Dynamic Detection of Node Replication Attack in Wireless Sensor Network using MANET

M.Balaganesh
Asst.Prof/Dept of CSE
Sembodai Rukmani varatharajan Engineering College

S.Nithyadhevi
PG Scholar/ Dept of CSE
Sembodai Rukmani varatharajan Engineering College

ABSTRACT

In this paper aims to detect the cloned node in the environment network. The most conspicuous attack in Wireless Sensor Network is node replication attack. In this attack the nodes are replicated manually based on their id and key values. Cloned node or adversary promotes the node key or id of the original node, creates more replicas of the particular node in the current network with the same id and also this node may cripple the entire network. In Mobile Network the detection of replicated node is somewhat difficult and easy manner. In this paper the proposed scheme is well defined and easy manner to detect the replicas in mobile Wireless Sensor Network where the location makes the detection of replication attack even more challenging and easy thing. The proposed scheme will not only trace the location of the node, but also detect the replicas using multiple scenarios such as id recognition, frames, key values, and neighbor replica detection in dynamic manner not only for static.

General Terms

Bloom, EDD, MANET, Replication

Keywords

Cloning Node, Sybil Attack, Temper.

1. INTRODUCTION

In this world so many problems are arises due to replication attack in the network. Mainly wireless sensor networks are used to solve major problems in the way of both industrial and environmental Sensing. -Wireless Sensor Network is classified into two ways, first one is dynamic and another is Static. Mostly vulnerable attack is one of the most node replication attacks, in that attack the adversary collects the secret information about the current node from a compromised node, and generates a large number of conspicuous replicas and also share the node's keying materials and ID, and then spreads these replicas throughout the entire network in the current environment. From a single captured node, the adversary can create as many more replicated node in this current network.

1.1 Replication Attack

Wireless sensor networks are mainly deployed in hostile environments, where an opponent can physically capture some of the nodes. Suppose once a node is corrupted or captured by any other node that particular, adversary collects all the information within a few seconds. After that the adversary uses that information and enters into network for doing illegal activities. From those activities the opponent Can re-program it and replicate the node in order to eavesdrop the messages or compromise the node based on the functionality of the network. In particularly a most harmful attack is replication attack against sensor networks where one or more node illegitimately generates and claims an identity as replicas as known as replication attack. Due to this replication attack, the following malfunctions are occurring such as routing, resource allocation, and misbehavior detection. This paper analyzes the threat posed by the replication attack, several novel techniques to detect and defend against the replication attack, and analyzes their effectiveness in the way both dynamic and static manner. The replication attack can be exceedingly injurious to many important functions of the sensor network such as routing, resource allocation, and misbehavior detection.

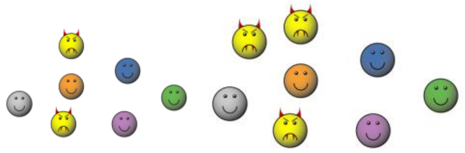


Fig 1: Replication Attack

In this paper analyzes the threat posed by the replication attack, and several novel techniques to detect and defend against the replication attack, and analyzes their effectiveness. In this paper assume that the adversary's goal is to replicate the node in current network and introduce new types of error, malfunctions and wish to apply any other types of unknown attacks in the source or destination environment. The attacker can either compromise a sensor node or a cluster head node for getting the secret information from the original node and use that information for degrade the node completely. This attack is totally different from the Sybil attack which consists of that a single Sybil node broadcasts many identities during the network period of life.

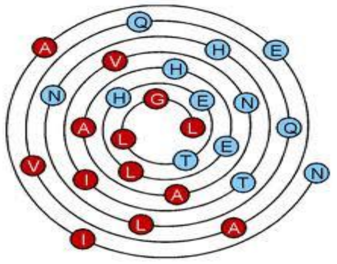


Fig 2: Node replication identification

Using Boom filter mechanism to detect the cluster node or replicated node in this network environment. It mainly focuses on minimizing the overhead communication compared to the other network. Mostly, hackers deploy them in the current network to launch a variety of inside attackers. By the way of algorithm in proposal work reduce the node capturing attack in percentage wise. Mostly replication attack deals with wormhole attack, it intimate a wormhole attack and inject false data into the source node. An adversary may replicate captured sensors and deploy them in the network to launch a tremendous amount of inside attackers in that particular source node itself.

