ISSN : 2455-135X

A Random Walk method on Replicate Node Attack detection SRW in Wireless Sensor Network

Mrs. M. Sangeetha
Research Scholar,
Erode Arts and Science College(Autonomous), Erode

Dr. Rizwana
Assistant Professor & Head
Erode Arts and Science College(Autonomous), Erode

Abstract

In wireless sensor networks, clone detection protocols demonstrate that RAWL yields the most favourable outcomes by utilizing Simple Random Walk (SRW). In order to simplify the process of selecting trustworthy IoT devices for the purpose of verifying location evidence, a paradigm has been developed for recognizing such devices based on their profile capabilities. We evaluated our system with LSM, RED, and P-MPC, noting that it exhibits a superior clone identification probability and reduced communication costs. Formulating an effective defence to address this problem is crucial. Numerous witnesses' node-based techniques are being established in order to address this issue; nevertheless, they frequently have higher connection and storage costs or lower detection accuracy, which renders them ineffectual. In Wireless Sensor Networks (WSNs), the HRWZ approach employs the random selection of Zone-Leader (ZL) in order to discover clones in an efficient manner while maintaining the resilience of the network. Comparing HRWZ against other well-known witness node-based approaches such as RM, LSM, and RAWL was one of our analyses, and TRAWL, and we did so over a range of simulation parameters.

Keywords: SRW, ZL, LSM, Random Walk Detection

Introduction

In order to identify clones, centralized detection systems need a central station or cluster head [5-8]. Despite achieving excellent clone detection rates, all of these solutions suffer from the drawbacks of having just one point of failure and raising the expenses associated with communication. Witness node-based approaches [9–14] are distributed detection strategies that are built on the claimer-reporter-witness model for clone detection. The authentication method is the main target of a clone node attack, which targets Internet of Things devices. Device replication attacks and cloning attacks are common terms for the clone node attack. Wireless sensor networks (WSNs) use clone node attacks detection, as adversaries can readily undermine authentication processes by generating replicas of valid nodes. Section 4 compares the cost of

ISSN : 2455-135X

our proposed technique HRWZ to that of the state-of-the-art Randomized Multicast (RM), Line-Selected Multicast (LSM), Random Walk (RAWL), and Table-assisted Random Walk (TRAWL). The experimental data that show that the HRWZ regimen is effective are presented in Section 5. In Section 6, the data is analyzed to determine how effective the HRWZ protocol was in enhancing the security of WSNs. In the end, the work is summarized in Section 7, which includes the main findings, acknowledges the limitations, and suggests directions for further research.

RAWL & RAND

To address the aforementioned difficulty and mitigate the significant deficiencies because of the pressure from RAND and RAWL, we must develop a better method of clone detection. This study adds to the existing literature by introducing a new random walk called Single Stage Memory Random Walk and a cutting-edge method called SSRWND that combines the best features of SSRW with Network Division. At the beginning of a random stroll in SSRWND, the subsequent node to be visited is selected under the requirement that it must not be the present node or the previously traversed node. 2. We conduct comprehensive simulations, contrasting the outcomes of SSRWND with RAND, RAWL, and TRAWL. Based on the results of the simulation, it has been determined that there is a decrease in the costs associated with communication and memory, while simultaneously ensuring the high security of witness nodes and increasing the likelihood of clone detection.

