ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2021.0354

NODE BASED CLONE ATTACK DETECTION IN STATIC WIRELESS SENSOR NETWORKS

J. Anthoniraj
Department of Computer Science, M.I.E.T Arts and Science College, India

Abstract

Wireless Sensor Network (WSN) is a combination of autonomous sensor nodes and used to monitor various physical conditions. Static and mobile are two types of WSN. In static WSN the sensor nodes do not alter their positions after deployment. Due to the security constraints, WSN is vulnerable to various types of attacks. In that, Clone attack is the most dangerous attack on WSN. In Clone attack an adversary physically captures a sensor node. It reprograms the detained node and generates many clone nodes. The real nodes and clone nodes are installed in the sensor field, so clone node identification is a difficult task. The new protocol proposed to identify the clone nodes in the static WSN called as Node Based Clone Attack Detection (NBCAD) protocol. This protocol detects the clones in a efficient manner compare with SET and RED protocols. The advantage of proposed NBCAD protocol include high clone detection ratio, minimum communication overhead, minimum end-to-end delay, minimum latency time and high throughput.

Keywords:

Clone Attack, Adversary, Node deployment, Zigbee, Elliptic Curve Cryptography, Cluster, Clone detection

1. INTRODUCTION

Wireless Sensor Network is a mixture of independent sensor nodes. These nodes are connected together in order to observe physical or ecological conditions. The sensor node of the network can operate independently and it has four basic components i) Sensing unit; ii) Processing unit; iii) Transmission unit; iv) Power unit so on. Sensing unit contains sensors and ADC. Processing unit has a CPU and small amount of memory. Transmission unit is used for radio transmission between the sensor nodes. Power unit is made up of batteries [1]. Position finding system helps the sensor node to find its location in the sensor field. The Base station is the central node of the sensor network. It monitors all the sensor nodes in the sensor network and communicates with them via radio link [2]. The major applications of sensor network are 1) Wild life monitoring: Sensor nodes are deployed in the dense forest in order to monitor the movement of the animals. 2) Medical applications: Sensor nodes are implanted in the human body used to monitor the blood pressure, sugar value and heart functioning of the patients.3) Traffic control: WSN is established in the road side and monitor the traffic of the vehicles. 4) Agricultural Applications: WSN can be established in the agricultural field in order to monitor soil moisture level, water irrigation to the plants, and influence of pest on plant growth. 5) Military applications: WSN can be used to track and coordinate the military troops and vehicles. Sensor nodes are densely deployed in the unsecure and unattended environment such as battle field and dense forest [3], [4].

The various security constraints of wireless sensor network are 1) Lack of hardware support: Sensor network has very low hardware configuration and lack of support for tamper resistance. 2) Low computation capability: Each sensor node has the CPU with 8MHz processing speed and 4kB RAM. 3) Insufficient power resources: Battery is the main power resource of sensor nodes. 4) Make use of insecure wireless communication channels: Sensor network uses wireless communication channels for its transmission and packets may be damaged due to channel errors. Due to the security constraints, WSN is vulnerable to the various types of attacks. WSN attacks are 1) Physical Layer attacks: Tampering, Jamming. 2) Data Layer attacks: Collision, Exhausting 3) Network Layer attacks: Wormhole attack, Sinkhole attack4) Transport Layer attacks: Flooding, De-synchronization 5) Application Layer attacks: False-Data injection, over whelmed attack 6) Layer Independent attacks: Sybil attack, Clone attack so on [5].

In clone attack the attacker detains a sensor node and reprograms the captured node. It creates a clone node from the detained node. After that clone node is deployed in the sensor field. Clone attack is a dangerous one and very much difficult to identify the clones if they are deployed along with original nodes. In this paper, we propose a new protocol called as Node Based Clone Detection to find the clone nodes in the static wireless sensor network. So many existing protocols are available to detect the clone nodes in the static wireless sensor network, they are discussed in the Section 2.