1.2 Boom Filter

In previous days, there is no algorithm to detect the detection methods in smooth manner. At that time, no specific detection mechanisms are established; the attacker easily enters the node and corrupts the data. So the users are deciding to rectify the false rate in minimized way so use the boom filter. In this work, first introduce a one of the most familiar algorithm based on new hierarchical methods of distribution using a Bloom filter mechanism and those get the remedy for adversary attack.

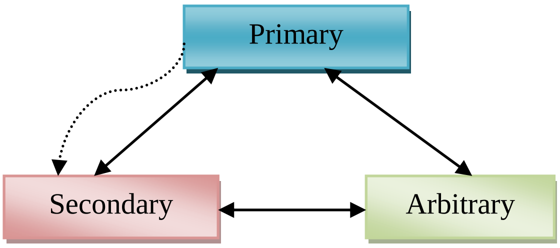


Fig 3: Adversary Attack

From the above diagram represent the adversary attack in three ways.Compression capability is one of the major advantages in Bloom filter. Generally Bloom filters are made up of elements and those elements are represented by an array representation of bits. Initially all these array values are set into 0. A Bloom filter uses different hash methods for getting the output value in the way of bits and maps. Each output is compare with other consecutive position of the array. Using wireless links the networks are composed at short distance with low cost. Mostly sensors are collect and transmit data of the physical world to one or more destinations are referred as sinks. Some of the adversary can create replicas and may be compromise the original node other than the cryptographic algorithms. For most of the places the same activities are going on so in this paper addresses the problem of nodes replication attack in efficient way.

2. LITERATURE SURVEY

Bettstetter et.al [1] discussed that RWP model in a formal manner as a discrete time stochastic process. Based on this derivation typical stochastic parameters of a source node. Using geometrical probability theory to calculate traveled distance and time during one movement transition to other movement transition in the manner of systematic approach. and compare those theoretical values with the graphical values and analyze the detection in duplicate way. In particularly, the equations are satisfy the given values but not to satisfy the current values for the expected value, variance and probability density function of the transition length. This paper fully discusses about the mapping function from one node to another in the same network where the scenarios are considered as both with and without meantime at the destination waypoints. Conti,M.[2] describes contributions of this work are classified as threefold. First, to analyze the properties of a distributed mechanism for the detection of node replication attacks in static manner. Second, analyze the requirements and known to find the solutions for concluding the requirement usages.To show that the known solutions for this problem do not completely meet our requirements. Third, that is to introduce a most efficient linear algorithm referred as RED (Randomized, Efficient, and Distributed protocol) for the detection of node replication attacks and that it is completely satisfactory the user needs in smooth manner.Yu, C.M. et.al.[3],describes the one of the most challenging problem is node cloning detection in infrastructed network. In this approach only few problems are satisfied so introduce new methodology in proposed scheme. In this paper, an Efficient and Distribute Detection (EDD) scheme is proposed to resist adversary against node replication attacks in mobile sensor networks. Finally compare the percentage of performance of EDD scheme with existing methods.Johnson D.B.[5] discussed that the adhoc network is a collection of wireless network and forming a temporary network without any help of established infrastructure or centralized network. In such a particular environment, it may be necessary for one mobile node and transmit the message to the host node. After that forward the individual packet information to its destination node. This paper introduces a protocol for routing purpose. In ad hoc networks mainly use the dynamic source routing protocol. The protocol hugely adapts the routing changes whenever necessary in the environment and reduces host movement in frequent manner. Depends upon the results from a packet-level simulation of mobile hosts are mainly operating in an ad hoc network, the new protocol performs very well in a variety manner of environmental conditions such as density rates, packet level, frameset and movement rates.Newsome,J.[6] analyzes the Sybil attack consecutively and its defenses in sensor networks. This paper creates the various forms of Sybil attack to analyze the following contributions for introducing taxonomy in systematic manner. To analyze the method for how to attack the node in this network.zeng, Y.et.al [7] explained to avoid existing drawbacks, and introduce the new replica-detection methods must be non-deterministic and fully distributed and satisfy the necessary security requirements based on witness selection. Randomized Multicast is the only protocol to fulfill their user needs and NDFD has very high communication overhead. Y.et.al propose two major protocols based on random walk, Random Walk (RAWL) and Table-assisted Random Walk (TRAWL), which fulfill the requirements while having only moderate communication characteristics and memory limits. The random walk creates the adversary cannot easily find out the critical witness nodes based on critical values. Nodes are theoretically the analyze the required number of walk step value for ensuring and acquiring detection. The first protocol, Random Walk, starts several random walks randomly in the network for each node *a*, and then selects the previous nodes and as compare the witness nodes of node *a*. Our walk steps are more sufficient to detect clone attacks with high probability and good way. The second protocol, Table-Assisted Random Walk (TRAWL), is based on previous protocol and adds a trace table at each node to reduce memory cost and communication overhead. Usually the memory cost is increased due to only the storage of location client areas. In TRAWL method captures the node only stores *O* (1) location. Our simulation results shows that our resulting protocols performance will the best result using NDFD protocol with LSM features depends upon choosing the witeness.The communication overheads of our protocols are slightly higher than LSM, but are not consider the previous topologies and existing methods.

