The study Dynamic Discovery and Avoidance using Position Verification Method in Code cloning in Wireless Sensor Network

Manpreet Kaur[1],Tanisha Saini[2]
M.Tech(Scholar), Assistant Professor
Chandigarh Group of College, Landran

***Abstract* -** In wireless sensor network are given designed in contrary environments where an intruders can normally recognize some of the sensor nodes, initialize could re-build the program and then could replicate them in huge number of clones, easily take-over the mechanism of network. Wireless sensor network largely in-dispensable for secure network protection. Numerous studies the clone attack is a massive dangerous attack against the sensor network where various number of original duplications are used for prohibited entrance into a network. The clone attack, Sybil attack, sink-hole attack and worm-hole attack while multi-casting is a high impact task in the WSN. In this paper described that the previous approached efficient, randomised and division has only a method of self-healing method, which just identify the sensor node verifies by studying the nearest nodes. The survey has studied of the detection and prevention techniques i.e position verification method with message verification and passing approach for discovery, destroying and avoidance the entrance of clone attack nodes within the network.

Keywords: Wireless Sensor Network, Position verification method, clone attack, message verification and passing.

I. INTRODUCTION

Wireless Sensor Network usually consists of a large amount of battery-powered sensor nodes. For lifetime extension, it is of utmost importance in WSNs to plan an energy-efficient medium-access control protocol that minimizes energy consumption while achieving the end-to end delay constraint to meet applications' requirements [1]. Wireless sensor networks are becoming an active topic of research, where sensors are units with sensing, processing, and wireless networking capability. They can automatically collect the data and report the quantities to the sink. Lately, many wireless sensor networks have been planned and deployed for kinds of applications. An important role in several WSN operation models and applications, such as average access scheduling, information fusion, beam-forming, target tracking, etc. The applications such as keep-track of structure target tracking, military, health monitoring and other recovery options, designed and initialize of topology have important events in study work [2]. The procedure of wireless network in a various applications is significant for ensuring security. Now, recovery and avoidance of clone attacks of every level might be low and high in the wireless sensor network. The several of intruders against the network like clone, worm-holes, sink-hole and select forward attacks on against the wireless network are being noticed.

The latest network structure, sensor nodes could appear in replica and perform as original sensor nodes. Normally, there is no single master node in the social and defence network for considering inter-communication between network sensor nodes intense [3].

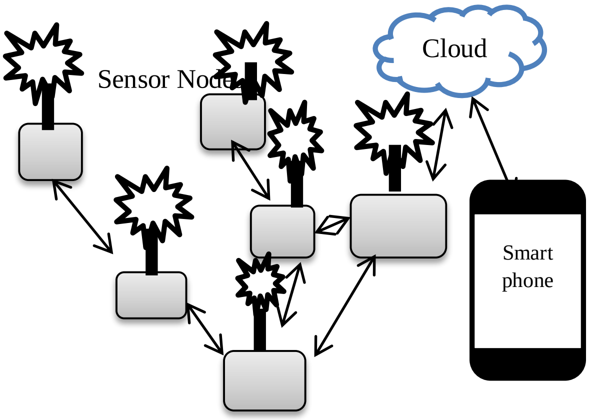

Fig.1 Wireless Sensor Architecture

In above figure 1 described that the architecture of wireless sensor network. In sensor node sent the data to the intermediate nodes.

Several advantages of wireless sensor network like the network setups can be carried out without fixed infrastructure. It is suitable for the non-reachable places such as over the sea, mountains, rural areas or deep forests [4]. The wireless sensor network flexible if there is random situation when additional workstation is needed. Its implementation pricing is cheap. It avoids plenty of wiring [5]. It might accommodate new devices at any time. It's flexible to undergo physical partitions. WSN can be accessed by using a centralized monitor. But some drawback also in wireless senor network like less secures because hackers can enter the access point and obtain all the information. And lower speed as compared to a wired network [6]. The WSN more complicated to configure compared to a wired network. Easily troubled by surroundings (walls, microwave, large distances due to signal attenuation, etc). It is easy for hackers to hack it we couldn't control propagation of waves. WSN is comparatively low speed of communication. Its gets distracted by various elements like Blue-tooth and still Costly (most importantly) [7].