ISSN : 2455-135X

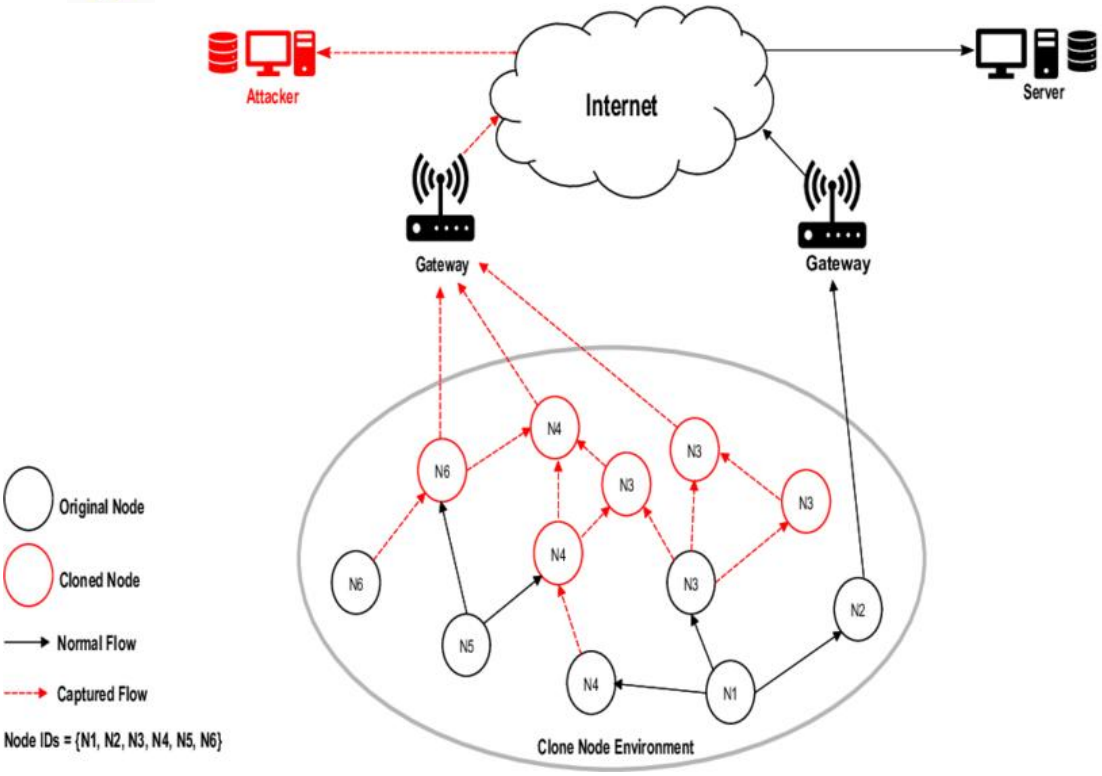


Figure 1: Clone Node Eniveronmet

A further objective of the proposal is to reduce the amount of information that must be communicated to zone leaders in order to disseminate information about zone membership. The approach that we have presented is location-independent, in contrast to previous location-dependent node replica detection algorithms that have been published in the various pieces of literature. As a consequence of this, there is no memory overhead that is incurred for the purpose of storing location information.

Related Work

Table-assisted Random Walk (TRAWL) and Random Walk (RAWL) were both first presented by Y. Zeng and colleagues [12]. In RAWL, SRW is employed to identify witnesses capable of revoking replicated nodes from the network upon receipt of contradicting allegations. TRAWL employs the identical detection methodology as RAWL, although minimizes memory expenses by utilizing a trace table at each node. To get elevated detection probability, RAWL and TRAWL necessitate an increased number of random walks with extended step lengths, resulting in greater communication and memory expenditures relative to LSM. Random Walk (RAWL) and Table-assisted Random Walk (TRAWL) were introduced by Y. Zeng et al. [12]. In RAWL, SRW is employed to identify witnesses capable of revoking replicated nodes from the network upon receipt of contradicting allegations. TRAWL uses a trace table at each node to

ISSN : 2455-135X

save memory usage, but its detection approach is identical to RAWL. To get a higher likelihood of detection, RAWL and TRAWL necessitate an increased number of random walks with extended step lengths, resulting in greater communication and memory expenses relative to LSM. Depicts exactly RAWL and TRAWL work. There are two stages to RAND [13,14] that combine SRW with network segmentation. The first is network setup, which involves developing hierarchical tiers for the whole network and assigning each region a certain number of levels. Reporters begin SRWs in each randomly selected site to recruit witnesses during the replica detection phase. In a random walk, every node that passes will also become a witness and keep its location claim. The network division mitigates communication and memory expenses while ensuring the robust security of witness nodes. The operation of RAND can be exemplified by Fig 3, which illustrates the functionality of RAWL and TRAWL.

Conti et al. [7] proposed a randomized, efficient, and distributed (RED) methodology for identifying node replicas in wireless sensor networks (WSNs). Their detection technique differs from that of Par et al. [11] in the following ways: (i) The base station distributes a random value to all nodes inside the network, and (ii) Witness nodes are selected using a pseudo-random process.

