www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 2 February, 2014 Page No.3817-3821

An Optimized Localization Algorithm against Node Replication Attacks in Wireless Sensor Networks

[1]R.M.Sinthiya, [2]J.Vijipriya,

RVS College of Engineering and Technology, Dindigul,sinthiya_3987@rediff.com

Assistant Professor, *RVS College of Engineering and Technology, Dindigul, vijipriyajkv@gmail.com*

***Abstract*— A wireless sensor network (WSN) consists of a number of tiny, low-cost, and resource-constrained sensor nodes, but is often deployed in unattended and harsh environments to perform various monitoring tasks. Security is important for many sensor network applications. As a result, WSNs are susceptible to many application-dependent and application-independent attacks. WSNs are often deployed in harsh environments, where an attacker node can physically capture some of the sensor nodes. Once a sensor node is captured then the attacker node can collect all the credentials like keys, identities etc. The attacker can modify the message and replicate in order to overhear the messages or interrupt the functionality of the sensor networks. IPD and PSD are proposed as an optimized localization algorithm for defending against the node replication attacks. Each node in the localized algorithm can communicate only with its one-hop neighbors. The node can meet again, it can be compared with the first node, previous node location, and attack replication node.**

***Index Terms*— Wireless Sensor Networks (WSNs), Intensely Profitable Detection (IPD) and Proficient Scattered Detection (PSD).**

I. INTRODUCTION

A Wireless Sensor Network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions such as temperature, sound pressure etc and cooperatively pass their data through the network to a main location. The ease of deploying sensor networks contributes to their appeal. They can quickly scale to larger configurations, since administrators can simply drop new sensors into the desired locations in the existing network. To join the network, new nodes require neither administrative intervention nor interaction with a base station; instead they typically initiate simple neighbor discovery protocols by broadcasting their restored credentials (e.g. Their unique ID and/or the unique ID of their keys).

Unfortunately, sensor nodes typically employ low cost commodity hardware components unprotected by the type of physical shielding that could prevent access to a sensor's memory, processing, sensing and communication components. Cost considerations make it impractical to use the shielding that could detect pressure, voltage, and temperature changes that an adversary might use to access a sensor's internal state. Deploying unshielded sensor nodes in hostile environments enables an adversary to capture, replicate, and insert duplicated nodes at chosen network locations with little effort. Thus, if the adversary compromises even a single node can replicate it indefinitely, spreading the influence throughout the network. If left undetected, node replication leaves any network vulnerable to a large class of insidious attacks. Using replicated nodes, the adversary can subvert data aggregation protocols by injecting false data or suppressing legitimate data.

Previous approaches for detecting node replication typically rely on centralized monitoring, since voting systems cannot detect distributed replication. Centralized schemes require all of the nodes in the network to transfer a list of their neighbor claimed locations to a central base station that can examine the lists for conflicting location claims. If the adversary can compromise the base-station or interfere with its communications, then the centralized approach will fail. Also, the nodes surrounding the base station are subject to an undue communication burden that may shorten the network's life expectancy.

In this paper, an optimized localization algorithm is introduced to detect the node replication attacks occurred in WSNs. The technique developed in these algorithms has the following advantages: Confined detection algorithms are beneficial to refuse node duplication attacks, provides better veracity, cancellation recession of the replicas that can be implemented by each node, instance management recession.

The rest of the paper is organized as follows. Section II presents a description about the previous research which is relevant to the flooding attacks and the possible solutions. Section III involves the detailed description about the proposed method. Section IV presents the performance analysis. This paper concludes in Section V.

II. Related Work

Conti et al proposed a self-healing, randomized, efficient and distributed RED protocol for the detection of node replication attacks. The system analyses the desirable properties of a distributed mechanism for the detection of node replication attacks [1]. *Deng et al* proposed a protocol to detect the replicas in mobile wireless sensor networks (WSNs). A polynomial based pairwise key pre-distribution scheme and counting bloom filters were used to guarantee that the replicas can never lie about their real identifiers. It collects the number of pairwise keys established by each sensor node. Replicas were detected by looking at whether the number of pairwise keys established by them exceeds the threshold [2]. *Manjula et al* analyzed the threat posed by the replication attack [3]. *Meng et al* proposed a note based protocol for detecting node replication attacks. This system doesn't need the geographic locations of nodes. It had no significant overhead on the resource constrained sensors [4].

