MDSClone: Multidimensional Scaling Aided Clone Detection in Internet of Thing

Mr. S. Sivaprakash
M.E.,(Ph,D).,[1],
[1] Assistant Professor
Department of Computer Science and Engineering,
K.S.R College of Engineering
Tiruchengode, India.

P. Yokabalaji[2], T. Prakash[3],
V. Rajeswari[4], K. Sridhar[5],
[2,3,4,5] UG Students
Department of Computer Science and Engineering,
K.S.R College of Engineering
Tiruchengode, India.

Abstract*: - 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. In this paper, we propose MDSClone, a novel clone detection method based on multidimensional scaling (MDS). MDSClone appears to be very well suited to IoT scenarios, as it: 1) detects clones without the need to know the geographical positions of nodes; 2) unlike prior methods, it can be applied to hybrid networks that comprise both static and mobile nodes, for which no mobility pattern may be assumed a priori. Moreover, a further advantage of MDSClone is that 3) the core part of the detection algorithm can be parallelized, resulting in an acceleration of the whole detection mechanism. Our thorough analytical and experimental evaluations demonstrate that MDSClone can achieve a 100% clone detection probability. Moreover, we propose several modifications to the original MDS calculation, which lead to over a 75% speed up in large scale scenarios. The demonstrated efficiency of MDSClone proves that it is a promising method towards a practical clone detection design in IoT.

1. INTRODUCTION

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. 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. In current MOSN applications, nodes can collect real ID based encountering information easily since neighbor nodes communicate with real IDs directly. We define two nodes as neighbor nodes when they are within the communication range of each other. However, when using real IDs directly, the disclosure of node ID to neighbor nodes would create privacy and security concerns. For example, a malicious node can first know the IDs of some central nodes or nodes with specific interests. Then, as shown in Figure 1(a), when neighbor nodes communicate with real IDs, a malicious node can easily identify attack targets from neighbors and launch attacks to degrade the system performance or steal important documents. Further, without protection, malicious nodes can also easily sense the encountering between nodes for attacks.

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). In such a scenario, the captured device is reprogrammed, cloned, and placed back in the network. 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

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 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. 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.

2. RELATED WORK

In recent years, owing to the increasing interest in adopting WSNs in several applications, there has been a surge of interest in providing WSN-specific security solutions, amongst which clone attack detection has attracted significant attention. In this section, we review the clone detection methods that are most closely related to our work, and clarify the difference between our proposal and the existing related work.

Researchers have proposed several classifications for clone detection approaches based on the required information (i.e., location-based or location-independent), detection methods (i.e., centralized, distributed, or partially distributed), and supporting network type (i.e., mobile or static networks). Our proposed MDSClone approach falls in the category of location-independent centralized methods supporting hybrid (both static and mobile) networks. We believe that the centralized nature of MDSClone is not a drawback, considering the emerging municipality-scale IoT networking technologies such as NarrowBand-Internet of Things (NB-IoT) and LoRaWAN. Indeed, a centralized security monitoring solution is perfectly inline with the hierarchical architecture fostered by such technologies, which are currently being supported by key players, including among others Cisco and Orange. For instance, the current LoRaWAN deployment being developed in the city of Rome concentrates all IoT sensor traffic collected by several tens of radio stations spread across the whole of the Rome municipality and relevant neighbors in a (logically) single centralized network server, which therefore appears to be a natural candidate to further host anomaly detection approaches such as MDSClone.

In the case of static networks, a popular approach for detecting clones is witness finding. In essence, the idea behind witness finding is that the existence of clones must lead to location conflicts. More specifically, each node u collects the location information, L(v), of its neighboring nodes, e.g., v, and sends the collected location claims hv;L(v)i to some selected nodes. Nodes receiving two location claims with the same ID v, but with two distinct locations, will serve as witness nodes, and witness the location conflict. The witness finding strategy not only detects the existence of clones, but also identifies the clone IDs.

A network-wide broadcast is the simplest way to find a witness, but this incurs a prohibitive communication cost. In, the authors proposed two approaches, randomized multicast (RM) and line-selected multicast (LSM), in order to reduce the communication costs of network-wide broadcasts. Two other approaches proposed in, i.e., single deterministic cell (SDC) and parallel multiple probabilistic cells (P- MPC), share the same spirit as RM and LSM. However, SDC and P-MPC are only efficient when the network is partitioned into cells. Compared with the aforementioned approaches, the protocol proposed in, i.e., the randomized, efficient, and distributed (RED) protocol, provides an almost- perfect guarantee of clone detection. RED utilizes a special centralized broadcasting device, such as a satellite and UAV, in order to periodically broadcast the node IDs responsible for detecting particular conflicting location claims. In another study, Zhang et al. proposed four clone detection methods that take advantage of double ruling and the Bloom filter. Recently, Dong et al. proposed the low-storage clone detection (LSCD) method, taking into account the memory requirements and residual energies of nodes. An inherent weakness among all of the witness finding-based approaches is the assumption of the knowledge of location information available for each node. A couple of solutions take alternative approaches to detect clones, such as the social fingerprint, predistributed keys, and random clustering methods.

