International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 13, 2017 ISSN: 2348-6600
Reference ID: IJCS-218 PAGE NO: 1359-1364
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

A SURVEY ON SYBIL ATTACK AND DETECTION FOR SECURITY

K.Girija[1], K.S.Saravanan[2],
M.Phil Full time Research Scholar, PG and Research Department of Computer Science[1]
Asst. Professor, Department of Computer Science & Applications [2]
Vivekanandha College of Arts & Sciences for Women (Autonomous),
Tiruchengode,Namakkal-637 205,
Tamil Nadu, India
k.girija1993@gmail.com[1], Sarvkesh22022006@gmail.com[2].

ABSTRACT- Wireless sensor networks constitute of sensor nodes which are small in size, running on battery, limited computation power. we investigate, Sybil attack which is a node illegitimately asserts numerous characters and acquires multiple identities and performs as the original nodes causing disrupts in routing, voting, data leakage and data aggregation. Therefore the current research is going on how to handling the situation of different traffic levels and transmission power for security.

Keywords- Sensor network, Sybil attack, RSSI, TDOA,CRSD

I. Introduction

Wireless sensor network is distributed autonomous system, collection of sensor node that has densely deployed through the environmental phenomenon like physical, chemical and biological so which has simply sensing and communicating analysis by properties. This area is very useful to many applications like military application,environmental application, home based application etc…

There are the constraints in sensor node such as limited storage, low power, low latency, low bandwidth, low physical size and limited energy. These sensor node constraints are very obstacles to sensor security. There are different types of attacks has been happened while communication take place between among the node, whetherit is within communication range or out of range (i.e.) insider attack or outsider attack, so the security issues onrouting such as data aggregation, route discovery, are considered to be two types (i.e.) insider attack activities like as stolen the parameters of node, run code by malicious node which can be compromised by attacker node and outsider attack like as wormhole attack. In detail, the attacker can be classified according by different layers, the layers are physical layer, Link layer,Network and routing layer ,Transport layer and application layer.

topology management. So Security is important broadcast nature for wireless communication concern of the wireless sensor network. So these

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 13, 2017 ISSN: 2348-6600
Reference ID: IJCS-218 PAGE NO: 1359-1364
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

constraints are also very much challenges issues in security of
data dissemination etc.. Sensor network is based on wireless sensor network.Security is applied to the nodes depends upon rules and regulations to check whether the node is normal node or attacker node such as, to ensure that the data can be accessed by authorized person (confidentiality of data), to ensure that data can be obtained from correct source node (Authenticity of data), data freshness, data authentication, availability, self organization, time synchronization and secure localization.. The attacks

II.Various Attacks on wireless sensor network

A. Jamming:

Jamming node interrupt the entire network randomly because using the nature of interference on radio
frequencies, that it can be change the behaviour of node become a out of service.

B. Collision:

When node A have to communicate to node B at the same time node C communicate to node B for transmitting the packets, In this case, altering of packet transmission in-between the nodes, signal collisions has been take place, it leads to not able to communicate with each other.

C. Selective forwarding attack:

When node have to transmit the packets by multipath routing, in this mean time, any of the node may be
compromised by the attacker node, suppose if the node transmitted the packets by multiple nodes, in this meantime attacker could get the packets and which has dropping and transmitting the packets selectively. Therefore it could not relay the packets to correct path, at last it would not reach the correct destination.

D. Sinkhole:

This type of attack that number of attacker nodes will be covers the certain region by wrongly manipulated
information.

E. Wormhole:

This type of attack has replay attack, but this can bechanced into different part of the network

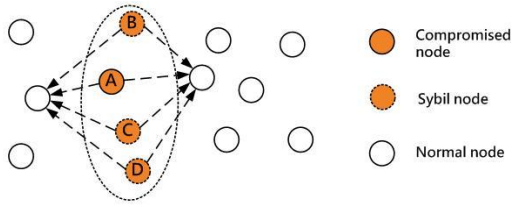
F. Sybil attack:

At the same time, same node acts as different one. This is one of the main attacks. Its present the introduction of Sybil attack,creation of Sybil nodes, and types of Sybil attack, some defense mechanisms.

