Advances and Applications in Mathematical Sciences
Volume 18, Issue 8, June 2019, Pages 731-740

IMPACT OF CLONE NODE ATTACK ON WIRELESS SENSOR NETWORKS

SACHIN LALAR, SHASHI BHUSHAN and SURENDER

CSE, IKGPTU
Kapurthala, India
E-mail: sachin509@gmail.com

CGC, Landran
Punjab, India
E-mail: shashibhushan6@gmail.com

GTB, Bhawanigarh
Punjab, India
E-mail: ssjangra20@rediffmail.com

Abstract

Wireless Sensor Networks (WSN) are the large network of limited-resource sensor nodes that can be transmitted data over narrow bandwidths and shorter distances. The networks suffer from various attacks by its nature. In clone node attack, the attacker gets legal nodes from the network, reflects the encrypted information in new sensors, and implements them in the network. This paper first analyzes the impact of clone node attacks in wireless sensor network in different scenarios. The simulation effects of clone node attack in wireless sensor network are performed in ns2 simulator on two performance parameters. The performance of network is evaluated in standard and clone node network with respect to number of attackers and location of clone node in network. The result shows that impact of clone node is high when number of nodes is large and clone node is positioned near to base station.

I. Introduction

Wireless sensor networks differ from traditional networks because of limited resources, limited memory, and limited power of sensor nodes. The base node communicates with the sensor nodes to collect data / information and process it. Some types of networks are enforced in conflicting and

2010 Mathematics Subject Classification: 68M10.
Keywords: Wireless Sensor Network, Attacks, Clone Node Attack, PDR, Binary Search Tree.
Received February 19, 2019; Accepted March 23, 2019

accessible environments that cannot be centered on the network [1]. In this case, the network suffers various types of attacks. The attacker can intercept the nodes from the network and obtain information from the detected nodes. Using this information, an attacker reflects detected nodes and puts cloned nodes in the network [2]. This attack is called impersonation or clone node attack. In a clone node attack, an attacker first steals a legitimate node from the network and then sends sensitive information, including the detected node's key. The attacker then uses the extraction information to create various copies of that node and calls them back to the network. Clone nodes are also known for impersonation attacks. Using counterfeit attacks, the attacker can easily launch various attacks, such as black-hole, sinkhole, selective-forwarding and flooding attack etc [3]. With these attacks, the clone node controls the entire network, which affects network operation. The attacks also reduce network performance. This section describes various attacks that are triggered by the clone nodes. These attacks are described for each layer of a wireless sensor network. Physical attacks on WSN are initiated by blocking the radio channel. The radio channel can wirelessly transmit the clone node on radio channels that affect other sensor nodes. Physical sensor nodes are physically controlled to prevent physical attacks on WSN, but it is difficult. Jamming and Radio Interference are two physical attacks triggered by the clone node [5] [6].

The main task of data link layer is to make the access to a shared radio channel between the nodes. The clone nodes may interrupt the predefined protocol of the connection layer [7]. For example, a clone node may cause the collision of the packet to break or interrupt the sensor nodes from repeated iterations. The clone nodes can perform the Collisions Attack, Exhaustion Attack in link layer.

The WSN network layer finds the path for communication. The Clone nodes can perform False Routing, Hello Flood Attack, Sink Hole Acknowledgement Spoofing Attack, Black Hole, Selective Forwarding, Wormhole attacks that completely violate routing information [8][9][10]. This layer can be used by clone node for further generating the attack in the network. Data integrity attack, Flooding, Energy drain & De-Synchronization are different type of attacks that can be triggered by clone node on transport layer. The clone nodes can produce Overwhelming, Data Aggregation Attack

types of attacks on application-layer. The table I shows the attack which can be produced by clone nodes on layers of wsn.

Table I. Attack Caused By Clone Node.

