INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

DETECTION OF CLONE ATTACKS IN WIRELESS SENSOR NETWORKS: A SURVEY

Avneet Kaur[1], P. S. Mann[2]

Research Scholar in Computer Science and Engineering Department[1], er.avneetkaur14@gmail.com[1]

Faculty of IT Department[2], psmaan@hotmail.com[2]

Author Correspondence: DAV Institute of Engineering and Technology [1, 2], Jalandhar (Punjab), India,

8427799680[1] , 9888395367[2], er.avneetkaur14@gmail.com[1], psmaan@hotmail.com[2]

Abstract

Wireless Sensor networks (WSN) is a rising technology and have immense prospective to be employed insignificant situations like battlefields and commercial applications such as construction, traffic observation, habitation monitoring and many more circumstances. Wireless sensor networks (WSNs) deployed in such an environment in which sensor nodes are vulnerable to so many attacks like sinkhole, wormhole, selective forward, Sybil and clone attack, so security is a vital requirement for WSNs to maintain the integrity, validity, confidentiality and accessibility of data that is transmitted between the nodes in networks. In this paper, wide variety of attacks have been discussed and we concentrate on the most distinctive attack or threat known as node replication attack or clone node attack, where an enemy creates its own sensor nodes called clone nodes by physically capture one node's ID and cryptographic secrets. Detecting the node replication attack has turn into a crucial research topic in sensor network security. In this survey, we have deliberated the existing detection schemes for detection of clone attacks that comes under the centralized and distributed techniques.

Keywords: Wireless Sensor Networks, Security Requirements, Security Attacks, Clone Attack Detection Schemes.

1. Introduction

Wireless Sensor Network

An environment in which large number of sensor nodes is densely deployed and communicate wirelessly with each other over a limited frequency and bandwidth is known as Wireless Sensor Network. These sensor nodes sensed the data and forward it to the base station through multi-hop routing. In WSNs there are two other mechanisms, called "aggregation points" and "base stations", which have extra influential resources than normal sensors where aggregation points collect information from their nearby sensors, integrate them and then forward to the base stations to process gathered data, as shown in figure1 [1].

Generally, there are two kinds of applications for WSNs including, monitoring and tracking [2]; therefore, some of most common applications of these networks are: military, medical, environmental monitoring, industrial,

infrastructure protection, disaster detection and recovery, agriculture, intelligent buildings, law enforcement, transportation and space discovery as shown in figure2.

Limitations of Wireless Sensor Network such as limited storage memory, limited resources, cost and battery constrained which makes the network insecure and also their wireless nature makes them very attractive to attacker so security is a necessary requirement for these networks.

Organization: The remainder of this paper is organized as follows: Section 2 reviews Security and their principals. Section 3 describes various attacks in WSNs. Section 4 describes techniques for detection of clone attack in WSNs. Finally, the section 5, conclusion concludes the main text while references complete the article.

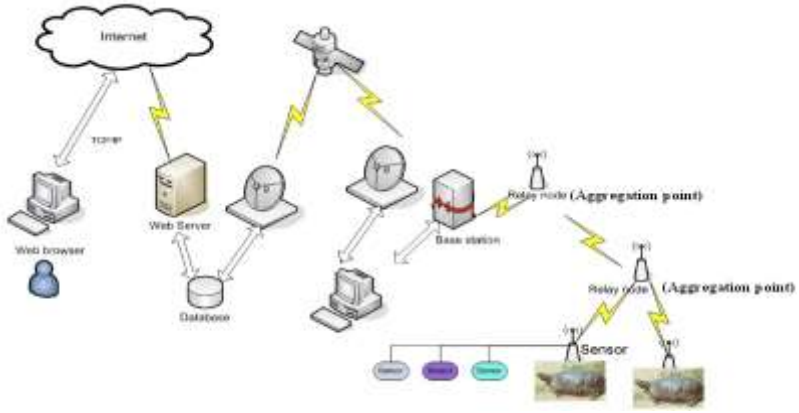

Figure 1: WSN's architecture [1]

