International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 10 99 – 102

Clone Node Detection in Wireless Sensor Networks

K.Anitha[1]
(Research scholar),
Dept. of Computer Science,
Tamil University,
Thanjavur, Tamil Nadu, India.
e-mail : anithameerak@gmail.com

A.Senthilkumar[2]
(Asst. Professor),
Dept. of Computer Science,
Tamil University,
Thanjavur Tamil Nadu, India.
e-mail : erodesenthilkumar@gmail.com

Abstract: Wireless Sensor Networks (WSNs) are often deployed in unfavourable situations where an assailant can physically capture some of the nodes, first can reprogram, and then, can replicate them in a large number of clones, easily taking control over the network. This replication node is also called as Clone node. The clone node or replicated node behave as a genuine node. It can damage the network. In node replication attack detecting the clone node important issue in Wireless Sensor Networks. A few distributed solutions have been recently proposed, but they are not satisfactory. First, they are intensity and memory demanding: A serious drawback for any protocol to be used in the WSN- resource constrained environment. In this project first investigate the selection criteria of clone detection schemes with regard to device types, detection methodologies, deployment strategies, and detection ranges. Further, they are vulnerable to the specific assailant models introduced in this paper. In this scenario, a particularly dangerous attack is the replica attack, in which the assailant takes the secret keying materials from a compromised node, generates a large number of assailant-controlled replicas that share the node's keying materials and ID, and then spreads these replicas throughout the network. With a single captured node, the assailant can create as many replica nodes as he has the hardware to generate.. The replica nodes are controlled by the assailant, but have keying materials that allow them to seem like authorized participants in the network.

Our implementation specifies, user will specify its ID, which means client id, secret key will be create, and then include the port number. The witness node will verify the internally bounded user Id and secret key. The witness node means original node. If the verification is success, the information collecting to the packets that packets are send to the destination.

Keywords*: Static WSN , Distributed mechanism, Node replication Attacks, Sequential probability ratio test.*

*****

I INTRODUCTION

In wireless sensor networks, sensor nodes are deployed in unattended environment and there is no security. An attacker can easily capture and compromise sensor node and make replicas of them. The replicas nodes are duplicate nodes which are created by an adversary make many replica nodes all having same ID and these replica nodes[1] are controlled by an adversary. Then these fake data are injected into a network which may cause eaves dropping in network communication. The fake data disrupt the network operations in network communication. Several replica node detection schemes[2] have been proposed to defend against in static sensor network and they do not work well in mobile sensor networks where sensors are expected to move.

To detect replica node in mobile sensor network,[3] the proposed system use a new technique called Sequential Probability Ratio Testing (SPRT). The uncompromised mobile node should never move at the speed in excess of system configured maximum speed. The compromised mobile node measured speeds will be maximum then the system configured speed because two or more nodes with the same identity are present in the network. If the system decides that a node has been replicated based on a single observation, the nodes moving faster than the system configuration speed many false positive errors occurred in speed measurement. If the system decides that a node is benign based on the single observation, the node moving less than the system configuration speed now the high false negative rates occurred. To minimize these false positive and false negative rates, SPRT a hypothesis testing method is used. That can make decisions quickly and accurately. SPRT is performed on every mobile node using null hypothesis the mobile node has not been replicated and in alternate hypothesis that it has been replicated. Once the alternate hypothesis is accepted the replica nodes will be revoked from the network.

Detection of Replica Node

Replica node attack is a dangerous because they allow the attacker to leverage the compromise of few nodes to exert control over much of network. In static sensor networks replica node detection scheme works well, because the nodes are static so it is possible to detect

the additional node which has the same sensor node ID. In mobile sensor networks it is difficult to detect which node is replica because all the nodes are dynamic.