2. RELATED WORK

Cho et al. [6] proposed a new centralized protocol called as SET. In this protocol, sensor network is randomly into groups. Each group leader collects the data from its members. After that group leader send it to the sub tree's root. The clone node can be identified by performing intersection operation on each sub tree's root.

A fingerprint based clone detection protocol was proposed by Xing et al. [7]. Before deployment each sensor node is loaded with code word. The node collects code words of its neighbor nodes. Then it computes the finger print from the code words of neighbor nodes. The node stores the Finger-Print in its memory. The Finger-Print attached with all messages which are forwarded to the Base Station.

Par et al [8] proposed a Broadcast protocol to detect the clone nodes in distributed sensor network. All the sensor nodes broadcast the position details to the neighbor nodes of sensor network. The sensor node stores position details of its neighbor nodes. If the node receives a conflicting claim for a particular node, it is identified as clone node.

Par et al. [8] suggested a technique for clone detection in static sensor networks called as Randomized Multicast. In this protocol location claim is broadcasted by node in the network. The neighbor nodes receive the location claim and forward the claim to witness nodes which are randomly selected randomly. The sensor node has two different location claims, it is identified as a clone node.

The Line Selected Multicast is a one of the clone detection protocol that is presented by Par et al. [8]. The location claim travels from sender to receiver, on the way its pass through several in between nodes that will create a claim message path. Conti et al [9] creates a new protocol called as Randomized Efficient and Distributed (RED) protocol. In this protocol the random value send by Base station to all the nodes. The location claim of the sensor node is broadcast to the nearby nodes. The location claim received by the neighbor nodes and forwards the claim to the witness nodes which are selected pseudo randomly. The clone node can be identified with the variance in the location claim.

A distributed clone detection scheme was proposed by Zna et al. [10] called as hierarchical Distributed Algorithm (HDA). The sensed data of the nodes can be forwarded to the Cluster Head of the cluster. After receiving the data, Cluster Head combined all the received information. After that Cluster Head forwarded them to the Base station. All the cluster heads in the network are connected with other cluster heads through a dedicated path. This form a tree structure and base station is the root of the tree. The cluster heads computes bloom filter to find the clone nodes.

Single Deterministic Cell is one of the localized protocol which is presented by Zhu et al. [11]. In this protocol the sensor node of the sensor network transmit its location claim to its neighbor nodes. The neighbor node checks the signature in the location claim. After verification over, it onwards the location claim of the node to the destination cell. Then the location claim of the node is transmitted to all the sensor nodes of the destination cell.

Memory Efficient Multicast using Bloom filters is one of the most important multicast protocol for static wireless sensor network which is proposed by Zha et al. [12]. In this protocol, starting of the detection period, sensor node transmits its location claim to the one hop neighbor nodes. The neighbor node receives the location claim and verifies its signature. If the location claim is validated, the neighbor node selects a destination node and transmits the location claim of the sensor node towards the destination node.

Zen et al [13] has proposed a clone detection protocol called as Random Walk (RAWL). In this protocol, the signed location claim broadcast by each and every node. The neighbor of the node receives the location claim and forwards the claim to some nodes which are selected randomly. The selected nodes send the claim to start walk in the network. Ho [14] proposed a new approach called as Node captured Attack Detection. In this approach, sensor node's absence time period is calculated and compared with predefined threshold value. If the absence time is larger than threshold value, the node is considered as a captured node.

3. PROTOCOL FRAMEWORK

3.1 SENSOR NODE HARDWARE

In this work, MicaZ sensor node is used for protocol implementation. The hardware configuration of MicaZ sensor node is given in the Table.1. The standard 51-pin expansion connector can be used to connect the MicaZ with all the boards.

