A Novel IoT Clone Detection Scheme for Hybrid Networks

Madhu M Nayak(Assistant professor , Dept.CSE), Kavya N, Kavya P.C, Kavyashree V, Sushma K.G
Dept. of Computer Science and Engineering
GSSS Institute of Engineering & Technology for Women, Mysuru

Abstract: A IoT is an emerging Networking in which a large number of interconnection devices. Communicate with each other to facilitate people and object Communication. Cloning is a very serious threat in the Internet of Things (IoT), owing to the simplicity for an attacker to gather configuration and authentication credentials from a non-tamper-proof node, and replicate it in the network. Internet of Things has become a victim of this attack since it is very easy for an attacker to collect the information and authentication credentials from a week node in the network. In this paper, we propose CDSH network, The proposed technique is apt for IOT network, because (i) Geographical locations of the nodes is not required to detect the replicas, (ii) this method can be used in hybrid IOT networks that includes both static and mobile nodes and (iii) the core part of the detection rule can be parallelized, which leads to speed-up the entire detection process. Taking all these factors into consideration, we propose this clone detection method as assuring method for a practical node replication detection design in IOT.

Key Words: Node Replication Attack, Internet of Things, Hybrid IOT, Localization via Multidimensional Scaling.

I. INTRODUCTION

Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer. A smart city, for example, consists of several smart sectors, such as smart homes, smart hospitals, and smart cars, which are important IoT applications. Each IoT gadget is equipped with built-in sensors and wireless communication capabilities in a smart home scenario. The sensors can gather information about the environment and communicate with each other, as well as the owner of the house and a central monitoring system. Patients wear implantable sensors that collect body signals and send the data to a local or remote database for further analysis in a smart hospital scenario that could be implemented using body sensor networks .IoT devices are vulnerable to several security threats due to their restricted features and capabilities. IoT devices could easily be captured for example ,resultingin a node replication attack .The captured device is reprogrammed, cloned, and returned to the network in such a scenario. In addition, devices that are supposed to be trusted can cause clone attacks in special cases. In current application nodes can collect real IDs based on encountering information easily since neighbor nodes communicate with real IDs directly. When using real IDs directly, the discloses of node ID to neighbor nodes would create privacy & security concerns. In this paper we deal with 4 dimensional aspects we going to detection of clone. They are Energy, Content, IP address, and Node. A clone attack is extremely harmful because it will be considered as legitimate devices for clones with legitimate credentials. Such clones can therefore easily perform various malicious activities in the network, such as launching an insider attack (e.g. black hole attack) and injecting false data leading to IoT scenario hazards.

1.1 PROBLEM STATEMENT

While there is quite extensive literature on approaches to clone attack detection in WSNs, when it comes to IoT scenarios, this remains an open problem. Two unique characteristics of the IoT environment compared to conventional WSNs make the establishment of clone detection schemes in IoT a more challenging issue. First, the devices lack accurate geographical position information. For example, devices embedded in smart cars are likely to derive location information through the car navigation system, i.e. geographic positioning system (GPS), whereas devices in a smart home or BSN are unlikely to have GPS capability embedded due to their high energy consumption and additional hardware requirements.

Secondly, IoT networks are hybrid networks made up of static and mobile devices with no a priori mobility pattern (they can be static or moving at high or low speeds), e.g. a patient carrying wearable sensors and living in a smart home. Wearable devices could be considered as mobile nodes because the patient can move around while most devices are still in a smart home. Indeed, IoT nodes can be relocated without a priori mobility pattern. While some of the existing clone detection methods for mobile networks could be applied to hybrid networks (consisting of both stationary and mobile devices), they suffer from a degradation of the probability of detection.

II. EXISTING SYSTEM

Internet of Things (IoT) is an emerging networking paradigm, in which a 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 WSNs 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, e.g., a patient carrying wearable sensors and living in a smart home. In fact, IoT nodes are reloadable, without an a priori mobility pattern

2.1 DISADVANTAGES OF EXISTING SYSTEM:

- 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.
- Moreover, in special 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 and injecting false data leading to hazards in an IoT scenario.

III. PROPOSED SYSTEM

We propose CDSH, a novel clone detection mechanism for IoT environments. CDSH specifically circumvents the two major above- mentioned issues that emerge in IoT scenarios by adopting a Clone Detection scheme for Hybrid Network algorithm. We propose a clone detection method that does not rely on geographic positions of nodes. Instead, by adopting the CDSH algorithm, we generate the network map based on the relative neighbor-distance information of the nodes.

3.1. 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 CDSH, we significantly advance the existing clone detection solutions for IoT.
- Compared to the related work, CDSH method is applicable for all pure static, pure mobile, and hybrid networks, and the detection probability of CDSH remains the same for all of these network topologies.
- We show that CDSH 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 CDSH compared to the state-of-the-art, as the parallelization capability of the existing clone detection methods remains unclear.

