Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 04, April-2020

Empirical Analysis of Clone Detection Mechanism Over Wireless Sensor Networks

[1]Vishakha Jadhav, [2]Seema Hanchate
[1,2] M.Tech student (ENC) SNDT UMIT Mumbai ,
Professor SNDT UMIT

***Abstract*: Wireless sensor networks (WSNs) are now used as supporting infrastructure in many applications. As WSN has broadcast approach, there is a need of security. Secure communication in WSNs is very important because information sent through these networks can be easily captured or replaced or altered. Clone attack is node replication attack, which one of the serious attack. In this, An adversary can steal a node from the network and altered data from stolen node and can reprogram that node to create a clone of a stolen node. Proposed clone detection protocol is to protect network from clone attack. In this paper distributed detection mechanism is used to provide high detection probability, Cross Unequal Clustering Routing Algorithm (CUCRA) for routing and clustering while transmission of data which enhanced network lifetime.**

Keywords: Wireless sensor network, security, clone attack, distributed approach, network lifetime,

1. INTRODUCTION

Wireless sensor network is recently enhancing technology due to advancements in Telecommunication field, which has enabled the development of network multitasking sensor nodes. Wireless sensor networks are widely used in very crucial applications such as battlefield surveillance, RADAR imaging, to monitor patient’s physiological parameters, automotive applications, in environmental applications which involve forest fire detection, precise agriculture, greenhouse, etc. As WSN has broadcast approach, there is a need of security. Wireless sensor networks (WSNs) are now used as supporting infrastructure in many applications. Secure communication in WSNs is very important because information sent through these networks can be easily captured or replaced or altered.

There are Different possible attacks on WSN are Selective forwarding attack, Sinkhole attack, Wormholes attack, Sybil attack, flood attack, Acknowledgement spoofing , Sniffing attack, Data integrity attack, Energy drain attack , Black hole attack, Denial of service attack, Physical attacks, Traffic analysis attack, Privacy violation by attack and clone Attacks. One of the serious physical attacks faced by the wireless sensor network is node clone attack. Various techniques are available to overcome the clone attack but existing protocols are have issues like requirement of large storage space, has high communication overhead, larger energy consumption which results in reduction in network-lifetime, less probability of protection against attack. So we are proposing clone detection protocol where we are trying to minimize above issues. Proposed protocol have low transmission overhead, while using reasonably small memory space, less power consumption and prolonged battery life with high detection probability against clone attack. Clone-detection protocols must be non-deterministic and fully distributed and fulfill security requirements on witness selection. In distributed clone detection protocols, because witness and detection routes are distributed, ensuring that detection routes encounter witness nodes is challenging.[11]

2. CLONE ATTACK

An adversary can capture a sensor node and take out its key materials. Once a node is captured, the adversary can reprogram it and generate a clone of a captured node. These clones can be placed in network. These clone attacks are very harmful to the wireless sensor networks. With a single captured sensor node, the attacker can create as many replica nodes as he wants. The replica nodes are forbidden by the adversary, but have keying materials that allow them to seem like authorized participants in the network. So it is very much hard to detect a clone attack.[10]

2.1 Impact of Clone Attacks on WSN Security

WSN has some common security goals such as data confidentiality, authenticity, availability, availability, freshness, data integrity, scalability. In clone attack replica of original node can be deployed anywhere in network, so its very dangerous for keeping the network secure.

3. CLONE ATTACK DETECTION

WSN has two methods to set the networks, it might be static (fixed) or mobile. 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 deployment.[10] In static WSN Two types of detection techniques are available those are centralized and distributed. In a centralized approach for detecting node replication, when a new node joins the network, it broadcasts a location claim containing its location and identity to its neighbours. One or more of its neighbours then forward this location claim to the base station. With location information for all the nodes in the network, the base station 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. 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 forwarded to the corresponding witness nodes. If any witness node receives two different location claims for the same node ID, then the existence of clone is detected [10].

3.1Distributed approaches

Distributed schemes do not need central control means the clone detection process runs on every node of the network. In clone node detection process, the node ID and location of node plays important role. Achieves 100% detection of duplicate nodes assuming the broadcast reaches throughout the network.

4. PROPOSED WORK

Security and data integrity are the major areas need to be concentrated while performing communications around WSNs. Proposed Clone Detection Protocol is designed and which efficiently analyze the communication data step by step without any interventions. Clone Detection methodology is highly helpful to remove the duplicate data while transmission, which leads the network performance to be more effective and produces two times better accuracy and speed while communication. The scenario starts with selecting the input data file and pass it to manipulation level by means of Clone Estimation algorithm; once the clone is detected the data is secured. The secured and clone eliminated data is meant for communication between source and destination and experimentally it illustrates the performance and efficiency of the wireless Sensor network communications.

