International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 5, Issue 4, July - August 2016 **ISSN 2278-6856**

A New Approach to Detect Clone Attack in WSN

Swati Raimule[1], Anjali Chandavale[2]

[1]Savitribai Phule Pune University, MIT College of Engineering,
Paud Road, Kothrud, Pune, India

[2]MIT College of Engineering, Savitribai Phule Pune University,
Paud Road, Kothrud, Pune, India

Abstract

Wireless Sensor Network (WSN) has wide range of applications from defense purpose to general purpose. Because of low cost, small size and compactness of sensors, they can be deployed anywhere for important tasks. Wireless sensor networks are often deployed in the areas where they cannot be monitored easily, and they are left unattended for long time. This makes wireless sensor networks prone to different types of attacks. One of them is Clone attack. In this attack, the adversary captures and compromises legitimate node and makes the clones or replicas. Then adversary inserts those nodes inside the network. Sometimes the sensors carry confidential data with it. If these clone nodes are not quickly detected, an adversary can be further mount a variety of internal attacks. As a result, the various protocols and sensor applications get deteriorated. Several protocols have been proposed in the literature to tackle the crucial problem of clone detection, which are not satisfactory as they have some serious drawbacks. In this paper we propose a new distributed protocol called Neighbor Division Random Walk (ND-RAWL) for Clone attack detection in static WSNs. It is based on claimer-reporter-witness framework. ND-RAWL detects clone nodes with the help of a claimer-reporter-witness framework and a random walk is used within each area for the selection of witness nodes. Our simulation results show that ND-RAWL do better than the existing witness node based strategies with moderate communication overhead.

Keywords- Clone Attack, Security, Wireless Sensor Networks, Claimer-Reporter-Witness framework.

1. INTRODUCTION

Wireless sensor network has various applications and in these applications, nodes are often deployed in the areas where they cannot be monitored easily, and they are left unattended for long time in hostile environment. They are exposed to various kinds of security threat, and clone attack is one among them. In this attack, an adversary captures a legitimate node from the network and creates a number of clones of the original node, and inserts the clones back into the network. By using these clones, the adversary can control the various network activities and launch other insider attacks. Various protocols are proposed to detect these cloned nodes. These protocols are divided in two schemes such as Centralized schemes and Distributed Schemes. Centralized schemes generally need the central control (e.g. Base Station) means the clone detection process is carried out at base station. The Distributed schemes do not need central control means the clone detection process runs on every node of the network. In clone node detection process, the node ID and location of node plays important role.

The most encouraging distributed techniques for the detection of clone attacks use the framework called claimer reporter witness (CRW) framework. So these techniques are called claimer reporter witness based or witness node based techniques. These techniques work according to the nature of WSNs. The goals of these techniques are as follows:

- To detect cloned nodes in a distributed as well as random manner with fair overheads.
- To give resilience against smart attacker and guarantee high detection probability of clones even in the presence of compromised nodes in the network.

But the existing CRW based techniques have not done well in achieving these important goals. They are either failed to achieve the desirable clone detection probability or they cannot protect the network against smart attackers, also have high overheads.

In this paper, we have selected a number of existing CRW based clone detection schemes for the evaluation: Randomized Multicast (RM) [3], Line Selected Multicast (LSM) [3], SDC and P-MPC [4], Randomized Efficient Distributed Protocol (RED) [2], Random Walk (RAWL) [1]. Amongst all the CRW based clone detection techniques in WSNs, Random Walk (RAWL) [1] shows the potential to of random walk and random witness nodes selection by initiating numerous random walks throughout the network, solving the drawbacks of other witness node based strategies [3]. Although RAWL has achieved high security of witness nodes but still it shows some considerable limitations as follows:

- RAWL shows increased communication and memory overheads.
- To get the intersecting witness nodes, RAWL needs more random walks with long walk steps.
- RAWL needs more reporters to forward the location claim to randomly selected witness nodes.

Thus, RAWL has some drawbacks. To overcome these drawbacks, we present an approach to detect clone attacks in WSNs with reasonable communication cost.
In this paper we present a new distributed solution called Neighbor Division-Random Walk (ND-RAWL) which shows the division of the witness nodes into different areas with a random walk. It is also based on claimer-reporter-witness framework.

The rest of the paper is organized as follows: The CRW architecture is described in Section 2. The selected CRW based schemes are summarized in Section 3. Section 4 presents some essential requirements of distributed witness based techniques, the network and adversary models used for our proposed scheme. Section 5 describes our proposed protocol to detect clone attacks. Section 6 presents the simulation results and finally in Section 7 we conclude the paper.

