International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 8, August - 2014

IDS for Node Replicas at Distributed & Centralized Levels in Mobile WSN

Mohit Gupta
PG Student, Dept. of ECE
Ludhiana College of Engineering & Technology, PTU
Ludhiana, Punjab, India

Manisha Lumb
Asstt. Prof., Dept. of ECE
Ludhiana College of Engineering & Technology, PTU
Ludhiana, Punjab, India

***Abstract*: Wireless Sensor Networks (WSNs) consist of sensor nodes, deployed in hostile environments where they are often vulnerable to physical capture and compromise. Once a sensor node is compromised, the adversary can extract cryptographic secrets from node, replicate the compromised node and distribute the clones at strategic positions in the network for malicious attacks. This is known as node replication attack. So it is critical to ensure the security of sensor networks. Existing detection schemes for node clone attacks are mainly focused on static networks which rely on the witness-finding strategy, which cannot be applied to mobile networks. In this paper, Distributed & Centralized Level (DCL) method is proposed to detect node replicas in mobile sensor networks. The security and performance analysis indicate that this method can identify clone attacks with a high detection probability at the cost of low energy consumption. Our simulation results show that our method achieves effective and robust replica detection capability.**

Keywords: clone detection, network security, node replication attack, wireless sensor network.

I. INTRODUCTION

Wireless sensor networks (WSNs) have been used in various applications, e.g., military, environmental, and health applications. When WSNs are deployed in hostile scenarios, such as surveillance on the battlefield, they must confront the threats from attackers (e.g., enemies on the battlefield). This is because the attackers may intend to learn information from the WSNs or disable the functions of the WSNs. For example, on the battlefield, the enemies would hope to learn the private locations of soldiers from, or inject wrong commands into the sensor network. So it is critical to ensure the security of sensor networks in such scenarios [1].

One important physical attack is the introduction of cloned nodes into the network. In a node replication attack or a node clone attack, an adversary physically captures a sensor node, extracts cryptographic secrets from the node, and distributes an arbitrary number of replicas of captured node throughout the network.

Replicated nodes will be recognized as legitimate members of the network since they carry all cryptographic secrets extracted from captured node, and thus could be used by the adversary to launch a variety of insider attacks. The capture of nodes is plausible because sensor nodes are usually unprotected by physical shielding due to cost considerations, and are often left unattended after deployment [2].

In mobile wireless sensor networks (MWSNs), the sensor nodes can move on their own, and after deployment, appearing at different locations at different times. Node mobility, routing attack and replica colluding are the main obstacles and hence authentication is difficult [3].

In this paper, a novel method for detecting node clone attacks in mobile wireless sensor network, namely Distributed & Centralized Level (DCL) method is proposed. Our contributions are as follows:

i) The method is fully distributed. All information exchange occurs in a single hop neighbourhood; therefore, the detection protocol will work even if there is no reliable communication path between the distant node pairs, which is likely to happen in a routing attack.

ii) The method is highly robust against replica colluding attack as it works even if replicas can communicate with one another at zero delay.

iii) The security and performance analysis indicate that the method can identify node clone attacks with a high detection probability at the cost of the low energy consumption. The simulation results show that our method outperforms the existing methods.

The remainder of this paper is organized as follows. In section 2, we introduce related works on node replication attack. In section 3, the network and security models are defined. Our proposed method DCL is presented in section 4 and the security and performance analysis are given in section 5. Finally, we conclude our work in section 6.

II. RELATED WORKS

Several approaches have been proposed in the literature for detecting the attacks in WSNs and for ensuring the security.

Based on the requirement that each node must broadcast a signed location claim of itself to its neighbours at a certain synchronized time, most of the existing distributed detection schemes such as RM [4], LSM [4], DM [12], Broadcasting [12], SDC [5], and RED [6] adopt the witness finding strategy, in which each node finds a set of sensor nodes somewhere as the witnesses for checking whether there are the same IDs

used at different locations, for replica detection. In the witness finding strategy, nodes are required to sign and transmit a location claim to its witness nodes. Two conflicting location claims that claim the same node ID (signed by the same key) appear at different locations, implies a node clone attack. The witness-finding strategy exploits the fact that one sensor node cannot appear at different locations, but unfortunately, the sensor nodes in mobile sensor networks have the possibility of appearing at different locations at different times, so the above schemes cannot be directly applied to mobile sensor networks.

Zhu et al. [7] proposed a key management protocol for sensor networks that provides a defense against the clone attack. The idea is to remove the master key once a sensor established pairwise keys so that although the adversary may generate clones of a node and deploy them, the clones cannot establish pairwise keys with the new neighbours. All afore mentioned detection schemes are designed only for static networks.