4.1 Block diagram

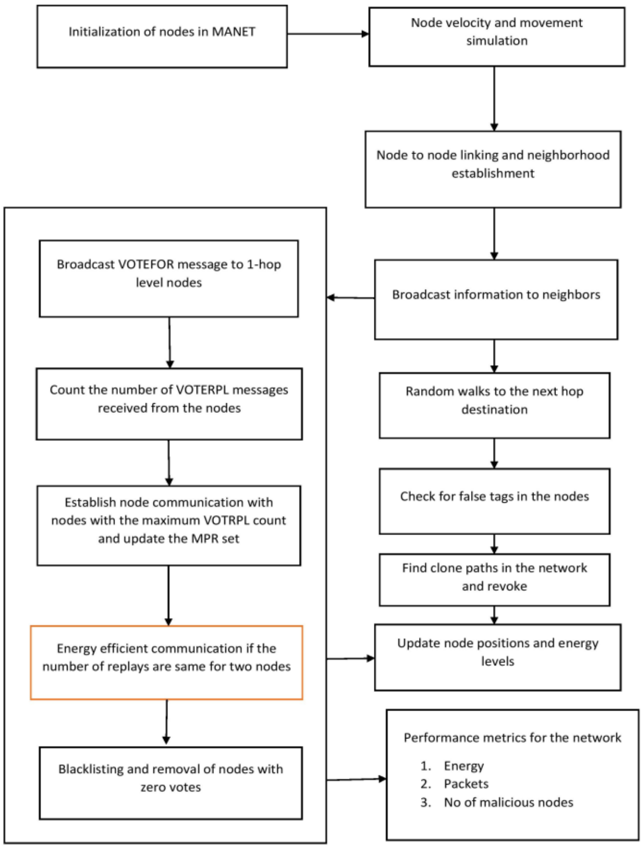
Initialization of nodes in MANET
Node velocity and movement simulation
Node to node linking and neighborhood establishment
Broadcast information to neighbors
Broadcast VOTEFOR message to 1-hop level nodes
Count the number of VOTERPL messages received from the nodes
Establish node communication with nodes with the maximum VOTRPL count and update the MPR set
Energy efficient communication if the number of replays are same for two nodes
Blacklisting and removal of nodes with zero votes
Random walks to the next hop destination
Check for false tags in the nodes
Find clone paths in the network and revoke
Update node positions and energy levels
Performance metrics for the network
1. Energy
2. Packets
3. No of malicious nodes

Fig. 1. Block diagram

The approach is to minimize transmission time while building a network. The basic theory is that clustering is done because the nodes which are clustered have a sensed data which vary in very insignificant amount.[18]

The existing network build in this paper is static wireless network, which is a continuously self-configuring, of node devices connected wirelessly. First initializing of nodes in the network is done. Initializing process includes the deciding g number of nodes deployed, considering its initial energy as well as transmitter and receiver energy.

4.2 Flowchart

Figure shows the flow chart of the proposed protocol:

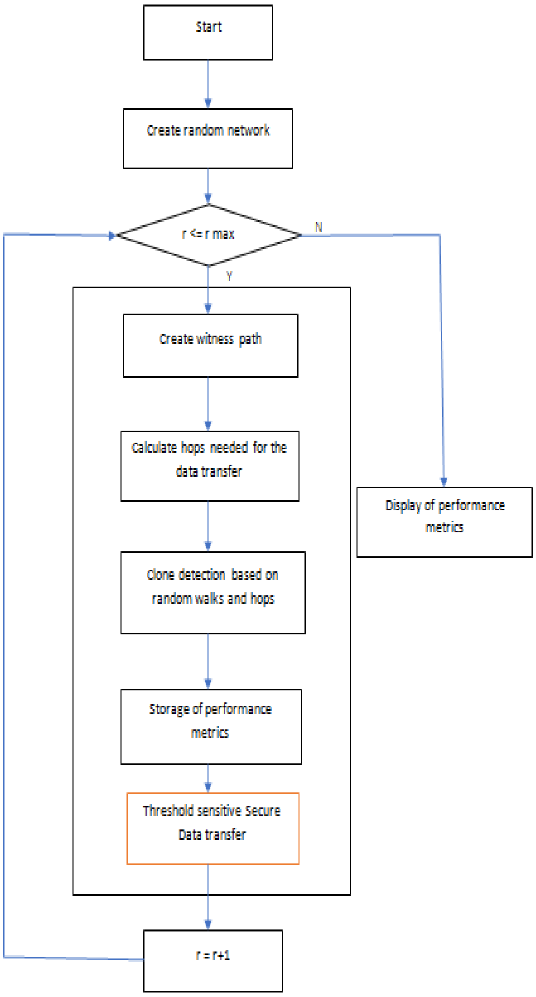
Start
Create random network
r <= r max
N
Y
Create witness path
Calculate hops needed for the data transfer
Clone detection based on random walks and hops
Storage of performance metrics
Threshold sensitive Secure Data transfer
r = r+1
Display of performance metrics