Table.1. Hardware configuration of MicaZ

Parameter	Description
Sensor Node	MICA z mote
Company	Berkley
Processor	ATmega128L
Processor Speed	8 MHZ
RAM size	4KB
Battery	2 X AA (3v)
Battery Capacity	2000 mAh
Radio transceiver	TICC40
Data Transmit Rate	250kbps

3.1 ZIGBEE TECHNOLOGY

There are so many IEEE wireless communication standards are available. Wireless Local Area Networks (Wi-Fi) use IEEE 802.11 standard for its communication. Wireless Personal Area Networks (WPAN) connects various devices within minimum distance and uses IEEE 802.15 standard for its communication. In that IEEE 802.15.1 standard can be used for Bluetooth technology and IEEE 802.15.4 standard can be used for Zigbee technology. It is suitable technology to connect large number of sensor nodes in to one network [15]-[18]. In this work, IEEE 802.15.4 LR-PAN Zigbee technology is used for protocol implementation. Zigbee parameters are listed in Table.2.

Table.2. Zigbee Parameters

Parameters	Description
Frequency	2.4 GHz
Coverage Area	10-100 m
Data transfer rate	20-250 kbps
Data Packet Size	512 B
Max.No.of Nodes	65,536
No.of channels	16-27
Power Consumption	25- 35mA
Communication Link	Bi-directional

3.2 NETWORK ARCHITECTURE

In this work, cluster based hierarchical architecture is used as network architecture for protocol implementation. In hierarchical architecture, Group of sensor nodes form a cluster, each cluster has a cluster head and set of sensor nodes. It is shown in the Fig.1.

The sensor nodes transfer information with its neighbor nodes and cluster head. Each node collects physical or environmental information and forwards to the cluster head. The sensor node in the network has very minimum memory size, data processing capacity and covers very short radio transmission range. The Cluster Head receives the data from the sensor node and reduce the size of the data. After that Cluster Head transmits the data to the base station [19].

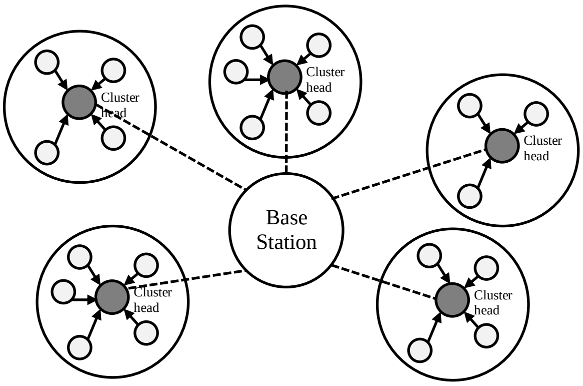

Fig.1. Hierarchical Architecture of Sensor Network

3.3 NETWORK MODEL

In the Wireless Sensor Network, all the nodes are installed in the unfocused and unprotected environment. In this work, sensor nodes are deployed in the sensor field using uniform random deployment method. GPS (Global Positioning System) is a very useful technique in order to identify the position of the sensor node in the sensor field [20]. This work uses static wireless sensor network, so that sensor nodes do not change their position after deployment. Parameters of network model are described in the Table.3.

Table.3. Network Model Parameters

Parameters	Description
Network Type	Static/ Mobile
Communication Range	50m
Deployment Type	Uniformly Random
Routing Protocol	GPSR protocol
Data packet size	512 B
Communication Standard	IEEE 802.15.4 LR-WPAN Zigbee
Channel Bandwidth	20kpbs
Raw Data Rate	868 MHZ : 20 Kbps
Transmission channels	868/915 MHZ : 12 Channels 2.4GHZ : 16 Channels
Location Identification	Global Positioning System
Communication Link	Bi directional
Key management	Diffee Helman Algorithm
Encryption Algorithm	Elliptic Curve Cryptography

4. NODE BASED CLONE ATTACK DETECTION

The proposed system Node Based Clone Attack Detection (NBCAD) protocol is used to identify the clone nodes deployed in the static wireless sensor networks. Important features of proposed mechanism are:

- Detect the clone nodes within a short period to avoid the damage,
- Improve the clone detection ratio and throughput value,
- Minimize the average memory consumption per node,
- Minimize communication overhead and latency time,
- Improve the average number of packets transmitted or received per node,
- Minimize the end-to-end delay during the transmitting or receiving packets

