Efficient Detection of Replicas and Secrecy of Data Forwarding in Wireless Sensor Network

Gonugunta Kishore[1], Chintada Sunil Kumar [2]

[1]*Final M.Tech Student,* [2]Asst.professor

[1,2]Dept of CSE, *Sarada Institute of Science, Technology and Management (SISTAM), Srikakulam, Andhra Pradesh*

Abstract: *The emerging Wireless Sensor Network (WSN) technology has many security issues due to its unattended nature. Node Replication Attack is a kind of application independent attack in which an adversary deploys its own inexpensive sensor nodes in the network as legitimate sensor nodes. In the existing system, using Localization Algorithm is to resist node replication attacks in mobile sensor networks. Localized algorithm includes localized detection, network-wide synchronization avoidance and network-wide revocation avoidance. Less performance comparisons with known methods are provided to demonstrate the efficiency of our proposed algorithms. In the proposed system, using fast randomized algorithm to identify the genuine node ID available in the network or not, which is verified and compared with the requested node ID to detect whether it is Replica or Genuine node ID. Here, Server maintaining each and every requested node ID's for data transmission. Before transferring data we can encrypt and generate signature of that data using Signcryption technique. By using this technique we can perform the encryption, decryption process and also generate signature of particular data. By implementing those concepts we can improve efficiency of network and also provide more security of transferring message in a wireless sensor network.*

Keywords: *Security and protection, authentication, network protocols, Jamming, Signature.*

I. Introduction

Mobile wireless sensor networks (MWSNs) can simply be defined as a wireless sensor network (WSN) in which the sensor nodes are mobile. MWSNs are a smaller, merging field of research in contrast to their MWSNs is much more versatile than static sensor networks as they can be deployed in any scenario and cope with rapid topology changes. 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. As a result, WSNs are susceptible to many kinds of threats and attacks. While most of them are dealt with them through cryptographic materials provided by the management protocols, some other threats like node replication attacks are one of the most redoubtable attacks where an attacker compromising a node uses its secret cryptographic key materials to successfully populate the network with clones of it.

The node replication attack, an adversary captures a node physically and reproduces the node using the secret credentials which has been extracted and deploys them in the network and disables the Wireless Sensor Network applications. It affects a wide variety of applications such as object tracking to battle surveillance because of its application independent nature. It is also known as clone attack wand the static and mobile wireless sensor networks, the security issues are the same. It creates an extensive harm to the network because the replicated node also has the same identity as the legitimate member. It creates various attacks by extracting all the secret credentials of the captured node. It corrupts the monitoring operations by injecting false data. It can cause jamming in the network, disrupts the operations in the network and also initiates the Denial of Service (DoS) attacks too. To instigate this attack, an adversary only needs to physically capture one node, and after collecting all secret credentials (ID, cryptographic keys, etc.), an adversary replicates the sensor node and deploys one or more clones of the compromised node into the network at strategic positions, damaging the whole network by carrying out many internal attacks.

The low-cost sensor nodes lack protective shield that would allow unauthorized ac- cess to their functional units such as memory, processing and communication. It is infeasible to manufacture tamper-resistant sensors due to cost-constraint. Deploying such vulnerable sensors in unsupervised environment encourages an adversary to launch physical attack with a little effort. In node replication attack, an ad versary physically captures a node from its deployed location. She then accesses the memory, processing, and communication unit of the captured node, and steals relevant information such as identity, secret keys, intrusion detection characteristics etc. Using the stolen information, she then generates a number of replicas of the captured node by incorporating useful stolen information, and deploys them back into the network. These replicas operate under the control of the adversary. They behave like a legitimate node, and participate in the communication using the stolen keying materials.

The aim of an adversary in node replication attack is to control the network activities using replicas. An adversary may either extract useful data from the network or hinder the network operations. With the help of replicas, an adversary can launch insider attacks such as wormhole, selective forwarding, hello flooding, false data injection etc. An adversary can perform all of the above mentioned activities only by compromising a single node in the network. Therefore, node replication is considered as one of the most serious threats in WSN [1, 2].
One of the important characteristics that make a node replication attack more challenging is to differentiate between a legitimate node and its clone1. Since, replicas execute the same network protocols and have the same keying materials as
that of a original node, they pass all authentication and verification process. Most of the solutions reported in the literature recommends for the detection of existence of replicas in the network [3]. These schemes mostly use the parameters such as position, a unique set of neighboring nodes etc. that can differentiate a replica from its original node.