Tran et al proposed two protocols to detect the node replication attack. The protocols were LANCE and SACRED. LANCE was designed to be lightweight in performance at the cost of slightly weaker security robustness and SACRED obtains a much greater security by trading off small performance [5]. *Xie et al* proposed a detection scheme against the node replication attack in WSN. The detection scheme was based on the bloom filter and QR decomposition. The bloom filter was used to generate geographic fingerprints of the nodes. QR decomposition guarantees the network security and provides the verification of the link [6]. *Xing et al* proposed two replication detection schemes TDD and SDD to tackle the challenges in the time domain and the space domain. TDD and SDD were used to provide high detection accuracy and resilience against smart and colluding replicas. TDD and SDD have no restriction on the number and distribution of replicas. Also, they have no restrictions on the number and distribution of the cloned frauds [7]. *Zhu et al* proposed a distributed approach called Localized Multicast for detecting node replication attacks [8].

Zhu et al proposed a neighbor-based detection scheme to cope with replication attacks. The scheme features distributed detection and takes node mobility into account. This system was subjected to various replication attacks that can circumvent the detection [9]. *Zhu et al* proposed a lightweight token based authentication approach for detecting node replication attacks. The detection scheme was based on statistics to harness the encounters between physical nodes [10]. *Zeng et al* proposed Random-Walks based approach to detect the clone attacks in WSNs. The replica-detection protocol was used, the protocol must be non-deterministic and fully distributed (NDFD) and it fulfills three security requirements on witness selection. Also, two new protocols were used, Random Walk (RAWL) and Table-Assisted Random Walk (TRAWL). It fulfills the requirements about moderate communication and memory overheads [11].

Bonaci et al proposed an optimization approach for the detection of clone attacks. The authors [12] considered the impact of leaving undetected cloned nodes in the network. An optimization framework was developed for choosing clone detection parameters based on the costs. *Ho et al* proposed a mobile replica node detection scheme. This scheme was based on the sequential probability ratio test [13]. *Vardhan et al* proposed an active replication mechanism for file replication; file access and performance transparency to the system. A File Replication Server (FRS) was used to replicate the file when the total number of requests for it reaches the threshold value. The file replica was updated on-demand by only propagating the required partial updates. The master replica immediately computes the file content modifications. It uses the basic trust parameters and adaptive factors in computing trustworthiness of peer FRS namely frequency of the request for a particular file that an FRS perform [14].

Mishra et al proposed a location dependent zone based node replication technique. The network was divided into a number of zones. Each zone had a zone leader to detect the clone. This scheme was a deterministic one to detect the clone attacks on the WSNs [15]. *Zhu et al* reviewed a survey on the detecting node replication attacks in WSNs [16]. Here, a typical threat in the latter category known as the node replication attack, where an adversary prepares own-cost sensor nodes and deceives the network into accepting them as legitimate ones. The authors provide necessary technical details and certain comparisons to detect the node replication attacks.

III. Proposed Work

This section presents the details of our techniques to detect replicating attacks in wireless sensor networks. The following architecture describes the overall node duplication attacks using an optimized localization algorithm.

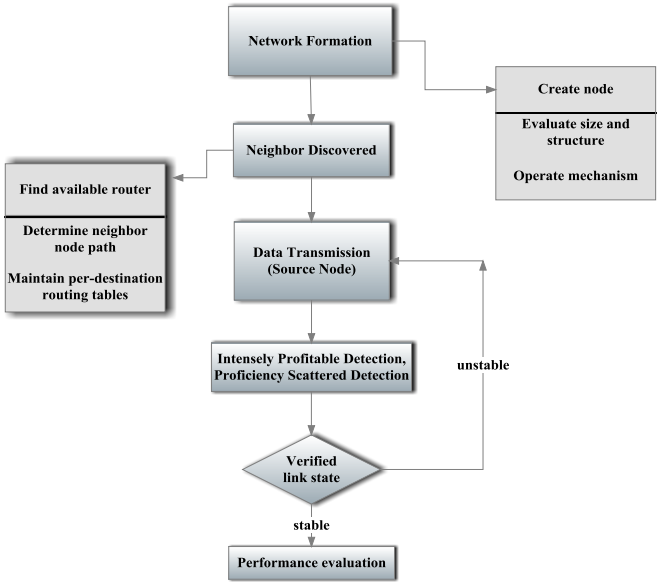

Fig.1. Architecture of node replication attacks using IPD and PSD in WSNs.

To detect the node replicas in wireless sensor networks, two localized algorithms, IPD (Intensely Profitable Detection) and PSD (Proficient Scattered Detection) are proposed. Each node in the localized algorithm can communicate only with its one-hop neighbors. The node can meet again, it can be compared with the first node and previous node location, and attack replication node.