4.1 PUBLIC KEY MANAGEMENT

The cluster head collects all the Node ID and Location of the nodes in the Cluster and stores it in the memory. In the same way, the base station collects node ID and location of the Cluster Heads and stores in its memory. The Base station first send the Public key to all its Cluster Heads after that it send the private key to the Cluster Heads. The Public and Private keys are distributed by the Base Station to all the sensor nodes in the network. The public key of the corresponding cluster head is also stored in its member nodes.

4.2 CLUSTER HEAD AUTHENTICATION

The cluster head broadcasts the authentication message to all its member nodes. This message is encrypted using the private key of the cluster head. Each node in the cluster decrypts the message using the public key of the cluster head and authenticates the received message

4.3 NEIGHBOR NODE DISCOVERY

The sensor nodes in the sensor network identify the neighbor nodes with help of some operation. Each sensor node can communicate with the nearby nodes which are in its communication range. The neighbor node discovery is performed by transmitting the hello message. The neighbor nodes in the communication range receive the message and responds to the message.

4.4 SESSION KEY ESTABLISHMENT

Each node creates a session key establishment with the nearby sensor nodes. When the node receives the confirmation message for public key distribution, it sends the session key to that neighbor node. In the same way it distributes the session keys to the neighbor nodes.

4.5 SEEKING ADMISSION

In order to communicate with the cluster head, all the nodes in the cluster must get admission with the cluster head. In the same way, in order to communicate with the base station, the entire cluster heads must get admission with the base station.

4.6 COLLECTING LOCATION CLAIMS OF THE SENSOR NODES

Each node sends the location information request to its neighbor nodes. The neighbor nodes verify the request for sender node’s authentication. The neighbor nodes forward the location information to the requested node. The requested node receives the location information (node Id and location claim) and stores in the neighbor table. Each node maintained the neighbor table.

4.7 CLONE NODE VERIFICATION

The cluster head has the node ID and the Location claim of all the nodes in its cluster. The node sends its entire neighbor node list to the Cluster head for verification. The cluster head verifies the node ID and its Location claim with the already existing information. If any node has correct node ID but different Location claim for a particular node means, it is identified as a clone node. The node receives the clone node list from the cluster head and removes all the clone nodes from the neighbor table.

4.8 CLONE NODE DETECTION USING FINGER PRINT

The node sends all its neighbor list to the Cluster head, verifies the nodes and gives the clone node list to node. According to that, node removes all the clone nodes and prepares a new neighbor node list. With the help of the new neighbor node list, the finger print of the node is computed with the Boolean sum of the neighbor node IDs. If the node sends any content to the cluster head, it should attach the finger print with the message.

The cluster already computes the finger print of all the nodes, with help of the updated neighbor node list of that node. When the node sends any message to cluster heads, it first decrypts the message and verifies the signature. Now compares the finger print given in the message with existing finger print of the node. If both are same, the content of the node is accepted. If the finger print given by the node is not match with the existing finger print, then the node is identified as the clone node.

5. SIMULATION RESULTS AND PERFORMANCE EVALUATION

In the static WSN, the sensor nodes cannot alter their positions after deployment**.** NBCAD (Node Based Clone Attack Detection) protocol is proposed to identify clone attack in Static Wireless Sensor Network. This protocol is implemented and tested by using Castalia 3.2 simulator that runs on the OmNet++ platform.

In this implementation 10,000 sensor nodes are deployed in the geographical area of 1000×1000 m^2. This protocol is compared with existing static clone attack detection protocols SET and RED for the following evaluation factors.

5.1 NUMBER OF CLONES DETECTED

Once the adversary deploys the clone nodes in the sensor field, it will do all the damage to the network within a minimum time period. But it is very difficult to detect the clone nodes in the network, when large number of sensor nodes that are located in unsecure environment. The clone nodes must be detected immediately after the deployment. The Efficient protocol must detect more number of clones at a time.