III. Sybil attack

A Sybil attack is an attack which creates multiple identities from same malicious node. This attack is veryvulnerable to wireless sensor network because this nature could be gateway of any other attacks such as wormhole, sinkhole, selective forwarding etc… The Sybil attack was introduced by Douccer in peer to peer network, this attack makes more threatening problems in distributed storage, voting and resource allocation,same as appeared in wireless sensor network, and this was also identified by author Douccer.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 13, 2017 ISSN: 2348-6600
Reference ID: IJCS-218 PAGE NO: 1359-1364
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com



A. Creation of Sybil nodes in sensor network

There are several ways to creates Sybil attack in sensor network based upon the communication, simultaneity and fabricated identities. It shows that when one of the nodes communicate with other node (i.e.)one hop communication in that case any compromised node get the access from normal node and it would be easily get the information's from normal node such as position, id etc… by using this parameters attacker would be create a same type of identities and establish the attacks to normal node, at last it will confuse and corrupt the networks.

(i) Direct and indirect communication

In direct communication, Sybil node which has created by attacker and it has communicated to normal node,directly. In indirect communication, Sybil node could not directly communicate with normal node but via malicious node (intermediate node).

(ii) Stolen and Fabricated identities

Fabricated identities deals with creates new absolute identities with the help of attacker. Stolen identities deals from stolen the identities from legitimate node with help of malicious node. It would create a new identities as same as stolen identities.

(iii) Simultaneous and non simultaneous

Simultaneous means attacker creates multiple identities; those are participating in network at same time. Non simultaneous means attacker presents multiple identities; those are participating as one by one (certain amount of time).

B. Types of Sybil attack

There are different views of Sybil attack in wireless sensor network. To encounter the behaviour of
attacks in such as voting, distributed storage, data aggregation, voting, resource allocation and misbehavior detection.

(i) Distributed storage:

The attack has happens on data replication and data fragmentation. Data replication means that "consistency between excess resources by ensuring the sharing of information", it related to same data stored in multiple storages. Data fragmentation is same processing tasks, executes many times. In that case attacker listen the same computation of tasks, it will broadcast the identity and get the data from memory easily. While the system may be designed to replicated or fragmented the data across several nodes, it could be actually storing data on Sybil
identities generated by same malicious node.

(ii)Routing:

Sybil attack is forges to number of nodes with multiple identities while it is used by multiple alternate paths through a network. Geographical routing protocol and location based routing protocol are attacked by this Sybil attack because of multipath routing. During this routing, node can exchange the location information between the

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 13, 2017 ISSN: 2348-6600
Reference ID: IJCS-218 PAGE NO: 1359-1364
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

nodes and addressing the packets geographically. In that case, any one of the node send the packet to compromised node (handled by malicious node) and then attacker node is not transmitting the packet to correct
destination.

(iii)Data Summarization:
Data aggregation is a reduction tool to cost of communication is reduced, energy conserving and easily avoiding the redundancy of data. It is used to summarize the result by using queries from different deployment region through sensor nodes and then it will be passed the information on one node to another node, at last it reaches the base station . For example, forest fire detection. But any one of the malicious nodes has contributed to the aggregation information then the result will be wrong.

(iv)Voting:
Voting is the most one to take decisions by sensor network. It represent same node can handle the way more times.

C. Defense mechanisms:
This mechanism is handling by two ways such as direct validation and indirect validation. [4], [5], [6]:
Direct validation is the node directly validate the another node. Indirect validation states that node verifies by other node, not directly.
Sybil attack nature has number of Sybil node greater than the normal node when one of the nodes has
communicating with other node via broadcasting (Omni directional). So this case has been to detecting the malicious identities by collecting information from neighboring node. Because multiple identities created by each node that it has referred to as Sybil node. Neighboring information is used to avoid the less respected status of attacks in data aggregation and voting methods. The main concern is to concentrating the node density with the combination of Sybil nodes and normal nodes from that case to protect the normal node from Sybil node
collecting information from other nodes checked by threshold value. It overcome the some demerits such as takes communication time is less, subset of neighboring information it tolerates that size of the node density is high(not detect the Sybil node easily) But sometimes the range of communication makes impossible to detect the fake node is the worst case. A Sybil attack is detected when two or more different identities have almost the same position. Localization algorithm is used to detect and verify the physical location mapping from multiple node identities. RSSI and TDOA are the localization techniques.

