ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 5, May 2017

Detection of Clone Attack in Wireless Sensor Networks

[1]Vishakha Pawar, [2]Seema Hanchate
[1] Student,[2] Professor,ENC department, UMIT,SNDT
[1]vishakhapawar2008@gmail.com,[2] mshanchate@gmail.com

Abstract: **-- These Recent trends of wireless communication is Wireless sensor network,this is upcoming technology which has enabled the development of network with huge number of tiny, low power, multitasking sensor nodes. 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. Clone attack is node replication attack. 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. To protect network from clone attack is vital in WSN. The main objective of proposed clone detection protocol is to provide strong protection against clone attacks, high detection probability, low storage requirements with enhanced network lifetime by increasing energy efficiency with distributed detection mechanism.**

Keywords:— **Wireless sensor network, security, clone attack, distributed approach, networklife**

I. INTRODUCTION

Wireless sensor network is recently enhancing technology due to advancements in Telecommunication field, which has enabled the development of network with huge number of tiny, low power, 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.In this paper we are finding out some techniques which can be useful to overcome the clone attack. Solution should have low transmission overhead, while using reasonably small memory space, less power consumption and prolonged battery life with Good detection probability.

II. CHALLENGES OF WSN

The important challenges faced by WSNs are:

- Less power consumption
- Threat of failures of nodes
- Large scale network
- Survival in adverse environmental conditions
- Network lifetime
- Security of nodes

III. SECURITY THREATS IN WIRELESS SENSOR NETWORKS

The security of a wireless sensor network is observed by considering that an adversary is capable to capture a genuine sensor node or more. Since an adversary can capture the nodes in the network, it can definitely change replace or spoil any protocol running in the network.The attacker might read the cryptographic information from the memory of any node.The nodes under the attacker's control can easily damage the whole network.[3] Most of the network layer attacks in wireless sensor networks fall into one of the following categories:

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 5, May 2017

A. *Denial of Service*

Denial of Service (DoS) is occures because of the sudden failure of nodes or malicious action in network. The simplest DoS attack make an interruption in network to access the resources by sending extra unnecessary information and thus prevents authorized network users from accessing services or resources. DoS attack is meant not only for disrupt, or destroy a network, but also for activities that degrade the capability of network to provide service.

B. *Sybil Attack*

In many cases, the sensors in a wireless sensor network might need to work together to accomplish a task, hence they can use distribution of tasks and redundancy of data. In such a condition, a node can act to be more than one node using the identities of other legitimate nodes. This type of attack where a node forges the identities of more than one node is the Sybil attack. Sybil attack tries to degrade the integrity of data, security and resource utilization. Sybil attack can be performed for attacking the distributed storage, routing mechanism, data aggregation, appropriate resource allocation and misbehavior detection. Any peer-to-peer network is vulnerable to sybil attack.

C. *Blackhole/Sinkhole Attack*

Here, a malicious node acts as a sinkhole to attract the flows in the network. In this attack, the attacker listens to requests for routes then responds to the targeted nodes that it contains the highe energy or shortest path to the base station. Once the malicious device has been able to insert itself between the communicating nodes,it is able to do anything with the packets passing between them.In fact, this attack can affect even the nodes those are considerably far from the base stations.[3]

D. *hello flood attack*

This is the attack in sensor networks where protocols need nodes to broadcast HELLO packets to declare themselves to their neighborhood nodes in network, and a node which receives such packet may assume that it is within range of the sender. Flood attacker broadcast information could convince other node that the adversary is neighbor node in the network.

E. *Wormhole Attack*

This is the attack whrere the attacker records the information data at one location in the network and tunnels those to another location.The tunneling or retransmitting of bits could be done.This type of attack may occurred at initial state of network establishment.

F. *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]

Impact of Clone Attacks on WSN Security

WSN has some common security goals such as data confidentiality,authenticity,availability,availability,fressness, data integrity,scalability.in clone attack replica of original node can be deployed anywhere in network, so its very dangerous from the network security point of view.

IV. 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 neighbors. One or more of its neighbors 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].

Distributed 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. There are various protocols which works under distributed approach:

A. Broadcast Protocol

Each node in the network uses an authenticated broadcast message to flood the network with its location information. Each node stores the location information for its neighbors. If it receives a conflicting claim, it revokes the offending node[15].

B. Deterministic Multicast (DM) Protocol

Each node shares a node‟s location claim with a limited subset of deterministically chosen by witness nodes. When a node broadcasts its location claim, its neighbors forward that claim to a subset of nodes called witnesses. The witnesses are chosen as a function of the node‟s ID. If the adversary replicates a node, the witnesses will receive two different location claims for the same node ID.the mismatched location can found out as a clone.[15]

C. RED

In this protocol witnesses chosen pseudo-randomly based on a network wide seed. In exchange for the assumption that we are able to efficiently distribute the seed. RED is also more robust against attacks.[16]

D. Line Selected Multicast (LSM) Protocol

In this protocol, when a node announces its location, every neighbor first locally checks the signature of the claim and then forwards it to randomly selected destination nodes. Node replication is detected by the node on the intersection of two paths generated by two different node claims carrying the same ID and coming from two different nodes.