In the case of mobile sensor networks, by using a simple challenge-and- response strategy, XED presents the first distributed clone detection method for mobile networks. However, it is vulnerable to collusions of the cloned nodes. EDD is a distributed clone detection method based on the discrepancy between the distributions of the numbers of encounters with clone and ordinary nodes. In a base station (BS) collects the geographical positions of nodes, looking for a clone moving with a speed exceeding the pre- configured speed limit. In, the same idea is employed, but the ordinary nodes play the role filled by the BS in.

We argue that, although most existing clone detection methods proposed for mobile networks could be applied to hybrid networks as well, this adoption will degrade the security and clone detection probability. The clone detection methods for mobile networks that do not (fully) rely on velocity violations include XED, EDD, TDD, SDD-LC, SDD-LWC, and HIP-HOP. The reason that XED and EDD suffer from a security degradation when applied to hybrid networks is that clones that are aware of the positions of static nodes can either choose not to enter the proximity of static nodes, or to enter at certain time slots. If so, static nodes in XED do not have a chance to exchange secret information with different clones. Moreover, in EDD the number of times that each static node will encounter a clone 3 node will be controlled by clones. Therefore, if clones adopt the above evasion strategy, then only the mobile nodes (rather than both static and mobile nodes) will be able to detect clones, reducing the probability of clone detection. On the other hand, the detection effectiveness of TDD, SDD-LC, and SDD-LWC partly relies on whether each node encounters a particular node too many times (similarly to EDD). As a consequence, if the clones adopt the above-mentioned evasion strategy, then the detection capabilities of the TDD, SDD-LC, and SDD-LWC methods will also be degraded. In addition, the HIP- HOP approach detects clones based on the fact that if two witness nodes are either one-hop or two-hop neighbors, then either the witness nodes or the node connecting two witness nodes will find the location conflict of clones. However, if witness nodes far away from each other happen to both be static, then they have no chance of being either one-hop or two-hop neighbors, thus reducing the probability of clone detection.

3. PROBLEM STATEMENT

3.1 EXISTING MODEL

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.

3.1.1 Drawbacks

First, there is a lack of accurate geographical position information for the devices.

3.2 PROPOSED SYSTEM

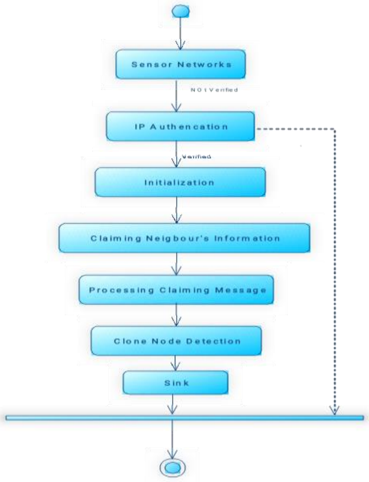
we propose MDSClone, a novel clone detection mechanism for IoT environments. MDSClone specifically circumvents the two major above- mentioned issues that emerge in IoT scenarios by adopting a multidimensional scaling (MDS) algorithm.

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.

3.2.1 Advantages Of Proposed System

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

3.2.2 Flow Diagram



4.0 METHODOLOGY

Network Model

We consider an IoT network as a hybrid network consisting

of two main entities: 1) n static and mobile nodes with unique IDs: ID 2 f1; : : :

; ng; and 2) a base station (BS). Each IoT device periodically measures its distance with its neighboring nodes, and sends the information to the BS. In our system model, the BS is in charge of executing our proposed MDSClone algorithm and locating the “clones” (for a definition please refer to Section III-B) in the network. In particular, the BS periodically receives neighboring information for each node in the network, and constructs a location map (based only on the information received from the nodes) in order to detect clones (we explain the details of the MDSClone algorithm in Section V-A). The BS executes MDSClone offline, and each generated location map is dedicated to a snapshot of the network at time t. The main idea in our proposed method is that at time t, a node x cannot have two different sets of neighbors, which means that x cannot be in two different locations of the network at time t. In our network model, we make the following assumptions:

We assume that nodes are not “necessarily” aware of their exact geographical position. This assumption is based on the following two factors explained in the existing literature: i) As explained in, using GPS is costly in terms of energy and the requirements for extra hardware, and ii) researchers believe that GPS-based positioning is not efficient in indoor scenarios. Therefore, we assume that some nodes (e.g., smartphones) may be GPS- enabled, and others (e.g., home appliances) may not. Hence, our proposed method does not rely on geographical positions of nodes. This assumption is to address the first challenge that we mentioned in the“Problem Statement” Section, i.e., lack of accurate geographical position information of the devices.