Layer	***Attack***
Physical Layer	Jamming, Radio interference
Data Link Layer	Collisions Attack, Exhaustion Attack
Network Layer	False Routing, Hello Flood Attack, Sink Hole Acknowledgement Spoofing Attack, Black Hole, Selective Forwarding, Wormhole
Transport Layer	Flooding, Data integrity attack, Energy drain attack, De-synchronization
Application Layer	Overwhelming, Data Aggregation Attack

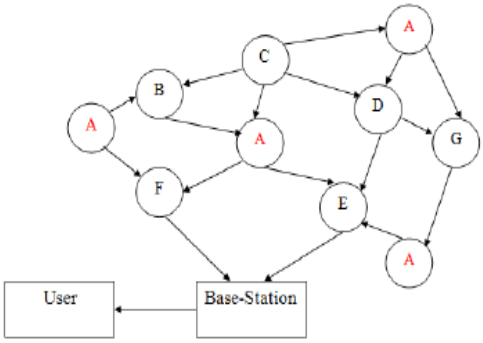

Figure 1. Clone Node Example.

The wireless sensor network diagram is shown in Figure 1, where it is replicated in the clone node *A* in the network. The clone node can launch various attacks on WSN. The clone node may receive a valid packet from a legitimate node and the packet is discarded. Thus, re-packet transmission affects network performance [4].

The purpose of this paper is to analyze the impact of clone node attacks on network. The paper is maintained in the following sections: Clone node attacks implementation describes in section II and also describes the effects of clone node attacks on wsn. The section III explains the proposed method to detect the clone node in the network. The entire works conclude in section IV.

II. Simulation and Result

In this section, we perform the simulation of clone-node attack on the NS2 simulator. The static sensor nodes implement on the network simulator including the base stations. The network consists of 75 nodes, each of which can wirelessly communicate with nodes adjacent to its transmission line. Two different scenarios have simulated to test the effects of clone node attacks on WSN. We have counted the network performance with PDR and packet loss performance parameter. The clone nodes are inserted on the same network and check the performance with the same parameters. In the first scenario, we changed the number of clone nodes in the network. In the second scenario, we changed the position of the clone node in the network.

A. Varying the Number of Clone nodes

The clone nodes in the network have been changed from 1, 2, 4 and 6. The network has simulated with a clone node attack for 4 variations & without clone node attack. We calculate the results of packet delivery ratio (pdr) and packet loss for networks. Figure 2 shows a comparison of the outputs of the PDR of a standard network and the network with clone nodes. As a result, the performance of the network will be degraded if there is a clone node in the network. As the number of clone nodes in the network increases, the network performance also degrades. If there are no clones in the network, the pdr is high. If there is a clone node in the network, the pdr value is reduced by 35%. With two clone nodes the PDR drops by 45%. At 4 clone nodes, the PDR dropped by 70 percent.

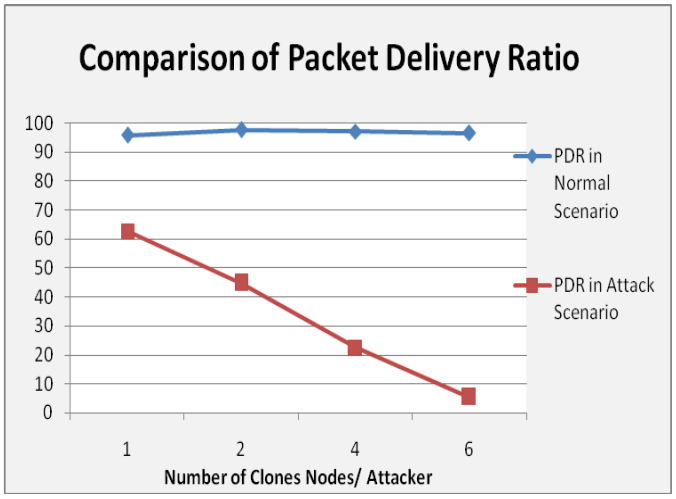

Figure 2. Comparison of Packet Delivery Ratio in Scenario-1.