II. RELATED WORK

In this section we studied that the previous work, techniques and attack used. Previous work described in below:

Balmukund Mishra et al., 2015 [8] examined the dispersed node clone detection methods in wireless sensor networks. While there are many protocols in works proposed for node clone discovery, but we have conversed some well-organized procedure like LSM and RED less the category of witness based node clone detection. It has examined the detection level, memory, and energy above of LSM, RED and planned protocol. Presented a method for the optimization of witness based disseminated node clone discovery. For the authentication of planned protocol performance, we have provided accurate as well as reproduction consequences for the numerous parameters of the WSN.

Neenu George et al.,2014 [9] considered wireless sensor network consist of hundreds to thousands of sensor nodes and are widely used in civilian and security applications. One of the serious physical occurrences faced by the wireless sensor network is node clone attack. Thus two node clone detection protocols are introduced via distributed hash table and randomly directed exploration to detect node clones. The former is based scheduled a hash table value which is already distributed and provides key based facilities like examination and secreting to detect node clones. The later one is using probabilistic directed forwarding method and border resolve.

J.Anthoniraj et al., 2014[10] described that the less cost hardware mechanisms consists of sensor nodes with restrictions on battery-operated life, memory size and computation abilities to monitor physical/ conservational conditions. WSN is positioned in unattended and unsecure environments, so it is vulnerable to various types of attacks. One of the corporeal attacks is node replication attack / clone attack. An opposition can easily capture one node from the network and abstract information from captured node. Then reprogram it to create a clone of a detained node. Then these clones can be organized in all network areas, they can be measured as sincere members of the network, so it is problematic to detect a simulated node. WSN can be either static (or) mobile, in that central and distributed clone attack discovery methods are accessible.

The conclusions of wireless sensor networks are positioned in unreceptive environment and vulnerable to numerous types of attacks. This paper delineated the dissimilar kinds of attacks on WSN and largely about clone attack. We have provided numerous approaches to find the cloned node.

Table no: 1 Description in Attack and Technique used

Sr no.	Technique Used	Attack
1.	Line selected multicast and Randomized efficient and distribute	Clone attack
2.	Probabilistic directed forwarding	Clone attack
3.	Set Protocol	Clone attack

III. MODEL OF WSN

In this section described that the wireless sensor network model in below:

A.Network Model: Network is measured area with n number of randomly deployed little sensor nodes. Every sensor node recognizes its id, location, public and isolated key with some memory and dispensation competence. So a sensor node is characterised by {Aid, la, Ka, k-1 a, ma, Pa} .Every node in sensor network can communicate the statistics to any node in the system or outside the network. For that we used shortest path multichip routing using the Euclidean detachment. Statement for the network is no traffic overwork on the intennediate nodes used while direction-finding [11].

B. Threats Model : We measured a time dependent challenger who detentions a node at any time and quotations all the data (node id, public and private keys, all sensed data). This challenger will deploy the clone of taken sensor node with that appropriated modulation into the network area.

IV. DETECTION AND PREVENTION USING MESSAGE VERIFICATION AND PASSING

In this paper described that the Detection and Prevention using Position Verification Methods used i.e message Verification and passing.

A. *Message Verification and Passing*

Message verification and passing assumes a key part in impeding unapproved and tainted messages from being sent in systems to spare the appreciated sensor vitality. Hence, numerous verification plans have been proposed in writing to give message realness and trustworthiness confirmation for remote sensor systems (WSNs). These plans can to a great extent be partitioned into two classes [12]:

Open key based methodologies and symmetric-key based methodologies. The symmetric-key based methodology obliges complex key management, absences of flexibility, and is not adaptable to huge quantities of node compromise attack as message sender and the collector need to share a mystery key. The mutual key is exploited by the sender to create a message authentication code (MAC) for each transmitted message. Nonetheless, for this system, the genuineness and uprightness of the message must be patterned by the node with the common mystery key, which is for the maximum part shared by a gathering of sensor nodes. An interloper can bargain the key by catching a solitary sensor node. What's more, this approach does not work in multicast systems. To tackle the adaptableness issue, a mystery polynomial based message confirmation plan was presented in. The thought of this plan is like an edge unidentified sharing, where the limit is uttered by the level of the polynomial. This methodology offers data theoretic security of the common mystery key when the quantity of messages communicated is not exactly the edge. The reasonable nodes check the genuineness of the message through a polynomial assessment. Be that as it may, when the amount of messages communicated is bigger than the limit, the polynomial can be completely recuperated and the framework is totally broken. The proposed verification and passing plan goes for accomplishing the accompanying objectives: Message Authentication [13].

1. Hop by Hop message authentication.
2. Source privacy.

Message Verification and Passing of Advantages

1. By using the Elliptic curve cryptography, this scheme generates key with smaller size.
2. This scheme does not have the threshold limitations.

Formation of Clone activity through use of the same personal individualities is well known. Most of the current work deals with the detection of the Replication attack through verification of clone ID.

B. *Position Verification Method*

The PVM algorithm is used through the detection and data transmission in the network, where the nodes info is checked from the Base Station iNODEINFO table. After confirmation of PVM algorithm, the procedure collects the ID, timestamp, and current location address of the nodes and associates with initial information when they are recorded.

The consequences of the PVM algorithm can deliver only the trusted nodes in the way to ensure secured data broadcast. Otherwise the precise nodes are treated as interloper nodes or Cloned node and data communication in the current remains stopped and alternate path is selected [14].

V. CLONE ATTACK IN WSN

WSN can be both static and moveable .In static WSN sensor nodes are deployed randomly and after deployment their positions do not change. In mobile WSN, the sensor nodes can move their own after disposition. Two types of detection practices available in static WSN are centralized and distributed. In a centralized approach for detecting node replication, when a new node joins the network, it broadcasts a position claim comprising its position and identity to its neighbours. One or more of its neighbours then forward this location claim to the base station. With position information for all the nodes in the network, the base position can easily detect any pair of nodes with the same identity but at different locations. The main disadvantage of this approach is that if the base station is compromised or the path to the base station is blocked, adversaries can add any number of replicas in the network [15].Distributed approaches for detecting clone nodes is based on location information for a node being stored at one or more witness nodes in the network. When a new node joins the network, its location claim is furthered to the corresponding witness nodes. If any spectator node receives two different location claims for the same node ID, then the existence of clone is detected [16].Some of the protocols to detect clone attack in motionless sensor systems are introduced in the following paragraph.

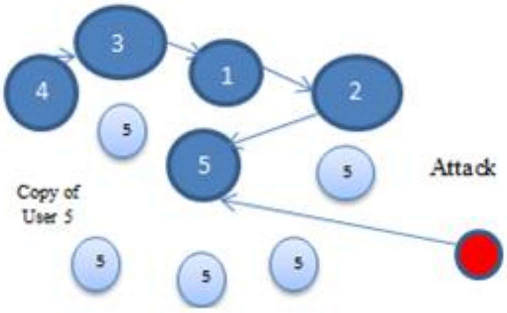

Fig.2 Clone Attack

VI. CONCLUSION

In this paper the message verification and passing method is functional for examining the trustworthiness or then for a detecting the Cloned node. The exploit of a node as a Cloned node with matching information can chance only when the node has complete material about other nodes. Verification of the node needs the request of PVM. Instead of progressive time for PVM to check each and every node, the message verification and passing process is applied for authentication previous to statement. If a node does not have any agreement by the base station, it cannot interconnect with any other node in the network. The message confirmation and passing method is so effective for more time intense than any other method. Message authentication and passing method requires adjustment and reduction in time consumption and for cost efficiency.