2. Security

Security plays a vital role to defend against various types of attacks in wireless sensor networks. To protect the information and resources from attacks is the main goal of security services. The basic security requirements are:

- **Availability:** it ensures that services should be available by WSN whenever it is required.
- **Authorization:** it guarantees that only legal sensor can provide information to network.
- **Authentication:** it empowers a node to guarantee the identity of neighbor to which it is communicating.
- **Confidentiality:** it makes sure that only authorized sensor node is accessing the content of messages.
- **Integrity:** it measures that received data has not been modified by an adversary.
- **Freshness:** it makes sure that no old messages have been repeated.

3. Attack

Security attacks can be categorized into two broad classes [3]:

- Passive and
- Active attacks.

Passive attacks are against data confidentiality where an adversary gather and steal the information and active attacks are against both the data confidentiality and data integrity where an adversary introduces defective data into the networks.

3.1 *Security Attacks on WSN*

There are number of attacks in Wireless Sensor Networks. Let us explain it one by one as follows:-

- **Sinkhole Attack:** The main goal of an adversary in sinkhole attack is to attract all the traffic toward itself through an agreement node. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes. [4]

- **Wormhole Attack:** In wormhole attack, packets are recorded by an attacker at one location then attacker tunnels them into another location and again transmits them into the network. In figure 3, packets established by node X is replayed through node Y and vice-versa.

- **Selective Forward Attack:** In this attack an attacker comprise itself in a data stream lane and can selectively drop only distinct packets. In sensor networks it is assumed that nodes faithfully forward received messages but some compromised node might refuse to forward packets, though neighbors may start using another route.

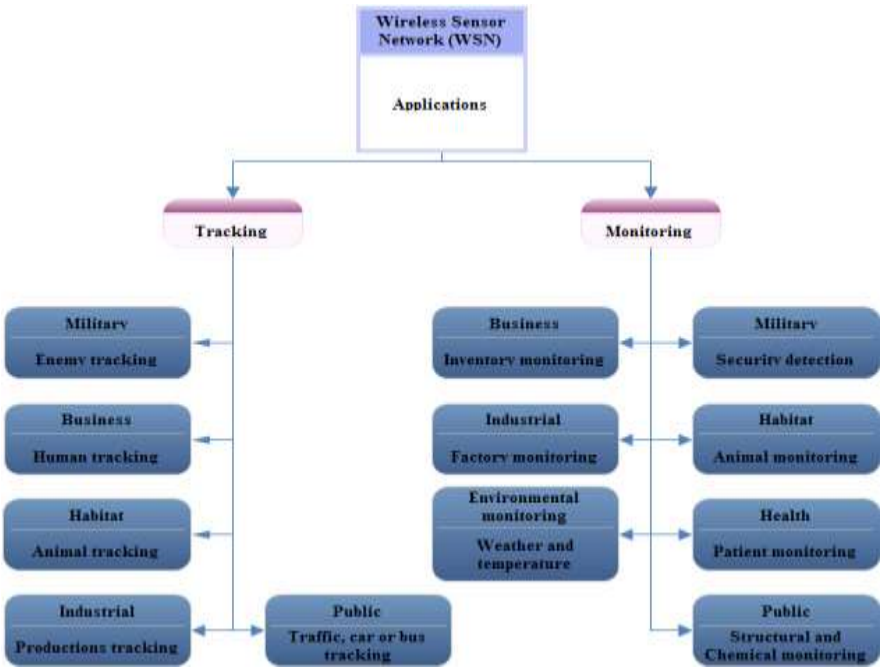

Figure 2: WSN's applications [1]

- **Sybil Attack:** In Sybil attack, a single node makes replicas of it and distributes it in multiple locations of the network. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network. [4]

- **HELLO FLOOD Attack:** In this type of attack an attacker with high energy and high radio transmission range broadcasts HELLO packets to a numerous nodes in the network and then these sensor nodes are influenced that adversary is their neighbor. Due to this an injured node ultimately deceived by an attacker.