Zhu et al. introduced two procedures for replica detection: (i) single deterministic cell (SDC) and (ii) parallel multiple probabilistic cells (P-MPC). They considered a global grid system divided into several cells. In SDC, each node is allocated to a specific destination cell by the location mapping algorithm. Each neighbour of a node conveys the node's ID and positional assertion to the node's assigned cell with an expectation pf. Upon receiving the location claim, nodes in the target cell store it with a certain probability following signature verification. When an identical ID from different sites is sent to the target cell, a conflict is more likely to occur. In P-MPC, the location assertion is conveyed to several destination cells instead of a singular one, as is the case in SDC.

Proposed methodology

The network model includes many entities: the initial node, its cloned node, the gate node, along with a description of their operational procedures and the hypotheses that underpin those procedures. Subsequently, within the framework of the threat model, we provide the presumptions and capabilities of an adversary who is capable of carrying out hostile operations within an Internet of Things network. In addition, we provide an explanation of the batch verification process for ECDSA*, which is intended to serve as the foundation for our proposed detection system by taking use of its essential algorithms.

ISSN : 2455-135X

List of Network Notations and Symbols

Network Assumptions

With regard to sensor networks, the following assumptions are applicable: (i) The nodes have static, invulnerable to manipulation, and uniformly distributed throughout the observation area; (ii) transmission links are wireless; (iii) There is no centrally located trusted authority; (iv) Nodes lack knowledge of their position, which means there is no basic mechanism to be able to determine the node's physical location; and (v) Prior to deployment, each node is given a unique identification number.

Assumptions about Adversary

When it comes to the opponent, the following assumptions are relevant: (i) An adversary is only able to compromise a limited number of sensor nodes; (ii) Once an adversary has the ability to compromise a node, they are able to gain complete control over that node; (iii) By utilizing captured nodes, an adversary is able to generate a limitless amount of copies for installation within the network; and (iv) An opposition is unable to generate a new ID for a sensor node.

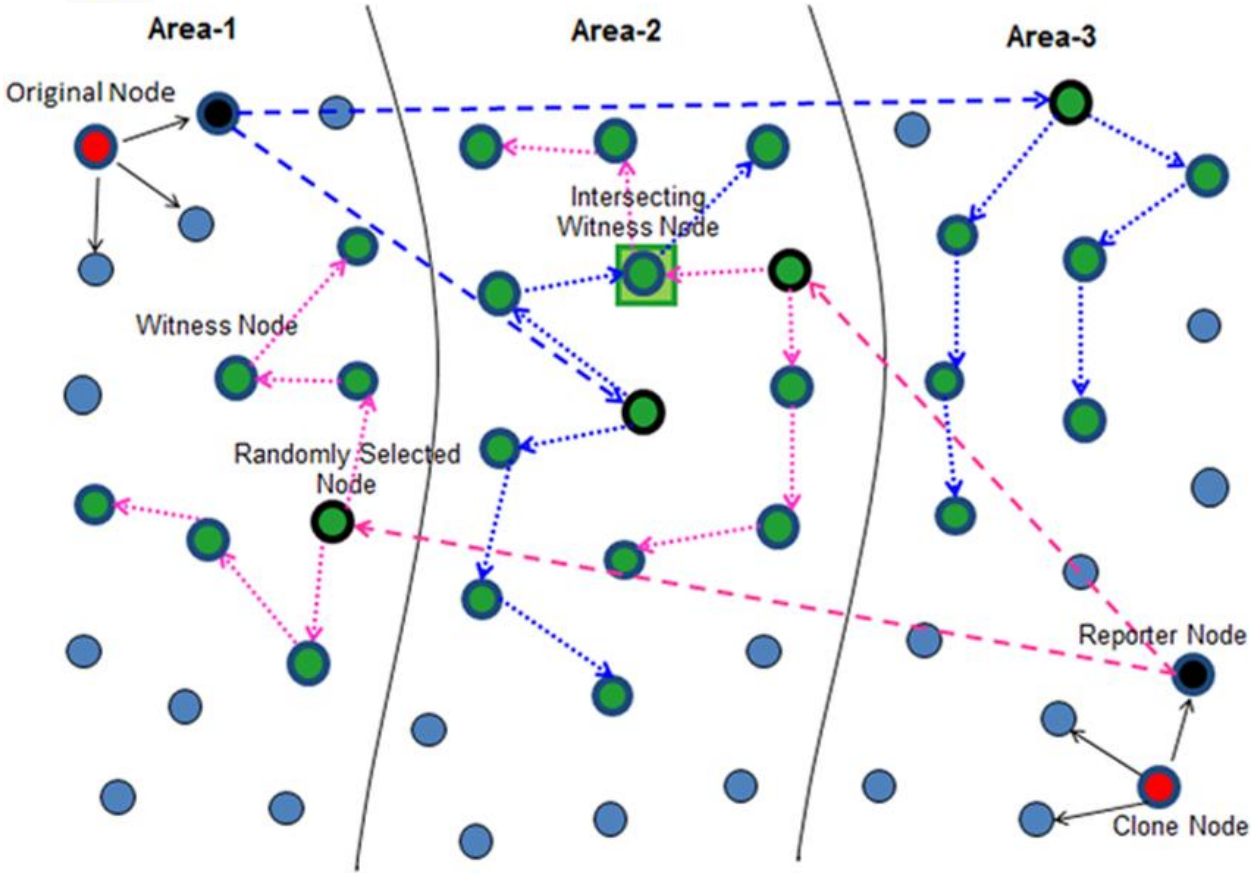
Zone-Based Node Replica Detection Scheme