2. CRW Framework

Some of the distributed techniques of detecting clone attacks are witness node based techniques. These techniques follow the claimer-reporter-witness (CRW) framework to detect the clones. The CRW framework consists of three components, claimer, reporter and witness node. The Claimer node is a node which locally broadcasts its location claim (Node Id, location) to its neighbors. The Reporter node is the neighbor node that is responsible to forward the location claim to witness nodes. The Witness node is a node that is responsible for storing the location claim as well as finding out the conflicting location claims. In this framework, each node can be a claimer or reporter or witness at the same time. The working of CRW based techniques is shown in Fig. 1.
The most important roles of each component of CRW framework are as follows:

Claimer node:

- Generates the Signature and signs the location claim.
- Forwards the location claim to its neighbors.

Reporter node:

- Receives the location claim from its neighbors.
- Verifies the Signature.
- Checks the plausibility of the location claim.
- Forwards the location claim to randomly selected nodes or location in the network.

Witness node:

- Receives the location claim from the reporter nodes.
- Verifies the location claim.
- Stores the location claim.
- Checks the location conflict.

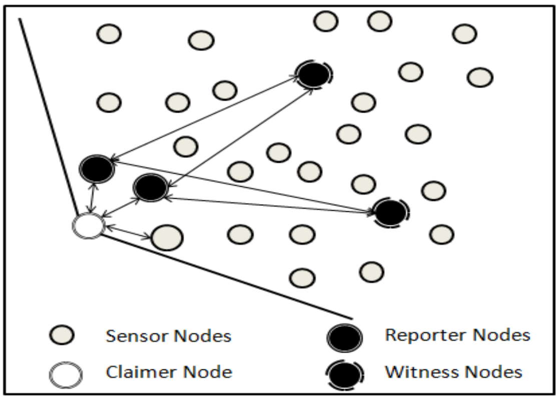

Figure 1 The Claimer Reporter Witness Based Framework

3. Related Work

To achieve high detection probability with moderate overheads, the CRW based techniques use the claimer reporter witness framework. Some of the CRW based techniques are described below:
The two protocols Randomized Multicast (RM) and Line-Selected Multicast (LSM) were proposed by B.Parno et al. [3] for the detection of clones in wireless sensor networks which use the claimer reporter witness framework.

3.1 Randomized Multicast (RM)

In RM [3], a claimer node declares its location by broadcasting the signed location claim to the nodes in its neighborhood. Then every neighboring node becomes a reporter after verifying the plausibility of the location. Each reporter then selects arbitrary destinations in the network and passes the authenticated location claim to the nodes near to those arbitrary locations. These nodes are called witness nodes. So reporters of cloned node (present in the network) also select arbitrary destinations. This protocol uses the birthday paradox; at least one common witness will receive two conflicting location claims with high probability. This witness node can immediately announce the evidence of incoherent location claims in the network to revoke the clone node.

Drawback: High communication costs as each and every neighbor sends a lot of messages to get common witness node.

3.2 Line-Selected Multicast (LSM)

To reduce the communication cost and increase the probability of detection, Line-Selected Multicast (LSM) protocol is proposed. When a location claim travels from reporter node to witness nodes, it also passes through several intermediate nodes and these intermediate nodes also store the location claim. Thus, a line can be effectively drawn across the network. If a conflicting location claim crosses the line, then the node at the intersection will detect the conflict and initiate a revocation broadcast.

Drawbacks:

- In LSM, the adversary protects the replica by jamming or compromising the intersection node.
- In LSM, the energy of the witness nodes is reduced because the most of witnesses are selected from the center of the network; so such exhausted nodes become the attractive point for the adversary.

3.3 SDC and P-MPC Protocols

Two distributed protocols Single Deterministic Cell (SDC) and Parallel Multiple Probabilistic Cells (P-MPC) are proposed by Zhu et al. in [5]. To get high detection probability, the network is divided into cells and all the nodes within the cell as witnesses. In the SDC protocol, each node ID is attached to one cell. Geographic hash function [6] is used to send the location claim of each node to the mapped cell and transmitted within the cell [5]. Nodes in the cell become witnesses with some probability by storing the location claim. [5]. In P-MPC, each node ID is forwarded to the multiple cells with different probabilities by using Geographic Hash function. So, the group of mapped cells is fixed only.

