International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

MDS Clone: Multidimensional Scaling Aided Clone Detection in Internet of Things

Kshama K B Giri[1]
M Tech, CSE
Dept. of Computer Science and Engineering
PESCE, Mandya

Mamatha B. S[2]
Associate professor, CSE
Dept. of Computer Science and Engineering
PESCE, Mandya

Abstract:- **Node replication attack is a very serious type of attack using which an attacker can affect the operations of the network by inserting a replica or clone 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 MDSClone, a novel clone detection method based on multidimensional scaling (MDS). MDSCloneappears to be very well suited to IoT scenarios, as it (i) detects clones without the need to know the geographical positions of nodes, and (ii)this method can be used in hybrid IOT networks that includes both static and mobile node, for which no mobility pattern may be assumed a priori. Moreover, a further advantage of MDSClone is that (iii) the core part of the detection algorithm can be parallelized, resulting in an acceleration of the whole detection mechanism.Taking all these factors into consideration, we propose this clone detection method as assuring method for a practical node replication detection design in IOT.**

Keywords— MDS Clone, IoT, Clone Attack, Hybrid Network.

I. INTRODUCTION

Association rule mining is an emerging research in data 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 [1]. For example, a smart city is composed of several smart sectors, such as [2] smart homes, smart hospitals, and smart cars, which are significant applications of IoT. In a smart home scenario, each IoT gadget is equipped with embedded sensors and wireless communication capabilities. The sensors are able to gather environmental information and communicate with each other, as well as the house owner and a central monitoring system. In a smart hospital scenario, which could be implemented using body sensor networks (BSN), patients wear implantable sensors that collect body signals and send the data to a local or remote database for further analysis. As another example, in a smart traffic scenario embedded sensors in cars are able to detect accident events or traffic information, and collaboratively exchange such information.

Problem Statement:

While there exists fairly extensive literature on clone attack detection approaches in WSNs, this remains an open problem when it comes to IoT scenarios. In particular, compared with conventional WSNs, two unique characteristics of IoT environment make the establishment of clone detection schemes in IoT a more challenging issue. 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 carnavigation 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.

Secondly, IoT networks are hybrid networks composed of both static and mobile devices without a priori mobility pattern (they can be s atic or moving with high or low velocity), e.g., a patient carrying wearable sensors and living in a smart home. Wearable devices could be considered as mobile nodes, because the patient may move around, while most of the devices in a smart home are immobile. In fact, IoT nodes are relocatable, without an a priori mobility pattern (they can be static, moving with high velocity, or moving slowly) . 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. In what follows, we explain how we address these challenges and advance the state-of-the-art solutions in detecting clone attacks.

II. LITERATURE SURVEY

“Bringing context awareness to iot-based wireless sensor networks” (S. Gaur 2015) In this paper, researchers have proposed several classifications for clone detection approaches based on the information required (i.e., location-based or location-independent), methods of detection (i.e., centralized, distributed or partially distributed) and network type support (i.e., mobile or static networks). Our proposed approach to MDS Clone falls within the category of centralized location-independent methods that support hybrid (static and mobile) networks.

“Smart health: a context-aware health paradigm within smart cities”(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 2014) In this paper, they proposed alternative clone detection approaches, such as social fingerprints. A key issue in the security of the sensor network is that sensors are susceptible to physical capture attacks. The adversary can easily launch clone attacks once a sensor is compromised by replicating the compromised node, distributing the clones across the network, and starting a variety of insider attacks. Previous work against clone attacks has either a high overhead of communication / storage or poor accuracy of detection.

"A survey of security issues in wireless sensor networks" (Y. Wang, G. Attebury, and B. Ramamurthy) In this paper, they proposed an alternative approach, such as pre distributed keys, to detect clones. Because of their low overhead, random key pre-distribution safety schemes are well suited for use in sensor networks. However, cloning attacks can compromise a network's security using pre distributed keys. Opponents breaks into a sensor node in this attack, reprogram it, and inserts several node copies back into the sensor network.

"Security considerations in the ip-based internet of things" (O. Garcia-Morchon, S. Keoh, S. Kumar, R. Hummen, and R. Struik, 2012) In this paper, researches suggested an alternative approach, such as random clustering, to detect clones. Sensor nodes are vulnerable to capture and compromise when deployed in hostile environments. An opponent may obtain, clone, and intelligently deploy private information from these sensors in the network to launch a variety of insider attacks. This process of attack is widely referred to as a clone attack.

III. METHODOLOGY

A. System Architecture

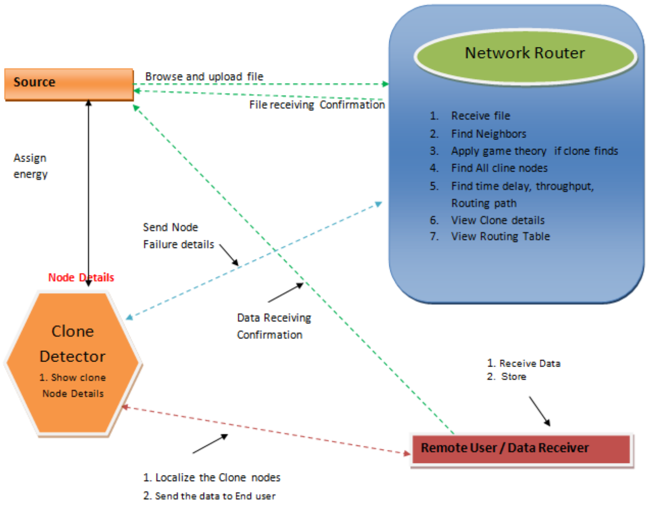

Network Router
Source
Browse and upload file
File receiving Confirmation
1. Receive file
2. Find Neighbors
3. Apply game theory if clone finds
4. Find All cline nodes
5. Find time delay, throughput, Routing path
6. View Clone details
7. View Routing Table
Assign energy
Send Node Failure details
Node Details
Clone Detector
1. Show clone Node Details
Data Receiving Confirmation
1. Receive Data
2. Store
Remote User / Data Receiver
1. Localize the Clone nodes
2. Send the data to End user

Fig 1: System Architecture

Sender: In this module, the Sender will browse the file, Initialize the nodes, distribute Mac address for every node and then upload to the particular Receivers (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 nodes (node A, node B, node C, node D, ….) to provide data storage service. In a router we can view the node details, assign cost and view clones. 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.

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.

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.

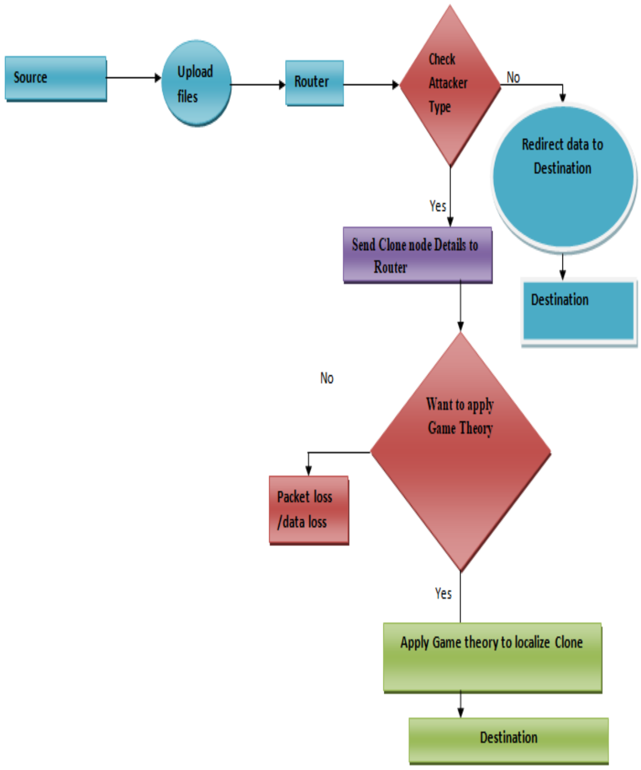
B. Algorithm

```
• Step 1: Input- Neighbour Node distance Information
  at i, DT: Distortion Threshold
• Step 2: Initialize BS
• Step 3: from i-1……….n number nodes
• Step 4: Calculate distance b/w nodes i,j
• Step 5: Update distance matrix D
• Step 6: if DT(N,I,E,C)-True
• Step 7: for i-1……n
• Step 8: Reconstruct matrix X
• Step 9: calculate neighbour node distance L at BS
• Step 10: Update distance matrix D
• Step 11: X- MDS[DT(N,I,E,C)
• Step 12: Select coolest data R
• Step 13: send packets P
      else
      select coolest data R

                    send packets P
• Step 14: Update routing table T
```