The components of node duplication attacks in WSNs are explained as follows: A network formation is the process of creating the node. Here, each node is in separated manner and can be evaluated in terms of size, structure and also illustrates how these mechanisms operate. A neighbor discovered, can find the available router and also the link of the address. It knows how to determine the path of a neighbor node. To determine the link-layer addresses of neighbors known to reside on attached links, and maintain per-destination routing tables for active connections. The data transmission is used to transfer the data from one network to another network in wireless approach. The data will be in the form of binary information 1s and 0s.

A. *Intensely Profitable Detection (IPD)*

The basic operations of this protocol are as follows: Once two sensor nodes encounter each other, they respectively generate a random number, and then exchange the random numbers. If the two nodes meet again, both of them request the other for the random number exchanged at an earlier time. If the user cannot reply or replies a number which does not match the number stored in its memory, it announces the detection of a replica. To a smart attacker, this scheme is weak, and he/she can establish secret channels among replicas. By this way, replicas can share the random numbers, and fail the protocol. Only constant communication cost *O(1)* is required and the location information of sensor nodes is unnecessary.

In IPD, the replicas cannot connive with each other but this assumption will be evacuated in the following description of PSD. In inclusion, all of the swapped messages should be indicated unless specifically noted. The IPD scheme is composed of two steps: an offline step and an online step. The former is executed before sensor deployment while the latter is executed by each node after deployment.

1) Offline Step

A security parameter and a cryptographic hash function are accumulated in each node. Two arrays of length of *i*, is used to check the authority of acknowledged random numbers. Two lengths are initialized to zero vectors and also blacklisted node is initialized to be empty.

2) Online Step

Let *u* and *v* be the sensor nodes. When *u* meets *v*, it foremost verifies if *v* is in the blacklist or not. If the former condition is satisfied *v* is regarded as a replica by *u* and *u* turns down to correspond with *v*. If it is not in the blacklist, they exchange the random numbers as the length of *u* of *v* and length of *v* of *u*. From the perspective of node *u*, after the response of random number posted by *v*, *u* checks if length (*u*) is the random number posted to *v* at preceding time. The hash function of length *u* (*v)* is similar to length *v* (*u)* holds. Node *v* is added into blacklist of *u*, if confirmation fails. Calculate hash function of randomly generated number and send it to the respective sensor node. Or else calculate blacklist of the respective sensor node.

B. *Proficient Scattered Detection (PSD)*

The basic idea behind Proficient Scattered Detection (PSD) schemes is: 1) for a network without replicas, the number of times, μ1, that the node *u* encounters a specific node *v*, should be limited in a given time interval of length T with high probability 2) for a network with two replicas *v*, the number of times μ2, that *u* encounters the replicas with a same ID should be larger than a threshold within the time interval of length T. According to these observations, if each node can discriminate between these two cases, each node has the ability to identify the replicas. The PSD scheme composed of two steps: off-line and on-line. Off-line step is performed by the network planner before sensor deployment, to calculate the parameters time period T and threshold. An online step is performed by each node per move. Each checks whether the encountered nodes are replicas by comparing threshold with number of encounters at the end of time interval T. This scheme leads to the storage overhead since each node should maintain lists L.

The idea behind PSD is motivated by the following observations. Encounters with a specific node should be limited to high probability during a fixed period of time, while the minimum number of times that encounters the replicas with the same ID should be larger than a threshold during the same period of time.

The witness finding strategy exploits the fact that one sensor node cannot appear at different locations. Unfortunately in mobile networks, the sensor nodes have the possibility of appearing in different locations at different time. In addition, setting a fixed time window *t* in advance and performing the witness finding for every *t* units of time can also keep witness finding strategy feasible in mobile networks.

The Proficient Scattered Detection (PSD) protocol is proposed to address the node replication attacks in mobile networks by adopting a proposed strategy, *remember and challenge*. Moreover, the sensor nodes do not need to be aware of their respective locations when PSD is performed. It should be noted that the location information, however, is necessary for all detection protocols.

1) Offline Step

The array of length (*u)* of length (*n-1)* is used to store the number of encounters with every other node in a given time interval, while blacklist set contains the IDs having been regarded by *u* as replicas. Since the length of the time interval is positively proportional to both the time required to detect the replicas and to the storage overhead, is required to be the smallest value where each node can distinguish the replicas from the genuine nodes.

2) Online Step

Each node locally maintains a counter to record the elapsed time after the beginning of each time interval. After a time unit is reached, the counter should be reset.

After the link state is verified and found that link state is stable, it will evaluate the performance measures. Or else, it will seem to be unstable and it will back to the source node.

