Intricate Calibrating for Clone Detection in Internet of Things

Harshini C[1] ShashiRekha H[2]

1Fourth Sem M. tech, Department of Studies in CS&E, VTU PG Centre, Mysuru

2Assistant professor, Department of Studies in CS&E, VTU PG Centre, Mysuru

(E-mail:harshinishekar25@gmail.com)

Abstract— The Internet of Things is the developing technology in the smart world which will makes the every activity of the system and humans, in smart way like the home system is now converted to the smart home system ,the hospital system to smart hospital system , In the smart home system scenario the home appliances are integrated with the wireless sensors and these sensors will collect the information of the particular environment and update the collected data to the base station or where these sensors are connected mainly the sensors will form the network that is wireless sensor network in this network the sensors will communicate with each other and exchange the information similarly the smart hospital system has installed the sensors in the patient's body these sensors will collect or monitor the nature of the body like temperature, blood pleasure etc.. and this information are send to the hospital system. These Internet of Things(IoT) devices can be easily captured, by accessing the authorized credential and get the information of the nodes(sensors) of the particular network, and that nodes are cloned or replicated the particular node and that node is manipulated and placed in the network. The clone attack is the very serious threat in the network so to detect these clone attack we have proposed the system to detect the clone nodes using "Multidimensional scaling algorithm" (MDS), this system will detect the clones without the need to know the geological position of the node in the network, this method is suitable for the hybrid network means it works efficient in both static and mobile network and the core part of the clone detection algorithm can be parallelized. The proposed system is auspicious method for the clone detection in Internet of Things(IoT).

Keywords— *Clone Detection, Multidimensional Scaling algorithm, geological position*

I. .INTRODUCTION

The Internet of Things is spreading technology which is used in all sectors of technologies. By this technology the normal activity system is translated into smart system. For example, smart home system is the system which has installed sensors to the home appliances where these home appliances can be operated by the remote places, these sensors are connected to the centralized system. These sensors in the home system will form the wireless sensor network these sensors in network will communicate with each other and the information collected by the sensors are forwarded to the centralized system the make sensors to perform the desired task. Similarly, in the hospital system the sensors are integrated in human body and monitor the body condition and collect that information and then forwarded to the centralized system of the hospital then further process is done by the hospital people. The sensors are most important devices in the Internet of things technology, these devices can be attacked easily by get the authorization configuration and can access the credential details to reprogram the application and placed in the network to get or hack the information which is sending to the destination node. This type of clone attack detecting is very difficult using existing method so the proposed system has the efficient idea for detecting the clone attacks or clone node in the network, it uses the Multidimensional Scaling algorithm for detecting the clone nodes in the particular network, this system works good for hybrid network means the proposed system perform the operation of detecting clone attack in the static and mobile network. The Multidimensional Scaling algorithm(MDS) will create the network map to send the information from the source node to destination node, and this network map is created using the relative neighbour distance information of the nodes. The nodes in the network map will be aware of the its geographical positions. If some intruder introduces the new node to the network, then the algorithm can identify the clone node and inform the base station. The base station will forward the requested data to the destination node using another network route.

The proposed system is capable of identifying the clone nodes in network based on the topography manipulation and does not consider any mobile pattern. The system performs accurate in any network, in the existing clone detection algorithm it works good on static or mobile network. For example: In the smart hospital system the wireless sensors will be installed in the patient body so that the hospital people can monitor the health

condition of particular patient periodically, in this example the patient who has installed the wireless sensors is considered as the mobile network here because the location of the patient will be changing rapidly. On other hand the wireless sensors installed on the home appliances of the smart home system is the static network means the location of the home appliances will not change it is static. In the existing system of the clone detection method the efficiency of detecting clone attack in the different types network will not be same. But in the proposed system the performance of detecting the clone nodes in the any network will be same, it works good on hybrid network (static and mobile network).

II. BACKGROUND

A. Purpose

The main purpose of developing this new Multidimensional dimensional scaling(MDS) clone detection is to identify the clone attack in the network. The Internet of Things devices are most emerging technology which is used in all the areas like the home appliances are converted into smart home appliances which has installed the wireless sensors in the home appliances these sensors will from the network which will collect the data or information periodically and update the information to the centralized system, by using this we can perform the desired task from the remote places. Here in this new system it creates the network map from the source node to destination node using MDS algorithm, this network map is created based on relative neighbour distance information, here each node will be aware of its geographical positions and if any new node is added or any node is cloned then the MDS algorithm can easily identify the cloned node and inform to the base station that the particular node is cloned so that the base station will not forward information to the destination node in that route, the base station will forward the requested information to destination node by another route. The proposed system will make the secure communication between the source and destination node without any clone attack.

III. EXISTING SOLUTION

Internet of Things (IoT) is an emerging networking technology, in which it supports large number of interconnected devices communicate with each other to facilitate communications between people and objects. For example, a smart city is composed of several smart sectors, such as smart homes, smart hospitals, and smart cars, which are significant applications of IoT. While there exists fairly extensive literature on clone attack detection approaches in Wireless sensor network this remains an open problem when it comes to IoT scenarios.

First, there is a lack of accurate geographical position information for the devices. For instance, the devices embedded in smart cars are likely to derive their location information via the car navigation system, i.e., geographical positioning system (GPS), while the devices in a smart home or BSN are unlikely to have embedded GPS capability, owing to its high energy consumption and extra hardware requirements.

Second, IoT networks are hybrid networks composed of both static and mobile devices without a priori mobility pattern (they can be static or moving with high or low velocity), e.g., a patient carrying wearable sensors and living in a smart home.

In fact, IoT nodes are relocatable, without an a priori mobility pattern (they can be static, moving with high velocity, or moving slowly).

There are some disadvantages

- On account of their restricted features and capabilities, IoT devices are vulnerable to several security threats. For example, IoT devices could easily be captured, leading to a clone attack (also known as a node replication attack).
- Moreover, in special cases (e.g., misconfiguration or production by untrusted manufacturers with adversarial intentions) devices that are supposed to be trusted can cause clone attacks.
- A clone attack is extremely harmful, because the clones with legitimate credentials will be considered as legitimate devices. Therefore, such clones can easily perform various malicious activities in the network, such as launching an insider attack (e.g., blackhole attack) and injecting false data leading to hazards in an IoT scenario.
- Although some of the existing clone detection methods for mobile networks could be applied to hybrid networks (composed of both stationary and mobile devices), these suffer from a certain detection probability degradation.

IV. PROPOSED SYSTEM

In this paper, the propose system MDSClone, a novel clone detection mechanism for IoT environments. MDSClone specifically circumvents the two major above-mentioned issues that emerge in IoT scenarios by adopting a multidimensional scaling (MDS) algorithm. In particular, our main contributions are as follows.
This paper propose a clone detection method that does not rely on geographic positions of nodes. Instead, by adopting the MDS algorithm, we generate the network map based on the relative neighbour-distance information of the nodes.

The proposed MDSClone method is capable of detecting clones in the network based on topology distortion, without considering any specific mobility pattern. This is an important

feature of MDSClone, IoT nodes do not follow a particular mobility pattern, and existing clone detection methods for mobile networks do not have reasonable performance in hybrid networks(static and mobile network). Here it creates the network map from source to destination node and the source send the information to the destination node by using this network map and this map is created using MDS algorithm. If the clone node is introduced in the network that clone node if will be identified by the algorithm and then the base station will be updated the information that the clone node is introduced so the base station will stop forwarding the information using that route.

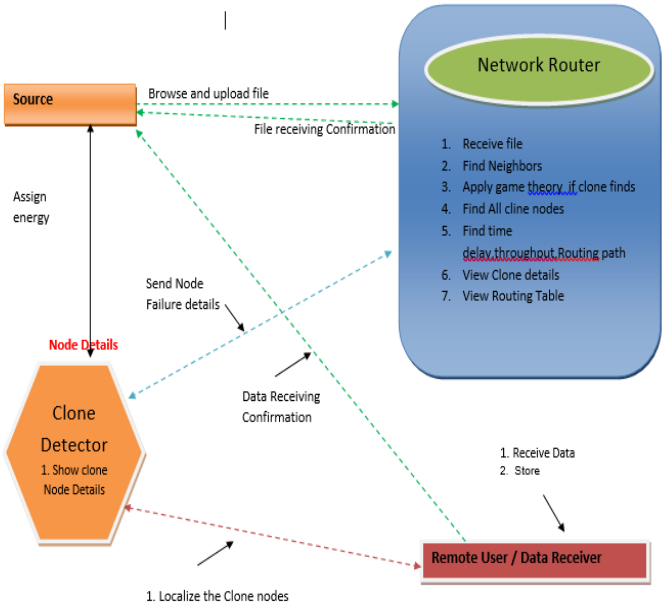

Figure 4.1: Architecture diagram of the proposed system

Advantages of Proposed System

- While most of the state-of-the-art clone detection methods assume that each node is always aware of its geographical position, this assumption does not hold for all the IoT devices. Therefore, by removing such an assumption in MDSClone, we significantly advance the existing clone detection solutions for IoT.
- Compared to the related work, MDSClone method is applicable for all pure static, pure mobile, and hybrid networks, and the detection probability of MDSClone remains the same for all of these network topologies.