VII. REFERENCES

[1]. Maheswari, P. Uma, and P. Ganesh Kumar. "Dynamic Detection and Prevention of Clone Attack in Wireless Sensor Networks." *Wireless Personal Communications*: 1-12.

[2]. Bonaci, Tamara, Phillip Lee, Linda Bushnell, and Radha Poovendran. "Distributed clone detection in wireless sensor networks: an optimization approach." In *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011 IEEE International Symposium on a*, pp. 1-6. IEEE, 2011.

[3]. Pulivarthi, Murali, Shafiulilah Shaik, and M. Lakshmi Bai. "Detection of Clone attacks in Wireless Sensor Networks

Using RED (Randomized, efficient, and distributed) Protocol."vol. 2,Issue 3, pp- 49-57 , March 2014.

[4]. Conti, Mauro, Roberto Di Pietro, Luigi Mancini, and Alessandro Mei. "Distributed detection of clone attacks in wireless sensor networks." *IEEE Transactions on Dependable and secure computing* 8, no. 5 (2011): 685-698.

[5]. Lisy, KM Mary, and Uma Rani. "Distributed Detection of Clone Attacks in Wireless Sensor Networks Using Detection Protocols." *Wireless Communication* 4, no. 10 (2012).

[6]. Li, Zhijun, and Guang Gong. "DHT-based detection of node clone in wireless sensor networks." In *International Conference on Ad Hoc Networks*, pp. 240-255. Springer Berlin Heidelberg, 2009.

[7]. David, G., and K. Srujana. "A Novel Approach of Node Clone Detection in Wireless Sensor Networks." International Journal of Science and Research,2012.

[8]. Mishra, Balmukund, and Yashwant Singh. "An approach toward the optimization of witness based node clone attack." In *2015 Third International Conference on Image Information Processing (ICIIP)*, pp. 506-510. IEEE, 2015.

[9]. George, Neenu, and T. K. Parani. "Detection of node clones in wireless sensor network using detection protocols." *arXiv preprint arXiv:1403.2548*(2014)..

[10]. Anthoniraj, J., and T. Abdul Razak. "Clone Attack Detection Protocols in Wireless Sensor Networks: A Survey." *International Journal of Computer Applications* 98, no. 5 (2014).

[11]. T.Bonact,P.Lee,L.Bushnell and R.Poovendra, "Distributed clone detection in wireless sensor networks: an optimization approach ",in Proceedings of the 2nd IEEE International Workshop on Data security and Privacy in Wireless Networks ,Lucca,Italy,June 2011.

[12]. Zhou, Yuping, Zhenjie Huang, Juan Wang, Rufeng Huang, and Dongmei Yu. "An energy-efficient random verification protocol for the detection of node clone attacks in wireless sensor networks." *EURASIP Journal on Wireless Communications and Networking* 2014, no. 1 (2014): 1-12.

[13]. Prabhudutta Mohanty, Sangram Panigrahi, Nityananda Sarma and Siddhartha Sankar Satapathy, "Security issues in wireless sensor network data gathering protocols: A Survey", Journal of Theoretical and Applied Information Technology, pp14-29, 2005-2010.

[14]. Bekara and M. Laurent- Maknavicius,"A New Protocol for securing Wireless Sensor Networks against nodes replication attacks"Third IEEE International Conference on Security and Privacy in communication networks,2008.

[15]. Udgata, Siba K., Alefiah Mubeen, and Samrat L. Sabat. "Wireless sensor network security model using zero knowledge protocol." In *2011 IEEE International Conference on Communications (ICC)*, pp. 1-5. IEEE, 2011.

[16]. Lisy, KM Mary, and Uma Rani. "Distributed Detection of Clone Attacks in Wireless Sensor Networks Using Detection Protocols." *Wireless Communication* 4, no. 10 (2012).