NBCAD protocol detects more number of clones compare with SET and RED protocols. As shown in the Table.4, if 2000 sensor nodes are deployed in the sensor field, in that, the SET protocol detects 42 clones, the RED protocol detects 47 clones and the proposed NBCAD protocol detects 50 clones.

Table.4. Number of clones detected

Nodes	SET	RED	NBCAD
1000	43	47	48
2000	42	47	50
3000	40	49	48
4000	41	47	48
5000	41	48	48
6000	40	46	50
7000	42	46	49
8000	42	46	49
9000	43	49	50
10000	42	46	48

5.2 CLONE DETECTION RATIO

The clone detection ratio refers total number of clone nodes correctly found among the total number of existing clone nodes. Clone detection ratio of SET, RED and NBCAD protocols are compared, and that is shown in the Table.5. For 2000 nodes SET protocol provides 84% clone detection ratio, RED protocol provides 94% detection ratio but the NBCAD protocol provides 100% detection ratio. For 6000 nodes SET protocol provides 80% clone detection ratio, RED protocol provides 92% detection ratio but the NBCAD protocol provides 100% detection ratio. The NBCAD protocol provides highest clone detection ratio than other existing detection protocols.

Table.5. Clone detection Ratio

Nodes	SET	RED	NBCAD
1000	86	94	96
2000	84	94	100
3000	80	98	96
4000	82	94	96
5000	82	96	96
6000	80	92	100
7000	84	92	98
8000	84	92	98
9000	86	98	100
10000	84	92	96

5.3 MEMORY OVERHEAD

In WSN, sensor node has very small amount of memory for storing the code. The comparison of the existing SET, RED protocols with the proposed NBCAD protocol for memory consumption are described in the Table.6.

Table.6. Memory overhead

Nodes	SET	RED	NBCAD
1000	3359	3552	3167
2000	3401	3580	3153
3000	3404	3562	3176

4000	3421	3650	3206
5000	3451	3618	3241
6000	3523	3671	3304
7000	3509	3744	3327
8000	3561	3729	3317
9000	3565	3777	3368
10000	3603	3840	3393

Each and every security algorithm must have particular code size that should be reduced to make a well-organized security method in the sensor network. The number of location claims stored in a sensor node at a particular period is called as memory overhead. The proposed NBCAD protocol uses very minimum memory space than SET and RED protocols.

5.4 COMMUNICATION OVERHEAD

The sensor nodes send and receive the location claims between the nodes of the network. This process is called as communication overhead. The comparison of SET, RED and NBCAD protocols for communication overhead are given in the Table.7 and Fig.5.

Table.7. Communication overhead

Nodes	SET	RED	NBCAD
1000	23	26	23
2000	32	29	22
3000	28	25	26
4000	31	25	22
5000	32	27	26
6000	24	26	26
7000	27	32	20
8000	27	25	20
9000	30	30	22
10000	26	23	27

In this, for 2000 nodes, the SET protocol has thirty two seconds of communication overhead, the RED has twenty nine seconds of communication overhead and the NBCAD protocol has twenty two seconds of communication overhead.

For 4000 nodes, the SET protocol has thirty one seconds of communication overhead, the RED has twenty five seconds of communication overhead and the NBCAD protocol has twenty two seconds of communication overhead.

For 8000 sensor nodes, the SET protocol has 27 Seconds of communication overhead, the RED protocol has 25 Seconds of communication overhead and the proposed NBCAD protocol has 20 Seconds of communication overhead. Compared with the SET and RED protocols, the NBCAD protocol has a very minimum communication overhead.

5.5 END-TO-END DELAY

The total time need for the packet to travel from source to destination is called end-to-end delay. The comparison study of the existing SET and RED protocols with the proposed NBCAD protocol for end-to-end delay are shown in the Table.8.

