ENERGY EFFICIENT DISTRIBUTED DETECTION OF NODE CLONES IN WIRELESS SENSOR NETWORK

Shriya Autkar, Prof. Manisha Dhage, Prof. Shashank Bholane

Department of Computer Engineering, Sinhgad College of Engineering, Vadgaon BK, Pune.

ABSTRACT:

Wireless Sensor Network (WSN) consists of tiny sensing devices which co-operate and communicate with each other to perform certain tasks. These are generally deployed in hostile environment where an adversary may capture nodes, replicate them and use it for its own purpose. If the clone nodes remain undetected, it can disrupt the network functions making it vulnerable to attacks. Hence false data can be injected or the legitimate data can be taken out. Thus to detect the clone nodes is the fundamental problem in WSN. The objective of distributed node clone detection is to detect clone nodes with minimum communication and storage overhead. The proposed project is a node clone detection system for sensor networks, which will be capable of detecting the node clone attack in a distributed way.

Keywords: Wireless Sensor Networks, Node Clone attack, Distributed, Energy efficient, Attack.

INTRODUCTION

A wireless sensor network (WSN) consists of large number of sensor nodes which are limited in resources like memory and energy. They communicate and co-operate with each other to measure certain task. Sensor nodes are densely deployed in the area of interest. Each node can sense up to a limited area and has wireless communication capabilities [1], which allow it to gather the sensed information from the environment and then send the data to other nodes in the sensor network and finally to the sink. Wireless Sensor Network is used in various fields such as military, healthcare, environmental and in commercial applications [2]. Considering the limited energy capabilities of a sensor node, it can sense only up to some limited area, so a wireless sensor network has a large number of sensor nodes deployed in a high density.

Generally the sensor nodes are being deployed in a harsh and unattended environment where the nodes are not having tamper-resistant hardware, making it easy for an adversary to capture a node, gets access to all data stored on the node. Thus an attacker can physically capture the nodes, obtain the cryptographic information from these sensors, make clones (replicas) of them and insert these clones back in the network. Cloning provides an easy way for an adversary to build a number of replica nodes that can disrupt the entire network.

Security is one of the key concerns for the proper functioning of WSNs. If the clone nodes are not detected they can join the sensor network as the legitimate nodes and can disrupt the entire network functionality by corrupting the network data or by disconnecting some parts of the
network. Presence of clone nodes can be injurious to important sensor network function such as routing [3]. Thus detection of the node clones is important to discard them from further network activity.

The rest of the paper is organized as follows: In section II, node clone attack is explained. Section III; discuss previous existing techniques for detection of node clones from the network. In section IV, the proposed methodology is given. Section V gives the result. And Finally Section VI provides conclusion of the paper.

[2] NODE CLONE ATTACK

Node clone (replication) attack is an Identity based attack [3], where all the clone nodes are having the same Identity as that of compromised node. Identity based cryptography [4] is used where each node has a public key and a private key. ID of each node is given prior deployment. To perform the node clone attack, an adversary simply captures the sensor node physically from the sensor field, collects all the credentials of that node like its ID and keys, produces clones (replicas) of it and deployed these clones at various locations in the network [5]. The clone nodes thus can establish communications with their neighbor nodes using the cryptographic keys and appear as legitimate nodes in the network. A scenario of clone nodes deployed in the network by an adversary is given below, where node A is replicated and deployed at various locations.

![Figure: 1. Network consisting of node clones.](image)

[3] RELATED WORK

To detect the node clones present in static WSN, many approaches have been proposed which are broadly categorized into centralized techniques and distributed techniques [6]. In a centralized approach for detecting node clone, each node sends its ID and neighbor list in a message called as claim to the Base station. Base station is responsible for examining every neighbor list to detect any replicated nodes. The network is flooded with an authenticated revocation message if it finds two nodes with same ID and different locations. Examples of centralized approaches are SET [7], Random key predistribution scheme [8]. Though 100% node clones are detected, the main drawback of centralized method is single point of failure. Thus Distributed methods are more subtle than centralized methods, because no central authority is present, detection is not limited to nodes neighbor and each node is responsible for detection of node clones present in the network.

In Node to Network broadcast [9] every node broadcasts its location claim and collects the IDs and locations of its neighboring nodes. When a node receives a broadcast message from the others, the nodes compares the other neighboring node with its own neighbors, and if there is a
collision of IDs in the two neighboring nodes of distinct locations, then corresponding nodes are cloned and revoked. Drawback of this method is high communication cost is required.

To reduce the communication cost, Deterministic Multicast sends the location information [9] to only a subset of nodes. When node broadcasts its location claim to all neighbors, these neighbors forward it to only limited set of nodes which are called as witnesses. These witnesses are selected based on function of node ID. If there is a replicated node, any one of witness may receive the different location claims with same ID and it revokes the replicated node.

Parno proposed Randomized multicast (RM) and line-selected multicast (LSM) in 2005[9], which is the distributed node replica detection mechanism proposed for the first time. The first algorithm is called Randomized multicast. In RM, each node broadcasts its location claim to its neighbor. Then its neighbor (with probability p) sends its location claim to a randomly selected witness node by using geographic routing. They claim using Birthday Paradox that can ensure at least one witness node will receive the location conflict of a replicated node with higher probability. Because of the RM protocol’s high communication cost, Parno proposed another protocol to reduce the communication overhead and increase the probability of detection, which is called line-selected multicast (LSM). In LSM, a location claim travels a line from one node to another. Every intermediate node in this line has to store the location claim and each of them can also be witness nodes. Thus nodes at the intersection of two lines can detect a conflict location claims. Compared with RM, LSM has a lower communication cost.

