Efficient Detection of Node Masquerade Attack in WSN using Centralized Approach

Amanpreet Kaur[1] Dinesh Kumar[2]
[1]P.G. Student [2]Assistant Professor
[1,2]Department of Computer Science and Engineering
[1,2]GZS, PTU Campus, Bathinda Punjab Technical University, Jalandhar

Abstract— Wireless Sensor Networks are consists of number of tiny sensor nodes that are used in monitoring and the tracking systems for the purpose of sensing, communication and computational capabilities. Sensor networks are frequently deployed in an unattended manner, probably exposed to physical attacks and be totally compromised. When a sensor node is captured, it may expose any secret information to attackers. Thus, any security mechanism for sensor networks has to be elastic against node compromise attacks. In this paper we propose a novel technique to detect the node masquerade attack (clone attack) by using rssi values and centralized method. Simulation and performance analysis shows the effectiveness of our solution and also provides a high detection rate.

Key words: Wireless Sensor Network, Clone Nodes, Energy Consumption, Node Masquerade Attack, Detection Rate, Routing Overhead

I. Introduction

Wireless Sensor Networks are composed of large number of small nodes with sensing, wireless communication and computation capabilities. The important areas of WSN are environmental monitoring and target tracking. The application areas of WSN are monitoring, remote sensing, warning systems, industrial applications, fault tolerance, military applications, health care systems.[1][2].

Because of the limited energy and memory sources of the sensor nodes, the security confronts in these networks are meeting more difficulty as contrasted to other mobile telecommunication networks. These difficulties are increased if the sensor nodes have mobility. Due to the unattended nature and harsh deployment in military and civil applications, WSN are easily susceptible to the internal and external attacks. The sensor nodes can physically captured easily in harsh environments. This paper considers the node masquerade attack by which the adversary can capture the sensor node physically and take all its key materials. Then by using key material of captured node an adversary can compromise another node with same id and cryptographic material. The clone node acts as a legitimate node as it has same cryptographic material as original one. So node masquerade attack is not easily detected. For the security concern node masquerade attack is severe for the network as an adversary can also initiate a number of malicious activities. Clone nodes also launch a variety of insider attacks such as wormhole, blackhole and also inject false data aggregations to bias the final results.

Rest of the paper is organized as follows – section 2 represents the related work to node masquerade attack detection in WSNs, section 3 represents the existing method, section 4 represents the improved method 5 represents the simulation results and section 6 concludes the work of the paper.

II. Related Work

Geetha C et all proposed a token based detection technique [3]. In this algorithm a token is generated by the source node. In every iteration, one node is chooses as intermediate node to forward the token. In this technique the node ID and Location are attached in to the token every time and so the token size acquires increased but it is only one encrypted message. The node that receives the tokens from source node and the clone node is called as the witness node that will only performs the contrast of the contents of both tokens. If clone node is detected, the repudiation procedure is invoked. This method decreased the communication overhead. This algorithm shows effectiveness in detecting the clone nodes easily and simply.

Chia-Mu Yu et all proposed a Compressed sensing-based clone identification method [4]. This clone detection method is based on a state-of-the-art signal processing technique and compressed sensing, called CSI. This method has not only different design philosophy fundamentally from the existing methods, but also it has the least communication cost among all other detection techniques

Sheela et all proposed two protocols: RWS AND MRWS to detect the clones [5]. Random Witness Selection (RWS) Protocol & Minimized Random Witness Selection (MRWS) protocols accomplish the obligations that having only restraint communication and memory overheads. Their results shown that, contrasted to earlier distributed and centralized approaches RWS and MRWS is more efficient in provisions of communication costs in large-scale sensor networks, and also attains a higher detecting probability of clone attacks.

Sajnani H. Et all proposed a parallel and efficient approach to large scale clone detection [6]. This method uses the popular MapReduce framework to horizontally scale clone detection across multiple machines. To enhance the efficiency to prune the number of code block comparisons, this method used a filtering heuristic. The filtering heuristic can be used in combination with other techniques to increase their efficiency.