Drawback: An adversary launches the attack by compromising the witnesses and restricts the number of nodes that can act as witnesses.

3.4 RED Protocol

Randomize Efficient Distributed (RED) algorithm was proposed by Conti et al. in [2]. In RED, the witness nodes are chosen Pseudo randomly. A Pseudorandom function takes Claimer node ID and Rand value broadcasted by base station as arguments and generates the ID's of witness nodes. RED algorithm requires centralize system to transfer the rand value to whole network.

Drawback: Because of centralize system, RED adds some overhead.

3.5 RAWL and TRAWL Protocols

Random Walk (RAWL) and Table-assisted Random Walk (TRAWL) protocols are proposed by Y.Zeng et al in [1] for the detection of clone attack in wireless sensor networks. The Random Walk (RAWL) starts several random walks randomly in the network for each node, and then selects the passed nodes as the witness nodes of that node. RAWL works in following steps in each execution.

(1) Each node broadcasts a signed location claim.
(2) Each neighbor of these nodes probabilistically forwards the claim to some randomly selected nodes.
(3) Then, each randomly selected node sends a message with the claim to start a random walk in the network, and the passed nodes are selected as witness nodes and will store the claim.
(4) If any witness receives different location claims for a same node ID, it can use these claims to revoke the replicated node.

The second protocol, TRAWL is based on RAWL and adds a trace table at each node to reduce memory cost. The RAWL needs more random walks and random walk steps for achieving high detection probability that leads to higher communication and memory cost which is more than twice communication overhead of LSM [3].To reduce the memory cost the authors proposed TRAWL but the communication cost still exists. Fig. 2 shows the working of RAWL protocol.

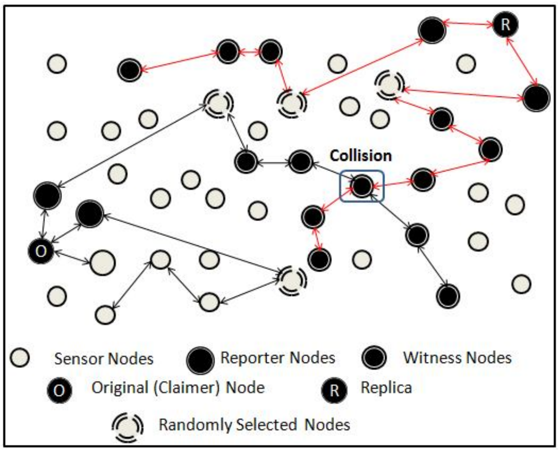

Figure 2 The RAWL protocol based on CRW framework

4.Requirements of Distributed Detection

Witness node plays an important role in witness node based techniques as these witnesses finally detect and revoke the clones in the network. So security of such witness nodes is very important. For this, each distributed detection protocol should satisfy following security requirements.

- The witness selection should be non-deterministic [1].
- All the nodes in the network should have an equal probability of being witnesses.
- The witness nodes should be uniformly distributed throughout the network [1].
- The witness nodes should not be selected repeatedly from any particular location of the network.
- The distributed detection protocol should generate small overhead in such a manner, that it should be sustainable by the WSN as a whole, and (almost) evenly shared among the nodes.

4.2 Assumptions

4.1.1 Network model

Nodes are uniformly distributed in deployment field. Nodes know their own locations. Nodes are stationary, at least during the execution of replica-detection protocol. Each node in the network has unique ID. The communications between any two nodes are protected by pair-wise keys. The adversary cannot create new IDs for replicas. New sensor nodes can be added into the network in order to replace the old ones with necessary requirements.

4.1.2 Adversary model

We assume a simple but powerful adversary who can launch a clone attack. The compromised nodes and replicas are fully controlled by the adversary and can communicate with each other at any time. Adversary tries to prevent clones from being detected by detection algorithm. An adversary may select only limited number of nodes to capture and compromise.

5. PROPOSED METHOD

5.1 Neighbor Division-RAWL (ND-RAWL)

Amongst all the clone attack detection techniques in WSNs, Random Walk (RAWL) is the most promising witness node based solution which uses random walks. But still it has some drawbacks such as high communication cost, need more random walks to find intersection node, and needs more reporters to forward location claim. So, to reduce the communication cost and to overcome the drawbacks of RAWL, we propose a new distributed protocol called Neighbor Division Random Walk (ND-RAWL) for Clone attack detection in static WSNs. This ND-RAWL is based on claimer-reporter-witness framework.

