ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Recovery Based Low Storage Clone Detection for Secure Data Transmission in Wireless Sensor Network

Ashvini Lal, Dr.J.Selvakumar

PG Scholar, Department of Computer Science and Engineering, Sri Ramakrishna Engineering College, Coimbatore, India

Professor, Department of Computer Science and Engineering, Sri Ramakrishna Engineering College, Coimbatore, India

ABSTRACT: In wireless sensor networks, the sensor nodes are usually deployed in varied geographic locations to keep track of the environmental changes. The tracked information is exchanged between the nodes to perform its operations. Security and data integrity are the major areas need to be concentrated while performing communications around WSNs. An adversary can physically capture any nodes in the network, reprogram the node, and then replicate the nodes in a large number of clones and take authority over the whole network. There are various methods to identify the cloned nodes in the network, in this paper a novel approach is introduced namely, Secure Low Storage Clone Detection protocol with a recovery mechanism. SLSCD works by manipulating the input data file using a Clone Estimation algorithm. Then the data is secured using Advanced Encryption Standard (AES) algorithm. The secured and clone eliminated data is used for communication between the sensor nodes. A dynamic node creation principle is used for placing a resolver node which can be used to recover the cloned node from affecting the networks performance and helps in successful communication. SLSCD performs clone detection in non-hotspot region so it requires less amount of energy and also the data transmitted is free of clones and the data is not stored in any intermediate nodes therefore, it requires low storage capacity and increases the lifetime of the network.

KEYWORDS: Clone detection, clones, cloned nodes, distributed approach, network lifetime

I. INTRODUCTION

Wireless sensor networks is used in a wide range of applications such as environment tracking, target tracking, health monitoring, smart homes, surveillance system, military applications, etc. In sensor network, various number of sensor nodes are deployed in different geographic locations where it can sense and track the environmental changes that occurs. The tracked data are used for different purposes in various fields. In a wireless sensor network, there are possibilities for an adversary to capture a sensor node and acquire all its information. Then, the captured information can be used replicated the nodes and deploy them in various locations in the network. This is done to perform various malicious activities by misusing all the privileges of the legitimate nodes. The adversary can leak the sensitive data flowing through the network or inject false data into the network.

In this paper a new approach is introduced to identify the cloned nodes in the network namely Secure Low Storage Clone detection using a recovery based mechanism. In this method, the SLSCD works by eliminating theidentical data that is sensed and encrypts it before transmission. During transmission the cloned nodes are identified using a witness based mechanism. When a cloned node is identified in the network the recovery node helps the cloned node to get back to its original state and continue to perform all the activities that were performed before being cloned by the adversary. The SLSCD has small amount of Storage Requirements since, there is a tradeoff between storage capacity and energy consumption, and namely, more detection routes can ensure a higher clone detection probability with decreased number of witnesses. Compared to the earlier works [1], [5], [16], the SLSCD protocol fully utilizes the remaining energy to

DOI: 10.15680/IJIRCCE.2017. 0504282

create as many detection routes as possible to reduce the storage requirements of the node and achieves small constant storage requirements.

The wireless sensor network can be either static or dynamic. In dynamic WSN, the location of the sensor node changes as the nodes are mobile. In a static wireless sensor network, once the sensor nodes are deployed in one position, it remains the same and does not change. The clone detection in static wireless sensor networks can be carried out using centralized approach or distributed approach. In centralized approach, a node is present at the centre of the network which is responsible for all the activities in the network. In distributed approach, [3] all the nodes are equally responsible for all the activities and perform activities in a distributed manner.

In wireless sensor network, [6] the SET protocol performs in a centralized manner and detects cloned nodes by dividing the network area into exclusive subsets. Each subset will contain a subset leader and members. The members of the subset are at a distance of one hop away from the subset leader. The subset leader collects the subnet member's information and forwards it to the root of the sub-tree. Each root in the sub tree performs an intersection operation to identify the cloned nodes. If the result of the intersection operation is zero, then there are no cloned nodes in the network. This operation is performed at the base station. The cloned nodes are identified by performing the intersection operation on any two received sub trees. In Compressed Sensing Based Clone Detection [3], a fixed sensed data is shared among one hop neighbors that are then shared to their neighboring nodes in an aggregate tree fashion with base station as the root of aggregation.