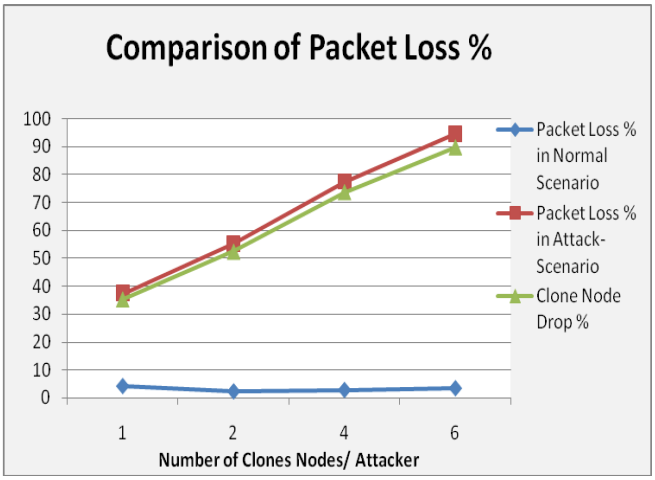

Figure 3. Comparison of Packets Loss in Scenario-1.

When the clone nodes are 6, pdr is below to 10%. If the number of clone nodes in the network is large, network performance may be further degraded. The packet loss comparison is shown in Figure 3. From this result, nodes in the network confirm that more packets fall into the network if there is clone node in the network. If the number of clone node increase, then packet loss and drop by clone node also increase.

B. Varying the Position of Clone nodes

In this case we have varied the placement of the clone node in the network. The network has simulated without attack and with clone-node attack in three different positions of the clone node. Three positions of the clone node: near the base station, from the base station and in the middle of the network. We calculate the results in pdr and pocket loss of network.

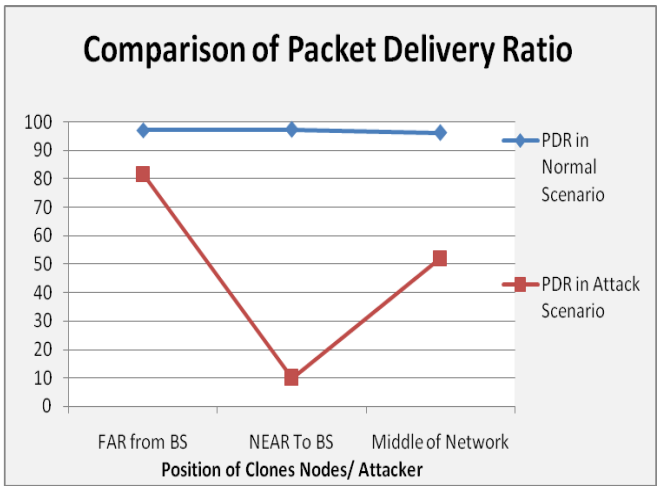

Figure 4. Comparison of Packet Delivery Ratio in Scenario-2.

Figure 4 shows the PDR comparison with the two networks with respect to the location of the clone node in the network. Thus, if the clone node is near the base station, then the performance of the network will be highly degraded. If the clone node is take away from the base station, the PDR decreases by only 18% to the normal pdr value. If there is a clone node in the middle of the network, the pdr value is about 50%. However, if the clone node is near the base station, the PDR value is decreases by 80%. The packet loss comparison is shown in figure 5. From this result, it is determined that the base of the clone node remains close to the base station, and the packet drop in the network is also large. Since the location of the clone node is near the base station, the packet loss and the clone node drop is very high.