- **Clone Attack:** In this attack an attacker capture a node and extract its cryptographic secrets and make copies of this node in the entire networks due to this an attacker can easily misroute the packets.

- **Denial of Service:** Denial of Service (DoS) is created by the accidental crash of nodes or wicked action. DoS attack is intended not only for the enemy's attempt to threaten, interrupt, or destroy a network, but also for any incident that diminishes a network's potential to distribute a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed, at physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion and unfairness, at network layer, neglect and greed, homing,

misdirection, black holes and at transport layer this attack could be performed by malicious flooding and de-synchronization.[4]

- **False Node:** In this attack an adversary add a spiteful node to the network which generates a false data in the network. This kind of attack is one of the dangerous attacks which can destroy whole of the network.
- **Message Corruption:** Any modification of the content of a message by an attacker compromises its integrity. [6]
- **Physical Attack:** Unlike other attacks, physical attacks obliterate sensors eternally.

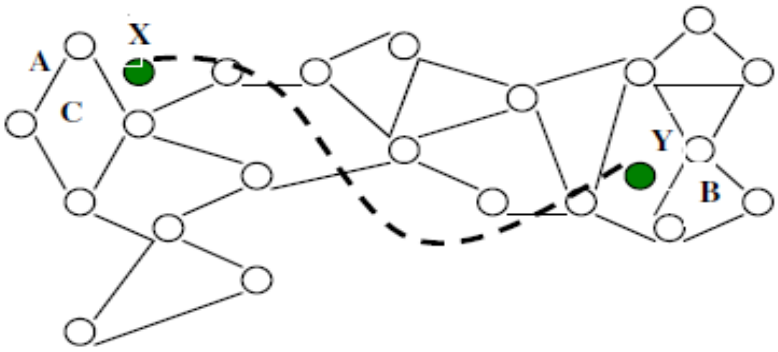

Figure 3: Wormhole attack [5]

4. Clone Attack Detection Schemes for WSNs:

Wireless Sensor Networks are vulnerable to above mentioned attacks and one of them most dreadful attack is clone attack and following are some previous schemes that helps to detect clone attacks in wireless sensor networks which are classified into centralized and distributed techniques. Let us explain it in brief:

4.1 Centralized Techniques:

In centralized techniques, every node in the network sends its location id and location info to the central powerful base station via its neighboring nodes. On receiving this information, if base station finds two different locations of same ID then it generates a clone node alarm. Various techniques come under this category are explained below:

4.1.1 On the Detection of Clones in Sensor Networks Using Random Key Pre distribution:

R. Brooks, P. Y. Govindaraju,M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir [7] have proposed a cloned key detection protocol and the basic idea behind that the keys engaged according to the random key pre distribution scheme must follow a certain configuration, and those keys whose norm exceeds a threshold can be arbitrated to be replicated. In the protocol, counting Bloom filters is used to assemble key usage numbers and each node attaches a random number to the Bloom filter and encodes the result by base station's public key then forwarded it to base station. Base station decodes the Bloom filters it collects and counts the numeral of time each key used in the network and if keys used beyond a threshold value are deliberated as cloned.

4.1.2 SET: Detecting Node Clones in Sensor Networks:

H. Choi, S. Zhu, and T. F. L. Porta [8] have proposed a clone detection approach in sensor networks called SET in which network is arbitrarily divided into limited subsets. Every subset has a subset leader and each subset is a node of the subtree. Members are placed one hop away from their subset leader and every subset leader gathers member

information and sends it to the root of the subtree. Each root performed an intersection operation and if intersection of all subsets of a subtree is empty then there are no clone nodes in this subtree and this report is forwarded to the base station (BS). The BS detects the clone nodes by calculating the intersection of any two received subtrees.