Bonaci et all proposed a system theoretic approach to detect node capture attack [7]. In this technique authors model physical node capture, cloned node recognition and revocation of compromised nodes by using a control theoretic framework. By merging probabilistic analysis of logical key graphs and linear control theory, they originated a dynamical model that effectively describes network performance under attack. They developed a network response strategy by using LQR and LQG finest control theory tools that ensures secure network connectivity and stability under attack.

Heesook Choi et all proposed a SET method to detect clones [8]. The main aim of SET is to detect clones by calculating set operations (union and intersection) of exclusive subsets in the network. First, SET securely figure exclusive unit subsets between one-hop neighbours in the network in a distributed means. SET then utilize a tree structure to calculate non-overlapped set operations and combined interleaved confirmation to prevent illicit falsification of subset information during forwarding. Simulation shows the consistency and flexibility of SET by analyzing the probability that an adversary may efficiently block the set operations.

Naruephiphat et all proposed An Area-Based Approach for Node Replica for identifying node replication attacks [9]. The simulation results demonstrate that the proposed ABCD method attain high successful detection rate and decrease the communication overheads

Jokhio et all proposed SCADD protocol [10]. This protocol composed of two building blocks: node attack detection block and defence advocating measure block. The previous offers strategic-based attack detection to reduce the risk of misjudgement and the later uses a self-destruction defence measure against node capture attack, without actually destroying the node`s radio service, to evade a major security contravene.

Udgata et all proposed a Zero Knowledge Protocol [11]. In this protocol the cloning attack is tackled by attaching a unique fingerprint to each node, that rely on itself and the set of neighbouring nodes. The fingerprint is attached with every message that a sensor node sends. The ZKP is used to certify non transmission of vital cryptographic information in the wireless network in order to avoid man-in-the middle (MITM) attack and replay attack.

Khan et all proposed a detection scheme using Single Stage Memory Random Walk with Network Division [12]. In this method SSRAND merge the single stage memory random walk with network division for clone detection and simulation results confirm that it decreases the memory and communication costs and also provides more security with improved detection probability of clones

III. EXISTING METHOD – HIP AND HOP PROTOCOL

HIP and HOP are distributed, efficient, cooperative protocol [13] that leverages only one-hop communication and node mobility to impose the emergent property of node replica detection. Each sensor i) records ID and location of met neighbours; and, ii) compares its own records with the ones of met neighbours. In this way the clones can be detected only using one-hop local communications. *HIP* (History Information-exchange Protocol) and *HOP* (History Information-exchange Optimized Protocol) leverages the same level of collaboration between nodes, but exhibit a different level of thoroughness in order to detect the clone. In particular, HOP improves the clone detection rate, at the price of an increased computational cost.

In HIP protocol, each node compares its own log with the logs received from the neighbours. Comparing history logs with just direct neighbours only requires one-hop communications. But in HOP protocol each sensor node compares its own logs with the logs from received neighbours and also compares the received logs between the neighbours not just with the history log it owns.

This detection scheme composed of two procedures: spread and receive. In spread procedure every sensor creates a new message with its own data, namely its ID, its position claim, and its history log collected until that round. Then, it uses the Broadcast function to broadcast the message to its neighbourhood. The receive procedure consists of three phases: collecting messages from neighbours, comparing identifiers and positions of neighbours, and checking history logs received from neighbours.

IV. IMPROVED METHOD – USING RSSI AND CENTRALISED METHOD

Sensor networks may interact with sensitive data and operate in hostile unattended environments. So these are more prone to the attacks. Node masquerade attack is the challenging one to detect. Due to the irreplaceable and limited battery life of sensor nodes, the detection scheme is good that consumes less energy. In HIP AND HOP protocols, if clone node is not neighbor of two witness nodes then even if witness nodes meet each other and also if clone node is neighbor of two witness nodes and witness nodes never meet each other then clone will not be detected. So we propose a more efficient detection scheme to detect the clones with low energy consumption. The methodology used is:

- Divide network into clusters.
- Every node within a cluster will exchange Hello message
- Now every node will check signal strength of each hello message received and will arrange in ascending order

A. *Case 1: If Clone is Present within the Same Cluster:*

- Each node will send two smallest RSSI values along with their id to cluster head
- If two nodes have same id and different RSSI values then it indicates presence of clone nodes

B. *Case 2: If Clone Nodes Present Outside the cluster:*

- Each cluster head will send list of members to base station along with their ids. If two clusters have members with same id then it indicates presence of clone outside the cluster.