Choi et al. [14] proposed SET technique for detecting node clones in sensor networks. In this technique, the system is arbitrarily partitioned into the subsets. Numerous roots are haphazardly chosen to develop various sub-trees, and every subset is a hub of the sub-tree. Every subset pioneer gathers data and advances it to the base of the sub-tree. The convergence operation is performed on every base of the sub-tree to recognize imitated hubs. Then, it is passed to the BS. The BS catches the clone hubs by processing the convergence of any two accepted sub-trees.

Yu et al. [8] present a challenge and response strategy to construct the first distributed replica detection scheme, eXtremely Efficient Detection (XED) for mobile sensor networks. The idea behind XED is motivated from the observation that for the networks without replicas, if a sensor node n1 meets the other sensor node n2 at earlier time and sends a random number r to n2 at that time, then when n1 and n2 meet again, n1 can ascertain whether this is the node n2 met before by requesting the random number r. Based on this observation, a "remember and challenge strategy" is proposed.

Ho et al. [9] also propose a detection scheme for mobile sensor networks by using sequential probability ratio test (SPRT) in which an uncompromised mobile sensor node measured speed will appear to be at most the system-configured maximum speed as long as speed measurement system with low error rate is employed. On the other hand, replica nodes will appear to move much faster than original nodes, and thus their measured speeds will likely be over the system-configured maximum speed because they need to be at two different places at once. Accordingly, if it is observed that a mobile node measured speed is over the system-configured maximum speed, it is then highly likely that at least two nodes with the same identity exist and thus replicas are detected.

Yu et al. [10] proposed two schemes: Efficient and Distributed Detection (EDD) and its variant, SEDD to detect the node replicas in mobile sensor networks in a distributed fashion without involving the base station. For a network without replicas, the number of times t1, in which the node n1 encounters a specific node n2, should be limited in a given time interval of length l with high probability. For a network with two replicas n2, the number of times, t2, in which n1 encounters the replicas with the same ID n2, should be larger than a threshold within the time interval of length l. According to these observations, if each node can discriminate between these two cases, each node has the ability to identify the replicas.

Lou et al. [2], proposed Single Hop Detection (SHD) protocol which consists of two phases, the fingerprint claim and the fingerprint verification phases. In the fingerprint claim phase, each node is required to sign its neighbour node list. The signed neighbour node list is a fingerprint of its current neighbourhood community, hereafter referred as fingerprint claim. The fingerprint claim is broadcasted in one-hop neighbourhood. Upon reception of a fingerprint claim from a neighbouring claim node, the receiver node will decide whether to become a witness node of the claim node. When it decides to become a witness node, the node will then verify the fingerprint claim using and finally store the fingerprint claims of the witnessed nodes locally if the claim passed the verification process. In the fingerprint verification phase, when two nodes meet with each other, they exchanges their witnessed node lists and the two nodes then check for a possible fingerprint claim conflict with received claims. In a fingerprint claim conflict, there are two fingerprint claims with the same ID and private key claiming two different neighbourhood communities, which implies two detected replicas.

It is found that only few schemes are proposed for mobile sensor networks. Due to the consideration of nodes' mobility and the distributed nature of sensor networks, it is desirable, but very challenging, to have an efficient distributed scheme for detecting the replicas in mobile WSNs.

III. NETWORK AND SECURITY MODELS

A. *Network Model*

The WSN usually contains hundreds and sometimes thousands of cheap and small size wireless sensor nodes, which are accidentally or in a pre-designed way distributed in a vast geographic area. In WSNs it is assumed that every moment there is the possibility that a number of sensor nodes get lost or be added to the network. The communication is assumed to be symmetric. In addition, each node is assumed to periodically broadcast a beacon containing its ID to its neighbours. In DCL method, the sensor nodes have mobility and move according to the random waypoint model [11], which is commonly used in ad hoc networks.

B. *Security Model*

In our method, sensor nodes are not tamper resistant. In other words, the corresponding security credentials can be accessed after sensor nodes are physically captured. We assume that sensor nodes could be captured by the adversary immediately after the sensor deployment i.e. there is no secure bootstrapping time available after the sensor deployment. Replicas have all the legitimate credentials from the captured nodes. Replicas are assumed to achieve simultaneous collusion, which implies they can communicate with each other without incurring time delay or with zero time delay. We assume that the adversary cannot create senor node with a new ID (ID which is not pre-existing in the network) because it is difficult for the adversary to have the corresponding security credentials.