4.1.3 Real-Time Detection of Clone Attacks in Wireless Sensor Networks:

K.Xing, X. Cheng, F. Liu and D.H.C.Du [9] have proposed real-time detection of clone attacks in WSN in which each sensor calculates a fingerprint by integrating the neighborhood information through an overlaid s-disjunct code and stores the fingerprint of all neighbors. When the communication is start between nodes, one node sends its fingerprint along with message and neighbors will verify the fingerprint. If there is a clone node which is deployed in other place, it will send its own fingerprint which does not belong to the same community as other nodes, then this clone node will be detected because a clone node can have the same ID, keys but cannot have same community neighborhood.

4.1.4 Hierarchical Node Replication Attacks Detection in Wireless Sensor Networks:

W. Znaidi, M. Minier and S. Ubeda [10] have proposed a cluster head selection-based hierarchical distributed algorithm in which Bloom filter mechanism is used. This algorithm is based on local negotiated clustering algorithm (LNCA) protocol. This algorithm works in three steps. In the first step, an entirely material essential for Bloom filter calculations and for cryptographic procedures will be pre distributed in each sensor node. The second step accomplishes the cluster head voting. In the third step, Bloom filter creation is performed by all cluster head and Bloom filter authentication is performed by the other cluster heads. By following these three steps, node replication attacks can be determined.

4.1.5 CSI: Compressed Sensing-Based Clone Identification in Sensor Networks:

C. M. Yu, C. S. Lu and S. Y. Kuo [11] have proposed a centralized technique called compressed sensing-based clone identification (CSI). In CSI every node transmits a stable sensed data (α) to its one step neighbors then sensor nodes forward and combined the received statistics from successor nodes along the aggregation tree by means of compressed sensing-based data gathering techniques. Since Base station (BS) is the root of the aggregation tree will receives the aggregated result and improves the sensed data of the system. After reconstructing the result authors defines the node as a clone node whose sensory reading is greater than α.

4.1.6 Fast Detection of Replica Node Attack in Mobile Sensor Networks Using Sequential Analysis:

J.W. Ho, M. Wright and S. K. Das [12, 13] have proposed a mobile replica detection scheme based on the sequential probability ratio test (SPRT) which is based on the fact that an uncompromised mobile node should not ever move at speeds in addition of the system-configured maximum speed. On the other hand, replica nodes will seem to move considerably faster than original nodes, and thus their measured speeds will possible are above the system-configured maximum speed as they must be at two different locations at once. So, if it is over the system-configured maximum speed then it is extremely like that, at least two nodes with equal identity are present in the network. The SPRT is executed on every mobile node by a null hypothesis and if the existence of a speed that either lowers or beats the system-configured maximum speed will lead to approval of the null and alternate hypotheses, correspondingly. When the alternate hypothesis is established, the replica nodes will be repealed from the network.

4.1.7 *A New Protocol for the Detection of Node Replication Attacks in Mobile Wireless Sensor Networks*:

X. M. Deng and Y. Xiong [14] have proposed a new protocol to detect the replicas in mobile WSNs and have used the knowledge of polynomial based pair-wise key pre-distribution and Bloom Filters which assure that the replicas cannot ever lie around their actual identifiers and assemble the number of pair-wise keys recognized by every sensor node. Replicas are identified by observing at whether the number of pair-wise keys recognized by them beyond the threshold value. There are three phases in the protocol. In first phase that is node initialization, the key server arbitrarily generates a bivariate symmetric polynomial in a limited field before the deployment of nodes. After

deployment of nodes, in second phase pairwise keys are recognized. Every node periodically creates a report having its ID and counting Bloom filter and refers it to the base station. Then at last bloom filters will assemble the number of pairwise keys established by each node at base station. Nodes whose value of pair-wise keys exceeds the threshold value are considered to be the clones.

4.2 Distributed Techniques:

In distributed techniques a special mechanism is used called as claimer-reporter-witness in which the detection is accomplished by nearby distributed node which sends the location claim to a selected node called witness node not to the base station (sink). Various techniques come under this category are explained below:

4.2.1 A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks:

M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei have proposed a randomized, efficient, and distributed protocol called RED [15, 16] for the detection of node replication attack which consists two steps. In first step, an arbitrary value rand is shared among all the nodes over base station. The second step is detection phase in which each node transmits its ID and location to its neighboring nodes. Each neighbor node that perceives a claim send it to a set of g pseudo randomly selected network locations and every node in the pathway from claiming node to the witness node onwards the message to its neighbor nearest to the destination and thus replicated nodes will be discovered in every detection phase.

