computing systems based on Internet of Things. Taking this into consideration, the following assumptions are made in view of the network model:

1. The base station and sensor nodes present in the network are fixated and cannot move once they are deployed. Moreover, sufficient amount of energy is used by these base station nodes.

2. An infinite buffer is used to move the mobile edge node at a predefined rate in the deployed area such that it has strong computing power and sufficient energy.

3. The sensor nodes possess a unique identity and have limited energy.

4. It is possible to adjust the transmission power based on the distance between the moving collection elements. This will also help save energy and a tree architecture is built in order to decrease the energy consumption of nodes and also to satisfy the time criteria. G(V, E) represents a geometric tree where V represents the cluster head nodes and E represents the mobile edge node.

$$V = \{c_0, \ldots. c_i, \ldots., c_{n-1}\}$$

Here i is the count of the node and c_i is cluster head node. A number of cluster head nodes are passed by the mobile edge node as it travels through the restricted path. When the cluster head node is detected close to the mobile edge node, data is transmitted from the cluster head to the edge node. On the other hand, the other nodes which are not within communicating node of the mobile edge node, other algorithms, like Dijkstra algorithm are adopted. The cluster head collection nodes collect the data transmitted by means of multihop method.

4. Results and Discussion

The output observed in Fig.2 shows that when there are more than 50% malicious nodes in the network, it will automatically decrease the trust value of the node. This will further be reflected in the trustworthiness of the cluster. Similar results are obtained in other methodologies such as BTEM and ETRES. It is seen that the trust value drops to a pre-fixed neutral range when there are many malicious nodes present in the network.

Moreover, when compared to ETRES and BTEM, VFDC is said to have many favourable advantages when there are more than 60% of malicious nodes. Fig.3 shows the validity of VFDC as a visual illustration for collecting trustworthy data. Here the distance between the nodes and a particular point on the trustworthy path is calculated and demonstrated. It is observed that as the process is repeated, an increase in the distance between trustworthy path generated and the untrustworthy node. Moreover, the proposed methodology to gather trustworthy data will push the path along which it is moving towards the trustworthy area and further directs from other unwanted area as a result of the resultant force direction.