In the next part, the Zone-Based Node Replica Detection Scheme (ZBNRD) that has been suggested is described. ZBNRD is a network that is separated into numerous zones, just like SET[3], which is another example. However, with ZBNRD, it is possible that not all members of a zone are located inside the neighborhood of the zone leader during a single hop. In contrast to the approach proposed by Ho et al., which relies on deployment knowledge, ZBNRD dynamically forms zones. Authentication and message signing are both accomplished through the utilization of an authenticated public key system.

Zone Registration

In the immediate aftermath of the deployment of sensor nodes in the selected region, the zone registration phase will get underway. The zone leaders are responsible for enrolling interested nodes within their respective zones during this phase. The transmission of a zone registration message (ZONE_REGD) by the zone leaders is the first step in the process of zone registration. Specifically, the ZONE_REGD message format is composed of the following components: Z, IDLZ, and SIGSKIDLZ (H(Z||IDLZ)), where Z and IDLZ are the IDs of a zone and its zone leader, respectively. With the ZONE_REGD message, a zone leader extends an invitation to nodes to join its zone. This message acts as an invitation. The zone leaders are represented by the nodes A, B, C, D, and E in the diagrams.

ISSN : 2455-135X



Gateway Nodes in networking modules

One of the devices that acts as an interface between Internet of Things devices and other systems, including the cloud, is known as a gateway. There are two types of Internets of Things gateways: physical and virtual. When connected devices in the Internet of Things (IoT) submit data to a cloud service, the gateway collects the data and sends it on. In order to interact with one another via the internet, Internet of Things devices often connect to one another through a gateway. In the network model that we have proposed, a gateway node is tasked with a number of responsibilities. These include the following: (i) making it easier for Internet of Things devices to connect to the outside server; (ii) making sure that location proof signatures are checked; (iii) having important supplies. These important files include the public key for checking signatures on all Internet of Things devices that are already in use, as well as its own key pair, which is made up of a public key and a private key; and (iv) maintaining a record of all deployed Internet of Things devices and the contextual information associated with them, which is represented by a set CI = {,,, …, }.

ISSN : 2455-135X

ECDSA* batch verification

According to the information batch verification is a technique that allows for the efficient certification of numerous digital signatures in a shorter amount of time than is required for individual validation. According to this approach, the signer is responsible for the generation of t signatures through interaction with the verifier, who simultaneously validates all of the t signatures. ECDSA is a common way to sign things digitally that is used in the Internet of Things (IoT). It uses smaller keys than public-key cryptography but delivers the same level of security. Because of this, it makes sure that devices are real and that data can be shared between them. In light of this, the emphasis of our study was on ECDSA signatures, which are utilized to validate location proof signatures that are created by IoT 15/55. Similar to the ECDSA, the ECDSA* requires the execution of the following algorithms: (i) the production of keys, (ii) the generation of signatures, and (iii) the verification of signatures. The following provides an overview of the implementation as well as details of a number of different algorithms.

TBC stands for transpose bit-pair coding. In order to generate a code for the bit pairs that are situated at locations (i, j) and (j, i), TBC makes use of the prefix coding concept. A unique code is generated by the method for each and every possible combination of bits that are contained inside the matrix. In Algorithms 1 and 2, respectively, the TBC coding and decoding procedures are broken down in detail.