4.2.2 A Neighbor-Based Detection Scheme for Wireless Sensor Networks against Node Replication Attacks:

L. C. Ko, H. Y. Chen, and G. R. Lin [17] have proposed a real time neighbor-based detection scheme (NBDS) for node replication attack in wireless sensor networks. In this technique when a node moves to another community, it will transmit a rejoining claim to its new neighbors for joining the network then each neighbor verifies its authentication by checking its ID in the neighbor table. If its ID does not find in the table then it is taken as a clone node.

4.2.3 Distributed Detection of Node Capture Attacks in Wireless Sensor Networks:

J. W. Ho [18] has proposed a node capture detection scheme for wireless sensor networks in which captured nodes detected by using sequential analysis. They use the reality that from the captured time to the redeployment time the physically captured nodes are not present in the network. The captured nodes can be detected by using the sequential probability ratio test (SPRT) in which first of all absence time period of a sensor node is measured and then it compared with predefined threshold. If it is greater than threshold value, the sensor node is deliberated as a captured node.

4.2.4 Randomly Directed Exploration: An Efficient Node Clone Detection Protocol in Wireless Sensor Networks (RDE):

Z. Li and G. Gong [19] have presented a novel clone node detection protocol called randomly directed exploration. In this protocol each node has to know its neighbor nodes. When the detection phase starts, nodes issue claiming messages to randomly selected neighbors which consist of neighbor list with an extreme hop limit. The intermediate node tries to forward the message. During promoting messages, the intermediate nodes discover the claiming messages for node clone detection. As a simple technique, the proposed protocol can expertly detect clone nodes in the dense sensor networks by consuming minimum memory.

4.2.5 Random-Walk-Based Approach to Detect Clone Attacks in Wireless Sensor Networks:

Y. Zeng, J. Cao, S. Zhang, S. Guo and L. Xie [20] have proposed two protocols RAndom WaLk (RAWL) and Table-assisted RAndom WaLk (TRAWL) for the detection of clone attack in wireless sensor networks. In RAWL protocol, every node broadcast a location claim and each of node neighbor forwards the claim to some randomly selected nodes and these selected nodes sends message which consists of location claim. These selected nodes starts random walk and the passing nodes are considered as a witness node which stores the location claim. If this witness node find different location claims for same ID it will declared it as a clone node. RAWL has lowest overheads in witness selection and basically TRAWL protocol is used to reduce the memory overhead of RAWL by adding trace table at each node.

4.2.6 A Resilient and Efficient Replication Attack Detection Scheme for Wireless Sensor Networks:

C. Kim, S. Shin, C. Park and H. Yoon [21] have presented a deterministic method to detect node replication attack. This scheme works in three steps: initialization, witness node location phase, and node reversal phase. In initialization phase, a base station (BS) companions a specific locality coordinate referred as verification point (which is fixed by a network operator) with each node id using geographical hash function *F* before the deployment. In witness node location phase, the imitations with the identical id but different deployment localities are detected over location claim message. In the last phase of node reversal, base station BS overflows the reversal node lists after inspection the reversal request message established from the witness nodes. After BS obtains this revocation request message, it examines whether the reversal request message is appropriately encrypted by witness node via a pair-wise key common. If the key is correct, a BS overflows a list of replica nodes together with reporter node over the network. If the key fails, the BS reputes that reporter node has been compromised.

