Clone Attacks Detection In Wireless Sensor Networks

Mrs.P.Radhidevi*1, D Gopi Krishna*2
Assistant Professor, Dept of Computer Applications, SNIST, Ghatkesar, Hyderabad, AP, India
M.C.A Student, Dept of Computer Applications, SNIST, Ghatkesar, Hyderabad, AP, India

ABSTRACT:

The general problem in wireless sensor network security (WSN) is the node Clone attack. This attack, is an adversary breaks into a sensor node. Once attacker captures sensor nodes, can compromise them and launch various types of attacks with those compromised nodes. Therefore, node capture attacks should be detected as soon as possible to reduce the harm incurred by them. Some of the solutions were introduced to meet the requirements of this problem. However, these solutions are not satisfactory. A serious drawback for any protocol to be used in the WSN resource constrained environment. To solve this, analyze the desirable properties of a distributed mechanism for the detection of node replication attacks. Here is a new self-healing, Randomized, Efficient, and Distributed (RED) protocol for the detection of node replication attacks, and we show that it satisfies the requirements.

INDEX TERMS: wireless sensor networks, node replication attacks, clone attacks.

I. INTRODUCTION:

Wireless communication is an application of science and technology that has come to be vital for modern existence. In advance, Wireless sensor Network(WSN) is used in Wireless communication for transferring the information. A WSN is a collection of sensors with limited resources that collaborate to achieve a common goal. Due to their nature, they are often unattended, hence prone to different kinds of novel attacks. For example, an adversary could drop all network communications; further, an adversary could capture nodes acquiring all the information stored there in sensors are commonly assumed to be not tamper-proof. Therefore, an adversary may replicate captured sensors and deploy them in the network to launch a variety of malicious activities. This attack is referred to as the clone attack, since a clone has legitimate information. It may participate in the network operations in the same way as a non-compromised node. Hence, cloned nodes can launch a variety of attacks.

Fig1: Components of sensor nodes

In this paper, we develop methods for finding the appropriate number of
witness nodes, such that the performance of the WSN is optimal. We consider the aspects of network performance, in particular the communication and the storage overhead involved in transmission and validation of location claims, as well as the impact of undetected captured nodes on WSN operation.

II.RELATED WORK:

Bugs in the software running on the sensor nodes or on the base stations give rise to attacks which can be easily automated and can be mounted on a very large number of nodes in a very short amount of time. Possible countermeasures include a heterogeneous network design and standard methods from software engineering.

Physical attacks on embedded systems, that is, on microcontrollers and smart cards, have been intensively studied before. Skorobogatov classifies them in the three categories of invasive, semi-invasive, and non-invasive attacks. Invasive attacks are those which require access to a chip’s internals, and they typically need expensive equipment used in semiconductor manufacturing and testing, as well as a preparation of the chip before the attack can begin. Semi-invasive attacks require much cheaper equipment and less time than the invasive attacks, while non-invasive attacks are the easiest. All of these attacks, including the so-called low-cost attacks, if applied to sensor nodes, would require that they be removed from the deployment area and taken to a laboratory. Most of the invasive and many of the semi-invasive attacks also require disassembly or physical destruction of the sensor nodes. The existing literature on physical attacks usually assumes that an attacker can gain unsupervised access to the system to be attacked for an extended period of time. Attacks which may take days or even weeks to complete present a real threat to the security of these systems. Continuous absence of a node can be considered an unusual condition that can be noticed by its neighbors. This makes time a very important factor in evaluating attacks against sensor nodes, as the system might be able to detect such attacks while they are in progress and respond to them in real-time. One of our aims has been to determine the exact amount of time needed to carry out various attacks. Based on these figures, the frequency with which neighbors should be checked can be adapted to the desired level of security and the anticipated threat model.

III.PROBLEM STATEMENT:

We first assume a static sensor network in which the locations of sensor nodes do not change after deployment. We also assume that every sensor node works in promiscuous mode and is able to identify the sources of all messages originating from its neighbors. We believe that this assumption does not incur substantial overhead because each node inspects only the source IDs of the messages from its neighbors rather than the entire contents of the messages. We assume that an attacker can physically capture sensor nodes to compromise them. However, we place limits on the number of sensor nodes that he can physically capture in each target region. This is reasonable from the perspective that an increase in the number of the captured sensor nodes will lead to a rise in the likelihood that attacker is
detected by intruder detection mechanisms. Therefore, a rationale attacker will want to physically capture the limited number of sensor nodes in each target region while not being detected by intruder detection mechanisms. Moreover, we assume that it takes a certain amount of time from capturing nodes to redeploying them in the network. This is reasonable in the sense that an attacker needs some time to compromise captured sensor nodes.

IV. CONCLUSION:

In this paper, a few basic requirements an ideal protocol for distributed detection of node replicas are presented and justified. Moreover, the overhead of such a protocol should be not only small, but also evenly distributed among the nodes, both in computation and memory. The proposal of this paper is about the Enhanced RED (Randomized, Efficient and Distributed) protocol to detect node replication attacks. The Enhanced RED protocol is more efficient and less overhead when compared to Randomized Multicast, Line Selected Multicast and RED protocol. This protocol outperforms RED in terms of efficiency and effectiveness. Finally, this Enhanced RED protocol is more robust in the process of attack detection than the rest of the protocol. It covers all requirements in clone nodes detection. Clone nodes are detected using ID and location. They are detected with less amount of overhead, less amount of memory.

V. REFERENCES:


