Abstract- Wireless sensor networks are deployed in hostile environment, capture some nodes, reprogram then replicate them into clones. There are few solution to address this basic problem have been proposed. These solutions are not satisfactory, because of memory demand and WSN is a resource constrained environment. In this paper we analyze the node replication attack detection and show that this solution should not satisfy our requirements completely. Next we introduce Randomized, Efficient, Distributed protocol to detect the node replication and show this protocol have high efficiency, memory, computation and more effective than other solutions.

Keywords—authentication, security, replication attacks

I. INTRODUCTION

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity.

The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

In computer science and telecommunications, wireless sensor networks are an active research area with numerous workshops and conferences arranged each year. Wireless sensor networks are quickly gaining popularity due to the fact that they are potentially low cost solutions to a variety of real-world challenges. Their low cost provides a means to deploy large sensor arrays in a variety of conditions capable of performing both military and civilian tasks. But sensor networks also introduce severe resource constraints due to their lack of data storage and power. Both of these represent major obstacles to the implementation of traditional computer security techniques in a wireless sensor network the unreliable communication channel and unattended operation make the security defenses even harder. Indeed, as pointed out, wireless sensors often have the processing characteristics of machines that are decades old (or longer), and the industrial trend is to reduce the cost of wireless
sensors while maintaining similar computing power. With that in mind, many researchers have begun to address the challenges of maximizing the processing capabilities and energy reserves of wireless sensor nodes while also securing them against attackers. All aspects of the wireless sensor network are being examined including secure and efficient routing, data aggregation, group formation, and so on.

In addition to those traditional security issues, we observe that many general-purpose sensor network techniques (particularly the early research) assumed that all nodes are cooperative and trustworthy. This is not the case for most, or much of, real-world wireless sensor networking applications, which require a certain amount of trust in the application in order to maintain proper network functionality. Researchers therefore began focusing on building a sensor trust model to solve the problems beyond the capability of cryptographic security. In addition, there are many attacks designed to exploit the unreliable communication channels and unattended operation of wireless sensor networks. Furthermore, due to the inherent unattended feature of wireless sensor networks, we argue that physical attacks to sensors play an important role in the operation of wireless sensor networks. Thus, we include a detailed discussion of the physical attacks and their corresponding defenses, topics typically ignored in most of the current research on sensor security. We classify the main aspects of wireless sensor network security into four major categories: the obstacles to sensor network security, the requirements of a secure wireless sensor network, attacks, and defensive measures.

1.1 ATTACKS

Sensor networks are particularly vulnerable to several key types of attacks. Attacks can be performed in a variety of ways, most notably as denial of service attacks, but also through traffic analysis, privacy violation, physical attacks, and so on. Denial of service attacks on wireless sensor networks can range from simply jamming the sensor’s communication channel to more sophisticated attacks designed to violate the 802.11 MAC protocol or any other layer of the wireless sensor network. Due to the potential asymmetry in power and computational constraints, guarding against a well orchestrated denial of service attack on a wireless sensor network can be nearly impossible. A more powerful node can easily jam a sensor node and effectively prevent the sensor network from performing its intended duty.

1.1.1 Types of Attacks

A standard attack on wireless sensor networks is simply to jam a node or set of nodes. Jamming, in this case, is simply the transmission of a radio signal that interferes with the radio frequencies being used by the sensor network. The jamming of a network can come in two forms: constant jamming, and intermittent jamming. Constant jamming involves the complete jamming of the entire network. No messages are able to be sent or received. If the jamming is only intermittent, then nodes are able to exchange messages periodically, but not consistently. This too can have a detrimental impact on the sensor network as the messages being exchanged between nodes may be time sensitive.

a) THE SYBIL ATTACK

The Sybil attack is defined as a “malicious device illegitimately taking on multiple identities. It was originally described as an attack able to defeat the redundancy mechanisms of distributed data storage systems in peer-to-peer networks. Sybil attack might utilize multiple identities to generate additional “votes.” Similarly, to attack the routing protocol, the Sybil attack would rely on a malicious node taking on the identity of multiple nodes, and thus routing multiple paths through a single malicious node.

b) NODE REPLICATION ATTACKS

Conceptually, a node replication attack is quite simple: an attacker seeks to add a node to an existing sensor network by copying (replicating) the node ID of an existing sensor node. A node
replicated in this fashion can severely disrupt a sensor network’s performance: packets can be corrupted or even misrouted. This can result in a disconnected network, false sensor readings, etc.

c) ATTACKS AGAINST PRIVACY

Sensor networks aggravate the privacy problem because they make large volumes of information easily available through remote access. Remote access also allows a single adversary to monitor multiple sites simultaneously.

Some of the more common attacks against sensor privacy are:

Monitor and Eavesdropping: this is the most obvious attack to privacy. By listening to the data, the adversary could easily discover the communication contents. When the traffic conveys the control information about the sensor network configuration, which contains potentially more detailed information than accessible through the location server, the eavesdropping can act effectively against the privacy protection.

Traffic Analysis typically combines with monitoring and eavesdropping. An increase in the number of transmitted packets between certain nodes could signal that a specific sensor has registered activity. Through the analysis on the traffic, some sensors with special roles or activities can be effectively identified.

II RED PROTOCOL

A clone is considered totally honest by its neighbors. In fact, without global countermeasures, honest nodes cannot be aware of the fact that they have a clone among their neighbors. To have a large amount of compromised nodes, the adversary does not need to compromise a high number of nodes. Indeed, once a single node has been captured and compromised, the main cost of the attack has been sustained. Making further clones of the same node can be considered cheap.

One of the first solutions for the detection clone attacks each node sends a list of its neighbors and their locations to a BS. The same node ID in two lists with inconsistent locations will result in clone detection. Then, the BS revokes the clones. Such as the presence of a single point of failure (the BS) and high communication cost due to the large number of messages.

Another centralized clone detection protocol has been recently proposed in this solution assumes that a random key distribution security scheme is implemented in the sensor network. Each node constructs a counting Bloom filter from the keys it uses for communication. Then, each node sends its own filter to the BS. From all the reports, the BS counts the number of times each key is used in the network. The keys used too often (above a threshold) are considered cloned and a corresponding revocation procedure is raised.

In the Sybil attack a node claims multiple existing identities stolen from corrupted nodes. Note that both the Sybil and the clone attacks are based on identity theft, however the two attacks are independent. The Sybil attack can be efficiently addressed with mechanism based on RSSI or with authentication based on the knowledge of a fixed key set. Detection of the node replication attack is Node-To-Network Broadcasting. In this solution, each node floods the network with a message containing its location information and compares the received location information with that of its neighbors. However, this method is very energy-consuming.

A randomized, efficient, and distributed clone detection protocol has been proposed. The RED protocol can be actually implemented in sensor network.

Also, it can be continuously iterated over the same network, as a self-healing mechanism, without significantly affecting the network performance (nodes energy and memory) and the detection protocol itself.

- While centralized protocols have a single point of failure and high communication cost
- Local protocols do not detect replicated nodes that are distributed in different areas of the network.
A new randomized, efficient, and distributed (RED) protocol for the detection of node replication attacks, and proves that our protocol does meet all the above cited requirements. Provide analytical results when RED and its competitor face an adversary that selectively drops messages that could lead to clone detection.

RED is similar, in principle, to the Randomized Multicast protocol, but with witnesses chosen pseudo randomly based on a network-wide seed. In exchange for the assumption that we are able to efficiently distribute the seed, RED achieves a large improvement over RM in terms of communication and computation. Finally, extensive simulations of RED show that it is highly efficient as for communications, memory, and computations required and show improved attack detection probability when compared to other distributed protocols.

III. CONCLUSION

Wireless sensor networks are deployed in hostile environment and vulnerable to various types of attacks. This paper outlined the different types of attacks on WSN and mainly about clone attack. We have provided various approaches to find the cloned node. In static centralized protocols, CSI protocol has the lowest communication overhead than SET, Real Time, New protocols. In static distributed protocols, we find that SDC protocol has lower communication cost than other protocols for smaller size network and RED protocol has the lowest communication overhead for larger network. We analytically compared RED with the state-of-the-art solution (LSM) and proved that the overhead introduced by RED is low and almost evenly balanced among the nodes; RED is both
ID-oblivious and area oblivious; furthermore, RED outperforms LSM in terms of efficiency and effectiveness. Extensive simulations confirm these results. Lastly, also in the presence of compromised nodes, we can analytically show that RED is more resilient in its detection capabilities than LSM.

REFERENCES