4.2.7 *Single-Hop Detection of Node Clone Attacks in Mobile Wireless Sensor Networks*:

Y. Lou, Y. Zhang and S. Liu [22] have proposed a node clone attack detection protocol, namely, the single hop detection (SHP) for mobile wireless sensor networks which feats the point that at any time, a physical node cannot act at different neighborhood community, else, there must be duplications in the network. This protocol involves two phases, the fingerprint claim and the fingerprint verification phases. In the fingerprint claim phase every node is mandatory to sign its neighbor node list. The signed neighbor node list is referred to as fingerprint claim which is a fingerprint of its current neighborhood community. The fingerprint claim is disseminated in one-hop neighborhood. After reception of a fingerprint claim the receiver node will choose whether to become a witness node of the claim node if it became a witness node, the node will verify the fingerprint claim. In the fingerprint verification phase, after two nodes encounter with each other, they interchange their witnessed node lists, if there is a conflict with received claims it implies replicas of one node is placed in a network.

4.2.8 *Mobility-Assisted Detection of the Replication in Mobile Wireless Sensor Networks:*

X. Deng, Y. Xiong and D. Chen [23] have proposed two schemes called unary time location storage and exchange (UTLSE), and multitime location storage and diffusion (MTLSD) for the detection of node replication attack in mobile wireless sensor networks. In these protocols the fact is used, when getting the time-location claims, witnesses bring these claims everywhere in the network rather than transmitting them. It will be promoted only when applicable witnesses meet with each other. After meet with each other they exchange their time location claim. UTLSE discovers the imitations by each of the two met witnesses which stores only one time-location claim. On the other side, MTLSD stores additional time-location claims for every traced node and announces time-location claims dispersion among witnesses. MTLSD protocol is better than UTLSE because MTLSD has higher detection probability than the probability of protocol UTLSE.

5. Conclusion

Wireless Sensor Networks are used in many applications like military, health and commercial applications but due to some limitations in WSNs like minimal energy and storage and due to deployment of sensor nodes in unattended environment makes very attractive to attacker so it is necessary to secure the network from attacks. This paper summarizes the classification of attacks and their explanation how these attacks arise in the network. In this paper there is a survey on various detection centralized and distributed schemes for detecting the clone attack and this

paper will confidently prompt future researchers to come up with more security mechanisms for detection of clone attack and make their system safer.

REFERENCES

[1] Dr. Shahriar Mohammadi and Hossein Jadidoleslamy, 2011, A Comparison of Link Layer Attacks on Wireless Sensor Networks, *International Journal on Applications of Graph Theory in Wireless Ad hoc Networks & Sensor* Networks, vol. 3.

[2] Jennifer Yick, Biswanath Mukherjee and Dipak Ghosal, 2008, Wireless sensor network survey, *Computer networks*, vol. 52, pp. 2292-2330.

[3] Asmae Blilat, Anas Bouayad, Nour El Houda Chaoui and M. E. Ghazi, 2012, Wireless sensor network: Security challenges, ,*Network Security and Systems, 2012 National Days of IEEE*, pp. 68-72.

[4] Chris Karlof and David Wagner, 2003, Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, *AdHoc Networks (elsevier)*, vol. 1, pp. 293-315.

[5] Mani Arora, Rama Krishna Challa and Divya Bansal, 2010, Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks, *Computer and Network Technology, 2010 Second International Conference on IEEE*, pp. 102-104.

[6] Zia Tanveer and Albert Zomaya A, 2006, Security Issues in Wireless Sensor Networks, *Systems and Networks Communications, ICSNC'06 International Conference on IEEE*, pp. 40-40.
[7] R. Brooks, P. Y. Govindaraju,M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, 2007, On the detection of clones in sensor networks using random key predistribution, *IEEE Transactions on Systems, Man and Cybernetics C*, vol. 37, pp. 1246–1258.

[8] H. Choi, S. Zhu and T. F. L. Porta, 2007, SET: detecting node clones in sensor networks, I*n Proceedings of the 3rd International Conference on Security and Privacy in Communication Networks*, pp. 341–350.

[9] K.Xing, X. Cheng, F. Liu and D.H.C.Du, 2008, Real-time detection of clone attacks in wireless sensor networks, *In Proceedings of the 28th International Conference on Distributed Computing Systems*, pp. 3–10.