IV. Performance Analysis

This section presents the performance evaluation of the proposed IPD and PSD algorithms. The performance is evaluated based on the following measures:

A. *Effect of communication cost*

The communication cost metric is defined as the ratio between the collected summations by the data aggregation scheme used and the real summation of all the individual sensor nodes. Fig.2 illustrates the communication cost and packet size with respect to different time intervals.

When sensor nodes have a larger communication range, the distributions of the number of encounters with the genuine node and replicas can be better separated.Fig.2 demonstrates the comparison of communication cost and packet size with respect to the performance of LSM (existing) protocol by means of IPD and PSD algorithms (proposed).

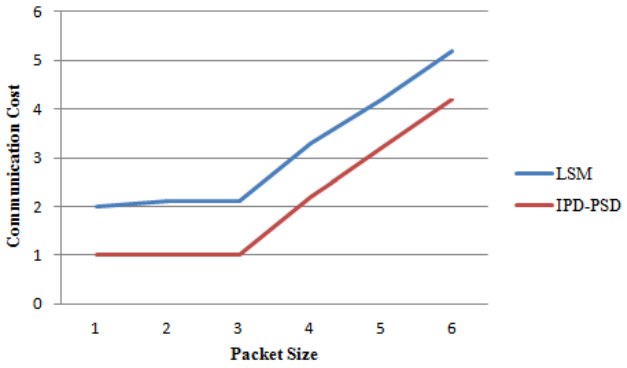

Fig.2.Packet size Vs Communication cost

B. *Effect of Recovery time*

Recovery time is the maximum desired length of time allowed between an unexpected failure and the resumption of normal operations and service levels. It defines the point in time after a failure at which the consequences of the interruption become unacceptable.

Fig.3 demonstrates the comparison of recovery time and faults with respect to the performance of LSM (existing) protocol by means of IPD and PSD algorithms (proposed).

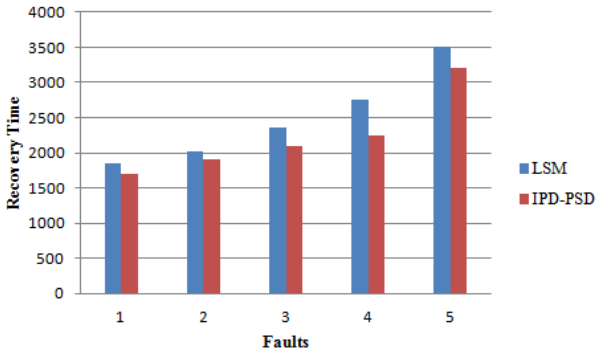

Fig.3.Fault Vs Recovery time

C. *Effect of Misdetection*

The term misdetection denotes incorrect or faulty detection. Fig.4 demonstrates the comparison of misdetection and faults with respect to the performance of LSM (existing) protocol by means of IPD and PSD algorithms (proposed).

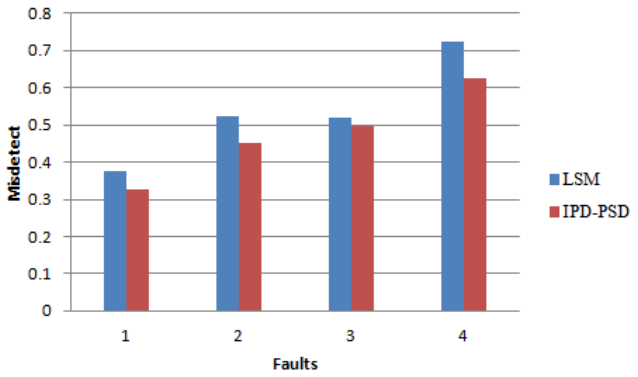

Fig.4. Fault Vs Misdetect

D. *Effect of Delay*

The delay of a network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another. It is typically measured in multiples or fractions of seconds. Delay may differ slightly, depending on the location of the specific pair of communicating nodes.

Fig.5 demonstrates the comparison of delay and faults with respect to the performance of LSM (existing) protocol by means of IPD and PSD algorithms (proposed).