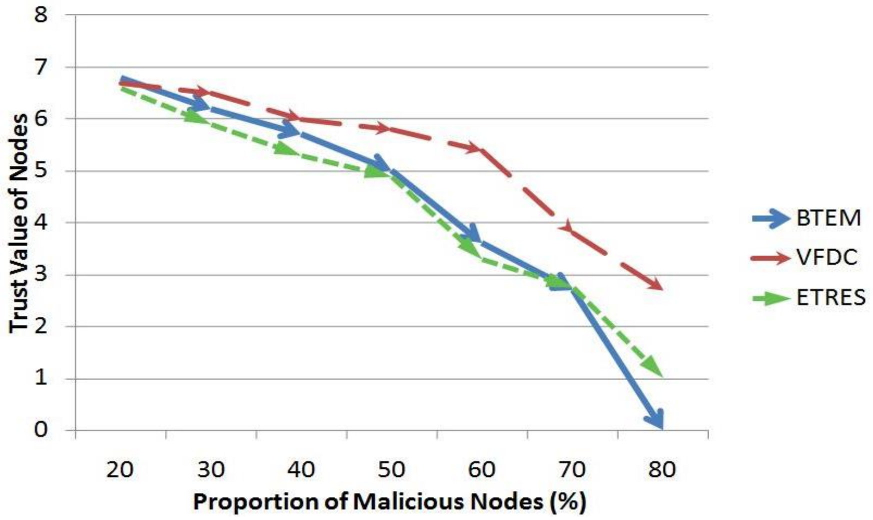

Fig.2. Change in Node Trust Value for Different Methodology

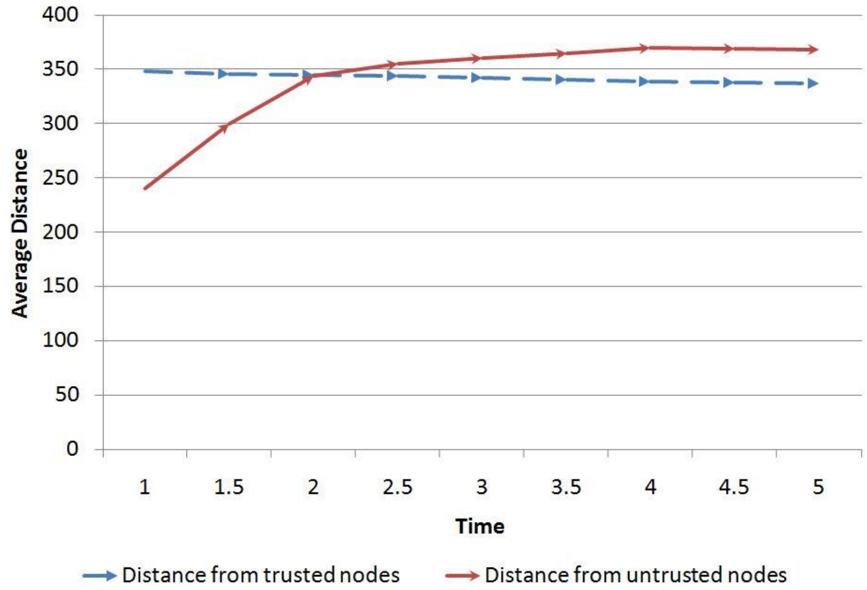

Fig.3. Distance between untrusted and trusted nodes

In Fig.4, it is noticed that the rate of recognition of the trust evaluation method is directly proportional to the number of iterations that occur along the moving path. It is also found that when compared to other methods like BREM and CTRUST, VFDC has a higher rate of detecting the presence of malicious nodes. On the basis of energy consumption, the three methodologies were analyzed based on node deployments and network architecture. It was found that as the node count increases, there is a subsequent increase in energy consumption by the network nodes. This consumption of energy is found to be quicker in CTRUST as well as BTEM method. However, when the proposed methodology of VFDC is incorporated, it is found that the energy consumed is very nominal and will be able to stabilize the system and creates a balance in order to increase the network's life cycle and the overall efficiency of the system.

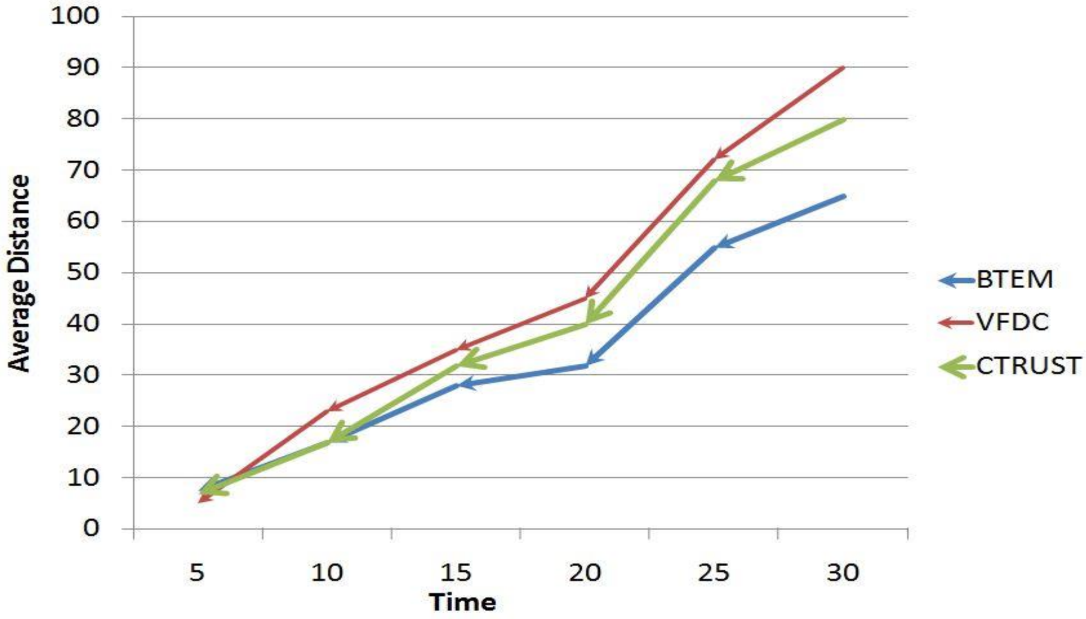

Fig.4. Malicious node detected using different methodologies

5. Conclusion

The limitation of Internet of Things are viewed with a new perspective using the innovative inventions in edge computing. Due to vulnerability to attacks and weakness of security, untrustworthy data is generated. To avoid collecting this, a novel methodology is proposed in the given paper that is dependent on edge computing in Internet of Things which shields the underlying sensor network against attacks. A comprehensive trust evaluation method which is observed from several perspectives are utilized in order to gather only trustworthy data from the sensor nodes. The collection of trustworthy data is done by means of a trustworthy path in an efficient manner. The results observed in this paper show that when virtual force is used, the optimal mobility path is formulated which has high susceptibility to attacks by other malicious nodes within the cluster and the path will also have high trust, to collect trustworthy data. Moreover, when the mobile data collector used is a mobile edge node, it will help to hold a constraint on storage capacity used as well as improve the computing power, when it is weak. Based on these factors, the edge computing framed offers an excellent environment for trustworthy data and underlying common nodes. However, there is much demand for research on trustworthy data collection done in similar mannerism, using IoT.