In replica node attack, an adversary may capture the node and take the data into his own sensor. Then he deploys those sensors in to the network for various

malicious activities. Replica node attack is a dangerous one since all the replica are having legitimate keys which makes the replica to be an benign node since there is no difference between the benign node and replica in terms of their authentication it is difficult to detect replica. Once the node is compromised the information get leaked adversary may inject false data on the node or modifying the data which is passed between the nodes. So finding the replica node is an important one for protecting the network from various attacks. Protection of sensor networks can be done in two ways: both centralized and distributed approaches are needed and also needed for static sensor networks and wireless sensor networks.

Several replica node detection schemes have been proposed for wireless sensor networks. The primary method used by the majority of these schemes is to have nodes report location claims that identify their positions and attempt to detect colliding reports that indicate one node in multiple locations. Since this method leverages the location information for replica detection, it cannot work without the help of secure localization or GPS techniques. If could detect replicas without the aid of these techniques, we would save the detection costs subject to employing these techniques.

Indeed could detect replicas without the use of location information in case of replica cluster attacks, in which multiple replicas of a single compromised node form a cluster in such a way that they are placed close to each other in the cluster. Specifically, in replica cluster attacks, multiple replicas with the same identity and secret keying materials are placed in the same small regions. All of these replicas want to maximize their malicious impact on the network and thus communicate with as many nodes as possible at the same time. Accordingly, it is highly likely that the number of nodes with which these replicas would communicate at a time would be much more than the one of their benign neighbors. By leveraging this intuition, every node performs the Sequential Probability Ratio Test (SPRT) on its neighbor node using a null hypothesis that a replica cluster of the neighbor node does not exist and an alternate hypothesis that a replica cluster of the neighbor node exists. In using the SPRT, if the number of communication peers of a neighbor node falls short of or exceeds a pre-configured threshold, it will lead to acceptance of the null or alternate hypotheses, respectively. Once the alternate hypothesis is accepted, the node will disconnect the communication with the neighbor node.

PROBLEM DESCRIPTION

Wireless Sensor Networks (WSNs), and particularly their security issues, have received great attention recently in both academia and industry. Since tiny sensor nodes in WSNs have meagre resources for computation, communication, power, and storage, it is challenging to provide efficient security functions and mechanisms for WSNs. Above all, since WSNs are frequently deployed in hostile environments, sensor nodes can be captured and compromised easily by an adversary who may extract secret information from the captured nodes. After such a compromise, a clone attack can be launched by replicating the captured nodes and injecting them sporadically over the networks such that the adversary can enlarge the compromised areas by employing the clones. The secret information, such as access keys, extracted from the captured nodes and still contained in clones, may allow the adversary to gain access to communication systems throughout WSNs. For instance, clones would be authenticated as genuine nodes in a key establishment scheme of WSNs in different locations, eventually taking over a local segment or an entire network to launch various attacks, such as corrupting data aggregation, injecting false data, and dropping packets selectively. Thus, it is essential to detect clone nodes promptly for minimizing their damages to WSNs.

In wireless sensor networks, sensor nodes are deployed in unattended environment and there is no security. An attacker can easily capture and compromise sensor node and make replicas of them. The replicas nodes are duplicate nodes which are created by an adversary make many replica nodes all having same ID and these replica nodes are controlled by an adversary. Then these fake data are injected into a network which may cause eaves dropping in network communication. The fake data disrupt the network operations in network communication. Several replica node detection schemes have been proposed to defend against in static sensor network and they do not work well in mobile sensor networks where sensors are expected to move.

The simplest defensive measure against the clone attacks is to prevent an adversary from extracting secret key materials from captured nodes by virtue of tamper-resistant hardware. However, the hardware-based defensive measures are too expensive to be practical for resource-restricted sensor nodes. Various kinds of software-based clone detection schemes have recently been proposed for WSNs, considering many different types of network configuration, such as device types and deployment strategies. The limitation of software based clone detection schemes is undoubtedly that they are not generic, meaning that their performance and effectiveness may depend upon their preconfigured network settings. For example, a clone detection scheme designed for mobile WSNs is useless in static WSNs. In order to choose an effective detection scheme for a certain sensor network, it is desirable to have a set of well-designed selection criteria.

