Volume 5, Issue 12, December 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Region based Detection of Clone Nodes in Wireless Sensor Networks

Deepali Kulkarni*, Gayatri Bajantri
Department of Computer Science and Engineering,
SIET- Bijapur, India

Abstract— Wireless sensor networks (WSN) are prone to different types of attack such as man in middle attack, replay attack, and duplication attack. Duplication attack is one of the most severe attacks in WSN. In this attack, an enemy deploys clones of a genuine. Clones participate in all network actions and behave identically same as the genuine. Therefore, detection of clones in the network is a tough task. The majority of the work reported in the literature for clone detection is location dependent. This work proposed a location independent region-based replica detection procedure. In the proposed method, the network is animatedly divided into a number of regions. Each region has a region-leader, which shares its membership list among all nodes in region. The responsibility of the region-leader is to detect the clone. Proposed Region-Based Replica Detection Scheme (RBNRD) elects a node as region leader which is responsible to share unique node IDs to base station; when and detect adversary in the region the detection of clone node is identified by signature of node known to region leader. The proposed work compares with LSM, RED, and P-MPC and observed that it has a higher clone detection probability, a lower communication cost and deterministic technique.

Keywords— WSN, Replica detection, Region formation, RBNRD, LSM, RED, P-MPC

I. INTRODUCTION

Wireless Sensor Network (WSN) is a group of sensors with limited resources that work together to achieve a common goal. WSNs can be deployed in callous environments to fulfill military and civil applications [1]. Due to its operating nature, WSNs are often unattended, hence has a threat of different kinds of novel attacks. For instance, an adversary could eavesdrop all network communications and read packets, acquire all info of network and may start replicating behavior of legitimate, and may launch a variety of malicious activities. This attack is called clone attack [2][3]. Since clone has legitimate information, it participates in the network operations in the same way as a legitimate; hence, cloned attack is severe attack. A few attacks driven from clones have been described in the literature [2]. Say for instance, a clone could create a black hole, initiate a wormhole attack with a collaborating adversary, or dropping, replaying packets, congesting network and degrades network and performance hence biasing final result. The threat of a clone attack can be characterized by following points:

- A clone is treated as honest by its neighbors. In truth, without global countermeasures, other s are not aware of the fact that clone is among their neighbors.
- Adversary cost is to read network info and get a place in network, the cost of attack is sustained. Making further clones of the same can be considered cheap.

With the exception of the protocol proposed, only centralized or local protocols have been proposed to overcome clone attack. Centralized protocols have a single point of failure and high communication cost; local protocols have a limitation that it will not detect replicated s that are distributed in different areas of the network. In proposed method, network self-healing mechanism is used, where nodes separately identify the presence of clones and exclude them from any further network operations. In particular, this proposed method is designed to iterate as a "routine" event: It is designed for continuous iteration without significantly affecting the network performances, while achieving high clone detection rate. In this work analyzes the desirable properties of distributed protocols.

II. LITERATURE SURVEY

[Akyildiz, I. F., Su,W., Sankarasubramaniam,Y.,&Cayirci, E. (2002).][1]. surveys says the flexibility, fault tolerance, high sensing fidelity, low cost, and rapid deployment characteristics of sensor networks create many new and exciting application areas for remote sensing. In the future, this wide range of application areas will make sensor networks an integral part of our lives. However, realization of sensor networks needs to satisfy the constraints introduced by factors such as fault tolerance, scalability, cost, hard-ware, topology change, environment, and power consumption. Since these constraints are highly stringent and specific for sensor networks, new wireless ad hoc networking techniques are required.

Many researchers are currently engaged in developing the technologies needed for different layers of the sensor networks protocol stack. The flexibility, fault tolerance, high sensing fidelity, low cost and rapid deployment characteristics of sensor networks create many new and exciting application areas for remote sensing. In the future, this wide range of application areas will make sensor networks an integral part of our lives.