In distributed approach, [2] the identity of each and every node is shared in a distributed manner. During data transmission, every node collects the information about its neighbor along with its location and broadcasts it in the network. The Low Storage Clone Detection technique (LSCD) protocol [4] has an increased probability for identifying the cloned nodes in the network. It is used to detect the cloned nodes in the sensor network. The cloned nodes are identified in two steps namely, witness building stage and clone detection stage. In the witness building stage, the node that has to transfer the data sends its ID and location to its witness node in the same network. The information is not directly transferred to the witness node but in an arc form around the sink node the data is passed to one hop neighbors. In the clone detection stage, the several clone detection routes are originated from the sink node which is compared with the witness path to identify the cloned nodes in the network.

In sensor network, [12] using the Deterministic Multicast (DM) Protocol, each and every node will share its location claim with a limited set of witness nodes that are selected deterministically. A node can broadcast its location claim to its neighbors and then forward to its subset nodes also known as witness nodes. Each node will have a specific witness node associated with the node's ID. If an adversary tries replicating a node, the witness will receive two different location claims for the same node ID. The conflicting claims of nodes location is a revocation of replicated nodes in the same network.

In Randomized Efficient and Distributed (RED) protocol, a random value [7], [10] is broadcasted by the base station to all the nodes in the network. Each node will broadcast its location claim to its neighbors, then each node will select a witness node to forward its location claims. The witness nodes are selected using a pseudo random codes that are generated using node's ID as input. [8] It is then broadcasted by the base station to a number of target locations. If same location claim occurs, then the node ID will be forwarded to the witness node in each phase of detection. This method is used to differentiate the cloned nodes. The witness node for each node varies at each detection phase as the pseudo random code generated by the base station. If any witness node receives two different location claims for the same node then it indicates that cloned nodes are present in the network.

The Randomized Multicast (RM) performs clone detection using a signature authenticating code is broadcasted along with the location claim. Each node forwards those claims to randomly chosen set of witness nodes. If any witness receives two different location claims for same node ID it can revoke the replicated node in the network [12].The Line Selected Multicast (LSM) protocol [11] allows a node to announce its location to all its neighboring nodes. Each node in the network has a unique signature assigned to it. When a location claim travels from source to location, it has to pass several intermediate nodes which form a claim message path. Cloned nodes are detected by the node on the intersection of two different paths that are formed by claims carrying the same ID to two different destination nodes.

Memory Efficient Multicast Protocolperforms using boom filters and boom filters along with cell forwarding. Using boom filters [12] when all the intermediate node serves, the first and last node serves as witness node. When a node receives a location claim, it performs the two-phase conflict check to detect all the conflict claims. [9] Using boom filters along with cell forwarding, the deployment area is divided into a number of virtual cells. In each cell an anchor point is assigned for every node in the network. The neighboring node near the anchor point is call anchor node. The location claim is transferred from one anchor node to another until it reaches its location. The anchor node in the first and last cell acts as witness while the other nodes act as watchers.

Using Random Walk, [4] each node broadcasts a signed location claim. Each of the node's neighbors probabilistically forwards the claim to some randomly selected nodes. Each randomly selected node sends a message containing the claim to start a random walk in the network. The passed nodes are selected as witness nodes and it will store the claim. If any witness receives different location claims for a same node ID. This will result in the detection of the replicated node [16]. In Table Assisted Random walk (TRAWL), when a randomly chosen node starts a random walk, all the passed nodes will still become witness nodes. They do not definitely store the location claim; instead, they store the location claim independently. Also, each witness node will create a new entry in its trace table for recording the pass of a location claim. When receiving a location claim a node will first find the entries which have the same node ID as the claim in its trace table. Then if any entry is found, the node will compute the digest of the claim and compare the digest with the digest in the entry. When two digest are different, the node detects a clone attack [4].

II. PROPOSED SYSTEM

In the proposed approach, a novel method is introduced to identify the cloned nodes present in the by a trust based mechanism. The trust mechanism works by exchanging request (RREQ) and response(RREP) to the neighboring nodes to achieve trust and to identify whether the node is under the control of an adversary. Then, the node proceeds with another set of verification by checkingits unique ID and location which will be known only to those two nodes exchanging the data packets. Each and every neighboring node will have a unique Id and location in the network. The data packet will be transferred to the neighbor node only if the node is trusted. If a cloned node is identified in the network, the cloned node is rectified with the help of a recovery node in the network.