C. *Case 3: If cluster heads are the clone nodes:*

- Base station checks the id of cluster heads and if two cluster heads have same id then it indicates the presence of clone.

V. SIMULATION AND ANALYSIS

In order to evaluate the performance of HIP, HOP and our centralised and rssi method, we have simulated existing distributed detection method and our proposed centralised method using NS2 simulator. Parameters which are considered for simulation are detection time, detection rate, energy consumption, packet delivery ratio and routing overhead.

A. Detection Time

Since energy consumption is the main issue in the wireless sensor networks along with network security, any approach that is being taken into account to make network more secure must also consume less energy. The proposed scheme takes less time to detect the clones in the network; this indicates less number of messages being exchanged between the nodes consequently less energy being consumed in the network.

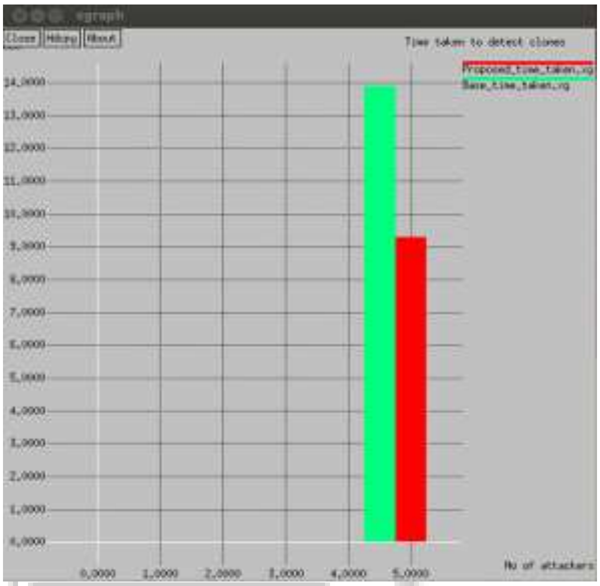

Fig. 1: Detection Time

B. Detection Rate

This is ratio of number of nodes successfully detected in the network to the number of attacker nodes that were being deployed. It indicates the efficiency of the scheme in detecting the malicious nodes in the network.

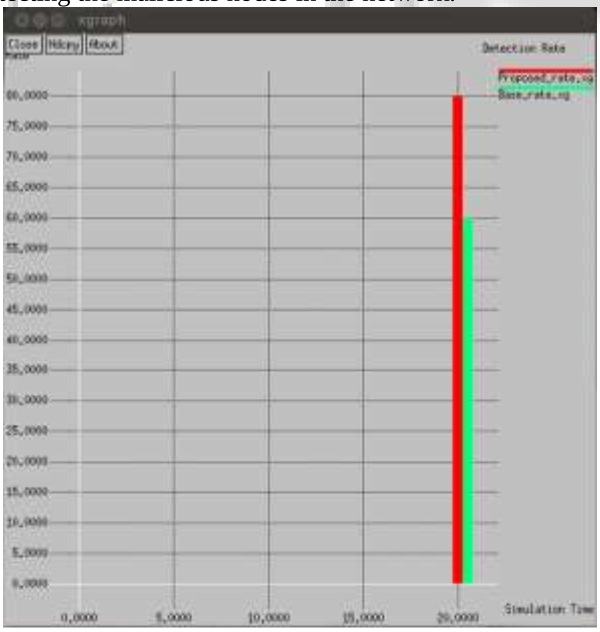

Fig. 2: Detection Rate

C. Energy Consumption

This factor is indicator of lifetime of the network. If the network is consuming more energy, less will be its lifetime. Our proposed scheme showed better detection rate along with less energy consumption in the network.