(i)RSSI method:
From [7], RSSI (Received Signal Strength Indicator) is used for measuring the power level at different
time on same physical location. "RSSI is time difference and misleading nature" states that fakes node difference in radio transmission power. This is indirect validation. The issue is to find the absolute location of the fake (Sybil) node. RSSI handle multiple observer algorithms is to easily

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 13, 2017 ISSN: 2348-6600
Reference ID: IJCS-218 PAGE NO: 1359-1364
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

identify the fake node, because of this algorithm fake node cannot adapting the radio transmission power. Multiple receiver nodes has focus on same node as sending ID at different time by calculating the ratio of RSSI from heterogeneous nodes. It could be calculated in different cases according to the detection.

(ii)TDOA method:
From[8] TDOA (Time Difference on Arrival) is focusing on the issues such as communication overhead and memory. It is a lightweight solution. This is indirect validation. This technique is similar to RSSI but instead of observing the node from various receiver, time based position scheme is used here. TDOA has based to taken the centroids from different region and then detect the sybil node by calculating the ratio for finding out most densely deployed location and its error in same location, this location error has considered to be sybil node.

(iii)CRSD method
From[2] CRSD (Cooperative RSS based Sybil detection) is used to deduce the distance between two individual identities by using received signal strength. This assumption has fixed transmission power and static network. This is direct validation. The position could be determined when nodes have same position and distance relationships, to be as one group with help of RSS. First phase is periodical detection, the node group its neighbours and broadcast the group result. Second phase its group result has been received and node can be run for Sybil recognition (distrust group) as well as Sybil relaxation (Sybil group). Like each and every node has been grouped with the help of same RSS neighbor node information's. It protects the system performance that decreasing the probability of false positive rate and false negative rate.

(iv)K-mean method
From[1] K mean method is RSS based detection method. It is used to detect the attack according to the changes of transmission power and time variation. This detection is indirect validation. The decision has based on status of observation by different nodes. If the observation belongs to acceptance region it will be accepted,otherwise not accepted. This is formed by clustering method.

IV. Conclusion

In this paper, presents some little information about Sybil attack and detection method for security.
This discussion is fully based on only power level, not for cryptography. End to end security is not applicable for wireless network. Therefore, the development of protocol is carefully design; need to concentrate on routing and data aggregation with respect to security.

V.References

[1] Yingying chen, "Detecting and localizing identity-based attacks in wireless sensor network",IEEE Journal, June 2010.
[2] Shaohe Lv, "Detecting the Sybil attack cooperatively in wireless sensor networks", IEEE Conference, June 2008

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 13, 2017 ISSN: 2348-6600
Reference ID: IJCS-218 PAGE NO: 1359-1364
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

[3] Dr. Manoj Kumar Jain, "Wireless Sensor Networks: Security Issues and Challenges", IJCIT,2011.
[4] Y.Zhou, Y.Fang, Y.Zhang, "Security Wireless Sensor Networks: A Survey", IEEE Communication Surveys, Vol.10, No.3, 3rd Quarter2008.
[5] J. Newsome, E. Shi, D. Song and A. Perrig. "The Sybil Attack in Sensor Network: Analysis & Defenses". In IPSN'04
[6] Karen Hsu, "Security Analysis on Defenses against Sybil Attacks in Wireless Sensor networks"IEEE Journal, 2008.
[7] M. Demirbasand Y. Song. ,"An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks", IEEE Journal,2006.
[8] WEN Mi,LI Hui, ZHENG Yan-fei, CHEN Ke-fei, "TDOA-based Sybil attack detection scheme for wireless sensor network",IEEEJournal 2006.