Node Cloning Detection Technique in Trusted Sensor Network

Syaidahtul Badriyah Aziz
Faculty of Electrical Engineering
University of Technology MARA(UiTM)
40450 Shah Alam, Selangor
azizsyaidahtul@gmail.com

***Abstract* - The evolution of technology in sensor node due to the transistor technology advancement enabled the emerging of diverse wireless application in human life. However, these create a much more vulnerable environment in daily life especially by the user. Wireless sensor network built of several to thousands tiny nodes that are communicate to each other. The malicious acts to steal another party confidential data are motivated by their different background and need. Physical attack, such as node cloning gives the adversaries another effort to steal the secret key that is used to decrypt any encrypted data by joining into the network system. There is a lot of research that tried to minimize and revoke the node clone deployed into the network system, however it exhaust the energy and memory of the sensor. For static sensor node, knowing the location of the sensor give the advantage to detect node cloning, it is small and easily implement into the sensor program. Thus increase the life span of the node. However it is high in memory utilization.**

Index Terms – Static sensor node, wireless sensor network, security, node cloning, location, adversary, NS2

I. INTRODUCTION

Wireless Sensor Networks (WSN) built of hundreds or thousands of tiny sensor nodes that communicate with each other via wireless channel. The sensor had the abilities to sense its environment, process the data and forward it to the base station (BS) or the neighbouring nodes. Unfortunately, sensors are extremely resource constraints, depending on its size and cost this result in restricting the memory, energy, computational speed, communications bandwidth [1] and lack of tamper-proof hardware. Sensor node typically deployed in remote or hostile environment with minimal intervention by the human, therefore leave it vulnerable to security attack.

According to [1], there are three factors that contribute to the demand of security that can be explained as "The different intention from the various background and identities create varies types of attack to tamper or steal the valuable information from the protected value. The vulnerabilities of the valuable entity will be the key for the successful attack." Attack is classified into two classes, active and passive attack. The adversaries does not claiming the confidentiality of the node such as jamming and flooding in the passive attack. On the other hand, active attackers carried malicious acts against data confidentiality and integrity [2] such as spoofing, Sybil and node cloning attack.

Node cloning is an attack that the adversaries try to deploy several nodes with the same identities at different places of the network or permanently replace the nodes. In hostile environment, unshielded sensor can be easily capture and replicate by the adversaries [3]. This attack affects the network layer, threatening the confidentiality, integrity and availability of the whole network [4]. If these attacks are not solved, the adversary may gain control over the network [5], therefore expose the network to the adversary or other party [6]. Moreover, when the nodes are control by the adversary, they can launch another attack such as DoS inside the network to corrupt the information [5].

The previous work by [7] a localization protocols are susceptible to replay attacks. While for wormhole attack, unfortunately an attacker could receive two transceivers in the network connected by a high quality out of-band link and replays messages heard at one location at the other location, thus make it easy for the adversaries to get the data.

In term of protecting the sensor network, the security goals are to protect the completely physical entities devices, packets, links, and ultimately the network. During the deployment of the network system, the securities of the system are indeed a crucial part because threats are attacking the vulnerability of the system while trying to conceal their appearance. To reduce the vulnerability of the node for physical tampering, nodes are usually features with unique ID and a trusted network system is tested and builds since the pre-deployment [8] of the node. Regardless the effort had made, once the adversaries captured and cloned the node, they had a control over the sensor in the node. Therefore, the complexity of the security is indeed needed to be harder, so it could minimize the attacker effort.

II. IMPLEMENTATION DETAILS

This model exploiting the property of stationary node, where it distances remain the same. The change of distance of the nodes indicates that the node is already compromised.

A. Network Model

Using NS2 simulator the nodes are created with flat address and have a unique identity. Initially the nodes are deployed in the network, and then the base station sends the coverage region to all the nodes.

Later, the sensor nodes gather their location and distance, by sending a packet to the base station and calculate their time taken to receive back the verified message from base station.

Base station will receive all the nodes information before broadcast the data to the network.

Base station will only broadcast (node information which are identity and location) the data according to the longest return time trip, and then the data will only be held by the receiving nodes. However, if the packets get dropped then the nodes won't be able to send any data to the base station.

As a prerequisite, all nodes cooperatively will have to build the routing table. The construction of the network is depending on the base station itself. Without the connection between the sensor node and the base station, there will be no connection between two nodes.

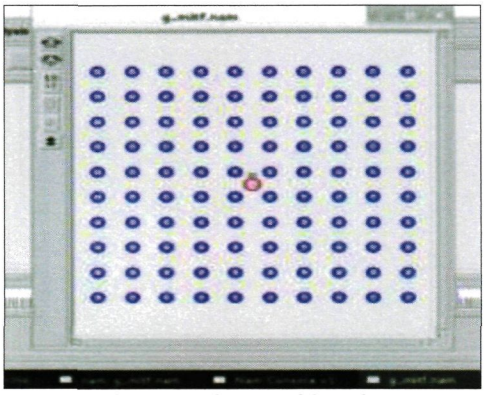

Figure 1: Deployment of the nodes

B. Adversaries and Environment Model

Assuming that the cloned node are deployed into an establish network, the base station and valid nodes are already well known to their neighbors based on ID and location. The node cloned is set to be exists only one in the simulation.