IV. SYSTEM REQUIREMENTS

HARDWARE REQUIREMENTS:

- System : Pentium Dual Core.
- Hard Disk : 120 GB.
- Input Devices : Keyboard, Mouse
- Ram : 1 GB

SOFTWARE REQUIREMENTS:

- Operating system : Windows 7.
- Coding Language : JAVA/J2EE
- Tool : Eclipse, Java JDK
- Database : MYSQL

V. SYSTEMARCHITECTURE

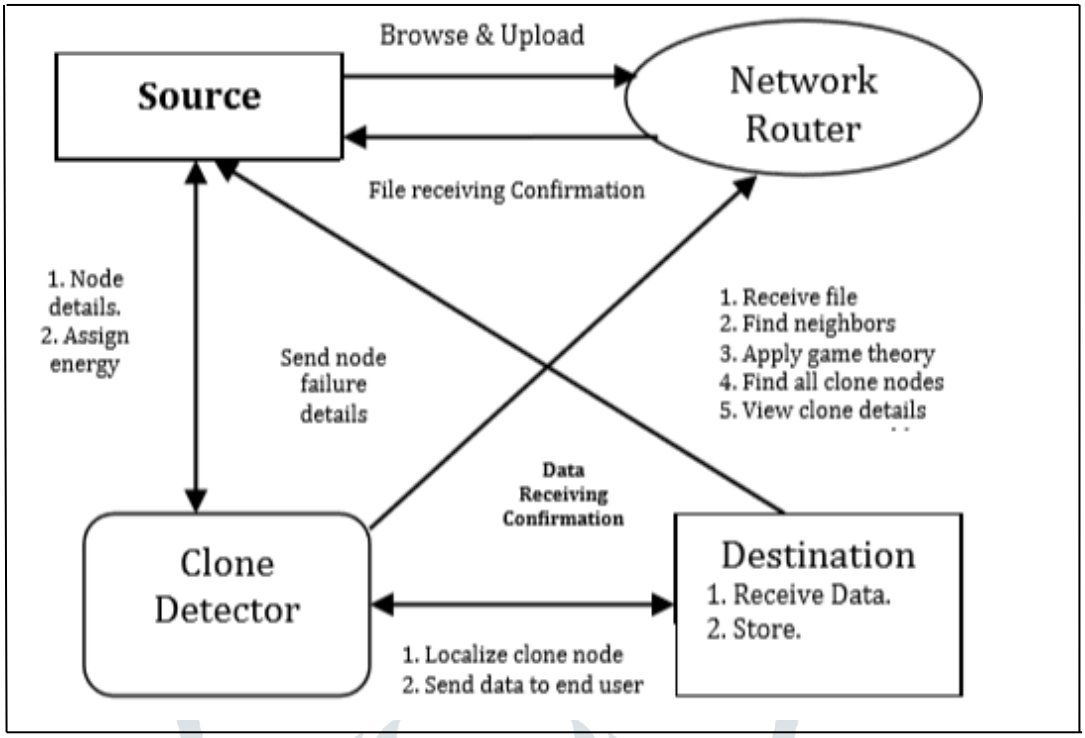

FIG 2.1. Proposed System Architecture

VI. IMPLEMENTATION

A Clone Detection Scheme for Hybrid (CDSH) Network is a way to visualize the similarity level of a dataset's individual cases. It refers to a set of related ordering techniques used in the visualization of information, especially to display the information contained in a distance matrix. It is a form of reduction of non-linear dimensionality. An CDSH algorithm is intended to place each object in N-dimensional space so as to preserve as well as possible the distances between the objects. In each of the N dimensions, each object is then assigned coordinates. An CDSH plot N's number of dimensions can exceed 2 and is a priori specified. In each of the N dimensions, each object is then assigned coordinates. An CDSH plot N's number of dimensions can exceed 2 and is a priori specified. Choosing N=2 optimizes a two-dimensional scatter plot for object locations.

Suppose there are n randomly distributed nodes for which distance is known between each pair of sensor nodes, then estimate position of unknown node Clone Detection Scheme Law of Cosines and linear algebra which helps to reconstruct relative node positions on the basis of pair wise distances. The technique can be performed using an algorithm with the following four steps:

1. Collect data from the network and create a distance matrix X, where xij is the range between i and j nodes.
2. To develop a complete matrix of internodes distances R, execute an algorithm to determine the shortest path for example Dijkstra, Floyd etc on X.
3. To find estimated node positions P, run a classical metric CDSH on X,
4. Transforming the metric P solution into global coordinates.

Following are the modules present in the system

- **Source**

In this module, the Sender will browse the file, Initialize the nodes, distribute Mac address for every node and then upload to the particular Receiver (receiver1, receiver2, receiver3 and receiver4). And router will connect to the particular receiver. After receiving successfully, it will give response to the sender. The Sender can have capable of manipulating the data file.