Fig.2. Flow chart

The basic theory is that clustering is done because the nodes which are clustered have a sensed data which vary in very insignificant amount. So cluster head in a cluster when take the data from their members is similar in nature. Cluster heads have to send similar type of data again and again to base station which is time consuming and wastage of energy by the cluster heads. [17] A threshold sensitive reactive proposed scheme to minimize the transmission time as transmission consume more energy than processing of data at the nodes. This was done to impart two threshold parameters, hard and soft threshold. A node only transmit when currently sensed value is greater than hard threshold and difference between current sensed and previous sensed value is greater than soft threshold .This is a kind of optimization technique which can optimize the communication.

5. DESIGN CONSIDERATIONS

Objectives of this proposed protocol are

(i) increased network Lifetime (ii) high Clone Detection Probability (iii) less Storage requirement. To fulfill these objectives, we have adopted following methodologies:

(a) In this proposed work for routing, clustering and hopping process during network formation and data transmission, Cross Unequal Clustering Routing Algorithm (CUCRA) is implemented. The Cross Unequal Clustering Routing Algorithm combines the advantages of various clustering algorithms and improves them. In the calculation of the cluster radius, two of the dynamic variables of the cluster size were introduced in the parameters. The node residual energy and the distance between node and the BS implement the dynamic variable of the cluster size. At the same time, introducing cluster adjacent node into the communication between clusters for data forwarding, it effectively reduces the energy loss of the cluster head. Such residual or individual nodes forward the sensed data either directly to the Base Station or by finding the next best hop by sending many control messages hence reduces the network lifetime.[20] The proposed protocol reduces/eliminates such individual node formation and improves the overall network lifetime when compared to the existing protocols.[19]

(b) There is a tradeoff between storage capacity

and energy consumption, namely, more detection routes can ensure a higher clone detection probability with decreased number of witnesses. Meanwhile, we found that, due to the “energy hole” phenomenon in WSNs, the remaining energy is as high as 90% under the premature death of the network. Therefore, this

protocol fully utilizes the remaining energy to create as many detection routes as possible to reduce the storage requirements of the node and achieves a small constant storage requirement.[11]

(c) Proposed Protocol Has Fully Distributed

Characteristics and Provides Strong Protection against Attacks and a High Detection Probability here witness nodes form route paths along circles, with a sink serving as the center, because clone detection is processed along the centrifugal (or centripetal) direction, and the distance between any two detection routes is shorter than the witness path length. Thus, the witness path must encounter the detection route, ensuring that this protocol theoretically has a 100% clone detection probability. Moreover, witness routes and clone detection routes are randomly generated. Thus, even if the adversary knows the algorithm, the locations of witness nodes and detection route information cannot be obtained. Therefore, this protocol has fully distributed characteristics and strong robustness to compromise attacks.[11]

A threshold sensitive secure data transfer scheme to minimize the transmission time as well as to provide more security against attack. This was done to impart two threshold parameters, hard and soft threshold. A node get transmit when currently sensed value is greater than hard threshold and difference between current sensed and previous sensed value is greater than soft threshold. This is a kind of technique which can optimize the communication.[17]

6. SIMULATION RESULTS

The empirical analysis of performance of randomly created wireless sensor network is done with the help of Matlab simulation software, shown below:

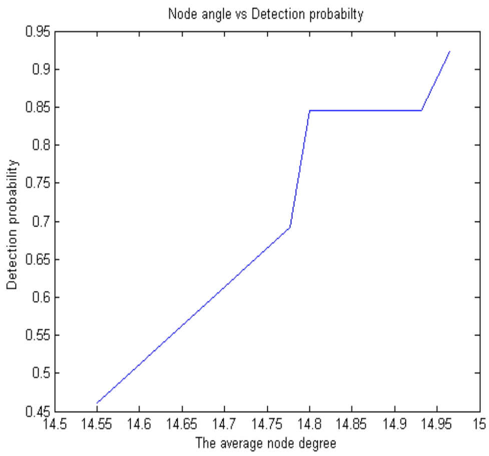

Fig.3 Detection probability vs node degree

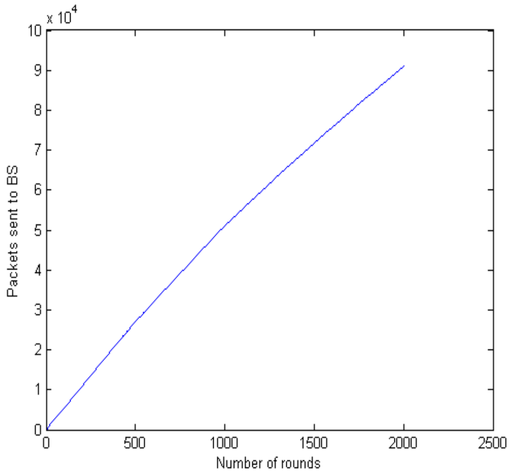

Fig. 4 Packets sent vs number of rounds

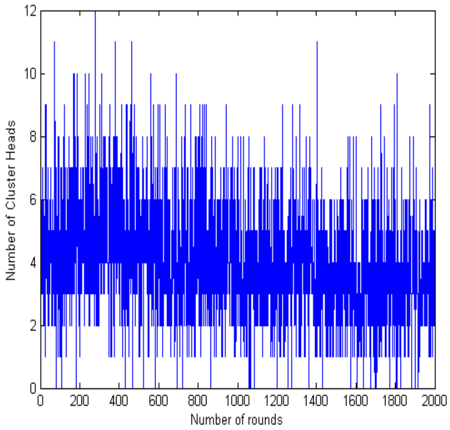

Fig 5 Number of cluster heads vs number of rounds

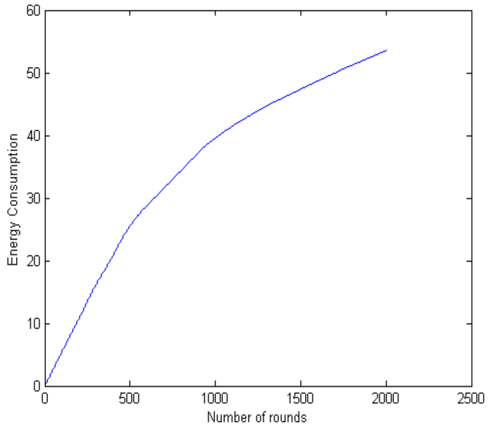

Fig. 6 Energy consumption vs number of nodes

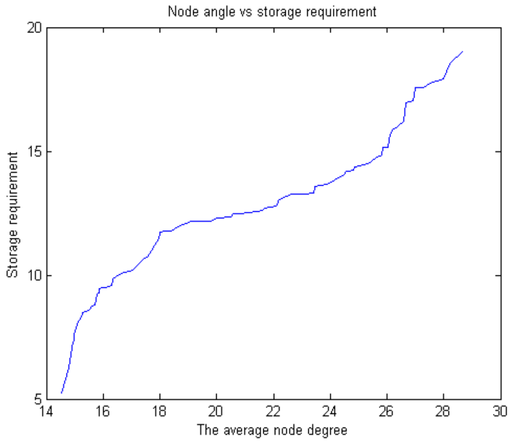

Fig. 7 Storage requirement vs avg node degree

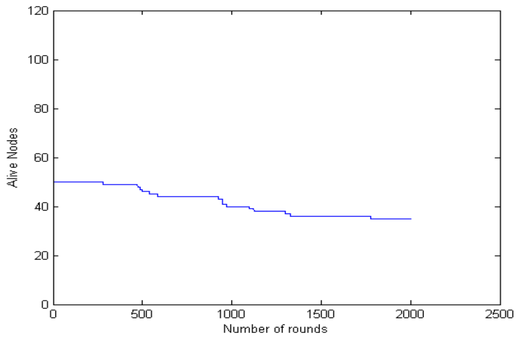

Fig. 8 Alive nodes vs number of rounds

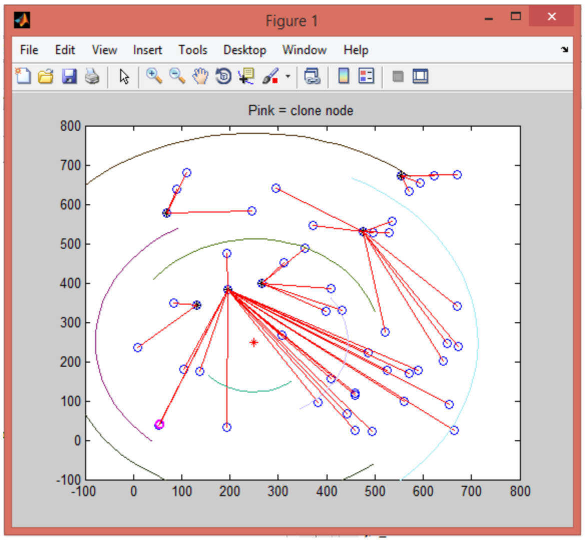

Fig. 9 Clone detection

6.2 Analysis of simulation results

Here we are analyzing the performance of simulation results of new clone detection protocol with the performance of Low storage clone detection protocol (LSCD).In the graphs shown, LSCD is named as "base" and new protocol simulated is named as "change".

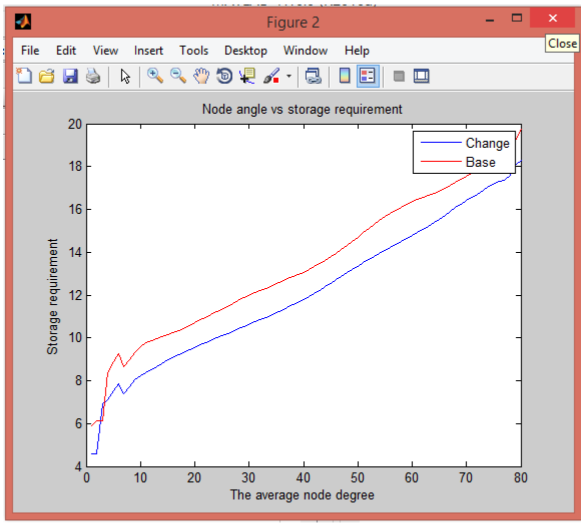

Fig. 10 Storage requirement under different nodal degree

Figure 10 shows the Storage requirement under different nodal degrees of our work compared with LSCD protocol. Storage requirement in proposed work is less.

The storage space requirements can increase with increasing number of nodes.