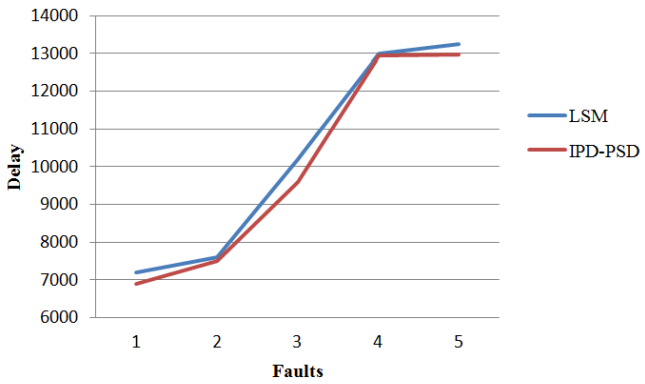

Fig.5. Fault Vs Delay

V. Conclusion and Future Work

Herein, two replica detection algorithms for wireless sensor networks (WSNs) IPD and PSD are proposed. Although IPD is not resilient against collusive replicas, its detection framework, *challenge-and-response*, is considered novel as compared with the existing algorithms. IPD protocol is based on the *remember and challenge* strategy for detecting node replication attacks in mobile networks. A unique feature of IPD is that each node is capable of detecting replicas per move, which contrasts sharply with other protocols that need to mobilize the whole network for replica detection. PSD not only achieves balance among storage, computation, and communication overheads, which are all, but also possess unique characteristics, including network-wide time synchronization avoidance and network-wide revocation avoidance, in the detection of node replication attacks.

In future, a Range-Based Detection Method (RBDM) algorithm will be used to detect replication attacks by all kinds of ranging method (like RSSI), so we can apply it to WSNs with different elements. The RBDM can be used not only as an independent protocol but also as a sub-protocol of any other communication protocol. Thus, it will provide good security, high scalability, low energy consumption and it will also be easy to detect the failure node.

References

[1] M. Conti, et al., "Distributed detection of clone attacks in wireless sensor networks," Dependable and Secure Computing, IEEE Transactions on, 2011, vol. 8, no. 5, pp. 685-698.

[2] X.-M. Deng and Y. Xiong, "A new protocol for the detection of node replication attacks in mobile wireless sensor networks," Journal of Computer Science and Technology, 2011, vol. 26, no. 4, pp. 732-743.

[3] V. Manjula and C. Chellappan, "The replication attack in wireless sensor networks: analysis and defenses," in Advances in Networks and Communications, ed: Springer, 2011, pp. 169-178.

[4] X. Meng, et al., "A note-based randomized and distributed protocol for detecting node replication attacks in wireless sensor networks," in Algorithms and Architectures for Parallel Processing, ed: Springer, 2010, pp. 559-570.

[5] T. D. Tran and J. I. Agbinya, "Early and lightweight distributed detection of node replication attack in sensor networks," in Wireless Communications and Networking Conference (WCNC), 2010 IEEE, 2010, pp. 1-6.

[6] W. M. Xie, et al., "A Detection Scheme against Node Replication Attack in Wireless Sensor Network Based on Bloom Filter and QR Decomposition," Applied Mechanics and Materials, 2013, vol. 427, pp. 1093-1096.

[7] K. Xing and X. Cheng, "From time domain to space domain: Detecting replica attacks in mobile ad hoc networks," in INFOCOM, 2010 Proceedings IEEE, 2010, pp. 1-9.

[8] B. Zhu, et al., "Localized multicast: efficient and distributed replica detection in large-scale sensor networks," Mobile Computing, IEEE Transactions on, 2010, vol. 9, no. 7, pp. 913-926.

[9] W. T. Zhu, "Node replication attacks in wireless sensor networks: Bypassing the neighbor-based

detection scheme," in Network Computing and Information Security (NCIS), 2011 International Conference on, 2011, vol. 2, pp. 156-160.

[10] W. T. Zhu, et al., "Detecting node replication attacks in mobile sensor networks: theory and approaches," Security and Communication Networks, 2012, vol. 5, no. 5, pp. 496-507.

[11] Y. Zeng, et al., "Random-walk based approach to detect clone attacks in wireless sensor networks," Selected Areas in Communications, IEEE Journal on, 2010, vol. 28, no. 5, pp. 677-691.

[12] T. Bonaci, et al., "Distributed clone detection in wireless sensor networks: An optimization approach," in World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011 IEEE International Symposium on a, 2011, pp. 1-6.

[13] J.-W. Ho, et al., "Fast detection of mobile replica node attacks in wireless sensor networks using sequential hypothesis testing," Mobile Computing, IEEE Transactions on, 2011, vol. 10, no. 6, pp. 767-782.

[14] M. Vardhan and D. Kushwaha, "File replication and consistency maintenance mechanism in a trusted distributed environment," CSI Transactions on ICT, 2013, vol. 1, no. 1, pp. 29-49.

[15] A. Mishra and A. Turuk, "A Zone-Based Node Replica Detection Scheme for Wireless Sensor Networks," Wireless Personal Communications, 2013, vol. 69, no. 2, pp. 601-621.

[16] W. T. Zhu, et al., "Review: Detecting node replication attacks in wireless sensor networks: A survey," J. Netw. Comput. Appl., 2012, vol. 35, no. 3, pp. 1022-1034.