We assume that mobile nodes are moving without any particular mobility pattern. This assumption makes our network model more realistic, because the mobility patterns of nodes (e.g., wearable sensors) in IoT scenarios are unpredictable, as explained in. We make this ssumption to consider the second challenge that we mentioned in the the "Problem Statement" Section, i.e., IoT networks are hybrid networks composed of both static and mobile devices without a priori mobility pattern.

We also assume that IoT devices are capable of enacting short-range device-to-device communication (as explained in). Therefore, each node can measure its distance from its neighboring nodes via radio signal strength (RSS) or time of arrival (ToA) (as comprehensively discussed in). Although the estimated distances are not perfectly accurate, they are sufficient for our approach. We make this assumption, as in our proposed approach, each IoT device should periodically measure its distance with its neighboring nodes and send to the BS.

We assume that the BS knows the geographic positions of IoT devices at the very beginning (only during the initialization of the network). However, after the network deployment, the BS is no longer aware of the positions of the devices. We make this assumption because the setup and deployment of IoT devices in the network are generally performed by the network designer, and so it is reasonable to adopt such an assumption. This assumption helps the BS in detecting and locating the clone nodes by comparing the constructed location map by the information received from the nodes and the original network map.

We also assume that there exists a loose time synchronization between the nodes1, and the network operation time is divided into time intervals, each of which has the same length. These assumptions are in line with other clone detection methods]. We make this assumption since each generated location map is dedicated to a snapshot of the network at time t.

We assume that the exchanged messages are digitally signed2 before being sent out, unless stated otherwise. We have studied the practicality and efficiency of such operations in. We make this assumption to ensure the confidentiality and accuracy of the exchanged neighboring information, based on which the location map will be generated.

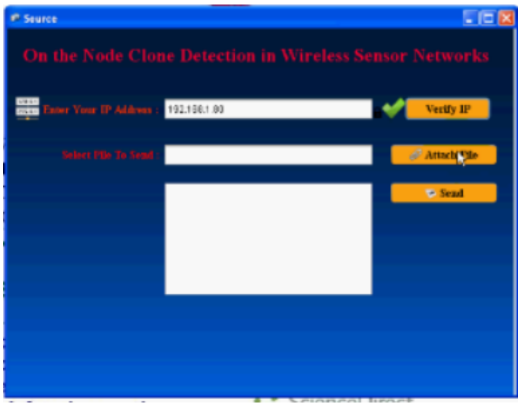
Attack Model

IoT devices are usually considered not to be tamper-resistant [34]. In other words, the stored security credentials can all be extracted in the case of a device bein compromised. Moreover, the adversary can compromise a device immediately after the node deployment. No secure bootstrapping time is available. Thus, the adversary can access all of the legitimate credentials of the compromised devices. In this paper, we consider an adversary that is capable of performing "clone attack", meaning that they are able to fabricate compromised devices and store the legitimate credentials from the compromised devices inside several fabricated devices, which is (consistent with related work on clone detection such as). A compromised node, as well as the fabricated nodes that have the same ID and credentials as the compromised node, are called clones. Clones can communicate and collude with each other, attempting to subvert the detection functionality in a stealthy manner. It should be noted that we only consider cloning attacks, and we assume there is no concurrent "node compromise" attack, meaning that no other nodes (beyond the clones) act in a malicious manner.

Multidimensional Scaling

Multidimensional scaling (MDS) is a hyperspace embedding technique, through which pairwise distances are
fit into a set of coordinates with the preservation of distance
restrictions. More concretely, MDS takes a distance matrix D as input, which is formed from the distances between all pairs of nodes. The output of MDS is a set of coordinates created using only D.