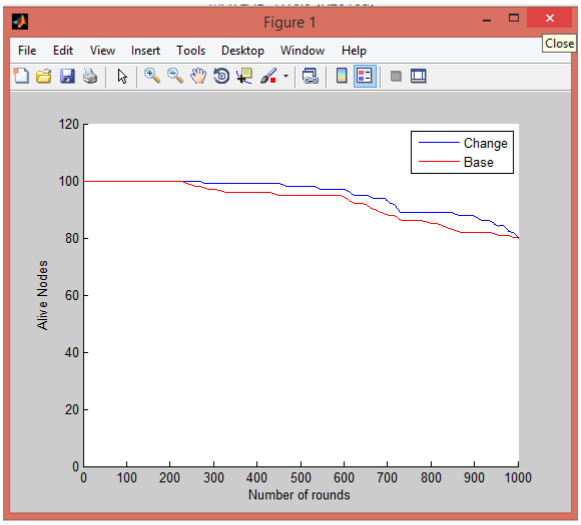

Fig. 11 Network lifetime

Figure 11 shows the network lifetime in terms of calculation of alive nodes. Because CUCRA takes into account both the remaining energy and the distance between the node and the BS in the clustering radius, cluster size can dynamically change with time and also the distance between the node and the BS. CUCRA and EEUC algorithms are using multi-hop communication, they successfully avoid long-distance communication between cluster head and the base station This contributes to the effective balance of energy loss and the extended network lifetime.[20]

CONCLUSION

Empirical analysis of network performance is done in this paper. The overall methodology to enhance the network lifetime, clone detection probability and to reduce the requirement of lesser storage space is described. Improving the results using Cross Unequal Clustering Routing Algorithm (CUCRA) for routing and clustering while transmission of data. In our future work, we would like to explore advanced mechanisms to ensure that our protocols continue to function even in the attack of powerful adversaries who replicate the node IDs.