Table.8. End-to-end delay

Nodes	SET	RED	NBCAD
1000	345	260	233
2000	354	269	227
3000	382	278	233
4000	347	255	239
5000	339	262	234
6000	378	241	228
7000	367	269	227
8000	351	261	257
9000	348	261	268
10000	359	255	261

$$\text{End-to-end delay} = \text{Transmission delay} + \text{Propagation delay} + \text{Processing delay} + \text{Queuing delay}$$

where,

Transmission delay = Amount of time required to transmit the packets through communication link

Propagation delay = Amount of time that takes for the head of the signal to travel from the sender to receiver

Processing delay = It is the time taken by the routers to process the packet

Queuing delay = It is the time a packet waits in a queue until it can be executed

For the deployed 1000 nodes, the SET protocol has 345 mS of end-to-end delay, the RED protocol has 260 mS of end-to-end delay and the proposed NBCAD protocol has 233mS of end-to-end delay. Compared with the SET and RED protocols, the NBCAD protocol has a very minimum end-to-end delay for the deployed sensor nodes.

5.6 LATENCY

The total amount of time taken for a packet to travel from a source to the destination of the wireless sensor network is called latency. When latency time increases, the performance of the network also increases automatically.

$$\text{Latency} = d / s$$

where, d - distance and s - speed of the medium

The comparison between SET, RED and NBCAD protocols for the network latency time is described in the Table.9. For 10000 nodes, the SET protocol has the latency time of 122ms, the RED protocol has the latency time of 112ms and the NBCAD protocol has the latency time of 86ms. Compared with SET and RED protocols the proposed NBCAD protocol has a very low latency time

Table.9. Latency

Nodes	SET	RED	NBCAD
1000	136	107	97
2000	126	96	98

3000	133	92	96
4000	124	94	93
5000	133	112	87
6000	141	98	83
7000	136	110	84
8000	138	112	82
9000	130	108	99
10000	122	112	86

5.7 THROUGHPUT

Total number of messages delivered per unit time is called throughput. It is defined as total file size transmitted in a given range. The throughput of the existing SET and RED protocols compared with proposed NBCAD protocol are described in the Table.10.

Table.10. Throughput

Nodes	SET	RED	NBCAD
1000	56897	68790	72473
2000	56306	68399	72822
3000	56610	68681	72538
4000	56495	68121	73465
5000	57087	68537	73137
6000	56168	68764	73296
7000	57118	68883	72812
8000	56311	68647	72981
9000	56928	69148	72678
10000	57025	68726	72669

$$\text{Throughput} = FS / TR$$

where, FS - File Size and *TR* - Transmission Range

For 10000 nodes, the SET protocol provides the throughput of 57025 bps, the RED protocol provides 68726 bps and the proposed NBCAD protocol provides the throughput of 72669 bps. As per the result the proposed NBCAD protocol provides the highest throughput than SET and RED protocols.

6. CONCLUSION

In this paper, the study proposed Node Based Clone Attack Detection protocol to find the clone nodes in the wireless static sensor networks. This protocol outperforms the existing SET, RED static clone detection protocols in following aspects. i) Detect the clone nodes within a short period to avoid the damage, ii) Improve the clone detection ratio and throughput value, iii) Minimize the average memory consumption per node, iv) Minimize communication overhead and latency time, v) Improve the average number of packets transmitted or received per node, vi) Minimize the End-to-End delay time when sensor nodes transmitting or receiving packets.

REFERENCES

[1] F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, “A Survey on Sensor Networks”, *IEEE Communications Magazine*, Vol. 40, No. 8, pp. 102-114, 2002

[2] G. Padmavathi and D. Shanmugapriya, “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks”, *International Journal of ComputerScience and Information Security*, Vol. 4, No. 1-2, pp. 115-119, 2009.

[3] A. Daniel and K.M. Balamurugan, “A Novel Approach to Minimize Classifier Computational Overheads in Big Data using Neural Networks”, *Physical Communication*, Vol. 42, pp. 1-23, 2020.