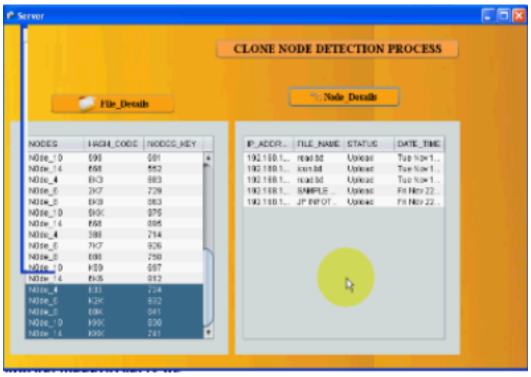
4.2 SAMPLE OUTPUT


Source

On the Node Clone Detection in Wireless Sensor Networks

Enter Your IP Address : 192.168.1.80

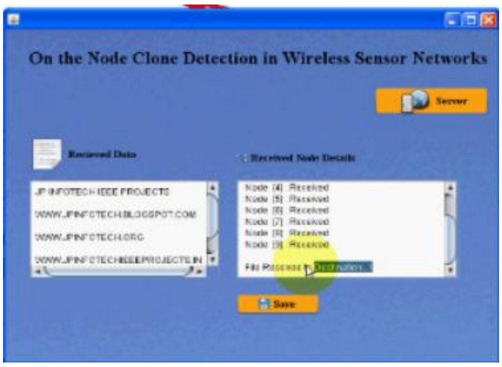
Select File To Send :


Server

CLONE NODE DETECTION PROCESS

NODES	HASH_CODE	NODES_KEY
NOde_10	699	691
NOde_14	888	552
NOde_4	8K3	883
NOde_6	2K7	729
NOde_8	8K8	863
NOde_10	9KK	876
NOde_14	888	895
NOde_4	388	714
NOde_6	7K7	926
NOde_8	888	750
NOde_10	K99	867
NOde_14	8K8	812
NOde_4	833	724
NOde_6	K2K	832
NOde_8	88K	841
NOde_10	KKK	830
NOde_14	KKK	741

IP_ADDR...	FILE_NAME	STATUS	DATE_TIME
192.168.1...	read.txt	Upload	Tue Nov 1...
192.168.1...	icon.txt	Upload	Tue Nov 1...
192.168.1...	read.txt	Upload	Tue Nov 1...
192.168.1...	SAMPLE ...	Upload	Fri Nov 22...
192.168.1...	JP INFOT...	Upload	Fri Nov 22...


On the Node Clone Detection in Wireless Sensor Networks

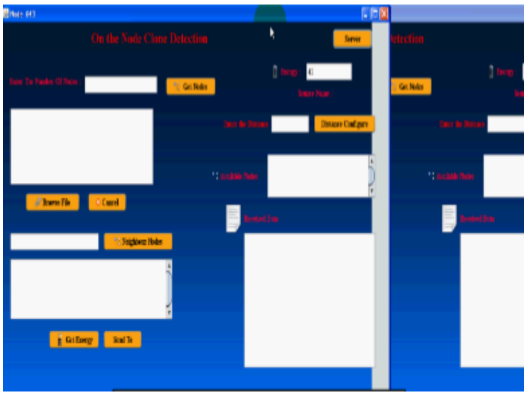
Received Data

```
JP INFOTECH IEEE PROJECTS
WWW.JPINFOTECH.BLOGSPOT.COM
WWW.JPINFOTECH.ORG
WWW.JPINFOTECHIEEEPROJECTS.IN
```

Received Node Details

```
Node [4] Received
Node [5] Received
Node [6] Received
Node [7] Received
Node [8] Received
Node [9] Received

File Received to Destination
```


Node 643

On the Node Clone Detection

Enter The Number Of Nodes :

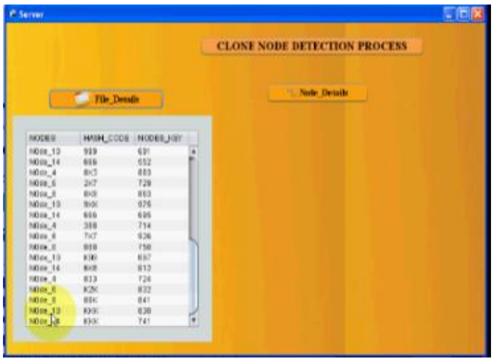
Energy : 41

Source Name :