The future research is focused on accomplishing more systematic and optimistic collection of trustworthy data using edge intelligence. As the advancement in artificial intelligence and edge computing progressing, the network architecture is also changing rapidly to suit the requirement. Though this advancement has given rise to novel techniques and methodologies in the networking perspective, they have also seen challenges in network attacks on edge network. Hence the future scope of this paper lies in identifying the threats and stabilizing the data collected into a more stable platform.

References

[1] B. Huang, W. Liu, T. Wang, X. Li, H. Song, and A. Liu, "Deployment optimization of data centers in vehicular networks," IEEE Access, vol. 7, pp. 20 644–20 663, 2019.

[2] Y. Chen, W. Xu, J. Zuo, and K. Yang, "The fire recognition algorithm using dynamic feature fusion and iv-svm classifier," Cluster Computing, 2018. [Online]. Available: https://doi.org/10.1007/s10586-018-2368-8

[3] T. Wang, L. Qiu, G. Xu, A. K. Sangaiah, and A. Liu, "Energy-e_cient and trustworthy data collection protocol based on mobile fog computing in internet of things," IEEE Transactions on Industrial Informatics, 2019. [Online]. Available: https://doi.org/10.1109/TII.2019.2920277

[4] T. Wang, Y. Liang, W. Jia, M. Arif, A. Liu, and M. Xie, "Coupling resource management based on fog computing in smart city systems," Journal of Network and Computer Applications, vol. 135, pp. 11–19, 2019.

[5] G. Zhang, T. Wang, G. Wang, A. Liu, and W. Jia, "Detection of hidden data attacks combined fog computing and trust evaluation method in sensor-cloud system," Concurrency and Computation: Practice and Experience, 2018. [Online]. Available: https://doi.org/10.1002/cpe.5109

[6] Muneera Begum H, D. A. Janeera, and AG, Aneesh Kumar. "Internet of Things based Wild Animal Infringement Identification, Diversion and Alert System" In Fifth International Conference on Inventive Computation Technologies (ICICT-2020), pp. 672-676. IEEE, 2020.

[7] J. Qi, P. Yang, L. Newcombe, X. Peng, Y. Yang, and Z. Zhao, "An overview of data fusion techniques for internet of things enabled physical activity recognition and measure," Information Fusion, vol. 55, pp. 269– 280, 2019.

[8] Y. Ren,W. Liu, T.Wang, X. Li, N. N. Xiong, and A. Liu, "A collaboration platform for e_ective task and data reporter selection in crowdsourcing network," IEEE Access, vol. 7, pp. 19 238–19 257, 2019.

[9] A. A. Adewuyi, H. Cheng, Q. Shi, J. Cao, A´ . MacDermott, and X. Wang, “Ctrust: A dynamic trust model for collaborative applications in the internet of things,” IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5432–5445, 2019.

[10] A. Sharma, E. S. Pilli, and A. P. Mazumdar, “Rrar: Robust recommendation aggregation using retraining in internet of things,” in 2019 IEEE 5th World Forum on Internet of Things (WF-IoT). IEEE, 2019, pp. 76–80.

[11] R. W. Anwar, A. Zainal, F. Outay, A. Yasar, and S. Iqbal, “Btem: Belief based trust evaluation mechanism for wireless sensor networks,” Future Generation Computer Systems, vol. 96, pp. 605–616, 2019.

[12] Bashar, A. AGRICULTURAL MACHINE AUTOMATION USING IOT THROUGH ANDROID.

[13] Kumar, T. Senthil. "Efficient resource allocation and QOS enhancements of IoT with FOG network." J ISMAC 1 (2019): 101-110.

Authors Biography

Dr.R.Dhaya, works as Professor in the Department of Computer Science, at Sarat Abida Campus -King Khalid University, KSA, her area of research are Sustainable information systems, Wireless Networks, Internet of Things, Computer Networks, Mobile Communication, Software Defined Wireless communication systems, Cyber Physical Systems, Green Data Centers, Cognitive principles and techniques.

Dr.R.Kanthavel, works as professor in the Department of Computer Engineering, at King Khalid University, Abha, KSA his research areas includes Wireless Systems, Communication Networks, Internet of Things ,Sustainable Computing