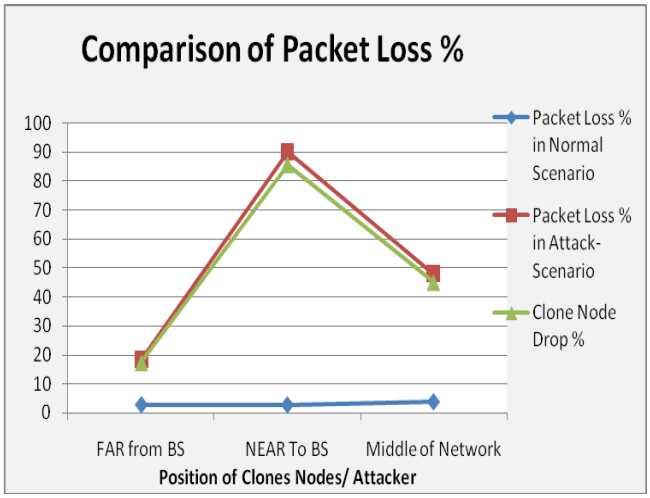

Figure 5. Comparison of Packets Loss in Scenario-2.

III. Proposed Method

In section II, we have observed that if clone nodes present in the network it will degrade the performance of the network. We have proposed a new method, TBCND, to identify the clone node in network. TBCND has two phases: Network Expansion and Detection phase. The nodes of the network are structured in Binary Search Tree (BST). Each sensor has a specific key node-id. Tree structure of network will configure by node-id. The deploy tree works on property of BST. The node id is smaller than to the root then it will become the left sub tree otherwise it will become right sub tree of root. We will select the middle id from the sorted list of node and deployed as the root of tree. After the BST root expansion, the sorted list is divided into two parts. The first subpart has node id which is smaller than to root and extends towards the left on the root. The second part consists of node-id which is larger than the root of the tree and will be positioned right side of the root. In the first and second parts of the list, middle node ids are selected & deployed as left and right node of root. When the middle value is selected from the list, the list is again divided into two parts. We will repeat the above steps to expand the network's remaining nodes. When BST tree is balanced, the complexity of each operation is $O(\log n)$. We will prove that the constructed tree is balanced binary tree.

Proof. The height (h) of a proposed tree of n nodes is $\log(n+1)$. We will prove the height of tree using induction.

Basis For $h = 1;\ n = 1,\ \log(n+1) = \log 2 = 1$ (i)

Inductive Hypothesis

Assume that the theorem is true for height $h \le k$

Inductive Step

We must prove that the inductive hypothesis is true for height $k+1$.

Let $h = k+1$. Note that the theorem is true (by the inductive hypothesis) of the sub tree of the root, since they have height k.

$$n = n_{\text{left}} + n_{\text{righ}} + 1 \quad \text{(ii)}$$

$$n = 2^* n_{\text{left}} + 1 \ \{\text{as tree is complete}\} \quad \text{(iii)}$$

$$\text{but } k = \log_2(n_{\text{left}} + 1) \text{ by inductive hypothesis} \quad \text{(iv)}$$

$$n_{\text{left}} = 2^k - 1 \quad \text{(v)}$$

$$\text{put in (iii) } n = 2^*(2^k - 1) + 1 \quad \text{(vi)}$$

$$n = 2^{k+1} - 1 \quad \text{(vii)}$$

$$n + 1 = 2^{k+1}. \quad \text{(viii)}$$

$$\text{Taking log both sides } \log_2(n+1) = \log_2(2^{k+1}) \quad \text{(ix)}$$

$$\log_2(n+1) = k+1 \quad \text{(x)}$$

$$\log_2(n+1) = h. \quad \text{(xi)}$$

Thus, the inductive hypothesis is true for height $K+1$ and, hence (by induction), true for all heights. A complete binary tree of n nodes has height $\log_2(n+1)$.

The replication detection phase will be started after deployment of tree. The detection phase will check whether node is position follow the BST rule or not. If any node does not follow the property of BST tree, then it may be clone node and verification of node will initialize by detection node. The

detection process will check the node id when it will communicate in the network. If communication of sender node is towards the base station, neighbor node will check the node id of sender whether it position as per BST or not. If sender is left side of neighbor then the node id must be less then to parent otherwise it will greater then to node id of neighbor. If the condition is satisfied then the packet of sender is forward to next node and same step is followed by the next node also. Otherwise, the sender node will be clone in the network and verification process is initialized and red alert signal is sent to the base station for further mechanism.