The adversaries can deploy their cloned nodes into a network by using the same captured node ID [3], that will compromised the network successfully without proper detection protocols. Adversary goal are to ensure their clone left undetected in the network system, therefore they might deploy small number of clone in the network area [6] as if their factures of clone are large in a network, the changes of behavior can raise an alert.

However, as the clone node has the same ID with any of the node inside the network, an honest neighbor might send a data to the cloned node

III. NODE CLONING DETECTION

The packets of each node are changed in this model. It is consists of i^{th} bit of node ID, their grid location.

Cloned node will try to connect with any of the nodes in the network; the neighbouring node possibly received the connection without proper detection scheme. This model will compare the location bit in the packet send with the request.

.

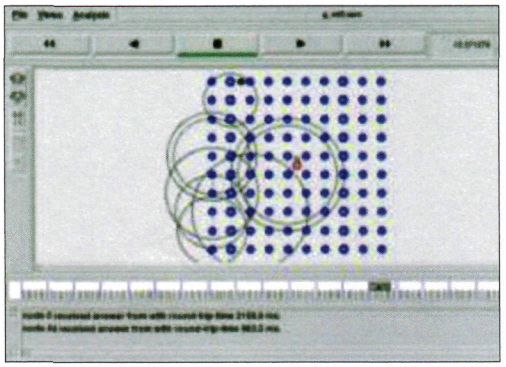

Figure 2: Node request and reply, the connection is establish when it pass the base station authentication

Algorithm case_1: Message

$N_i \rightarrow$ current node ID

$location_i \rightarrow$ current node coordinate

$N_i \rightarrow$ clone node ID

$location_j \rightarrow$ clone node coordinate

OUTPUT: NIL if the message is send to the node with the correct grid location.

Algorithm : Cloned detection when the location of node *x* is modified by the adversaries

Input : Node ID and location (id_i || $location_i$)

Output : Receive packet if the node ID and location is valid

```
1    N_i ← N_i(id_i || location_i)
2
3    If < ID_i == ID_j > then
4    Check location for node ID_j
5    else
6    Packet from different node
7    If < location.ID_j != location.ID_j >
8    Clone node detected
9    else
10   Receive packets
```

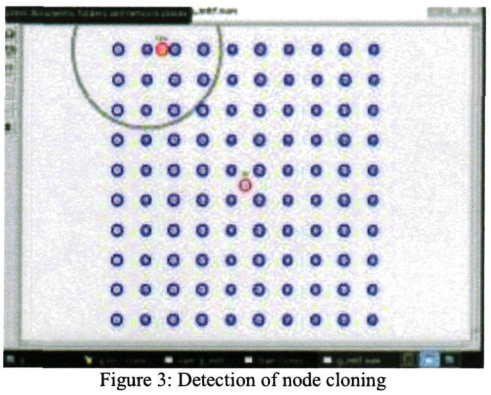

Figure 3: Detection of node cloning

Neighbour node then, will broadcast the node ID and it corresponding location to the other nodes and send a message to suspend the connection with the clone node.

IV. SIMULATION RESULT

The simulation is tested in different number of nodes with the same covered area of the base station.

The generated packets to send the nodes information are getting redundant as the number of nodes increase. The further the nodes from the base station, it will hop more nodes to reach destination. Thus, the neighbour nodes that have the information will drop most of the packet.

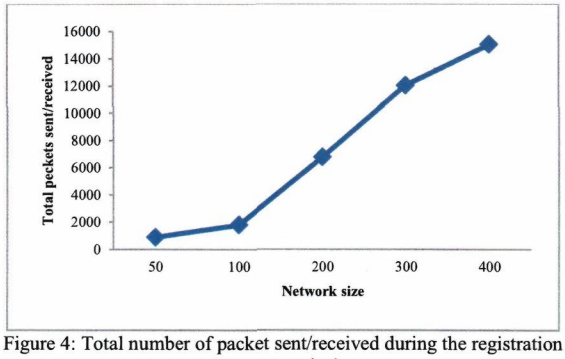

Figure 4: Total number of packet sent/received during the registration process vs network size

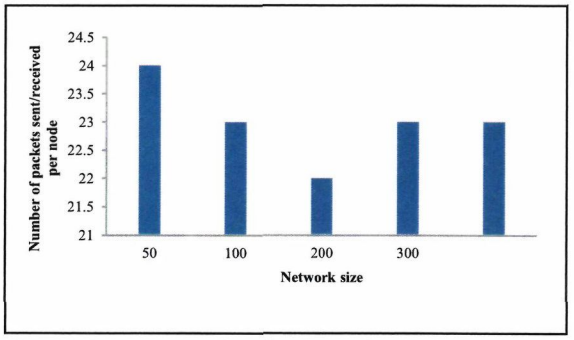

Figure 5: The average number of packet sent/received per node during the registration process vs network size

The plot for total packets sent/received during coloring process is shown in figure 4. It is observed that the number of packets sent/received increases with increase in the network size. With increase in the network size, the number of nodes in the network also increases. As a result, the total number of packets sent/received increases.