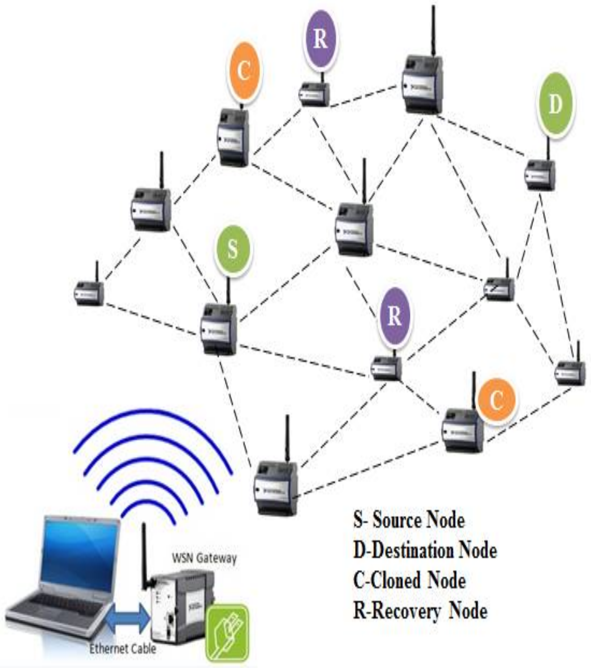

FIGURE-1: NETWORK ARCHITECTURE

The Figure-1 represents the deployment of sensor node in the wireless sensor network. The ‘S’ represents the source node, the ‘D’ represents the destination node, ‘C’ represents the cloned node and ‘R’ represents the recovery node in the network. The proposed approach works well with any network scale.

The proposed approach works well in a distributed environment. The wireless sensor nodes will assign to sense the environment to identify the changes. The sensed data can be used within or outside the network for various purposes. It can be used by exchanging the data to the base station or within the nodes in the network.

NETWORK FORMATION

The total number for sensor nodes in the network varies depending upon the purpose of the network. Each and every node will have a specific ID that is known only to that particular node and its witness node.Every node will have a witness node which will vary for every communication. The witness node communicates with the base station about all the activities taking place in the network.

COMMUNICATION OR EXCHANGE OF DATA BETWEEN THE SENSOR NODES

The sensed data has to be exchanged between sensor nodes to perform the activates successfully. The sensed data is checked for number of clones i.e., the number of identical data is identified and removed using Clone Estimation algorithm.

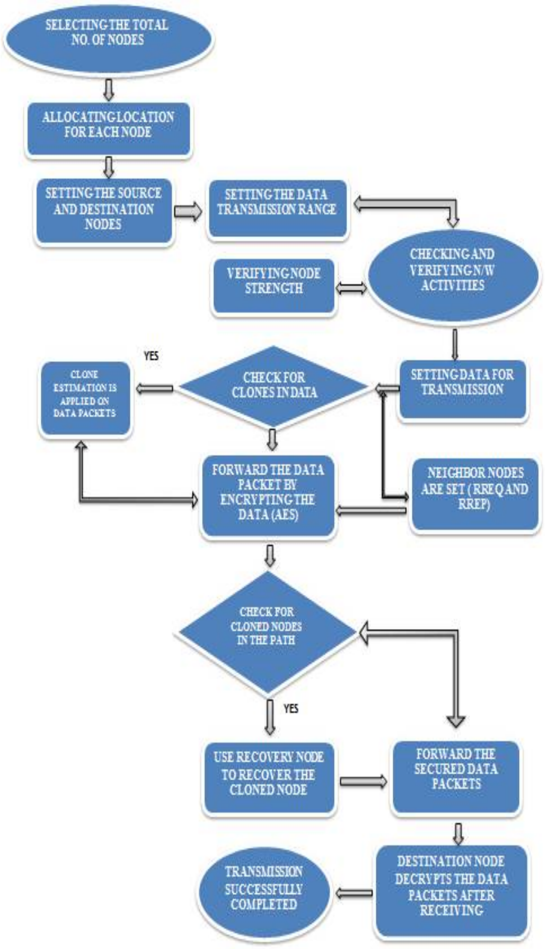
SELECTING THE TOTAL NO. OF NODES
ALLOCATING LOCATION FOR EACH NODE
SETTING THE SOURCE AND DESTINATION NODES
SETTING THE DATA TRANSMISSION RANGE
CHECKING AND VERIFYING N/W ACTIVITIES
VERIFYING NODE STRENGTH
YES
CLONE ESTIMATION IS APPLIED ON DATA PACKETS
CHECK FOR CLONES IN DATA
SETTING DATA FOR TRANSMISSION
FORWARD THE DATA PACKET BY ENCRYPTING THE DATA (AES)
NEIGHBOR NODES ARE SET (RREQ AND RREP)
CHECK FOR CLONED NODES IN THE PATH
YES
USE RECOVERY NODE TO RECOVER THE CLONED NODE
FORWARD THE SECURED DATA PACKETS
TRANSMISSION SUCCESSFULLY COMPLETED
DESTINATION NODE DECRYPTS THE DATA PACKETS AFTER RECEIVING

FIGURE-2: CLONE DETECTION USING RECOVERY BASED SLSCD

The clone estimation algorithm removes the identical data in the data to be transmitted. The clones removed data is encrypted using Advanced Encryption Standards algorithm. The encrypted data is then transmitted to the destination node. The transmission takes place via. intermediate nodes.