Where BS -Base Station, n- number of nodes, d- distance between nodes i,j, D-Distance matrix, X-Reconstructed matrix, DT-Distortion Threshold, L-Neighbour node distance Information given by BS, R-route or Data, P-packets, T-Routing table.

IV. FLOW CHART


Source
Upload files
Router
Check Attacker Type
No
Redirect data to Destination
Yes
Send Clone node Details to Router
Destination
No
Want to apply Game Theory
Packet loss /data loss
Yes
Apply Game theory to localize Clone
Destination

V. RESULTS & DISCUSSION

In this paper, we propose 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.

1) We 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 neighbor-distance information of the nodes. 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 forIoT.

2) Our 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, since as explained earlier, 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 (for more details please refer to Section II). 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.

3) 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.

4) Along with the main MDSClone algorithm, we also propose three techniques (i.e., CIPMLO, TI, and SMEBM) to speed up the core part of MDSClone, which comprises the MDS calculation.

5) We provide a thorough evaluation of our proposed method considering different evaluation criteria, i.e., the clone detection probability and computation time of our algorithm when adopting our proposed speed-up methods. Moreover, we provide analytical and experimental comparisons of MDSClone with state-of-the-art clone detection methods. Our reported experimental results exhibit a perfect detection of clone nodes in the network, requiring a constant amount of memory and a reasonable communication overhead.

IV.CONCLUSION

In this paper, we have proposed a Multidimensional scaling algorithm for both static and dynamic IoT environment, MDS clone provides outstanding approach, because it is the first method to support heterogeneous environment and it is location-independent method. Also MDS Algorithm leads to a shorter detection delay. Considering all of its advantages, we believe that MDS clone can be consider as a superior clone detection method in IoT scenario. However, our proposal may impose a communication overhead on the network in the case of dense network topologies. Hence, we aim to provide a distributed version of MDSClone for IoT scenarios in future work.

REFERENCES

[1] S. Gaur, “Bringing context awareness to iot-based wireless sensor networks,” in PerCom’15. IEEE, 2015.

[2] 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.

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

[4] O. Garcia-Morchon, S. Keoh, S. Kumar, R. Hummen, and R. Struik, “Security considerations in the ip-based internet of things,” 2012. [Online]. Available: https://tools.ietf.org/html/ draft-garcia-core-security-04

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

[6] M. Conti, “Clone detection,” in Secure Wireless Sensor Networks. Springer, 2016, pp. 75–100.

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

[8] W. T. Zhu, J. Zhou, R. H. Deng, and F. Bao, “Detecting node replication attacks in wireless sensor networks: a survey,” Journal of Network and Computer Applications, vol. 35, no. 3, pp. 1022–1034, 2012.

[9] 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.

[10] 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.

[11] C.-M. Yu, Y.-T. Tsou, C.-S. Lu, and S. 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.

[12] C.-M.Yu,C.-S.Lu,and S.-Y. Kuo,“Efficient and distributed detection of node replication attacks in mobile sensor networks,” in VTC’09. IEEE, 2009.

[13] K. Xing and X. Cheng, “From time domain to space domain: Detecting replica attacks in mobile ad hoc networks,” in INFOCOM’10, 2010.