E. Hierarchical Distributed Algorithm(HDA)

This protocol has three steps. In the first step, all the material required for Bloom filter computations and for cryptographic operations follow the tree hierarchical architecture. The sensor nodes send their data only to their cluster heads. The cluster heads forward them to the base station. Cluster heads communicate with each other through dedicated paths and create a kind of tree with base station as a root. The detection is performed by the cluster nodes using a Bloom filter mechanism and based on the hierarchical architecture of the wireless sensor networks.

F. Cell based Identification of Node Replication Attack(CINORA)

In this protocol, location claim from the nodes are distributed among a subset of cells to detect any replication. These cells are generated from a non null intersecting subset algorithm. During the authentication phase, at least one cell receives conflicting location claims, if adversary has ever attempted to replicate a legitimate node[15].

Drawbacks of the protocols

The broadcast protocol has high communication and memory overhead for large sensor networks. Some protocols does not provide much security, adversary easily compromises witness nodes LSM are unable to detect masked replication attacks and sometimes location claims of clone nodes also received to the witness node[13]. The SDC protocol flooding only through the first copy of a node location claim arrives at the cell and the other copies are ignored. The node in the cell that first receives the location claim is unable to distinguish between claims of original and cloned node. In RED protocol the deterministic selection of witness nodes and its infrastructure for distributing random seed may not always be available. It is unable to detect masked replication attacks.

As we have surveyed that existing protocols are have issues of requirement of large storage space,networklifetime,protection against attack.So we are proposing clone detection protocol where we are tring to minimize above issues.

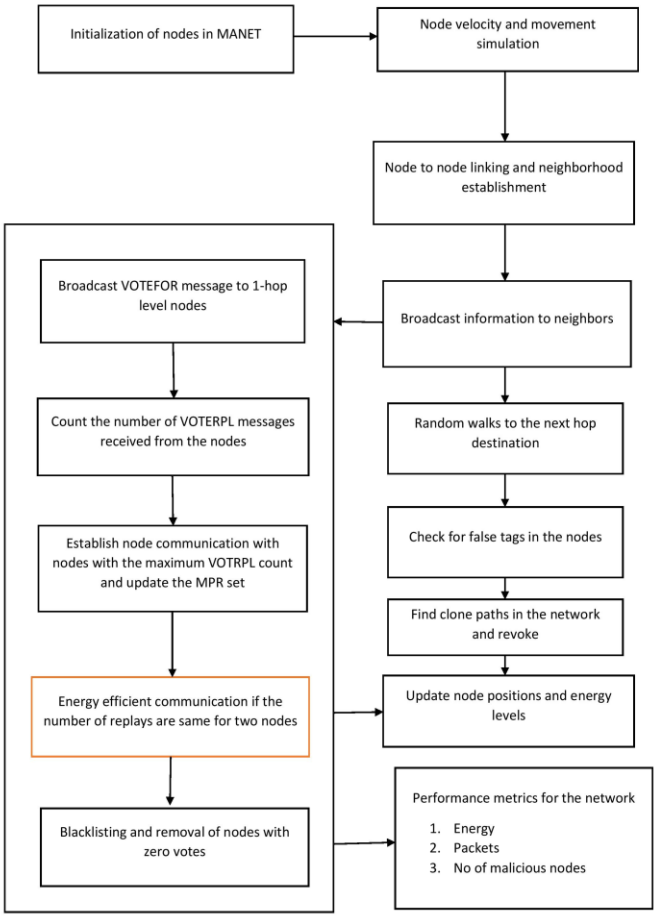
V. PROPOSED WORK

Security and data integrity are the major areas need to be concentrated while performing communications around WSNs.Low-Storage Clone Detection Protocol (LSCP) 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 via Advanced Encryption Standard (AES) algorithm. 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.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 5, May 2017

Block Diagram



proposed protocol consists of two components: 1) the witness building stage and 2) the clone detection stage.

1) Witness Building Stage:
The witness building stage can be divided into two stages:

Stage 1:In this stage node a route to the sink node.However, to confuse the adversary, in the protocol, node a does not directly route data to the node which are k hops away from the sink; rather, the following methods are used to enhance the security of the protocol. After node a is randomly routed a given distance using the random routing method, node a routes data to the nodes that are k hops away from the sink using a directional routing method.

Stage 2: The main task of stage 2 is to form a continuous length to the nodes that are k hops away from the sink. Similarly, to confuse the adversary, a routing path that cannot store the witness is formed at the beginning of the second stage; however, the true witness is stored in the node passed by in the last routing of the second stage.Therefore, it cannot compromise these witnesses in advance, thus achieving high security.

Clone Detection Stage: In this protocol, the main innovation is that the witness of each node is store in a route length.Considering that the the storage space required for storing the witnesses of nodes to minimize.Protocol requirement for storing the witness is not constant; it is related to the network scale so that the network lifetime can be improved.

VI. CONCLUSION

In the preceding discussion, we would like to explore a distributed approach of detection mechanisms to ensure that our protocols continue to function even in the face of powerful adversaries who can replicate node IDs. Proposed protocol will require lesser strorage space to lower the energy consumption to enhance the lifetime of the network.

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"

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#1,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 www.ijetsr.com 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)