The remainder of this paper is organized as follows. Section 2 discusses the Related work of our proposed system. Section 3 builds the mechanism and designs the algorithm that can efficiently deal with the hidden action and hidden information problem and ensure reliable multi-path routing in the link layer. Section 4 evaluates concludes this paper

II. Related Work

Various schemes based on random uniform deployment have been proposed in static WSNs. Parno et al. [4] proposed a centralized detection scheme using the base station. Each node sends IDs and estimated locations of its neighbors to the base station. If there is a collision of IDs in far distinct locations, then the base station revokes the corresponding sensor nodes by broadcasting an authentic command. Subsequently, Parno et al. [4] proposed two probabilistic detection protocols. The randomized multicast (RM) scheme distributes IDs and locations of neighboring nodes to randomly selected witness nodes, exploiting the birthday paradox to find collisions, whereas the lineselected multicast (LSM) scheme increases the collision probability of RM by adding check points. In the LSM scheme, in addition to the witness nodes, intermediate nodes within the multicast path also check replicas. Conti et al. [4] proposed the randomized, efficient, and distributed (RED) scheme that improves the LSM scheme by using a specially designed pseudo random function. Melchor et al. [5] also modified the LSMscheme, whereby each node does not transmit the pair information (ID and its location) to the selected witness node but receives the pair information from the selected nodes. There are several other derivatives and improved versions of the LSM scheme. Choi et al. [6] proposed a replica detection method using a subset of IDs, and Li and Gong [7] proposed a DHT-based scheme by exploiting the LSM and RED. DHT stands for a distributed hash table used for member checking. Further, Xing et al. [8] proposed a replica detection scheme using a fingerprint, which includes information of neighboing nodes. The fingerprints are fixed on deployment; however, additional complex processes are required to add new sensor nodes. In addition, Zeng et al. [9] proposed a replica detection scheme using a phantom routing technique.

Detection schemes based on grid deployment in static WSNs can be designed to detect replicas more easily than those based on random uniform deployment, by using the nodes' grid information, which has already been demonstrated by Cho et al. [9]. Zhu et al. [10] proposed two gridbased replica detection schemes, single deterministic cell (SDC) and parallel multiple probabilistic cells (P-MPC), which improved the collision probability of RM by using the grid information given to each node. In SDC, the IDs and locations of neighbors are forwarded to a single zone that is determined from a one-way hash function with node's ID as input; however, in P-MPC, the pair information is forwarded to multiple zones that are determined in the same way. Then, every node checks whether or not the IDs received from other nodes are in conflict. Although P-MPC requires a higher communication cost than SDC, it can detect replicas by virtue of nodes in other zones, even when all nodes in a certain zone are compromised by an attacker. We define a powerful attacker who compromises an entire
zone as an aggressive attacker. Unlike Zhu et al. [11], Ho et al. [12] used the distance between a redetermined zone and actually deployed zones to detect replicas. However, if a genuine node is erroneously located in a zone that lies beyond the threshold distance, this simple method may yield a detection error by determining it as a replica. Thus, Ho et al. [12] proposed two schemes, the location claim approach (LCA) and multi-group approach (MGA), to reduce the detection error of the simple method by making the neighbors of the erroneously deployed node send out its location to the nodes in the predetermined zone in an authentic form such as a digital signature. MGA improves the robustness of LCA against aggressive attackers similar to P-MPC. Ho et al. [13] also used a statistical decision process to detect replicas with multiple pieces of evidence. The base station uses the evidence to determine whether a suspected node is a replica.

III.Proposed System

Sensor networks are usually designed and deployed for a specific application. They are scalable with a minimal effort. Network topology changes frequently in WSN due to energy depletion, channel fading, node failure and damage. Sensor nodes are self-configurable and they are densely deployed in the target area. Battery is the only source of energy for most of the sensing devices.