3. EXISTING SYSTEM

In existing system mainly concentrate on the affects of black hole attack. The main features of the black hole attack is destroying the source node information without prior information to anyone and concentrate the outgoing and incoming signals from the source node. From those attacks the data may be corrupted or incomplete to reach the destination of the environment.

Two localised algortihms are used to detect the node replicas in mobile sensor networks, one is XED and another is EDD are proposed. Most of the techniques are developed in this current paper to avoid, challenge and response and encounter action are entirely different from the others in a localized manner. Each node in the localized algorithm is easily communicated with other node with help of its hop functions. This characteristic is mainly used for reducing the communication overhead significantly and enhancing the resilience against node compromise attack.

4. PROPOSED SYSTEM

In MANET, most of the replica allocation techniques are assuming that all mobile nodes cooperate fully in the network functionalities. Some nodes do not decide to cooperate partially or fully in the current situation Network performance and data accessibility are mainly affected by these selfish nodes in the way of using the strategic algorithm.

In this paper first capture the node and then detect the absence in the way of predefined methods. After that to check the temper resistance if the resistance is ready to available means to check the node replication. If it finds any selfish node in the current network to extract the information from captured node between shortest path of range between source and destination ,and to fulfill secret the information from captured node and deactivates the functionalities. Replica server sends signal to that selfish node using hardware and requests it make replicas of the captured node and deploy he replicas in efficient way. Finally detect the replicas using techniques to counter the number of replicas present in the network.

Consider the network with n number of inter connected nodes with different ID and the communication of each sensor is considered as both symmetric and asymmetric manner. When a node in the network is compromised it creates number of replicas. This paper detects clone replication attack in dynamic way. The network contains a mobile replica node s as a node having the same ID and secret keying materials as a mobile node s.

An adversary creates replica node s as follows: First compromises node s and extracts all secret keying materials from it. Then, prepares a new node s', sets the ID of s' to the same as s, and loads up’s secret keying materials into s' and create number of replicas in the same way and then inject the false data. The goal to detect the replicas in both s and s’ manner .In proposed system consists of six modules.They are Network Formation, XED Online, XED Offline, EDD Online, EDD Offline and Comparison.