IV. DISTRIBUTED & CENTRALIZED LEVEL (DCL) METHOD

In this section, we present our proposed Distributed & Centralized Level (DCL) method. The DCL method exploits the fact that at any time, a physical node (or equivalently, its node ID and private key) cannot appear at different neighbourhood community otherwise there must be replicas in the network. The neighbourhood community of a node is characterized by its one-hop neighbour node list, which is readily available in a typical WSN since sensor nodes need to know their neighbours in order to communicate with each other.

In DCL method, the detection takes place at two levels: Distributed and Centralized. At distributed level, the detection of clone nodes takes place by the cluster head (CH). At centralized level, the detection of clone nodes takes place by the base station (BS).

The steps to be followed while implementing the proposed protocol is explained as follows:

- The nodes are randomly deployed in the network. As the network considered is mobile wireless sensor network and nodes are mobile in nature, nodes start moving in the network; change their locations time to time.
- After deployment, cluster based approach is applied in the network in which whole network is divided into several segments called clusters. Clustering is done based on the coordinates (location) of the nodes at any instant.
- Each cluster has a cluster head (CH) which is selected among the cluster members. The node with the highest energy is chosen as cluster head in each cluster.
- Each node then finds its two shortest neighbour nodes and saves their IDs list.
- Each node sends its shortest neighbour list to their corresponding CHs for detecting whether the replicas are present in the network or not.
- If a node and its clone nodes are present in the same cluster, then the shortest neighbour list of both the nodes will be different and thus the clone is detected by the cluster head.
- Each CH obtains the list (known as member list) of node IDs present in their respective clusters.
- When CH move and come closer to the other CHs, they exchange their member lists.
- In case if the clones are present in different clusters then CHs will detect the clone by comparing the member lists.
- Then CHs will send their member lists along with their IDs to BS.
- If two or more CHs are clones of each other i.e. possessing same ID but different member list then BS will detect the clones.
- If CH of one cluster and node present in some other cluster are clones of each other then also BS will detect the clones or replicas.

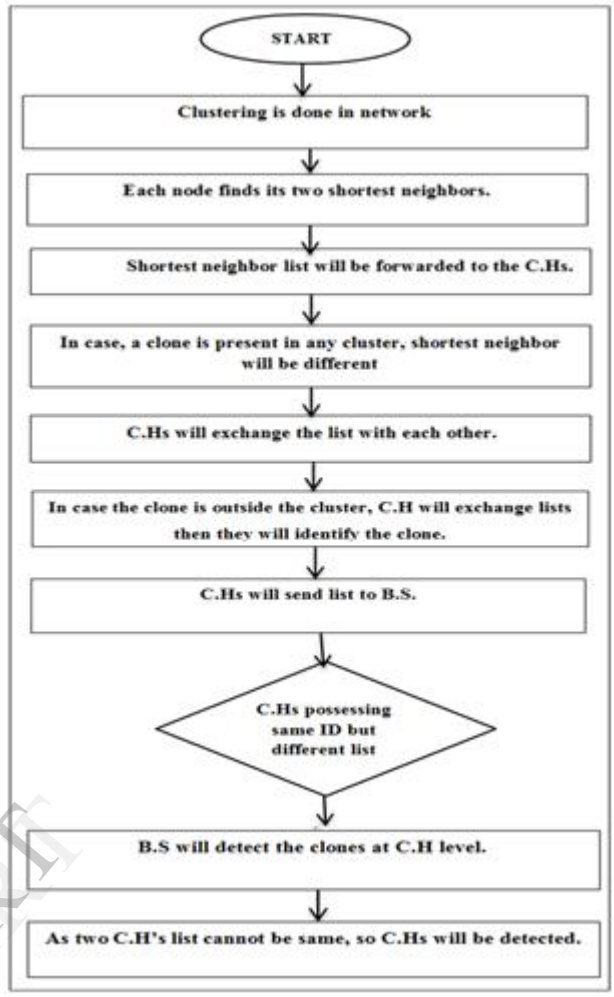


Fig. 1: Flowchart of proposed solution

V. PERFORMANCE EVALUATION

The proposed algorithm is implemented in Network Simulator-2 (NS2) and the performance is evaluated in terms of energy consumption, detection rate and routing overhead.