Most of the applications of WSN are data centric and the data-flows within the network obey many-to-one traffic pattern. Due to higher node density, data redundancy may exist in the network. The network consists of 'n' number of nodes. The nodes can request data from other nodes in the network. Since the Nodes have the mobility property, they can move across the network. Server is the module which is used to store all the nodes information like Node Id, packet limit L and replica limit.

Node creation:

In this process, the sample network formation is created. The dynamic network formation is based on node creation & node connection in MANET. The node creation is based on set of node deployment. After the node deployment, the connections are provided. Before establishing connection the server or trusted authority will sent node id (U_i), packet limit (P_L) and replica limit (R_L) to individual nodes in a wireless sensor network.

Trusted Authority or Server:

When a user joins the network, he will request a trusted authority for a rate limit, where authority acts as the network operator. In the request, this user specifies a proper value of L based on calculation of user file size. After getting that value L, authority just checks the request for approval. If the trusted authority approves this request, it issues a rate limit certificate to this user. The user can prove its authenticity to other nodes with rate limit certificate.

Replica Attack and Detection Using fast randomized algorithm:

The Fast Randomized Algorithm to identify the genuine node ID is available in the network or not, which is verified and compared with the requested node ID to detect whether it is replica or genuine node ID. If the node ID is same then it is a genuine node. Else it is a replica node and it is blocked from accessing the network. This is an algorithm which gives excellent results when detecting and verifying on both source location as well as destination location via the server in the networks and is much faster, typically thousands of times faster, than localized algorithms. It gives a new randomized algorithm for achieving consensus among asynchronous processes that communicate by monitoring for every node in the entire network.

Validation of Node:

The validation of node can be done by performing three stages i.e. proof generation, proof delivery and proof validation.

i) Proof Generation:

In this module each node will generate signature for transferring message. Before transferring message each node will convert message into unknown format by using Signcryption encryption process. The encryption process of signcrpytion is as follows.

1.Choose four large prime numbers p, q, r and s randomly and independently of each other. All primes should be of equivalent length.

2. Compute n = p x q, m= r x s, φ= (p-1) x (q-1) and λ=(r- 1) x(s-1).

3. Choose an integer e, 1 < e < φ such that Gcd (e, φ) =1

4. Compute the secret exponent d, 1 < d < φ, such that e x d mod φ =1.

5. Select an integer g=m+1. 6. Compute the modular multiplicative inverse: μ=λ -1 mod m. The public (encryption) key is (n, m, g, e).

The private (decryption) key is (d, λ , μ)

6.Select random number r, where r < m.

7.Compute cipher text as: $c=g^{s\wedge emodn}$ x r^m mod m^2 .

After generating cipher format data the source node will generate signature for that cipher formatted data using one way hash function. In this paper we are using sha-1 one way hash function for generation of signature.

ii) Proof Delivery:

In this module the sender or source node will send cipher formatted data to specified node in the network. Before transferring data to destination node the source node will perform the signature generation process and using that process we can generate signature for that cipher formatted data. After generating the source node will send both value of signature and cipher formatted data to destination node.

iii) Proof Verification process:

In this module the receiver or destination node will retrieve cipher formatted data and signature from the source node. After retrieving those values the destination node again generate signature for cipher formatted data and compare both signature are equal or not. If the both signature are equal the destination node will perform the decryption process of signcryption technique. If the both signatures are not equal the destination node will not get any data from the source node. The decryption process of signcryption technique is as follows.

$$S= (((c^{\lambda} \bmod m^2 -1)/m) \times \mu \bmod m)^{d} \bmod n$$

After performing the decryption process the destination node will get original plain formatted data.

IV. CONCLUSIONS

In this paper we are propose low cost efficient to detect replica in a static wireless sensor network. By implementing proposed system does not need any additional hardware component for identifying replicas in a wireless sensor network. The proposed system mainly contains two concepts for detect replica and also provide more security of transferring message. In this paper we are using fast randomized algorithm for finding replica in a wireless sensor network. Another concept for signcryption technique for data encryption, decryption and also generate signature for cipher format data. By generating signature we can easily identify transferring message will be corrupted or not. So that by implementing those concepts we can improve efficiency of wireless sensor network and also find out transferring message will be corrupted or not. By performing encryption and decryption of transferring message we can improve privacy of data.