Randomized Efficient Distributed (RED) protocol [10] executes at fixed intervals of time and consists of two stages. In the first step a random variable is shared between all the nodes with the help of base-station. In the later step each node broadcasts its location claim to neighbor nodes. Each neighbor node after hearing a claim sends it to a set of pseudo-randomly selected network locations. Every node in path forwards the message to its neighbor nearest to the destination. Hence node clones will be detected if received conflicting location claims.

Another method is Single Deterministic Cell (SDC) and Parallel-Multiple Probabilistic Cells (P-MPC) [11]. In SDC and P-MPC, sensor network is considered as a geographic grid where sensors are distributed uniformly in the network. Each unit in the grid is called as cell. In SDC, the ID of node sending the location claim is mapped to one of the cells in the grid through a geographic hash function. Ones the location claim arrives at the cell, sensor receiving the claim floods the claim within the cell. Each node with some probability decides whether to store the location claim or not. Thus at least one witness node is found who will receive a conflicting location claim and forwards it to base station which will broadcast the location claim to revoke the clone nodes. While in P-MPC instead of mapping to only one cell, node id is mapped to more than one cell using the geographic hash function.

In Randomly Directed Exploration (RDE) [12], each node only needs to know its neighbor nodes. During the detection round, nodes issue claiming messages containing neighbor list with a maximum hop limit to randomly selected neighbors. The node receiving the claiming message forwards it in an exact opposite direction to forward the message. While forwarding the message, each intermediate node checks the claiming messages for node clone detection. In such a simple way, the RDE protocol can efficiently detect node clones in the dense sensor networks. In addition to this, the protocol requires almost minimum memory during detection, and communication overhead is satisfactory.
[6] PROPOSED METHODOLOGY

Distributed hash table (DHT) based protocol [13] is used to detect the node clones in a distributed way.

The steps to detect the node clones in the network are as follows:

- Each node a creates a claiming message for its neighbor node b after verifying that signature is valid and the message nonce is greater than the last nonce. At the assigned time the node forwards the message through the overlay network. The message contains ID of node a, its location, ID of node b and its location. This claiming message is signed by node a by its private key. The claiming message is as follows:

$$M = IDa , La , IDb , Lb \{ IDa \| La \| IDb \| Lb \| nonce \}$$

- A claiming message is associated with a key that will be used to forward to its destination node using a Finger Table containing successor nodes of that node. For routing of messages, it considers nodes whose energy level is above the predefined threshold. If a node’s energy is below the set threshold, it will not participate in routing process thus saving its own energy as most of the energy is consumed by transmission. Thus nodes having energy level above threshold will participate in forwarding and nodes having energy below threshold will only store the incoming claiming messages to check any conflict.

Let $m$ be the number of bits in the key/node identifiers. Each node is responsible for the periphery of segments that ends at its co-ordinate. Key $k$ is assigned to the first node whose identifier is equal to or follows (the identifier of) $k$ in the identifier space. This node is called the successor node of key $k$, denoted by $\text{successor}(k)$. If identifiers are represented as a circle of numbers from 0 to $2^m-1$, then $\text{successor}(k)$ is the first node clockwise from $k$. The Chord ring is shown in below figure.

| TABLE I: DEFINITION OF VARIABLES FOR NODE N, USING m-BIT IDENTIFIERS [14] |

Each node $n$ maintains a routing table [14] with up to $m$ entries, called the finger table. The $i$th entry in the table at node $n$ contains the identity of the first node $s$ that succeeds $n$ by at least $2^{i-1}$ on the identifier circle, i.e., $s = \text{successor}(n+2^{i-1})$, where $1 \leq i \leq m$. The node $s$ is called the $i$th finger of node $n$, and denote it by $n:finger[i]$. 

Figure: 2. Chord Ring

The $i$th entry in the table at node $n$ contains the identity of the first node $s$ that succeeds $n$ by at least $2^{i-1}$ on the identifier circle, i.e., $s = \text{successor}(n+2^{i-1})$, where $1 \leq i \leq m$. The node $s$ is called the $i$th finger of node $n$, and denote it by $n:finger[i]$. 

TABLE I: DEFINITION OF VARIABLES FOR NODE N, USING m-BIT IDENTIFIERS [14]
Using this Finger Table the message associated with the key is forwarded to the destination node through several successor nodes. The key is hash value of concatenation of seed and ID of that node whose claiming message is being produced. i.e key = Hash(seed||key)

If a destination node or any successor node of the destination finds two different location claims for the same ID, it becomes the witness node and broadcast the two claiming messages containing different locations for same ID to entire network. These messages are called as evidence.

Also the revoked IDs will be remembered by every node to annul them from future network activities.

[6] RESULT

The experiment is run in Network simulator version 3. In this simulation, 8 nodes are deployed with different IDs. This is shown on terminal output:

One clone node with ID same as node 4 ID is inserted in network. The node clone detection starts which is shown as follows:
Once the node clone is detected with same ID and different location, it is shown on terminal as follows:

![Figure 5. Output Screen 3](image)

The average no of messages generated increases as no of nodes increases. Thus the Communication Graph is shown below,
CONCLUSION

The existing Node Clone Detection techniques are broadly categorized into two classes, Centralized and Distributed. In Centralized only Base-station is responsible for detection while in Distributed, nodes are responsible for detection of node clones. Both classes are proficient in detecting and preventing clone attacks, but both schemes also have some drawbacks. Using DHT-based Protocol, node clones are detected in a distributed way, which considers the energy of nodes. Thus nodes with same IDs are detected and revoked from further network functionalities.

REFERENCES


**Author[s] brief Introduction**

Myself Shriya V. Autkar, pursuing ME in Computer Networks (Computer Engineering) under the guidance of Prof. M.R. Dhage and Prof. S.P. Bholane.