We show that MDSClone is efficient in terms of the computational overhead, because the main computation is performed by the base station (BS), and the server-side computation can easily be parallelized to significantly improve the performance. This is an outstanding feature of MDSClone compared to the state-of-the-art, as the parallelization capability of the existing clone detection methods remains unclear.

V. CONCLUSION

In this paper, the proposed system a clone detection solution, called MDSClone, based on the multidimensional scaling (MDS) algorithm for a heterogeneous IoT environment. I have taken into account the specific features of IoT devices in designing MDSClone, i.e., unawareness of geographical positions, the possibility of being both static and mobile, and the lack of a specific mobility pattern. when compared with the existing clone detection methods, MDSClone provides an outstanding approach, because it is the first method that supports hybrid networks, its communication cost is affordable, and it is a location-independent method. Moreover, I have showed that the clone detection probability of MDSClone is almost 100%, and the MDS calculation algorithm could be parallelized, leading to a shorter detection delay. Therefore, considering all of its advantages, MDSClone could be considered as a superior candidate for clone detection in real-world IoT scenarios. However, in the case of dense network topologies, our proposal may impose a communication overhead on the network. The performance of the MDS algorithm to detect the clone node in the network will be same to the all types of network

ACKNOWLEDGMENT

The author would like to thank Dr. K Thippeswamy, Professor and chairman, Dept. of studies in computer science and engineering, VTU Regional office, Mysuru and anonymous reviewers encouragement and constructive piece of advice that of prompted us for new round of rethinking of our research, additional experiments and clearer presentation of technical content

REFERENCES

[1] A. Solanas, C. Patsakis, M. Conti, I. Vlachos, V. Ramos, F. Falcone, O. Postolache, P. Perez-martinez, R. Di Pietro, D. Perrea, and A. Martnez-Balleste, "Smart health: a context-aware health paradigm within smart cities," IEEE Communications Magazine, vol. 52, no. 8, pp. 74– 81, 2014. M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[2] M. Conti, "Clone detection," in Secure Wireless Sensor Networks. Springer, 2016, pp. 75–100.

[3] Z. Chen, F. Xia, T. Huang, F. Bu, and H. Wang, "A localization method for the internet of things," The Journal of Supercomputing, pp. 1–18, 2013.

[4] C.-M.Yu,Y.-T.Tsou,C.-S.Lu,andS.-Y.Kuo,"Localized algorithms for detection of node replication attacks in mobile sensor networks," IEEE Transactions on Information Forensics and Security,, vol. 8, no. 5, pp. 754–768, 2013.

5] O. Bello and S. Zeadally, "Intelligent device-to-device communication in the internet of things," IEEE Systems Journal, vol. 10, no. 3, pp. 1172–1182, 2016.

[6] J. B. Kruskal and M. Wish, Multidimensional scaling. Sage, 1978, vol. 11.

[7] C.-M.Yu,C.-S.Lu,andS.-Y.Kuo,"Efficient and distributed detectionof node replication attacks in mobile sensor

[8] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in IEEE Symposium on Security and Privacy. IEEE, 2005, pp. 49– 63.

[9] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," IEEE Communications Surveys & Tutorials, vol. 8, no. 2, pp. 2– 23.

[10] S. Gaur, "Bringing context awareness to iot-based wireless sensor networks," in PerCom'15. IEEE, 2015.

BIOGRAPHIES

Harshini C presently pursuing her M.Tech degree in department of studies in CSE at Visvesvaraya Technological University, PG Center, Mysuru 570029. She has completed B.E in ISE branch at Vidyavardhaka College of Engineering, Mysuru, Karnataka in the year 2017. Her M.Tech project area is on Internet of Things. This paper is a survey paper of her M.Tech project.

Shashi Rekha H presently working as Asst. Professor in DOS in CS & E , VTU PG Center , Mysuru since 2013. Her qualification is B.E, M.tech, (Ph.D). She has 11 years of teaching experience. She is currently pursuing research in the area of Big Data analytics. Her research interests are Image classification, Pattern recognition, Data Mining in E- healthcare. She has presented many papers in various journals and few conferences. She is a member of CSI, Research Gate Forum.