In this project first investigate the selection criteria of clone detection schemes with regard to device types, detection methodologies, deployment strategies and detection ranges, and then classify the existing schemes according to the proposed criteria. First, divide static and mobile sensors according to their mobility. A static sensor node cannot move, while the location of a mobile sensor changes depending on operational scenarios. Clone detection strategies can be classified in this sense as well. Second, classify the detection schemes to centralized and distributed schemes[4], i.e., in terms of the ways to collect and verify evidence of clones. One is that a central node, such as a base station (BS), acts solely on detecting clones, and the other is that a group of sensor nodes conduct the clone detection cooperatively. Third, according to the ways how to deploy sensor nodes divide them into random uniform deployment and grid deployment strategies. The former is that sensor nodes are scattered in a region randomly, and the latter works in a way that they are placed in prescheduled zones by dividing a given deployment field into a number of practical location zones. Finally, according to clone detection locations, divide the schemes into whole area and local area detection schemes. In the former schemes, all sensor nodes work jointly in detecting clones, but in the latter schemes only a subset of them will conduct it locally.

To summarize, classify the existing clone detection schemes based on the following criteria:

1) Device type: static (sensor) versus mobile (sensor);
2) Detection method: centralized (detection) versus distributed (detection);
3) Deployment strategy: random uniform (deployment) versus grid (deployment);
4) Detection range: whole (area detection) versus local (area detection).

II SYSTEM ANALYSIS

EXISTING SYSTEM

The Existed schemes rely only on fixed sensor locations in static sensor networks. A particularly dangerous attack is the replica node attack, in which the adversary takes the secret keying materials from a compromised node. The adversary can generates a large number of attacker-controlled replicas that share the compromised node's keying materials and ID, and then spreads these replicas throughout the network. For detecting replica node attacks is due to randomized and line selected multicast schemes to detect replicas in static wireless sensor networks.

- ***DEMERITS***
  - The locally generated outgoing messages in a network normally cannot provide the aggregate large-scale spam view required by these approaches.
  - Outgoing messages gives rise to the sequential detection problem.
  - Blocking policy is not adopted.

PROPOSED SYSTEM

It proposes a fast and effective replica node detection schema using the sequential probability ratio test. The sensor node is compare it to a predefine threshold, if it is more than threshold value, we decide the sensor node has a captured nodes. This simple approach achievers efficient node captures detection capability as long as a threshold value is properly configured. However, it is not easy to configure a proper a threshold value to detect captured nodes. If set threshold to a high value it is likely that captured nodes bypass the detection. On the contrary if we set threshold to a low value, it is likely that benign nodes can be detected as a captured nodes. It uses scheme for distributed detection of mobile malicious node attacks in mobile sensor networks. The key idea of this scheme is to apply sequential hypothesis testing[5] to discover nodes that are silent for unusually many time periods such nodes are likely to be moving and block them from communicating.

To design an effective, fast, and robust replica detection scheme specifically for mobile sensor networks. For the effective scheme a novel mobile replica detection scheme based on the Sequential Probability Ratio Test (SPRT)[6]. By using the fact that an uncompromised mobile node should never move at speeds in excess of the system-configured maximum speed. Also through quarantine analysis that the amount of time, during a given time slot, that the replicas can impact the network is very limited.

- ***MERITS***
  - To minimize these false positives and false negatives apply the SPRT.
  - That can make decisions quickly and accurately.
  - It is an effective, fast, and robust replica detection scheme specifically for mobile sensor networks.

III MODULE DESCRIPTION

- **Duplicate Node Detection**
- **Centralized Detection**
- **Local Detection**
- **Node-To-Network Broadcasting**
- **Probabilistic Failure Detection**
- **Detecting Replicas**

3.1 Duplicate Node Detection

The nodes which are captured by an adversary can compromise the sensor nodes and make many replicas of

them. These compromised nodes all have the same ID are present in the network. To understand the dangers of node compromise must first define what we mean by node compromise. Node compromise occurs when an attacker, though some subvert means, gains control of a node in the network after deployment. Once in control of that node, the attacker can alter the node to listen to information in the network, input malicious data[7], cause DOS, black hole, or any one of a myriad of attacks on the network. The attacker may also simply extract information vital to the network's security such as routing protocols, data, and security keys. Generally compromise occurs once an attacker has found a node, and then directly connects the node to their computer via a wired connection of some sort. Once connected the attacker controls the node by extracting the data and/or putting new data or controls on that node.