- **Router**

The Router manages a multiple node (node A, node B, node C, node D, node E, node F….) to provide data storage service. In a router we can view the node details, assign cost and view clones. The sender will upload data file to the router, the Router will select the smallest distance path and send to the particular receiver. If any clone is found in a particular node, the route replay will send to the Trusted Authority and then it will select another path. In a router service provider can view the node information details and view the routing table details.

- **Trusted Authority**

In this module, the Trusted Authority is responsible for identify the intrusion in the network. If the router found any type of clones, then it transfers the flow to Trusted Authority. Then the Trusted Authority is responsible for capturing the clones and identifies which type of clone (fake key clone, Destination IP clone and cost clone) and then response will send to the router. After getting a response from the TA, router will select another path and send to the particular receiver (receiver1, receiver2, receiver3 and receiver4). The Trusted Authority will make a list of failed node details and then all failed nodes are stored with tags such as node name, IP address, MAC address, node cost, time and date.

- **Receiver**

In this module, there are an n-numbers of receivers are present (receiver1, receiver2, receiver3 and receiver4). All the receivers can receive the data file from the sender via router. The sender will send data file to router and router will select the lesser distance path and send to the particular receiver (receiver1, receiver2, receiver3 and receiver4), without changing any file contents. The receivers may try to receive data files within the router or network only.

- **Clone**

In this module, the clone can attack the node in three ways fake node clone, Destination IP clone and cost clone. Fake key clone means he will inject fake key to the particular node; IP clone means he will change the destination IP address to the particular node, cost clone means he will inject fake cost to the particular node.

VII.EXPECTED RESULTS

While most state-of-the-art methods of clone detection assume that each node is always conscious of its geographical position, this assumption does not apply to all IoT devices. Therefore, we are significantly advancing the existing clone detection solutions for IoT by removing such an assumption in CDSH Network. CDSH Network method is applicable to all pure static, pure mobile, and hybrid networks compared to the related work, and CDSH Clone's detection probability remains the same for all these network topologies. We show that CDSH Clone is efficient in terms of computational overhead, because the base station (BS) performs the main computation, and the computation on the server side can be easily parallel to significantly improve performance. Compared to the state-of- the-art, this is an outstanding feature of CDSH Clone, as the parallelization capability of existing clone detection methods remains unclear.

VIII. CONCLUSION

In this paper, we have proposed a clone detection solution, called CDSH Clone, based on the CDSH algorithm for a heterogeneous IoT environment. We have taken into account the specific features of IoT devices in designing CDSH Clone, i.e., unawareness of geographical positions, the possibility of being both static and mobile, and the lack of a specific mobility pattern. We showed (in Table I) that compared with the existing clone detection methods, CDSH Clone provides an outstanding approach, because it is the first method that supports hybrid networks, while its memory cost is of order O(1), its communication cost is affordable, and it is a location-independent method. Moreover, we showed that the clone detection probability of CDSH Clone is almost 100%, and the four dimensional scaling calculation algorithms could be parallelized, leading to a shorter detection delay. Therefore, considering all of its advantages, we believe that CDSH Clone could be considered as a superior candidate for clone detection in real-world IoT scenarios.

REFERENCES

[1] M. Conti, R. Di Pietro, and A. Spognardi, “Clone wars: Distributeddetection of clone attacks in mobile wsns,” Journal of Computer andSystem Sciences, vol. 80, no. 3, pp. 654–669,2014.

[2] A. K. Mishra and A. K. Turuk, “A comparative analysis of node replicadetection schemes in wireless sensor networks,” Journal of Network andComputer Applications, vol. 61, pp. 21–32,2016.

[3] M. Dong, K. Ota, L. T. Yang, A. Liu, and M. Guo, “Lscd: A low-storageclone detection protocol for cyber-physical systems,” IEEE Transactionson Computer-Aided Design of Integrated Circuits and Systems, vol. 35,no. 5, pp. 712–723,2016.

[4] Z. Zheng, A. Liu, L. X. Cai, Z. Chen, and S. X. (Shermen), “Ercd: Anenergy-efficient clone detection protocol inwsns,” in INFOCOM’13.IEEE,2013.

[5] M. Conti, R. Di Pietro, and A. Spognardi, "Clone wars: Distributeddetection of clone attacks in mobile wsns," Journal of Computer andSystem Sciences, vol. 80, no. 3, pp. 654–669, 2014.

[6] A. K. Mishra and A. K. Turuk, "A comparative analysis of node replicadetection schemes in wireless sensor networks," Journal of Network andComputer Applications, vol. 61, pp. 21–32, 2016.

[7] W. T. Zhu, J. Zhou, R. H. Deng, and F. Bao, "Detecting node replicationattacks in wireless sensor networks: a survey," Journal of Network andComputer Applications, vol. 35, no. 3, pp. 1022–1034, 2012.

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

[9] Z. Chen, F. Xia, T. Huang, F. Bu, and H. Wang, "A localization methodfor the internet of things," The Journal of Supercomputing, pp. 118,2013.

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