REFERENCES

[1] Lathies Bhasker ”Genetically derived secure cluster-based data aggregation in wireless sensor networks” IET Inf. Secur., 2014, Vol. 8, Iss. 1, pp. 1–7 doi: 10.1049/iet-ifs.2013.0133

[2] K. Sindhukavi, P. Brundha, P. J. Beslin Pajila “ An Efficient Cloning Detection Protocol Using Distributed Hash Table for Cyber-Physical System in WSN”, 2016 IJSRSET — Volume 2 — Issue 5

[3] Sushma, Deepak Nandal, Vikas Nandal “Security Threats in Wireless Sensor Networks” IJCSMS International Journal of Computer Science & Management Studies, Vol. 11, Issue 01, May 2011

[4] Fabio Pasqualetti and Qi Zhu” Design and Operation of Secure Cyber-Physical Systems ”, ieee embedded systems letters, vol. 7, no. 1, march 2015

[5] Eric Ke Wang,Yunming Ye, Xiaofei Xu, S.M.Yiu, L.C.K.Hui, K.P.Chow,” Security Issues and Challenges for Cyber Physical System”, IEEE/ACM International Conference on Green Computing and Communications, 2010

[6] Mianxiong Dong, Kaoru Ota, Laurence T. Yang, Anfeng Liu, and Minyi Guo “LSCD: A LowStorage Clone Detection Protocol for Cyber-Physical Systems”, ieee transactions on computeraided design of integrated circuits and systems, vol. 35, no. 5, may 2016

[7] Anjali, Shikha and Mohit Sharma, Wireless Sensor Networks: Routing Protocols and Security Issues, 5th ICCCNT,IEEE 2014.

[8] Alekha kumar mishra thesis on “Node Replica Detection In Wireless Sensor Networks”,2014.

[9] Haafizah Rameeza Shaukat, Fazirulhisyam Hashim, Aduwati Sali, andM. Fadlee Abdul Rasid Node Replication Attacks in Mobile Wireless Sensor Network: A Survey, Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2014, 8 December 2014

[10] J.Anthoniraj,T.Abdul Razak,” Clone Attack Detection Protocols in Wireless Sensor Networks: A Survey”,International Journal of Computer Applications (0975 – 8887) Volume 98– No.5, July 2014

[11] Mianxiong Dong, Kaoru Ota, Laurence T. Yang, Anfeng Liu, and Minyi Guo,” LSCD: A Low-Storage Clone Detection Protocol for Cyber-Physical Systems”, ieee transactions on computer-aided design of integrated circuits and systems, vol. 35, no. 5, may 2016

[12] Heesook Choi, Sencun Zhu, Thomas F. La Porta, SET: Detecting node clones in Sensor Networks

[13] Neenu George,T.K.Paran,” Detection of Node Clones in Wireless Sensor Network Using Detection Protocols”, International Journal of Engineering Trends and Technology(IJETT) –Volume8 Number 6-Feb 2014

[14] K.Vijayan, Arun Raaza,” Secure and Energy Efficient Algorithms to Detect Node Replication Attacks in Sensor Networks”, International Journal of Engineering Technology Science and Research IJETSR ,ISSN 2394 – 3386 Volume 3, Issue 7 July 2016

[15] J.Anthoniraj1, Dr.T.Abdul Razak” Distributed Clone Attack detection Protocols in Static Wireless Sensor Networks: A survey” International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 5, May 2014

[16] Murali Pulivarthi1, Shafiulilah Shaik2, M Lakshmi Bai3,” Detection of Clone attacks in Wireless Sensor Networks Using RED (Randomized, efficient, and distributed) Protocol”, International Journal of Engineering Research and Development e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com Volume 4, Issue 7 (November 2012)

[17] Anamika Chauhan, Amit Kaushik,”TADEEC: Threshold Sensitive Advanced Dixzsxtributed Energy Efficient Clustering Routing Protocol for Wireless Sensor Networks”, International Journal of Computer Applications (0975 – 8887) Volume 96 – No.23, June 2014

[18] Yingpei Zeng, Jiannong Cao, Senior Member, IEEE, Shigeng Zhang, Shanqing Guo 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, JUNE 2010

[19] Rejina Parvin , Assistant Professor, Vasanthanayaki C, Associate Professor”Particle Swarm Optimization based Clustering by Preventing Residual Nodes in Wireless Sensor Networks”, DOI 10.1109/JSEN.2015.2416208, IEEE Sensors Journal

[20] Wang Tong,Wu Jiyi, Xu He, Zhu Jinghua, Charles Munyabugingo,” A Cross Unequal Clustering Routing for Sensor Network**”**, MEASUREMENT SCIENCE REVIEW, Volume 13, No. 4, 2013