Enter the Distance

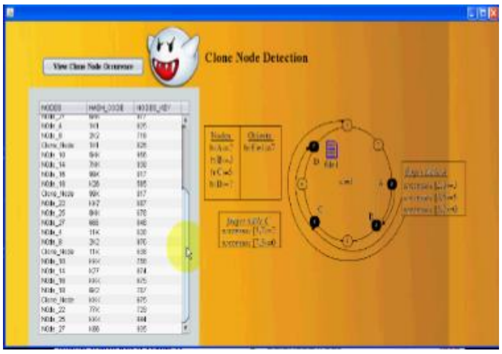
Available Nodes

Received Data


Server

CLONE NODE DETECTION PROCESS

NODES	HASH_CODE	NODES_KEY
NOde_13	999	691
NOde_14	666	652
NOde_4	8K3	883
NOde_6	2K7	729
NOde_8	8K8	863
NOde_13	9KK	876
NOde_14	666	695
NOde_4	388	714
NOde_6	7K7	936
NOde_8	888	758
NOde_13	K99	667
NOde_14	8K8	812
NOde_4	833	724
NOde_6	K2K	832
NOde_8	88K	841
NOde_13	KKK	838
NOde_1[illegible]	KKK	741


Clone Node Detection

NODES	HASH_CODE	NODES_KEY
NOde_[illegible]	[illegible]	[illegible]
NOde_4	1K1	825
NOde_8	2K2	716
Clone_Node	1K1	828
NOde_10	6KK	666
NOde_14	7KK	936
NOde_18	98K	817
NOde_18	K26	585
Clone_Node	98K	817
NOde_22	KK7	687
NOde_25	8KK	676
NOde_27	666	848
NOde_4	11K	830
NOde_8	2K2	670
Clone_Node	11K	638
NOde_10	KKK	756
NOde_14	K7F	674
NOde_18	KKK	675
NOde_18	6K2	727
Clone_Node	KKK	675
NOde_22	77K	729
NOde_25	KKK	444
NOde_27	K66	605

6. CONCLUSION

In this paper, we have proposed a clone detection solution, called MDSClone, based on the multidimensional scaling (MDS) algorithm for a heterogeneous IoT environment. We 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. We showed (in Table I) that compared with the existing clone detection methods, MDSClone 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 MDSClone is almost 100%, and the MDS calculation algorithm could be parallelized, leading to a shorter detection delay. Therefore, considering all of its advantages, we believe that 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. Therefore, in future work we aim to provide a distributed version of MDSClone for IoT scenarios.

7. REFERENCE

[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 & 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.

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

[15] Y. Shang, W. Ruml, Y. Zhang, and M. P. Fromherz, “Localization from mere connectivity,” in MobiHoc’03. ACM, 2003, pp. 201–212.

[16] Narrow Band Internet of Things (NB- IoT). [Online]. Available: http://www.gsma.com/connectedliving/ narrow-band-internet-of-things-nb-iot/

[17] LoRa Alliance - Wide Area Networks for IoT. [Online]. Available: https://www.lora-alliance.org/

[18] 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.

[19] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, “Localized multicast: efficient and distributed replica detection in large-scale sensor networks,” IEEE Transaction on Mobile Computing, vol. 9, no. 7, pp. 913–926, 2010.

[20] M. Conti, R. D. Pietro, L. V. Mancini, and A. Mei, “Distributed detection of clone attacks in wireless sensor networks,” IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 5, pp. 685–698, 2011.

[21] M. Zhang, V. Khanapure, S. Chen, and X. Xiao, “Memory efficient protocols for detecting node replication attacks in wireless sensor networks,” in ICNP’ 09. IEEE, 2009, pp. 284–293.

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

[23] K. Xing, F. Liu, X. Cheng, and D. H. Du, “Real-time detection of clone attacks in wireless sensor networks,” in ICDCS’08. IEEE, 2008, pp. 3–10.

[24] R. Brooks, P. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, “On the detection of clones in sensor networks using random key predistribution,” IEEE Transactions on SMC, Part C, vol. 37, no. 6, pp. 1246–1258, 2007.

[25] H. Choi, S. Zhu, and T. F. La Porta, “Set: Detecting node clones in sensor networks,” in SecureComm’07. IEEE, 2007, pp. 341–350.

[26] J.-W. Ho, M. Wright, and S. K. Das, “Fast detection of mobile replica node attacks in wireless sensor networks using sequential hypothesis testing,” in IEEE Transactions on Mobile Computing, vol. 10, no. 6. IEEE, 2011, pp. 767–782.

[27] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, “Random-walk based approach to detect clone attacks in wireless sensor networks,” IEEE Journal on Selected Areas in Communications, vol. 28, no. 5, pp. 677–691, 2010.

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

[29] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, “Internet of things: Vision, applications and research challenges,” Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, 2012.

[30] A. Yassin, Y. Nasser, M. Awad, A. Al- Dubai, R. Liu, C. Yuen, R. Raulefs, and E. Aboutanios, “Recent advances in indoor localization: A survey on theoretical approaches and applications,” IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 1327–1346, 2016.