[4] H. Karl, A. Willig, “Protocols and Architectures for Wireless Sensor Networks”, John Wiley and Sons, 2005.

[5] M. Umar, D. Babu and P. Singh, “Automation of Energy Conservation for Nodes in Wireless Sensor Networks”, *International Journal of Future Generation Communication and Networking*, Vol. 13, No. 3, pp. 1-12, 2020.

[6] H. Choy, S. Zhu and T.F.L. Porta, “SET: Detecting Node clones in Sensor Networks”, *Proceedings of International Conference on Security and Privacy in communication Networks*, pp. 341-350, 2007.

[7] K. Xing, F. Liu, X. Cheng and D.H.C. Du, “Real-Time Detection of Clone Attacks in Wireless Sensor Networks”, *Proceedings of International Conference on Distributed Computing Systems*, pp. 3-10, 2008.

[8] B. Parno, A. Perrig and V. Gligor, “Distributed Detection of Node Replication Attacks in Sensor Networks”, *Proceedings of IEEE Symposium on Security and Privacy*, pp. 49-63, 2005

[9] M. Conti, R. Di Pietro, L.V. Mancini and A. Mei, “A Randomized and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks”, *Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 80-89, 2007.

[10] W. Znaidi, M. Minier, S. Ubeda, “Hierarchical Node Replication Attacks Detection in Wireless Sensors Networks”, *Proceedings of IEEE International Symposium Personal, Indoor and Mobile Radio Communications*, pp. 82-86, 2009.

[11] Bio Zhu, Venkata Gopala Krishna Addada, Sanjeev Setia, Sushil Jajodia and Sankaradas Roy, “Efficient Distributed Detection of Node Replication Attacks in Sensor Networks”, *Proceedings of IEEE International Conference on Annual Computer Security Applications*, pp. 257- 266, 2007.

[12] M. Zhang, V. Khanapure, S. Chen and X. Xiao, “Memory Efficient Protocols for Detecting Node Replication Attacks in Wireless Sensor Network”, *Proceedings of IEEE International Conference on Network Protocols*, pp. 284-293, 2009.

[13] Y. Zeng, J. Cao, S. Zhang, S. Gao and L. Xie, “Random Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks”, *IEEE Journal on Selected Areas in Communications*, Vol. 28, No. 5, pp. 677-689, 2010.

[14] J.W. Ho, “Distributed Detection of Node Capture Attack in Wireless Sensor Networks”, *Proceedings of IEEE International Conference on Smart Wireless Sensor Networks*, pp. 345-360, 2010.

[15] K. Gill, S.H. Yang, F. Yao and X. Lu, "A Zig Bee-Based Home Automation System", *IEEE Transactions on Consumer Electronics*, Vol. 55, No. 2, pp. 1-13, 2009.

[16] B. Mihajlov and M. Bogdanoski, "Overview and Analysis of the Performances of Zig Bee based Wireless Sensor Networks", *International Journal of Computer Applications*, Vol. 29, No. 12, pp. 1-8, 2011.

[17] N.A. Somani and Y. Patel, "Zig Bee: A Low Power Wireless Technology for Industrial Applications", *International Journal of Control Theory and Computer Modeling*, Vol. 2, No. 3, pp. 1-14, 2012.

[18] Y. Rana, V. Nandal, K. Vats and R. Kumar, "IEEE 802.15.4 based Investigation and Simulation Evaluation of Zig Bee Tree and Mesh Topology using Different QoS", *International Journal of Computer Science and Mobile Computing*, Vol. 6, pp. 922-932, 2014.

[19] J. Deng, Y.S. Han and P.K. Varshney, "A Pair Wise Key Pre-Distribution Scheme for Wireless Sensor Networks", *Proceedings of IEEE International Conference on Computer and Communications Security*, pp. 42-51, 2003.

[20] B.H. Wellenhoff, H. Lichtenegger and J. Collins, "Global Positions System: Theory and Practice", 4th Edition, Springer, 1997.