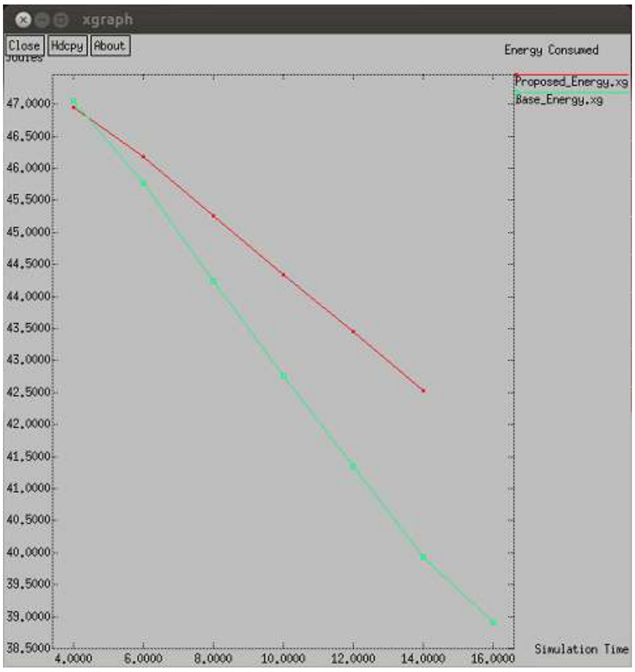

Fig. 3: Energy Consumption

D. Packet Delivery Ratio

This is ratio of number of packets successfully delivered to the number of number of packets sent. It indicates the efficiency of the scheme in delivering of packets in the network.

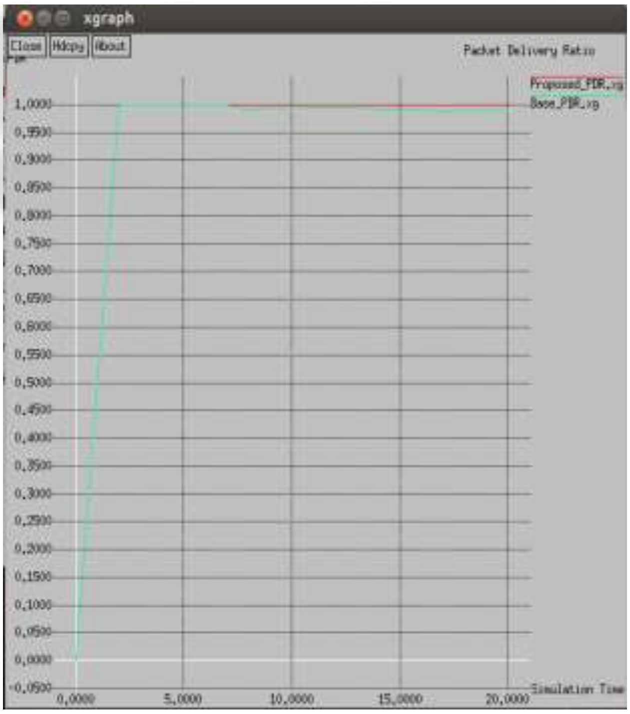

Fig. 4: Packet Delivery Ratio

E. Routing Overhead

Since routing overhead is the issue in the wireless networks along with network security. The proposed scheme has less routing overhead in the network; this indicates less number of messages being exchanged between the nodes consequently less energy being consumed in the network.