[Adib Rastegarnia and Vahid Solouk, (2011)][2], according to Adib and Vahid ; network in general consists of sensor nodes that are densely deployed over a geographical area to perform special tasks such as environmental measurements, target tracking, intrusion detection, climate control, and so on. To ensure a wide range of applications, sensor networks are equipped with some features. Compared to wireless networks, design and implementation of Wireless Sensor Networks (WSN) are more challengeable due to their special characteristics which introduce some limitations in power, storage, and process capability of sensor nodes. As these limitations in turn, affect nodes' lifetime, the energy efficiency is known as significant issue in WSNs, inspiring considerable research efforts on techniques to reduce power consumption of sensor nodes and prolong network lifetime. In addition to lifetime, sensor nodes should have the capability of self-organization in network due to their ad-hoc nature without planning and engineering. Furthermore, the topology of WSN changes frequently for reasons such as failure of nodes or mobility. Prior to any deployment, simulation of the designed WSN is an important step to help evaluate the performance from different aspects such as response time, availability, reliability, throughput, and energy consumption. This is due to the following reasons:

• Deployment of sensor networks in a geographical area is costly. In this sense, it is important to ensure about the performance of the network to avoid excess cost and time. Some deployment cases enforce limited opportunities of appearing in a field for implementation and therefore, there should be strict assurance about the performance of the network. Hence, simulation of sensor networks should be aimed to provide reliable results. The performance of a simulator depends on network design parameters such as MAC and routing protocols, topology, radio models and internal design of the simulator such as architecture of the simulator, programming language used for implementing algorithms in simulator etc. This paper intends to evaluate the performance of Castalia simulator from different aspects based on simulation results. To achieve this goal, Paper first develop a WSN model to acquire performance metrics including Goodput, application level latency, and total data transmitted to a sink node, number of failed packets, and execution time. These metrics are then utilized to evaluate the performance of simulated network under different conditions. They concluded that, the current study was conducted to investigate and evaluate the validity of simulation results produced by Castalia simulator for WSN in different cases and scenarios each related to specific topologies and conditions. To perform this investigation, specific performance metrics for all the cases were introduced, each reflecting some aspects of Castalia. These metrics are good put, application layer latency, total data transmission, and number of failed packets. These metrics are collected from two distinct WSN topologies namely, Grid and Uniform, while each scenario was tested for scalability with different number of nodes in each configuration. Through analysis of the results the execution time has been identified as the most vulnerable metric of the simulator performance. This vulnerability has especially shown for the number of nodes exceeding 501.

[Choi, H., Zhu, S., & Porta, T. F. L. (2007)][3], in this paper author states that, sensor nodes that are deployed in hostile environments are vulnerable to capture and compromise. An adversary may obtain private information from these sensors, clone and intelligently deploy them in the network to launch a variety of insider attacks. This attack process is broadly termed as a clone attack. Currently, the defenses against clone attacks are not only very few, but also suffer from selective interruption of detection and high overhead (computation and memory). This paper, proposed a new effective and efficient scheme, called SET, to detect such clone attacks. The key idea of SET is to detect clones by computing set operations (intersection and union) of exclusive subsets in the network. First, SET securely forms exclusive unit subsets among one-hop neighbors in the network in a distributed way. This secure subset formation also provides the authentication of nodes' subset membership. SET then employs a tree structure to compute non overlapped set operations and integrates interleaved authentication to prevent unauthorized falsification of subset information during forwarding. Randomization is used to further make the exclusive subset and tree formation unpredictable to an adversary. Paper shows the reliability and resilience of SET by analyzing the probability that an adversary may effectively obstruct the set operations. Performance analysis and simulations also demonstrate that the proposed scheme is more efficient than existing schemes from both communication and memory cost standpoints. Considering that sensors may not be equipped with tamper resistant hardware, it is crucial to provide a detection system against clone attacks. This paper, presented SET, a detection scheme based on a set model of the sensor network. SET is composed of four components: formation of exclusive subsets, authentication of subset covering, distributed set computation on

subset trees, and preservation of reliable set operations on the tree. The randomization schemes used in SET enable resilient and efficient detection, while providing distributed load sharing among nodes in the network. Paper provides with detailed security analysis for several types of attacks. The probabilistic analysis showed that SET provides a resilient and dependable detection under colluding attacks. And also evaluates the performance and overhead of the proposed algorithm. The results showed that solution has low transmission overhead, while using reasonably small memory space.