IV. Conclusion

Wireless sensor networks are exposed to various security threats. This paper describes various attacks caused by the clone nodes in the WSN and investigates the effects of clone node attacks on WSN. The performance of standard networks and cloned node networks is calculated in PDR and packet loss performance parameters. In the first scenario, we have changed the number of clone nodes in the network. As the number of clone nodes increases, the average loss increases by 80%. In the second scenario, we changed the position of the clone node in the network. When the position of the clone node is near to base station, the packet loss is increase to 75%. We can conclude that the performance of network will decreases when there are large number of clone nodes in the network and the location of the clone nodes near to base station. We have proposed a new clone detection procedure in which network is deployed in tree structure and clone node easily detected in the network. In the future, we will implement the TBCND method and compare with existing method.

References

[1] Sachin Lalar, S. Jangra and S. Bhushan, Study of Attacks & Countermeasures on Layers of Wireless Sensor Networks, International Journal of Control Theory and Applications 10(15) (2017), 153-162.

[2] I. Akyildiz, S. Weilian, Y. Sankarasubramaniam and E. Cayirci, A survey on sensor networks, IEEE Communications Magazine 40(8) (2002), 102-114.

[3] H. C. Chaudhari and L. U. Kadam, Wireless Sensor Network Security Attack and Challenges, International Journal of Networking, pp-04-16, 2011.

[4] Jing Deng, R. Han and S. Mishra, Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks, First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05), Athens, 2005, pp. 113-126.

[5] M. Franklin, Z. Galil and M. Yung, Eavesdropping games: a graph-theoretic approach to privacy in distributed systems, J. ACM 47(2) (2000), 225-243.

[6] Wenyuan Xu, Ke Ma, W. Trappe and Yanyong Zhang, Jamming sensor networks: attack and defense strategies, in IEEE Network, vol. 20, no. 3, pp. 41-47, May-June 2006. doi: 10.1109/MNET.2006.1637931.

[7] Shahriar Mohammadi and Hossein Jadidoleslamy, A Comparison of Link Layer Attacks on Wireless Sensors Network International Journal on Applications of Graph Theory in wireless ad hoc networks and sensor networks (GRAPH-HOC) Vol.3, No.1, pg 35-56, 2011.

[8] D. Sheela, C. N. Kumar and G. Mahadevan, A non cryptographic method of sink hole attack detection in wireless sensor networks, 2011 International Conference on Recent Trends in Information Technology (ICRTIT), Chennai, Tamil Nadu, 2011, pp. 527-532.

[9] Wazir Zada Khan, Yang Xiang and Mohammed Y. Aalsalem, Comprehensive Study of Selective Forwarding Attack in Wireless Sensor Networks, International Journal of Computer Network and Information Security (IJCNIS), pp. 1-10, 2011.

[10] Wang Xin-sheng, Zhan Yong-zhao, Xiong Shu-ming and Wang Liangmin, Lightweight Defense Scheme against Selective Forwarding Attacks in Wireless Sensor Networks, pp.226-232, 2009.

[11] Guorui Li, Xiangdong Liu and Cuirong Wang, A Sequential Mesh Test based Selective Forwarding Attack Detection Scheme in Wireless Sensor Networks, pp.554-558, 2010

[12] D. Buch and D. Jinwala, Detection of Wormhole attacks in Wireless Sensor Network, 3rd International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom 2011), Bangalore, 2011, pp. 7-14.

[13] Yih-Chun Hu, Adrian Perrig and David B. Johnson, Packet Leashes: A Defence against Wormhole Attacks in Wireless Networks, INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE, pp. 267-279, 2003

[14] R. K. Gill and M. Sachdeva, Detection of Hello Flood Attack on LEACH in Wireless Sensor Networks, Next-Generation Networks, Advances in Intelligent Systems and Computing, vol 638. Springer, Singapore (2018)

[15] M. J. Freedman and R. Morris Tarzan, A peer-to-peer anonymizing network layer, Proceedings of the 9th ACM Conference on Computer and Communications Security, 2002.