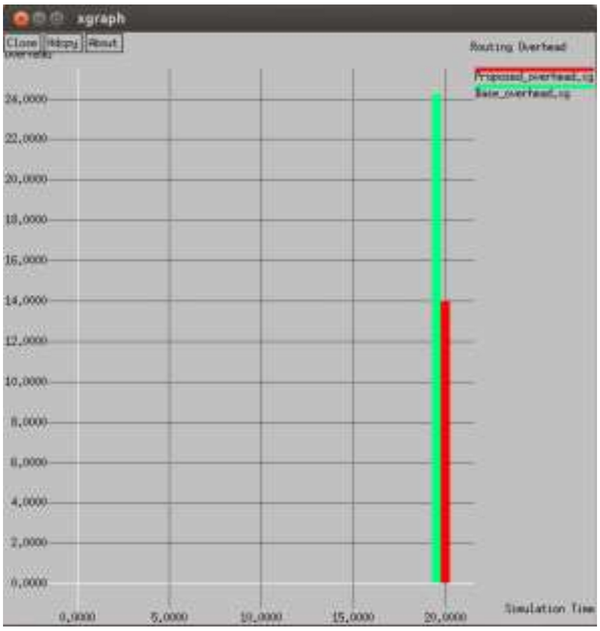

Fig. 5: Routing Overhead

VI. CONCLUSION

In this paper, we presented with an intrusion detection scheme to the protection of mobile WSNs when deals with the clone attack. Particularly, we have introduced novel and efficient method to detect the clones. Both analysis and extensive simulations support the quality and viability of our proposal. In this paper, performance analysis of HIP, HOP and our solution is performed based on detection rate, detection time, energy consumption, packet delivery ratioand routing overhead. Results show that our centralised detection method is better than HIP AND HOP protocols in each case.

REFERENCES

[1] I.F.Akyildiz,W.Su,Y.Sankarasubramaniam,E.Cayirci,Wirelesssensornetworks:asurvey,Int.J.Comput.Telecommun.Netw. 38(4)(2002)393–422.

[2] Carlos F. Garcia-Hernandez, Pablo H. Ibargu engoytia-Gonzalez, Joaquin Garcia Hernandez, and Jesus A. Perez-Diaz, Wireless Sensor Networks and Applications: a Survey Int. Journal of Computer Science and Network Security, VOL.7 No.3, March 2007

[3] Geetha C, Ramakrishnan M " A Token Based Approach for Detecting Replica Node Attack in Static WSNs" In International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, 11 November 2014

[4] Chia-Mu Yu; Chun-Shien Lu; Sy-Yen Kuo, "CSI: Compressed sensing-based clone identification in sensor networks," IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), vol., no., pp.290,295, 19-23 March 2012

[5] Sheela, D.; Priyadarshini; Mahadevan, G., "Efficient approach to detect clone attacks in Wireless sensor etworks," in 3rd International Conference on Electronics Computer Technology (ICECT), vol.5, no., pp.194,198, 8-10 April 2011

[6] Sajnani, H.; Lopes, C., "A parallel and efficient approach to large scale clone detection," 7th International Workshop on Software Clones (IWSC), vol., no., pp.46,52, 19-19 May 2013

[7] Bonaci, T.; Bushnell, L.; Poovendran, R., "Node capture attacks in wireless sensor networks: A system theoretic approach," 49th IEEE Conference on Decision and Control (CDC), vol., no., pp.6765,6772, 15-17 Dec. 2010

[8] Heesook Choi; Sencun Zhu; La Porta, T.F., "SET: Detecting node clones in sensor networks," Third International Conference on Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. vol., no., pp.341,350, 17-21 Sept. 2007

[9] Naruephiphat, W.; Yusheng Ji; Charnsripinyo, C., "An Area-Based Approach for Node Replica Detection in Wireless Sensor Networks," IEEE 11th International Conference on Security and Privacy in Computing and Communications (TrustCom), 2012, vol., no., pp.745,750, 25-27 June 2012

[10] Jokhio, S.H.; Jokhio, I.A.; Kemp, A.H., "Node capture attack detection and defence in wireless sensor networks," Wireless Sensor Systems, IET, vol.2, no.3, pp.161,169, September 2012

[11] Udgata, S.K.; Mubeen, A.; Sabat, S.L., "Wireless Sensor Network Security Model Using Zero Knowledge Protocol," IEEE International Conference on Communications (ICC), vol., no., pp.1,5, 5-9 June 2011

[12] Khan, W.Z.; Saad, N.M.; Aalsalem, M.Y.; Yang Xaing, "Detecting clones in wireless sensor networks using Single Stage Memory Random Walk with Network Division," IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), 2014, vol., no., pp.559,562, 17-20 Nov. 2014

[13] M. Contia, R. Di Pietrob, A. Spognardic, "Clone wars: Distributed detection of Clone attacks in mobile WSNs." Journal Of Computer and System Science, 654-669, 2014