[Chong, C. Y., & Kumar, S. P. (2003)][4], Wireless microsensor networks have been identified as one of the most important technologies for the 21st century. This paper traces the history of research in sensor networks over the past three decades, including two important programs of the Defense Advanced Research Projects Agency (DARPA) spanning this period: the Distributed Sensor Networks (DSN) and the Sensor Information Technology (SensIT) programs. Technology trends that impact the development of sensor networks are reviewed, and new applications such as infrastructure security, habitat monitoring, and traffic control are presented. Technical challenges in sensor network

development include network discovery, control and routing, collaborative signal and information processing, tasking and querying, and security. The paper concludes by presenting some recent research results in sensor network algorithms, including localized algorithms and directed diffusion, distributed tracking in wireless ad hoc networks, and distributed classification using local agents. When the concept of DSNs was first introduced more than two decades ago, it was more a vision than a technology ready to be exploited. The early researchers in DSN were severely handicapped by the state of the art in sensors, computers, and communication networks. Even though the benefits of sensor networks were quickly recognized, their application was mostly limited to large military systems. Technological advances in the past decade have completely changed the situation. MEMS technology, more reliable wireless communication, and low-cost manufacturing have resulted in small, inexpensive, and powerful sensors with embedded processing and wireless networking capability. Such wireless sensor networks can be used in many new applications, ranging from environmental monitoring to industrial sensing, as well as traditional military applications. In fact, the applications are only limited by imagination. Networks of small, possibly microscopic sensors embedded in the fabric of society: in buildings and machinery, and even on people, performing automated continual and discrete monitoring could drastically enhance understanding of our physical environment.

[Cocks, C. (2001). An identity based encryption scheme based on quadratic residues][5], A new threshold identity-based encryption scheme secure against a chosen identity attack is proposed in this paper. The construction extends the identity-based encryption scheme by Cocks. There were proposed several TIBE (Threshold Indentify Based Encryption) schemes based on the technique of elliptic curves for IBE schemes of the same type. However, there are IBE schemes based on the technique of quadratic residues that have smaller complexity of encryption (Cocks scheme and Boneh et al scheme). In this paper a new TIBE scheme for the IBE scheme by Cocks [2] is proposed. Paper proposed the TIBE scheme for the Cocks IBE (Indentify Based Encryption). This scheme is non-interactive and is the first TIBE proposed for a residual based IBE. From security point of view, it is proven to be secure against an adaptive-ID attack in the Random Oracle Model.

[Conti, M., Pietro, R. D., Mancini, L. V., & Mei, A. (2006)][6], Wireless Sensor Networks (WSN) are often deployed in hostile environments, where an attacker can also capture some nodes. Once a node is captured, the attacker can re-program it and start replicating the node. These replicas can then be deployed in all (or a part of) the network area. The replicas can thus perform the attack they are programmed for: DoS (Denial of Service) or influencing any voting mechanism are just examples. Detection of node replication attack is therefore a fundamental property of all the WSN applications in which an attacker presence is possible. The contribution of this paper is twofold: First, it analyses the desirable properties of a distributed mechanism for the detection of replicated IDs; second, it shows that the first proposal recently appeared in literature to realize a distributed solution for the detection of replicas does not completely fulfill the requirements. Hence, the design of efficient and distributed protocols to detect node identity replicas is still an open and demanding issue. This paper the preliminary notion of ID-obliviousness and area obliviousness that convey a measure of the quality of the node identity replicas detection algorithm; that is its resilience to an active attacker. Moreover, proposed scheme indicates that the overhead of such a protocol should be not only small, but also evenly distributed among nodes, otherwise the protocol itself could sensibly impact: On the network life as for the energy required by the number of exchanged messages and the computations performed; on the effectiveness of the protocol itself if the memory requirements exceed the storage available to the sensor. Finally, it has analyzed the state of the art solution for node identity replicas detection, and have shown that the proposed solution does not completely fulfill the issues above described. Open research directions are: complete characterization of the two notions of obliviousness provided together with a refinement of the appeal function; devising a protocol for node identity replicas detection compliant with the indicated requirements.

III. PROBLEM STATEMENT

Remote sensor systems (WSN) are vulnerable to different sorts of assault, and node replication assault is one of them. It is thought to be a standout amongst the most genuine assaults in WSN. In this kind of assault, an enemy sends clones of a honest to goodness node. These clones partake in all system exercises and act indistinguishably same as the honest to goodness node. In this manner, location of clones in the system is a testing task. WSNs are presented to different security dangers, for example, sybil, wormhole, node catch, blackhole, specific sending assault, etc.Node replication assault is a standout amongst the most genuine dangers that an enemy can dispatch inside a system. In this assault, a foe first bargains a sensor node in the system, and afterward she reinvents and produces various clones and conveys them at different areas in the system. Clones take after the same convention stack as its real node. Along these lines, it is hard to identify the vicinity of clones in the system.