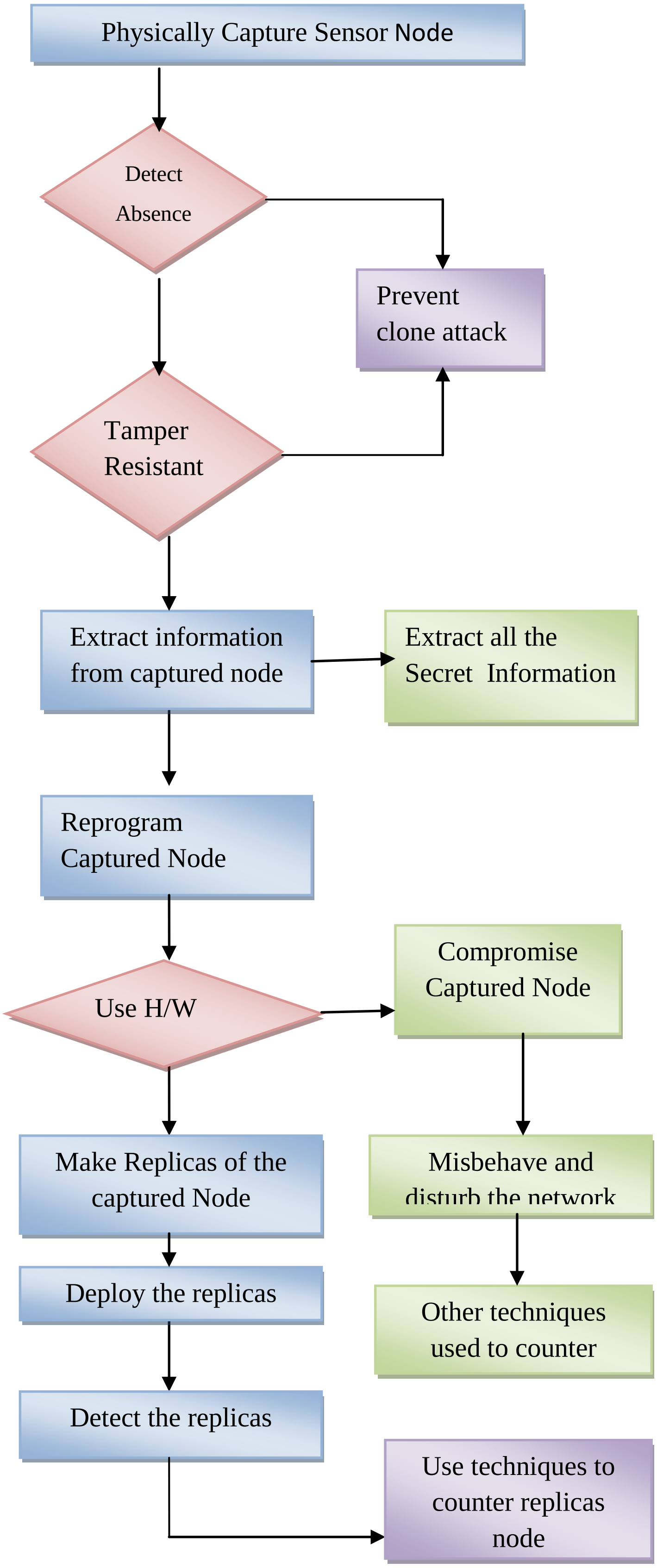

Physically Capture Sensor Node
Detect Absence
Prevent clone attack
Tamper Resistant
Extract information from captured node
Extract all the Secret Information
Reprogram Captured Node
Compromise Captured Node
Use H/W
Make Replicas of the captured Node
Misbehave and disturb the network
Deploy the replicas
Other techniques used to counter
Detect the replicas
Use techniques to counter replicas node

Fig 4: Existing System Methods

4.1 Network Formation

In this module the networks are formed based on the environment. The network consists of sensor nodes with IDs {1, n}.The communication is assumed to be symmetric. In addition, each node is assumed to periodically transmit t a message containing its ID and key values to its neighbor's node.