In Figure 5, the average number of packets sent/received per node is plotted versus the network size during registration process. From the figure, it is observed that the average number of packets sent/received per node remains almost constant irrespective of the network size. The average number of packets sent/received per node is independent of the distance of the node to the base station and to another node. Hence, it remains almost constant with different location of the nodes.

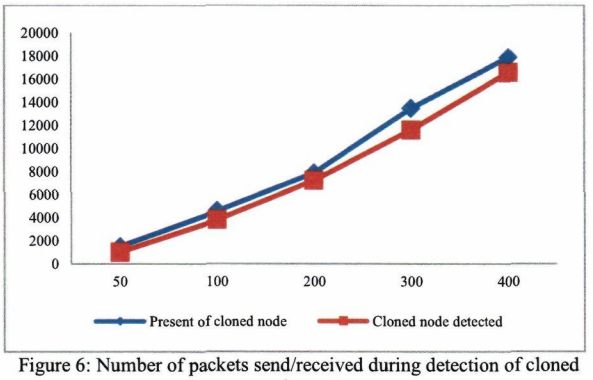

Figure 6: Number of packets send/received during detection of cloned node

Figure 6 is shown to verify that the method can detect the malicious node by comparing the nodes location. During the simulation process, the malicious node sending false message, thus increasing the number of packet send/received by the node inside the network. After the cloned node is detected, the false packet is drop and the packet send/received by the node can be maintained.

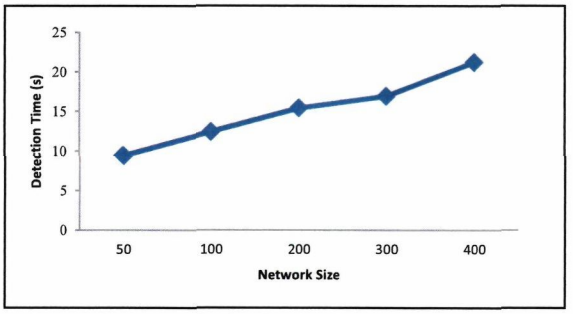

Figure 7: Time taken for the cloned node to be detected in seconds versus network size

From Figure 7 the time taken for the cloned node to be detected is depending on the network size. This is due to the size of the neighbor table in the interest node. The receiver node will check the node ID and location inside their neighbor table list.

V. CONCLUSION

From the user view, the appliance with the applied sensor node are considered low cost and cabling between two sensors are not needed, however the drawback is on its security, that cost in the energy consumption and especially in data integrity and confidentiality. Security issues become highly concerned as the node holds the cryptic keys and any other secret material.

Sensor node usually is unattended and left it vulnerable to attack. Furthermore, the advancement of sensor technology ~~is~~ will continuously extending the application of WSN and thus creating a much more threat into the whole network as the adversaries can use the improved device to attack. To prevent the adversary from establishing a significant control over the

network, a system that can identify and prevent the node clone from joining the network system need to be developed.

This model, however require very high assumption, because it solely depend on the location and distance of the sensor, a clone node could physically replace the node and by the same time controlled by the adversaries party. Thus future works in data security are important.

REFERENCES

[1] Y. M. Yussoff, H. Hashim, R. Rosli, and M. D. Baba, "A Review of Physical Attacks and Trusted Platforms in Wireless Sensor Networks," *Procedia Eng.*, vol. 41, no. Iris, pp. 580–587, 2012.

[2] A. Blilat, A. Bouayad, N. El Houda Chaoui, and M. El Ghazi, "Wireless sensor network: Security challenges," in *2012 National Days of Network Security and Systems*, 2012, pp. 68–72.

[3] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *2005 IEEE Symposium on Security and Privacy (S&P'05)*, 2005, pp. 49–63.

[4] Z. Li and G. Gong, "On the Node Clone Detection in Wireless Sensor Networks," *IEEE/ACM Trans. Netw.*, vol. 21, no. 6, pp. 1799–1811, Dec. 2013.

[5] K. Xing and D. H. C. Du, "Real-time Detection of Clone Attacks in Wireless Sensor Networks," pp. 3–10, 2008.

[6] J. Luo, L. Zhou, and H. Wen, "Lightweight and effective detection scheme for node clone attack in wireless sensor networks," *IET Wirel. Sens. Syst.*, vol. 1, no. 3, pp. 137–143, Sep. 2011.

[7] L. Hu, "Localization for Mobile Sensor Networks," no. October, 2004.

[8] Y. M. Yussoff and H. Hashim, "Analysis of Energy Consumption on IBE-Trust Security Framework," vol. 2, no. October, pp. 236–240, 2011.