V. REFERENCES

[1]. Wazir Zada Khan, Mohammed Y. Aalsalem, Mohammed Naufal Bin Mo- hammed Saad, and Yang Xiang. Detection and Mitigation of Node Repli- cation Attacks in Wireless Sensor Networks: A Survey. International Journal of Distributed Sensor Networks, 2013(2013):01 – 22, 2013.

[2] B. Gowtham and S. Sharmila. Location Traced Hybrid Detection of Node Replication Attack in Mobile Wireless Sensor Network. IJCA Special Issue on Information Processing and Remote Computing, IPRC(1):12 – 15, August 2012.

[3] Wen Tao Zhu, Jianying Zhou, Robert H. Deng, and Feng Bao. Detecting Node Replication Attacks inWireless Sensor Networks: A survey. Journal of Network and Computer Applications, 35(3):1022 – 1034, May 2012.

[4]. B. Parno, A. Perrig, and V. Gligor, "Distributed Detection of Node Replication Attacks in Sensor Networks," Proc. IEEE Symp. Security and Privacy, pp. 49-63, 2005.

[5]. C.A. Melchor, B. Ait-Salem, and P. Gaborit, "Active Detection of Node Replication Attacks," Int'l J. Computer Science and Network Security, vol. 9, no. 2, pp. 13-21, 2009.

[6] H. Choi, S. Zhu, and T.F.L. Porta, "Set: Detecting Node Clones in Sensor Networks," Proc. Third Int'l Conf. Security and Privacy in Comm. Networks and the Workshops (SecureComm '07), pp. 341-350, 2007.

[7]. Z. Li and G. Gong, "DHT-Based Detection of Node Clone in Wireless Sensor Networks," Proc. First Int'l Conf. Adhoc Networks, pp. 240-255, 2009.

[8] K. Xing, F. Liu, X. Cheng, and D.H.C. Du, "Real-Time Detection of Clone Attacks in Wireless Sensor Networks," Proc. 28th Int'l Conf. Distributed Computing Systems (ICDCS '07), pp. 3-10, 2008.

[9] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "Random-Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks," IEEE J. Selected Areas Comm., vol. 28, no. 5, pp. 677-691, June 2010.

[10]. K. Cho, M. Jo, T. Kwon, H.-H. Chen, and D.H. Lee, "Classification and Experimental Analysis for Clone Detection Approaches in Wireless Sensor Networks," IEEE Systems J., vol. 7, no. 1, pp. 26-
35, Mar. 2013.

[11]. B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, "Localized Multicast: Efficient and Distributed Replica Detection in Large-Scale
Sensor Networks," IEEE Trans. Mobile Computing, vol. 9, no. 7, pp. 913-926, July 2010

[12]. J.-W. Ho, D. Liu, M. Wright, and S.K. Das, "Distributed Detection of Replica Node Attacks with Group Deployment Knowledge in Wireless Sensor Networks," J. Ad Hoc Networks, vol. 7, no. 8,
pp. 1476-1488, Nov. 2009.

[13]. J.-W. Ho, M. Wright, and S.K. Das, "Zonetrust: Fast Zone-Based Node Compromise Detection and Revocation in Wireless Sensor Networks Using Sequential Hypothesis Testing," IEEE Trans. Dependable and Secure Computing, vol. 9, no. 4, pp. 494-510, July-Aug. 2012.

BIOGRAPHIES:

Gonugunta Kishore is student in M.Tech (CSE) in Sarada Institute of Science Technology and Management, Srikakulam. He has received his B.Tech (IT) Sarada Institute of Science Technology and Management, Srikakulam. His interesting areas are network security and web techonologis.

Chintada Sunil Kumar working as a Asst Professor of CSE in Sarada Institute of Science, Technology and Management (SISTAM), Srikakulam, Andhra Pradesh. He received his **M.Tech** (CSE) from Jntuk, Kakinada. Andhra Pradesh. His interest research areas are Database management sysytems,Computer Architecture, Image Processing, Computer Networks, Distributed Systems. He published 4 international journals and he was attended number of conferences and workshops.