3.1 Limitations of Existing Methodolgy

- Most of the node imitation discovery components are area needy and probabilistic in nature. In a probabilistic approach, it is hard to ensure a clone free sensor system.
- Maintaining area data causes an extra memory overhead in a memory-obliged sensor node.
- Most of the sensors work unattended and unsupervised in the objective range. Therefore, security is a noteworthy territory of concern

IV. APPROACHES AND METHOD

Based on the above survey and the problem stated, the suitable approaches and methods are as follows.

4.1 Proposed Work

In this proposed work, proposed work is a replica detection scheme which divides the network logically into a number of regions. Where each region has a leader responsible for detecting clones in the network.

Clone detection is done deterministically at two-level:

(i) Intra-region detection and
(ii) Inter-region detection.

The proposed work also attempts to minimize the message overhead in sharing region membership information among the region-leaders. Unlike many location dependent replica detection schemes reported in the literature, proposed work is location independent. Therefore, no memory overhead is associated for storing location information.

In the proposed work, the network is dynamically divided into a number of regions. Each region has a region-leader, and they share their membership list among themselves. It is the responsibility of the region-leader to detect the clone. The proposed technique is a deterministic one. This scheme is compared with LSM, RED, and P-MPC and observed that it has a higher clone detection probability and a lower communication cost.

4.2 Proposed region-based replication detection scheme assumptions

4.2.1 Network Assumptions:

Assumptions about sensor networks:

(i) Nodes are static, fixed, and are evenly deployed in the area of interest,
(ii) Communication channels are bidirectional,
(iii) No centralized trusted entity,
(iv) Nodes are unaware of their location, i.e., there is no built-in mechanism to know the node's physical location, and
(v) Node is assigned with an unique ID, prior to its deployment.

4.2.2 Assumptions about Adversary:

The following assumptions are made about the adversary:

(i) Only a limited number of sensor nodes can be compromised by an adversary,
(ii) Once a node is compromised, an adversary has full control over the ,
(iii) Using captured nodes; an adversary can create as many replica as its wishes to deploy into the network, and
(iv) An adversary cannot create a new ID for sensor node.

4.3 Region-Based Replica Detection Scheme RBNRD

This segment, portray the proposed Region-Based Replica Detection Scheme (RBNRD). Like SET [3], in RBNRD, the system is partitioned into various regions. Nonetheless, in RBNRD, all members of a region may not be inside of the one-bounce neighbor of the region-pioneer. Not at all like Ho et al. [7] plan that uses arrangement learning, in RBNRD, is region framed progressively. Character based open key framework [5] is utilized for validation and message signature. Every region in RBNRD has a region-pioneer; whose obligation is to identify imitations.

Region-pioneers are chosen from the earlier before organization. Every node in the system has a place with precisely one region. A region-pioneer keeps up the rundown of all individuals in its region, and the rundown of region-pioneers present in the work . RBNRD works in two stages: (i) Region Registration, also, (ii) Replica Detection. Delineate underneath the activities, performed in every stage.

Region-Based Replica Detection:

A productive alteration to disseminated methodology is called deterministic multicast, where nodes send ID and area data to choose nodes called witness. On distinguishing a conflicting region affirm, the witness node denies the conflicting. Deterministic multicast has lesser correspondence taken a toll in relationship to spread methodology. Then again, the recognizable proof handle only depends on upon witness. Therefore, it is less secured. Distributed replica detection mechanism was proposed for the first time by Parno et al. [4] in 2005. Two algorithms are proposed: (i) Randomized Multicast, and (ii) Line Selected Multicast. In Randomized Multicast, each node sends its location information to a set of randomly selected witness nodes. They claim; in a network of n nodes, if each generates O($\sqrt{n}$) witness nodes, then using Birthday Paradox, at least one witness node is expected to get the location conflict of the replicated with higher probability. Location information is sent over a line from one to another in Line-Selected Multicast. Each intermediate node stores the location claim. A at the line-crossing point will detect a conflict, if conflicting location claim line crosses the Line-Selected Multicast has a lower communication cost compared to Randomized Multicast Conti et al. [5] proposed a randomized, efficient and distributed (RED) mechanism for detection of replica in WSNs. Their detection mechanism differs from that of Parno et al. [6] in the following ways: (i) BS broadcasts a random value to all nodes in the network, and (ii) Witness nodes are selected based on a pseudo random function. The inputs to the pseudo random function are: node ID, BS random value and the number of witnesses. Detection of a non-empty intersection at any level of the tree is reported to the base station. Sei et al. [7] have proposed a replica resilient mechanism to overcome the pitfalls of RED [7] and P-MPC. Unlike RED and P-MPC, this mechanism does not require any trusted entity, and is resilient to a number of compromised nodes in the network. Each node is pre-loaded with detection process start time. When a node gets its turn, it sends a one-time seed, and its node ID with a signature to all other nodes. If a node fails to start the detection process in its turn within a pre-defined interval of time, then the next starts its process. To improve

resiliency against capture, nodes are divided into groups, and each node starts its detection process using a role ID assigned to it. A replica detection scheme based on deployment knowledge is proposed by Ho et al. In this scheme, sensors are deployed in groups, and each sensor knows about its deployment group. Nodes which are closer to the group deployment location are considered

4.4 Region Registration

Region enrollment stage begins instantly after the sending of sensor nodes in the objective territory. In this stage, region-pioneers register intrigued nodes into their regions. Region enlistment starts with the show of a region enlistment message (REGION_REGD) by the region leaders. REGION_REGD message configuration is Z, I DLZ , SIGSKI DLZ (H(Z||I DLZ)), where Z and I DLZ are the IDs of a region and its region-pioneer individually. REGION_REGD message is a welcome to nodes by a region-pioneer to end up an individual from its region. Fig 1,also, 2 demonstrates the region enrollment process, where the dabbed line shows the telecast of REGION_REGD message, and the strong line shows the network. In the figures, node A, B, C, D and E are the region-pioneers. Fig 1 demonstrates the show of REGION_REGD message to one-jump neighbors, and Fig. 2 demonstrates the telecast of REGION_REGD message by one-jump neighbors of region-pioneers. A node may get a REGION_REGD message from more than one region-pioneer. Be that as it may, the node will enlist itself to a region whose region leader is closer to it. A node turns into the individual from a region by sending a region join message (REGION_JOIN) to the comparing region-pioneer. The arrangement of REGION_JOIN message is I Dm, sI DLZ , SIGSKm (H(I Dm||I DLZ)) where I Dm is the ID of joining node. A on getting the first REGION_REGD message show it to all its neighbor, and toss the resulting REGION_REGD message from the same region. On the other hand, a node show a ONE_REGD message with a likelihood, pregd, if the message is from a region not quite the same as that it has effectively gotten. At the point when a REGION_JOIN message touches base at a region-pioneer, it checks the presence and validness of the asked for node before adding it to its participation list. At the point when a region-pioneer gets a REGION_REGD message from another region-pioneer, it overhauls the directing way to it. An instance of region development toward the end of region enlistment stage is appeared in Fig. 2.