5.1.1 Protocol description

Our purpose is to find the cloned node inside the network with less communication cost. When we study the RAWL protocol, it is noticed that RAWL need more random walks and longer random walk steps. The smaller number of walk steps result in the less communication and memory overheads. So to reduce the communication cost, there should be less witness nodes as one walk step corresponds to a witness node. So we proposed a detection method that will show good detection probability for the nodes having less neighbor nodes with controlling the overheads. In RAWL, the witness nodes are selected randomly by the neighboring nodes. They further initiate r random walks in the whole network followed by t random walk steps. Then each passing node also becomes the witness nodes. Thus in RAWL there are many witness nodes so communication cost is high. To reduce the no. of witness nodes we divide the neighboring nodes of a claimer node into different areas.

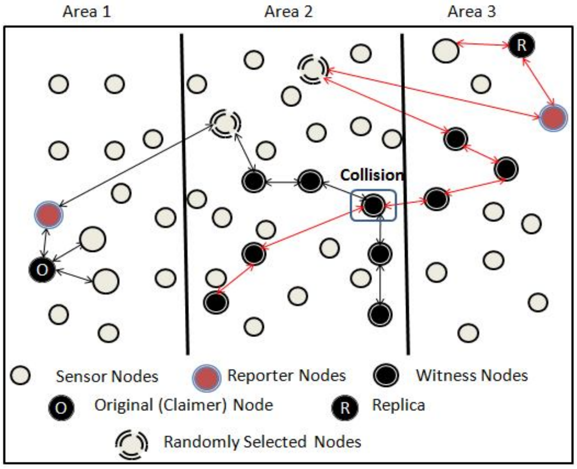

Figure 3 The ND-RAWL protocol based on CRW framework.

Fig. 3 shows the working of ND-RAWL protocol. This protocol is based on claimer-reporter-witness framework. In this protocol, the entire network is divided into different areas using Euclidian-distance. Here, the claimer node sends a signed location claim to its one hop neighbors. But in this protocol we select only one neighbor. Only this neighbor (reporter node) forwards the claim to randomly selected nodes from the remaining areas with some probability. The reporter of a claimer node will select a single node randomly from each area which will further select r nodes randomly, that will finally start the random walks and the passing nodes at each random walk step will become the witness nodes. These witnesses will finally store the location claim. If there are clones in the network they will forward the location claim in similar manner and if any witness node receives different location claims for the same node, a conflict is detected and finally a clone node will be revoked.

6. SIMULATION RESULTS

This section presents results of the NS-2 implementation of the proposed method to detect clone attack. The designed network consists of 103 wireless sensor nodes. Here the communication cost, packet delivery ratio (PDR) and throughput are used as performance parameters.

6.1Performance Parameters

6.1.1 Communication Cost

The communication cost is the ratio of no. of dropped packets to successfully sent packets.

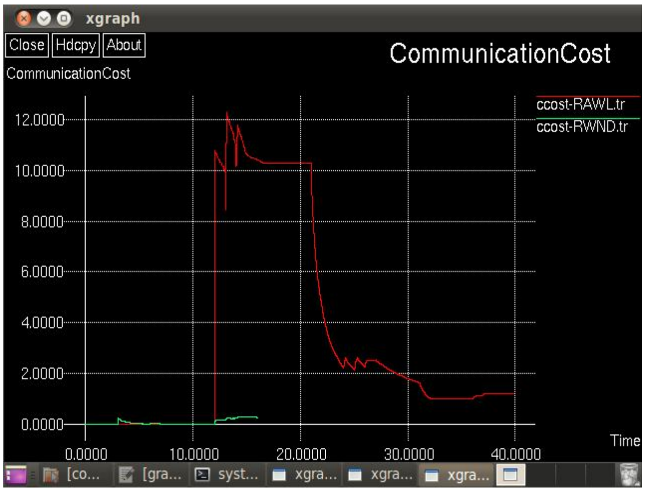

Figure 4 Communication cost for RAWL and ND-RAWL.

Fig. 4 shows the communication cost of RAWL and ND-RAWL. Because of division of network and random selection of reporter and witness nodes the communication cost of RAWL get reduced in ND-RAWL protocol.

6.1.2 Packet Delivery Ratio

Packet Delivery Ratio is nothing but the ratio of actual packets delivered to total packets sent. The calculation of Packet Delivery Ratio (PDR) is based on the received and generated packets as recorded in trace file. For better performance of protocol the PDR should be greater.