3.2 Centralized Detection

The most straightforward detection scheme requires each node to send a list of its neighbors and their claimed locations to the base station. The base station can then examine every neighbor list to look for replicated nodes. If it discovers one or more replicas, it can revoke the replicated nodes by flooding the network with an authenticated revocation message.

3.3 Local Detection

To avoid relying on a central base station could instead rely on a node's neighbors to perform replication detection. Using a voting mechanism, the neighbors can reach a consensus on the legitimacy of a given node. Unfortunately, while achieving detection in a distributed fashion, this method fails to detect distributed node replication in disjoint neighbourhoods within the network. As long as the replicated nodes are at least two hops away from each other, a purely local approach cannot succeed.

3.4 Node-To-Network Broadcasting

One approach to distributed detection utilizes a simple broadcast protocol. Essentially, each node in the network uses an authenticated broadcast message to flood the network with its location information. Each node stores the location information for its neighbors and if it receives a conflicting claim, revokes the offending node.

3.5 Probabilistic Failure Detection

In this section describe in detail the Protector probabilistic replica maintenance approach, and analyze its effectiveness. It begins by first describing the high level replica maintenance problem as context. Then describe the Protector approach in detail, and prove that its estimate on the number of remaining replicas is the most accurate. Finally describe in detail how to derive Protector's failure probability function[8] through both a Markov failure model and extraction from measurement traces of failure events.

3.6 Detecting Replicas

Unlike the Random Multicast and Line-Selected Multicast algorithms,[9] where the nodes storing the copies of a location claim are chosen randomly from the whole network, in Software Defined Concern (SDC) such nodes are chosen randomly from a small subset of all the nodes in the network, i.e., the nodes in the destination cell determined by the geographic hash function. In addition, since the location claim will be flooded within the destination cell, the SDC scheme can always detect any pair of nodes claiming the same identity. In other words, pdr = 100% in SDC, when $r > 0$ and $w > 0$.

IV CONCLUTION

The concludes detection of mobile replica node attacks in mobile sensor networks using speed measurement testing. Several replica node detection schemes have been proposed in the literature to defend against such attacks in static sensor networks. In this work, a fast and effective mobile replica node detection scheme using the Sequential hypothesis testing.

V FUTURE ENHANCEMENT

Finally some open issues have been identified that are left as future. This proposed system at the time several nodes are detected. But in this future work to increase the detection level.

REFERENCES

[1] Ambiritha M.A, Gomathi V "Efficient Node Replica Detection In Wireless Sensor Networks"2008.

[2] ChakibBekara and Maryline Laurent-Maknavicius"Defending Against Nodes Replication Attacks on Wireless Sensor Networks"2010.

[3] Dr.Chellappan..CandManjula.V,"Replication Attack Mitigations for Static and Mobile Wireless sensor networks"1999.

[4] jun-won ho, "Distributed Detection Of Replicas With Deployment Knowledge In Wireless Sensor Networks"2007.

[5] Jun-Won Ho,"Sequential Hypothesis Testing Based Approach for Replica Cluster Detection in Wireless Sensor Networks"2010.

[6] Jun-Won Ho, Matthew Wright "Fast Detection of Mobile Replica Node Attacks in Sensor Networks Using Sequential Hypothesis Testing" IEEE 2011.

[7] Pavithraa.S,Balakrishnan.C "Fake Data Termination in Wireless Sensor Networks" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-1, Issue-2, June 2012.

[8] Liang-Min Wang, and Yang Shi "Patrol Detection for Replica Attacks on Wireless Sensor Networks"2011.

[9] Conti et al. In their work "A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks " (2007).