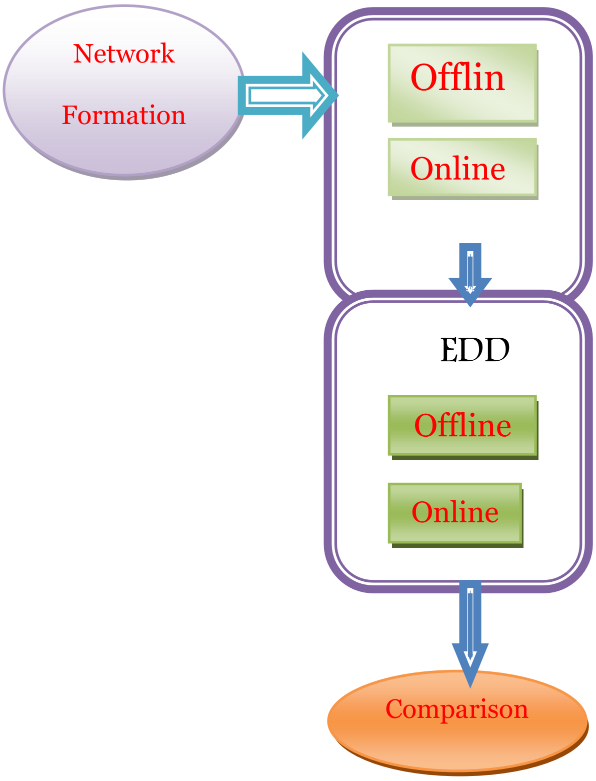


Fig5:Architecture Diagram

4.2 XED Online

In this step, u encounter the node v for the first time, u randomly generates and computes the cryptographic function. If it is first check, v is in the black list B $^{(u)}$.Then, Consider that node v is replicates. If not, precede the following procedures. A security parameter b and a cryptographic hash function h (.) are stored in each node. Additionally, two arrays, $O_r^{(u)}$ and $L_s^{(u)}$, of length n, which keep the received random numbers and the materials used to check the legitimacy of received random numbers, respectively, along with a set $B^{(u)}$ $O_r^{(u)}$ and $L_s^{(u)}$ are initialized to be zero-vectors. B $^{(u)}$ is initialized to be empty.

```
Algorithm: XED-On-Line-Step
Step:1 send $L_r^u[v1]$, $L_r^u[v_d]$ to[$v_{1\ldots\ldots\ldots}v_d$]
Step:2 receive $L_r^{v1}[u]$,….. $L_r^{(vd)}[u]$
Step:3 for k-1 to d
Step:4 if h ($L_s^{(u)}[v_k]$)=$L_r^{(vk)}[u]$
Step:5 Choose α £ [1,$2^b$ -1 ]&set $L_s^{(u)}$ [$v_k$] =α
Step:6 Calculate h(α) and send h(α) to vk
Step:7 else
Step:8 set β(u)= β(u) U {$s^{ki}$}
```

4.3 XED Offline

Initialize the blacklist B (u) is to be empty. Cryptographic function is denoted as h (.) Let us consider two array such as $Lr^{(u)}$ and $Ls^{(u)}$ with size of the length n.Using these arrays to check the random numbers legimate are not.

4.4 EDD Online

In next step i.e is online step performed in after sensor deployment in each node at each move. Each node checks its own between its neighboring node for its corresponding threshold. Finally analyse the number of encounters occur on each node.

```
Algorithm:EDD-On-Line-Step
Step:1 broadcast beacon $b_u$ contains the ID
Step:2 if t = t0
Step:3 receive beacons $b_{v2}\ldots b_{vd}$
Step:4 for k=1 to d
Step:5 $L^{(u)}[v^k] = L^{(u)}[v^k] + 1$
Step:6 if $L^{(u)}[v^k] > φ$ then $β^{(u)=}$ $β^{(u)}$ U {$v^k$}
Step:7 else // t = t0
Step:8 set $L^{(u)}$ [$s^k$] = 0, k=1….n.
```

4.5 EDD Offline

In offline step mainly performed in before sensor deployment. The goal of offline to calculate the parameter of each node, threshold, and length of the time interval. The calculating threshold is used for discrimination between the legimate node and the genuine node.

5. PERFORMANCE ANALYSIS

5.1 Good put

Generally it measures at the receiver rate in bits per second of useful traffic received. Good put excludes duplicate packets and packets dropped along the path.

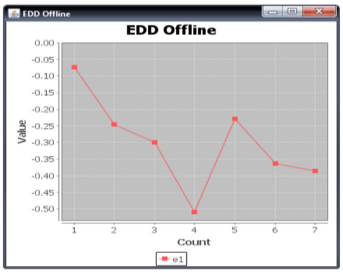


Fig 6: EDD Offline

5.2 Throughput

Number of jobs processed by the "system" per unit time and throughput is too high.

5.3 Response time

Time required receiving a response to a request.

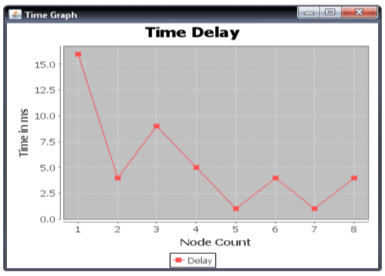
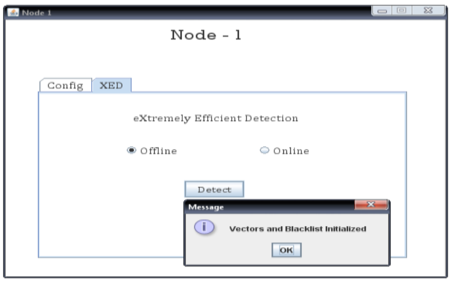