[10] W. Znaidi, M. Minier and S. Ubeda, 2009, Hierarchical node replication attacks detection in wireless sensors networks," *In Proceedings of the 20th IEEE Personal, Indoor and Mobile Radio Communications Symposium*, pp. 82–86.

[11] C. M. Yu, C. S. Lu and S. Y. Kuo, 2012, CSI: compressed sensing based clone identification in sensor networks, *In Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops*, pp. 290–295.

[12] J.W. Ho, M. Wright and S. K. Das, 2011, Fast detection of mobile replica node attacks in wireless sensor networks using sequential hypothesis testing, *IEEE Transactions on Mobile Computing*, vol. 10, pp. 767–782.

[13] J.W. Ho, M. Wright and S. K. Das, 2009, Fast detection of replica node attacks in mobile sensor networks using sequential analysis, *In Proceedings of the IEEE INFOCOM*, pp. 1773–1781.

[14] X. M. Deng and Y. Xiong, 2011, A new protocol for the detection of node replication attacks in mobile wireless sensor networks, *Journal of Computer Science and Technology*, vol. 26, pp. 732–743.

[15] M. Conti, R. Di Pietro, L. V. Mancini and A. Mei, 2007, A randomized, efficient and distributed protocol for the detection of node replication attacks in wireless sensor networks, *In Proceedings of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 80–89.

[16] M. Conti, R. Di Pietro, L. Mancini and A. Mei, 2011, Distributed detection of clone attacks in wireless sensor networks, *IEEE Transactions on Dependable and Secure Computing*, vol. 8, pp. 685–698.

[17] L. C. Ko, H. Y. Chen and G. R. Lin, 2009, A neighbor-based detection scheme for wireless sensor networks against node replication attacks, *In Proceedings of the International Conference on Ultra-Modern Telecommunications and Workshops*, pp. 1–6.

[18] J. W. Ho, 2010, Distributed detection of node capture attacks in wireless sensor networks, *In Smart Wireless Sensor Networks*, pp. 345–360.

[19] Z. Li and G. Gong, 2009, Randomly directed exploration: an efficient node clone detection protocol in wireless sensor networks, *In Proceedings of the 6th IEEE International Conference on Mobile Adhoc and Sensor Systems*, pp. 1030–1035.

[20] Y. Zeng, J. Cao, S. Zhang, S. Guo and L. Xie, 2010, Random walk based approach to detect clone attacks in wireless sensor networks, *IEEE Journal on Selected Areas in Communications*, vol. 28, pp. 677–691.

[21] C. Kim, S. Shin, C. Park and H. Yoon, 2009, A resilient and efficient replication attack detection scheme for wireless sensor networks, *IEICE Transactions on Information and Systems*, vol. 92, pp. 1479–1483.

[22] Y. Lou, Y. Zhang and S. Liu, 2012, Single hop detection of node clone attacks in mobile wireless sensor networks, *In Proceedings of the International Workshop on Information and Electronics Engineering*, pp. 2798-2803.

[23] X. Deng, Y. Xiong and D. Chen, 2010, Mobility-assisted detection of the replication attacks in mobile wireless sensor networks, *In Proceedings of the 6th Annual IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, pp. 225–232.

A Brief Author Biography

Avneet Kaur received the B.Tech degree in Computer Science and Engineering from the Punjab Technical University, Jalandhar in 2012. She is working toward the M.Tech degree in Department of Computer Science and Engineering at DAV Institute of Engineering & Technology under Punjab Technical University, Jalandhar. Her research interests include wireless sensor networks, security and computer networks.

P.S.Mann is currently working as Assistant Professor at DAV Institute of Engineering & Technology, Jalandhar. He is B.Tech with Hons, M.Tech and have experience of 8 years in teaching. His research interest includes Computer Networks, Wireless Communication, and Cloud Computing. He has published more than 25 papers in International Journals, 01 in National Journals, 01 in International Conferences and 07 in National Conferences. He is Life Member of Punjab Academy of Sciences and Computer Society of India.