RECOVERING THE CLONED NODES

If any cloned node is present in the intermediate nodes. It is recovered using a recovery node present in the network. Each and every node will have a recovery node and the recovery node will be different for each transmission. This process continues until the data packet reaches its destination.

After receiving the data packets, the destination node decrypts the data packets and uses it. Using this method to identify cloned nodes and rectify it provides improved probability for detecting the cloned nodes in the network. It improves security to the data packet transferred within the network. Since clone eliminated data is transmitted, it requires low storage in the sensor devices. Thus improving the lifetime of the network

III.PERFORMANCE ANALYSIS AND RESULTS

The proposed methodology has been implemented in NS2; the performance of the SLSCD protocol in a WSN environment was simulated and thus succeeded in identifying the cloned node with highest probability of clone detection. The figure-3 represents the graph generated from values obtained from networks with different scales. It indicates that the probability of clone detection has been improved when compared with the existing approach.

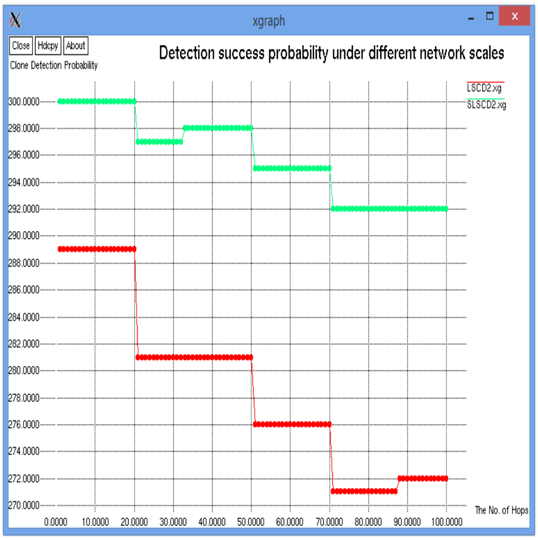

FIGURE-3: CLONE DETECTION PROBABILITY

The proposed result analysis shows that SLSCD requires only a minimum amount of energy to detect the cloned nodes. The figure-4 represents the comparison of low energy consumption by the proposed system and the existing approach. The low energy consumption is obtained by allowing the nodes to perform activities whenever required. Otherwise the nodes will be set to sleep state.

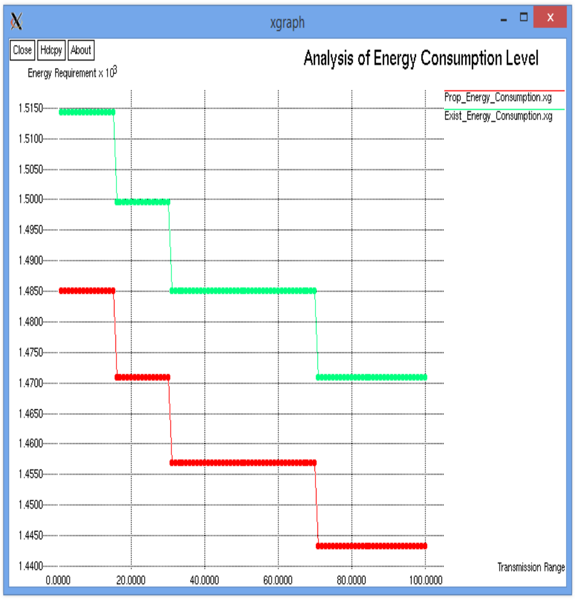

FIGURE-4: ENERGY CONSUMPTION

The figure-5 represents the graph plotted with the values collected to determine the lifetime of the network. Compare to the existing system, SLSCD prolongs the lifetime of the network.