A. Simulation Parameters

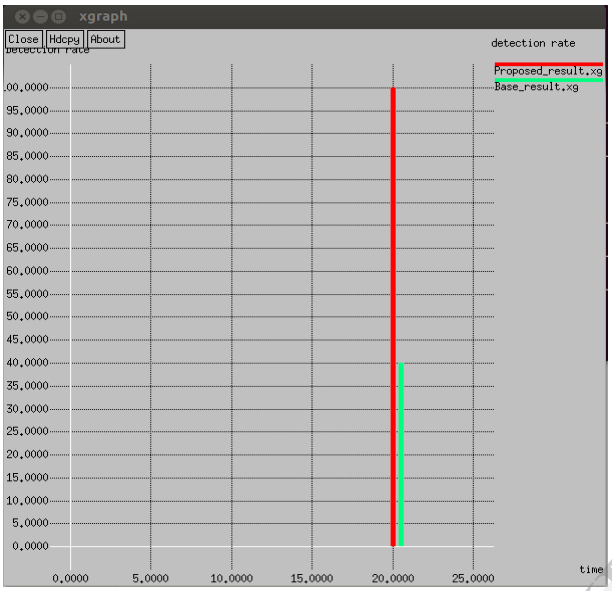
The parameters used in our simulation are shown in Table I. A few nodes are selected and given multiple identities which act as clone nodes.

Table I: Simulation Parameters

Channel Type	Wireless
Nodes	50
Transmission protocol	UDP
Traffic Generator	CBR
Topology	Flat Grid
Queue type	Drop tail
Propagation model	Two Ray Ground
Antenna model	Omni directional
Routing protocol	AODV
Initial energy	50 Joules

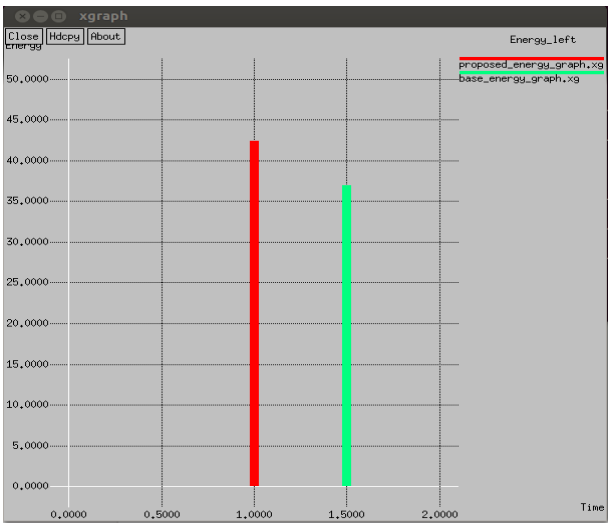
B. Simulation Results

1) *Detection Rate:* Our simulation results show that our method achieves higher detection rate than SHD protocol. A total of 5 clone nodes were deployed in the network and DCL method has managed to detect all the deployed clones whereas SHD was able to detect 40% of the clones. The reason to less detection rate of the SHD protocol may be attribute to the fact that some of the witness nodes might be the clone nodes and SHD defines no procedure to detect such clones.



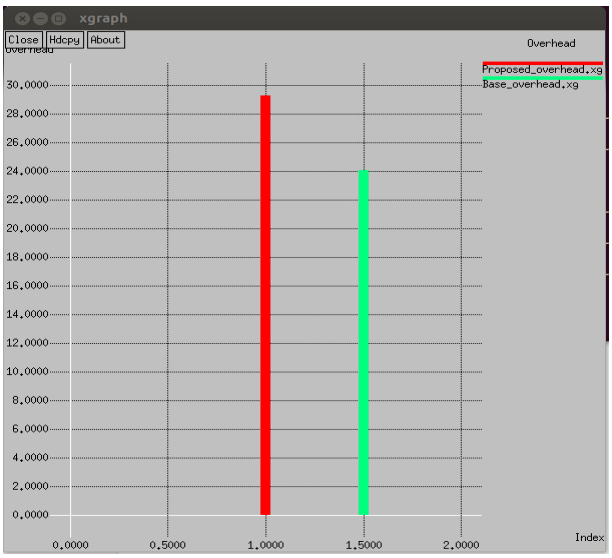
Graph 1: Comparison of Detection Rate

2) *Residual energy:* This graph shows the remaining energy in the network. The residual energy for SHD is less the DCL because of the fact that more mutual broadcasting takes place in the SHD while exchanging the neighbourhood communities.



Graph 2: Comparison of Residual Energy

3) *Routing Overheads:* Overheads occurred in DCL method is slightly more than that of SHD protocol. This reason is attributed to the fact that we have used decentralised as well as centralised method for the detection of the clones in the network.