Fig 7: Time Delay

6. CONCLUSION

In this paper, our proposed algorithms are easily to identify the replicated node in the entire network in dynamic manner using MANET. In our survey all the existing methods are identify the replication attack in only static manner and also those methods are very difficult to implement in network environment. But in this paper, rectify the existing defects in dynamic manner in both effective and efficient way of techniques and also compare those results with other proposals of the literature. In this paper XED, examines the randomized number in the node and EDD analyses the threshold and its parameter depend upon its location and avoid synchronization in wireless sensor networks And reduce the overall traffic level data security in various ways in terms of malicious data replication/cloning attack, communication overhead and traffic data security .Finally shows the effectiveness of our algorithm and its energy efficiency.

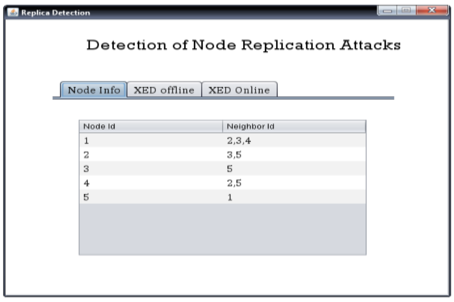


eXtremely Efficient Detection

● Offline ○ Online

Vectors and Blacklist Initialized

Fig 8: Detect vector and Blacklist



Detection of Node Replication Attacks

Node Id	Neighbor Id
1	2,3,4
2	3,5
3	5
4	2,5
5	1

Fig 9: Detect Node Replica Formation

7. ACKNOWLEDGMENTS

I would like to place on record my deep sense of gratitude to Mr.M.Balaganesh, Head of the Department, Computer Science & Engineering, Sembodai Rukmani Varatharajan Engineering college for his generous guidance, encouragement, help and valuable suggestions throughout.

8. REFERENCES

[1] Bettstetter, C. Hartenstein, H. and Costa, X. P. (2004) “Stochastic properties of the random waypoint mobility model, ” Wireless Netw., vol. 10, no. 5, pp. 555–567.

[2] Conti, M. Pietro, R.D Mancini, L. V. and Mei, A.(2007) “A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks,” in Proc. ACMInt. Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), Montreal, Canada, pp. 80–89.

[3] Yu, C.M. Lu, C.S. And Kuok, S.Y. (2009) “Efficient and distributed detection of node replication attacks in mobile sensor networks,” in Proc. IEEE Vehicular Technology Conf. Fall (VTC-Fall), Anchorage, AK, USA, pp. 1–5.

[4] Hu, Y.C. Perrig, A. et.al “Packet leashes:A defense against wormhole attacks in wireless networks,” in Proc. IEEE Int. Conf. Computer Communications (INFOCOM), pp. 1976–1986.

[5] Johnson D. B. and Maltz, D. A. (1996) “Dynamic source routing in ad hoc wireless networks,” Mobile Computing., pp. 153–181.

[6] Newsome, J. Shi, E. Song, D.and Perrig, A. (2004) “The Sybil attack in sensor networks: Analysis and defenses,” in Proc. Int. Conf. Information Processing in Sensor Networks (IPSN), Berkeley, CA, USA, pp. 259–268.

[7] Zeng, Y. et.al “Random-walk based approach to detect clone attacks in wireless sensor networks,” IEEE J. Sel. Areas Communication., vol. 28, no. 5, pp. 677–691.

[8] Zhang, M. Khanapure, V. Chen, S. and Xiao, X.(2009) Tinyecc: A Configurable Library For Elliptic Curve Cryptography In Wireless Sensor Networks,” in Proc. IEEE Int. Conf. Network Protocols (ICNP), Princeton, NJ, USA, pp. 284–293.

[9] M.Balaganesh and S.Nithyadhevi “A Survey of Node Replication Attack in Wireless Sensor Network “in International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682 Vol.18, No.18, October 2013.

[10] Xing K. and Cheng, X.(2010) “From time domain to space domain: Detecting replica attacks in mobile ad hoc networks,” in Proc. IEEE Int. Conf. Computer Communications (INFOCOM), SanDiego,CA, USA, pp. 1–9.