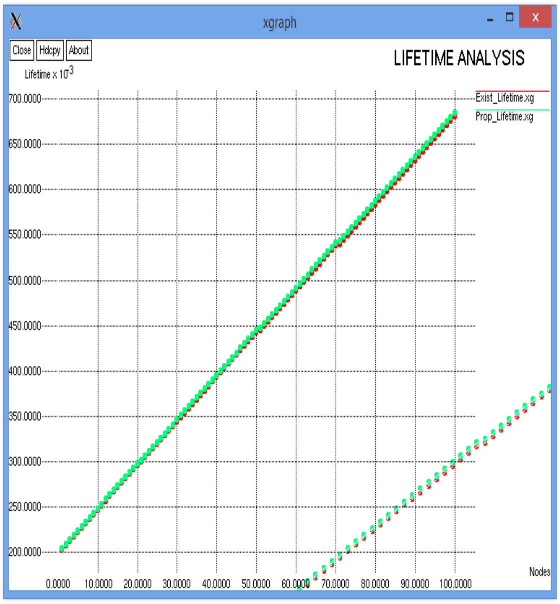

FIGURE-5: NETWORK LIFETIME

The figure-6 represents the comparison of the average delay with speed of the data packets delivery. It shows that the delivery of data packets delay reduces as the speed increases.

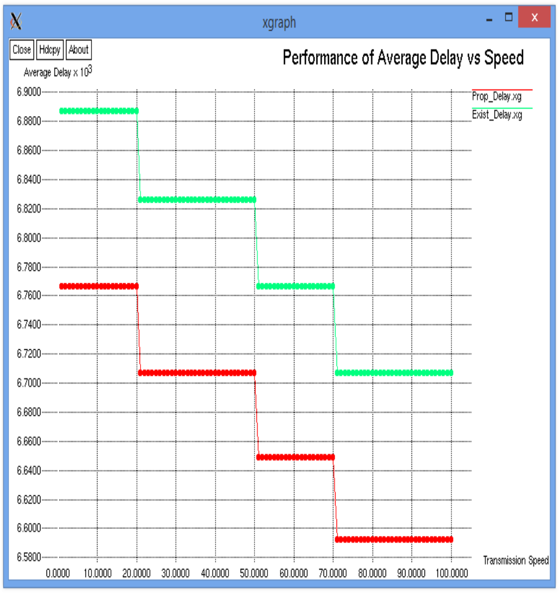

FIGURE-6: DATA TRANSMISSION SPEED

The figure-7 and figure-8 represents that the storage requirements under different network scenario i.e., with different network nodes and nodal degrees have been reduced when compare with the earlier proposed methods. This is due to the transmission of data packets by eliminating the similar data set. And also, the information about the source and destination nodes will node is stored anywhere in the network.