Algorithm

Input: ECDSA* Signature (r, s), Public Key Q

Output: Signature (r, s) Accept or Reject process VERIFICATION OF SIGNATURE(Signature (r, s), Public Key Q) Ascertain that both r and s are integers inside the interval [1, n-1].

Determine H(m) and translate it into an integer, e.

Compute w = s-1 mod n

Determine u1 = ew mod n and u2 = rw mod n.

Compute X = u1P + u2Q

If X =

If v = r, accept the signature; otherwise, reject the signature.

Transpose Bit Pair Decoding

Input : Matrix, Mem_Mat, of dimension DIM x DIM
Output: Msg_Bit_Str, the message bit string,

ISSN : 2455-135X

```
for i = 1 -> DIMwithincrement 1 do
   Send Mem_Mat(i,i) to Msg_Bit_Str
      for j = i +1 → DIM with increment1
        Send 0 to Msg_Bit_Str
           if Mem_Mat(i, j) = 0 & Mem_Mat(j,i) = 0;
              otherwise, send 10 to Msg_Bit_Str if Mem_Mat(i, j) = 1&Mem_Mat(j,i) = 0;
         otherwise, send 110 to Msg_Bit_Str if Mem_Mat(i, j) = 0&Mem_Mat(j,i) = 1;
      finally, send 111 to Msg_Bit_Str
 end  if
end  for
```

Selection for the trusted nodes

The confidence credibility aspect is crucial for selecting reliable devices, as it assesses many established trust criteria during transactions between basic IoT devices and reliable Internet of Things devices in order to determine the reliability of an IoT device. First, we split the dependability of each Internet of Things device into its implicit and explicit components, and then we use these two pieces to determine the confidence C. The evaluation of the Internet of Things device's independent reputation is included in the implicit confidence (IC) method of trust assessment. Under the explicit confidence EC model, trust is established by the suggestions of other nodes, which are based on the experiences that they have had in the past. The confidence measure for the t devices may be expressed as a set, where each element represents an independent variable and the set is referred to by the variables I = {1, …, t}.

Localization technique

Localization is a crucial notion in LPS, employing approaches that are independent of localization and network/location infrastructure to ascertain the user's device location. The term "localization" refers to the process by which a device determines its position in relation to other devices, satellites, or maps, amongst other references. For the purpose of localization, a number of software and hardware approaches have been utilized. These techniques include fingerprinting, technologies such as proximity sensing, triangulation, beaconing, distance-bounding protocols, and context-based modalities, and systems that are based on mobile networks or towers.

Attack detection analysis

Within the framework of our suggested method, we assessed the identification of clone node assaults by making use of two factors: detection time and detection probability. The likelihood that replicated or replica nodes would be effectively discovered is taken into account when determining the detection probability. Conversely, the detection time denotes the duration necessary to successfully identify a clone node assault on our network. Each component is investigated and quantified in further depth in the ensuing sub-sections, which are as follows:

ISSN : 2455-135X

Furthermore, when we were in the process of establishing the configuration of the clone nodes, we assessed two different kinds of environments.

• Sparse environment: For the purpose of constructing and maintaining the network, a limited number of Internet of Things devices are utilized inside a sparse device environment. In order to act as clone devices in our arrangement, we choose twenty devices from the total number of devices that are available on the network.

• Dense environment: The quantity of clone devices in a compact configuration varies from 25 to 50.

Conclusion

The purpose of this study is to offer a zone-based node replica detection technique for wireless sensor networks (WSN). As part of the proposed plan, the network will be divided into numerous distinct zones. There is a zone leader in charge of each zone, and their responsibility is to detect clones that are present inside the network. (i) Zone Registration and (ii) Replica Detection were the two processes that ZBNRD went through in order to function. After comparing our proposed method to other options that are already available, we came to the conclusion that it possesses a higher detection probability and a lower communication overhead. The techniques for detecting clones, such as RAND and RAWL, make use of SRW, which naturally revisits previously traversed nodes. Consequently, there is less chance of witness node intersection and detection. In this study, a distributed technique called Single Stage Memory Random Walk with Network Division (SSRWND) is presented to overcome the issue of node revisiting. By incorporating restricted memory random walk with network division, this technique enhances the RAND protocol. Through the utilization of a memory-enhanced random walk that keeps track of the most recently visited node within a record, SSRWND outperforms RAND, RAWL, and TRAWL. This results in a reduction in the number of node revisits.