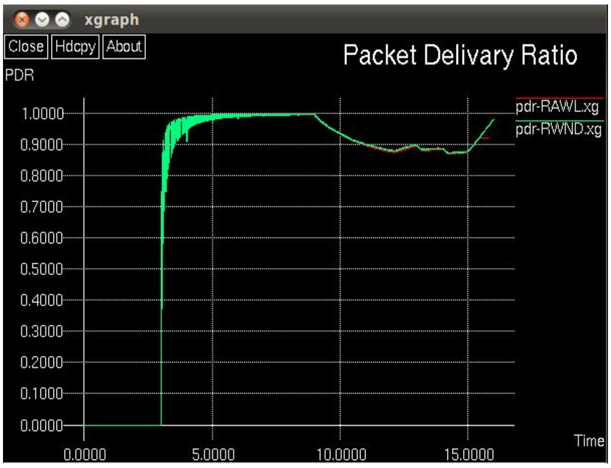

Figure 5 PDR of both RAWL and ND-RAWL.

From fig. 5 it is clear that PDR of ND-RAWL is greater than RAWL

6.1.3 Throughput

Throughput is the number of successfully received packets in a unit time. It is represented in bps or kbps. Throughput is calculated using awk script which processes the trace file and produces the result. Throughput should be greater for better performance of protocol.

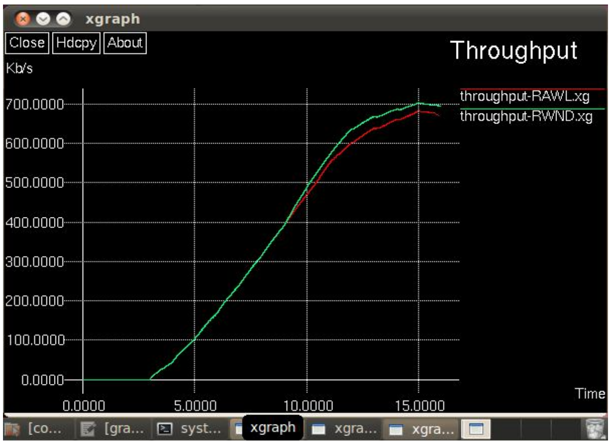

Figure 6 Throughput of RAWL and ND-RAWL.

Fig. 6 shows the throughput of RAWL and ND-RAWL protocols. From the simulation results we can see that the communication cost is less in our protocol. The ND-RAWL protocol shows better performance under clone attack through the performance parameters PDR and throughput.

7. CONCLUSION AND FUTURE WORK

In this paper, Clone attack is addressed. We evaluate various detection protocols. RAWL protocol is assumed to be the best protocol considering its simulation results. We have made an attempt to improve this protocol, and we come up with a new protocol called Neighbor Division-RAWL (ND-RAWL). This protocol is modified version of existing RAWL protocol. The simulation result shows that the communication cost of our protocol is less as compared to the RAWL. Simulation results demonstrate that proposed protocol achieved very good performance in terms of communication overhead, and message delivery latency, while assuring a high message delivery ratio.

We consider the detection of cloned nodes in mobile WSNs as our future work.

References

[1]. Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie "Random walk based approach to detect clone attacks in wireless sensor networks, IEEE Journal on Selected Areas in Communications, vol. 28, no. 5, pp. 677–691, 2010.

[2]. M. Conti, R. Di Pietro, L. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 5, pp. 685–698, 2011. R. Caves, Multinational Enterprise and Economic Analysis, Cambridge University Press, Cambridge, 1982. (book style)

[3]. B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor

networks," in Proc. IEEE Symp. Security and Privacy (S&P '05), 2005, pp. 49–63.

[4]. B. Zhu, V. Addada, S. Setia, S. Jajodia, and S. Roy, "Efficient distributed detection of node replication attacks in sensor networks," in Proc. 23rd Ann. Computer Security Applications Conference (ACSAC '07), Dec. 2007, pp. 257–267.

[5]. B. Zhu, V. Addada, S. Setia, S. Jajodia, and S. Roy, "Efficient distributed detection of node replication attacks in sensor networks," in Proc. 23rd Ann. Computer Security Applications Conference (ACSAC '07), Dec. 2007, pp. 257–267.

[6]. S. Ratnasamy, B. Karp, L. Yin et al., "GHT: a geographic hash table for data-centric storage," in Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications (WSNA '02), pp. 78–87, September 2002.

[7]. I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," Computer Networks, vol. 38, no. 4, pp. 393–422, 2002.