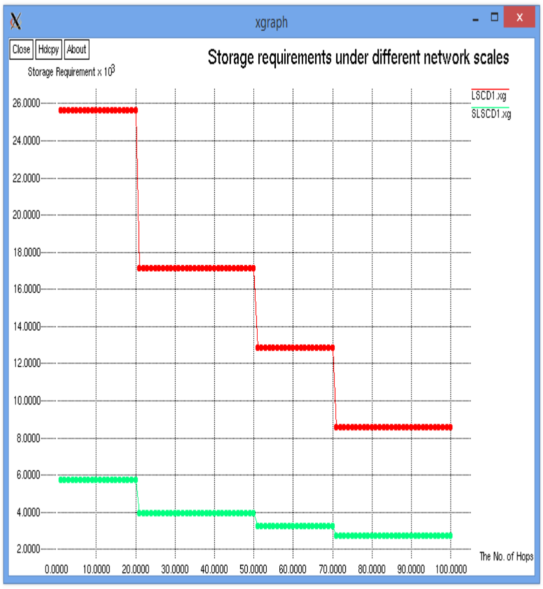

FIGURE-7: STORAGE REQUIREMENTS UNDER DIFFERENT NETWORK SCALES

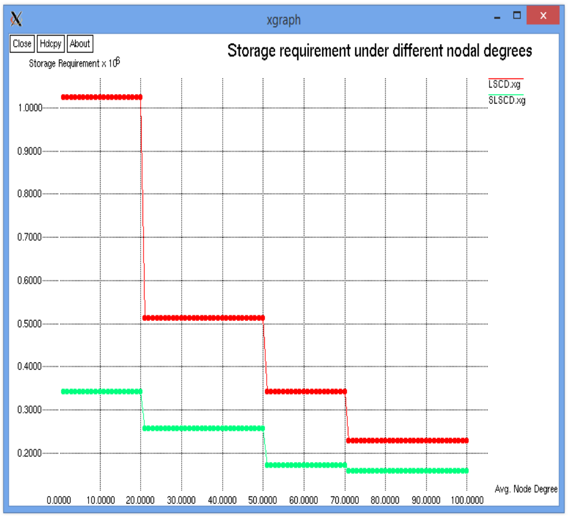

FIGURE-8: STORAGE REQUIREMENTS UNDER DIFFERENT NETWORK SCALES

IV. CONCLUSION

In this paper, a novel method to detect the cloned node in the WSN and to recover the cloned node using a recovery mechanism was introduced. Thus, the proposed methodology shows increased probability of detecting the cloned nodes. It also provides security to the data packets sent by encryption of the packets after eliminating number of clones present in the network analyzed data. Thereby, reducing the storage requirements and utilizing minimal energy for all its activities which improves the lifetime of the network.

REFERENCES

[1] A. Liu, X. Jin, G. Cui, and Z. Chen, “Deployment guidelines for achieving maximum lifetime and avoiding energy holes in sensor network,” Inf. Sci., vol. 230, pp. 197–226, May 2013.

[2] Bryan Parno, Adrian Perrig, Virgil Gligor, ” Distributed Detection of Node Replication Attacks in Sensor Networks “, In proceeding of the IEEE Symposium on Security and Privacy,2005

[3] C.M.Yu, C.S.Lu and S.Y.Kuo,”CSI: Compressed sensing based clone identification in sensor networks”in proceedings of the IEEE International conference on pervasive computing and communications workshops, pages 290-295, March-2012

[4] Dong, Kaoru Ota, Laurence T. Yang, Anfeng Liu, and Minyi Guo, Senior Member, IEEE “LSCD: A Low-Storage Clone Detection Protocol for Cyber-Physical Systems” Mianxiong, IEEE Transactions on Computer-Aided Design of Integrated Circuits And Systems, VOL. 35, NO. 5, May 2016

[5] Dr.G.Padmavathi, Mrs.D.Shanmuga Priya, “A Survey of attacks, security mechanisms and challenges in wireless sensor networks”, International Journal of computer science and information security, vol.4, no.1&2, 2009.

[6] Hesiod Choy, Cancun Zhu and T.F.La Porta,” SET: Detecting Node clones in Sensor Networks”, Proc of 3rd International Conference on Security and Privacy in comm...Networks (Secure Comm) Pages 341-350, 2007

[7] Jun-Won Ho, Dogging Lin, Matthew Wright, SajaiK.Das “Distributed Detection of Replicas with Deployment Knowledge in Wireless Sensor Networks”, Preprint submitted Elsevier, March 2009.

[8] Kai Xing,Fang Liu,Xiuzhen Cheng,David H.C.Du,” Realtime Detection of clone attacks in Wireless Sensor Networks”,IEEE ICDCS 2008

[9] L. Jiang, A. Liu, Y. Hu, and Z. Chen, “Lifetime maximization through dynamic ring-based routing scheme for correlated data collecting in WSNs,” Comput. Electr. Eng., vol. 41, pp. 191–215, Jan. 2015.

[10] Mauro Conti, Roberto Di Pieto, L.V.Mancini and A.Mei,”A Randomized and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks “, Proc.ACM MobiHoc, Pages 80-89, Sept 2007

[11] Mauro Conti, Roberto Di Pietro, Luigi Vincenzo Mancini and Alessandro Mei “Distributed Detection of Clone Attacks in Wireless Sensor Networks” IEEE Transactions on Dependable and Secure Computing, Vol 18, No 5, Pages 685-698, September/October 2011

[12] Ming Zhang, Vishal Khanapure, Shigang Chen,Xuelian Xiao, “Memory Efficient Protocols for Detecting Node Replication Attacks in Wireless Sensor Network” IEEE Pages 284-293, 2009

[13] 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.

[14] Wen Tao zhu, “Node Replication Attacks in Wireless Sensor Networks: Bypassing the Neighbor-Based Detection Scheme”, International Conference on Network Computing and Information Security, Pages 156-160, 2011

[15] Y. Liu, A. Liu, and Z. Chen, “Analysis and improvement of send-andwait automatic repeat-request protocols for wireless sensor networks,” Wireless Pers. Commun., vol. 81, no. 3, pp. 923–959, Apr. 2015.

[16] Yingpei Zeng, Jiannong Cao, Shigeng Zhang,Shanqing Gao and Li Xie “Random Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks “, IEEE Journal on selected areas in communications, vol 28, No.5 Pages 677-691, June 2010