Graph 3: Comparison of Routing Overheads

VI. Conclusion and Future Work

Node replication attack is a great threat to the security of wireless sensor networks. Existing detection methods fail to hold in mobile WSNs, or if nodes collude to subvert the detection protocol. In this paper, Distributed & Centralized Level (DCL) method is proposed, which is fully distributed and centralized in that all communication happens between single hop neighbours, highly robust against node colluding, and highly efficient. Our simulation results show that our method is efficient in detecting node replicas with a high detection probability at the cost of low energy consumption. The routing overheads in our method are slightly more than SHD protocol. In future, we would like to reduce the routing overheads so as to detect node replicas in the network more efficiently.

Acknowledgment

The paper has been written with the kind assistance, guidance and active support of my department who have helped me in this work. I would like to thank all the individuals whose encouragement and support has made the completion of this work possible.

REFERENCES

[1] Yingpei Zeng, Jiannong Cao, Shigeng Zhang, Shanqing Guo and Li Xie, "Random-Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks," IEEE Journal on Selected Areas in Communications, Vol. 28, No. 5, June 2010.

[2] Yanxiang Lou, Yong Zhang and Shengli Liu, "Single Hop Detection of Node Clone Attacks in Mobile Wireless Sensor Networks" in Proceedings of International Workshop on Information and Electronics Engineering (IWIEE), 2012 pp. 2798 – 2803.

[3] Raju Metal and Selvan Metal, "An Approach in Detection of Replication Node in Wireless Sensor Networks: A Survey," International Journal of Computer Science and Information Technologies, Vol. 5, No. 1, 2014, pp. 192-196.

[4] Bryan Parno, Adrian Perrig and Virgil Gligor, "Distributed Detection of Node Replication Attacks in Sensor Networks" in Proceedings of IEEE Symposium on Security and Privacy, 2005, pp. 49 – 63.

[5] B. Zhu, V. G. K. Addada, S. Setia, S. Jajodia, and S. Roy, "Efficient Distributed Detection of Node Replication Attacks in Sensor Networks" in Proceedings of Computer Security Applications Conference, 2007, pp. 257 – 267.

[6] M. Conti, R. D. Pietro, L. V. Mancini, and A. Mei, "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, 2007, pp. 80-89.

[7] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks" in Proceedings of the 10th ACM Conference on Computer and Communications Security, 2003 pp. 62 - 72.

[8] Chia-Mu Yu, Chun-Shien Lu, and Sy-Yen Kuo, "Mobile Sensor Network Resilient Against Node Replication Attacks" in Proceedings of IEEE Symposium on Sensor, Mesh and Ad Hoc Communications and Networks, 2008, pp. 597 - 599.

[9] Jun-Won Ho, Matthew Wright, Sajal K. Das, "Fast Detection of Node Replication Attacks in Mobile Sensor Networks," IEEE Transactions on Mobile Computing, 2008, Vol. 10, No. 6, pp. 767-782.

[10] Chia-Mu Yu, Chun-Shien Lu, and Sy-Yen Kuo, "Efficient and distributed detection of node replication attacks in mobile sensor networks," in Proceedings of IEEE Vehicular Technology Conference Fall, 2009 pp.1– 5.

[11] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," The International Series in Engineering and Computer Science, Vol. 353, pp. 153-181.

[12] Suvarna Game and Chandrashekhar Raut, "Protocols for detection of node replication attack on wireless sensor network," IOSR Journal of Computer Engineering, Vol. 16, No. 1, pp. 1-11.

[13] W.Z. Khan, M.Y. Aalsalem, M.N. Bin, M. Saad, and Y. Xiang, "Detection and Mitigation of Node Replication Attacks in Wireless Sensor Networks: A Survey," International Journal of Distributed Sensor Networks, Vol. 2013, Article ID 149023

[14] Heesook Choi, Sencun Zhu, Thomas F. La Porta, "SET: Detecting node clones in Sensor Networks", Security and Privacy in Communications Networks Workshop, Volume: 17, Issue: 9, 341 - 350, (2012).

AUTHORS PROFILE

Mohit Gupta received the B.Tech. degree in Electronics and Communication Engineering from Rayat- Bahra Institute of Engineering & Bio-Technology, Punjab, India in 2012. Currently, he is pursuing M.Tech. in Electronics & Communication Engineering from Ludhiana College of Engineering & Technology, Punjab, India under the supervision of Asst. Prof. Manisha Lumb.

Manisha Lumb is Assistant Professor in Electronics & Communication department, Ludhiana College of Engineering & Technology, PTU, Punjab, India. She received the B.Tech. degree in Electronics & Communication Engineering from Punjab College of Engineering and Technology and M.Tech. degree in Electronics & Communication Engineering from D.A.V.I.E.T, Punjab, India. She completed her M.Tech. Thesis on CBIR technique using five different types of image formats. She is now supervising several PG candidates.