References

1. Khan, W.Z.,Aalsalem,M.Y.,Saad,N.M.,Xaing,Y.,&Luan,T.H.(2014,April). Detecting replicated nodes in Wireless Sensor Networks using random walks and network division. In Wireless Communications and Networking Conference (WCNC),2014IEEE (pp.2623–2628).IEEE.
2. SeoW.J., IslamR.,KhanM.K.,&ChooK.K.R.(2015).ASecureCross-DomainSIPSolutionfor Mobile AdHoc Network Using Dynamic Clustering. In Security and Privacy in Communication Networks (pp. 649–664). Springer International Publishing.
3. ContiM., DiPietroR.,& Spognardi A.(2014). Clone wars: Distributed detection of clone attacks in mobile WSNs. Journal of Computer and System Sciences, 80(3),654–669.

ISSN : 2455-135X

4. KhanW.Z., HossainM.S.,AalsalemM.Y.,SaadN.M.,&AtiquzzamanM.(2016).Acostanalysis framework for claimer reporter witness based clone detection schemes in WSNs. Journal of Network and Computer Applications, 63, 68–85.
5. Devi and Jaison, 2020 Devi P., Jaison B. Google Scholar Protection on wireless sensor network from clone attack using the SDN-enabled hybrid clone node detection mechanisms Comput. Commun., 152 (2020), pp. 316-322
6. Shanmugam and Paramasivam, 2020 Shaukat et al., 2014 Shaukat et al., 2020 Sun et al., 2017 Wang et al., 2008 Wollschlaeger et al., 2017 Xing and Cheng, 2010 Xing et al., 2008 Yang et al., 2017 Yu et al., 2013 Shanmugam A., Paramasivam J. A two-level authentication scheme for clone node detection in smart cities using Internet of things Comput. Intell., 36 (3) (2020), pp. 1200-1220
7. KhanW.Z.,AalsalemM.Y.,&SaadN.M.(2015).DistributedCloneDetectionin StaticWirelessSen sor Networks: RandomWalkwithNetworkDivision.PloS one, 10(5), e0123069. doi: 10.1371/journal. pone.0123069 PMID:25992913
8. Yu et al., 2013, Yu C.-M., Tsou Y.-T., Lu C.-S., Kuo S.-Y. Localized algorithms for detection of node replication attacks in mobile sensor networks IEEE Trans. Inf. Forensics Secur., 8 (5) (2013), pp. 754-768
9. Shaukat et al., 2014 Shaukat H.R., Hashim F., Sali A., Abdul Rasid M.F. Node replication attacks in mobile wireless sensor network: a survey Int. J. Distrib. Sens. Netw., 10 (12) (2014), Article 402541
10. Ho, J. W., Liu, D., Wright, M., & Das, S. K. (2009). Distributed detection of replica node attacks with group deployment knowledge in wireless sensor networks. Ad Hoc Networks, 7(8), 1476–1488.
11. Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and counter measures. Ad Hoc Networks, 1(2 and 3), 293–315.
12. Sei, Y., & Honiden, S. (2008). Distributed detection of node replication attacks resilient to many compromised nodes in wireless sensor networks. In Proceedings of the 4th annual international conference on wireless internet, WICON ’08 (pp. 01–08). Brussels, Belgium: ICST.
13. Choi, H., Zhu, S., & Porta, T. F. L. (2007). Set: Detecting node clones in sensor networks. In Proceedings of third international conference on security and privacy in communications networks and the workshops, SecureComm 2007, IEEE, Nice, France, pp. 341–350.
14. Zhang, M., Khanapure, V., Chen, S., & Xiao, X. (2009). Memory efficient protocols for detecting node replication attacks in wireless sensor networks. In Proceedings of 17th IEEE international conference on network protocols, ICNP’09 (pp. 284–293). Princeton, NJ: IEEE.
15. Znaidi, W., Minier, M., & Ubeda, S. (2009). Hierarchical node replication attacks detection in wireless sensors networks. In Proceedings of IEEE 20th international symposium on personal, indoor and mobile radio communications, 09 (pp. 82–86). Tokyo: IEEE.