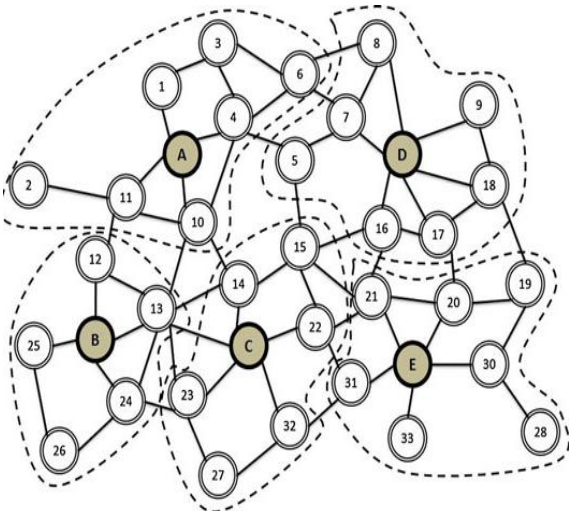

Figure 4.5.1: Case of region formation

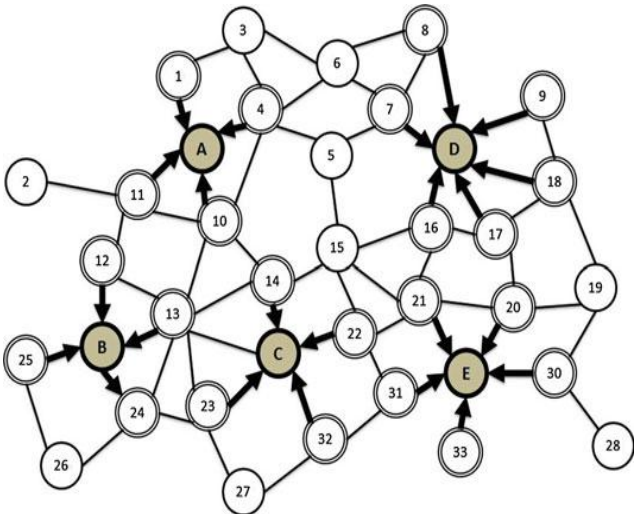

Figure 4.5.2: Neighbors enrolling with its Region Leader

4.5 Copy Detection During Registration

Toward the end of region enlistment stage, region-pioneers impart their enrollment rundown to each different and formation of region as appeared in Fig. 3. And region nodes registering with region leader is shown in Fig 4. A message of N bit is utilized to trade enrollment rundown between region-pioneers, where N is the system's extent. On the off chance that a node with ID, k, is available in a region, at that point the kth bit of the message is set. This message is spoken to by a participation lattice, Mem_Mat, of measurement DIM×DIM, where DIM×DIM = N. The framework Mem_Mat is typically a sparsematrix and bits are put away from left to right and start to finish. To decrease the message size, Two coding plans have been proposed: (i) Transpose Bit-Pair Coding (TBC), and (ii) Sub-Mat Coding (SMC). A region-pioneer on getting enrollment rundown code from other regions disentangles and confirms for the presence of copy. The presence of a node ID in two different region leads to a conflict. A region-leader on detecting a conflict initiates a revocation message (_REVOKE), which is broadcast to all its members and region-leaders as depicted in Fig 4. This process will detect replicas that are deployed during the registration phase.

V. RESULTS OF PROPOSED SYSTEM

- In proposed method, the network is divided into a number of regions. Each region has a region-leader, who is responsible for detecting clone in the network.
- Proposed System has higher detection probability and lower communication overhead.
- Value obtained from simulation is much lower in comparison to theoretical communication cost.
- Communication between the region-leaders is secured, since obtaining the private key is a difficult job as keys are assigned at the time of deployment.

VI. CONCLUSION

In this work, proposed region-based node copy location plan for WSN. In this proposed plan, the system is separated into various regions. Every region has a region-pioneer, who is in charge of identifying clone in the system. RBNRD worked in two stages: (i) Region Registration, and (ii) Replica Detection. In contrasted with proposed plan and existing ones and it is found that proposed scheme has higher discovery likelihood and lower correspondence overhead.

REFERENCES

[1] Akyildiz, I. F., Su,W., Sankarasubramaniam,Y.,&Cayirci, E. (2002).Asurvey on sensor networks. IEEE Communication, 40(8), 102–114.

[2] Adib Rastegarnia and Vahid Solouk, (2011),Performance Evaluation of Castalia Wireless Sensor Network Simulator

[3] 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.

[4] Chong, C. Y., & Kumar, S. P. (2003). Sensor networks: Evolution, opportunities, and challenges. Proceedings of the IEEE, 91(8), 1247–1256.

[5] Cocks, C. (2001). An identity based encryption scheme based on quadratic residues. In Proceedings of the 8th IMA international conference on cryptography and coding (pp. 360–363). London, UK:Springer.

[6] Conti, M., Pietro, R. D., Mancini, L. V., & Mei, A. (2006). Requirements and open issues in distributed detection of node identity replicas in wsn. In IEEE international conference on systems, man and cybernetics, SMC ’06 (pp. 1468–1473). Taipei: IEEE.

[7] Conti, M., Pietro, R. D., Mancini, L. V., & Mei, A. (2007). A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks. In Proceedings of the 8th ACM international symposium on mobile ad hoc networking and computing, MobiHoc ’07(pp. 80–89). Montreal, Canada: ACM.

