ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 2, February 2013

An Enhanced and efficient mechanism to detect Sybil attack in Wireless Sensor Networks

Heena Sharma, Awan Dhawan

Abstract-- Wireless sensor networks are used for many different applications these days such as in environment applications, military applications, queue tracking, etc. In today's scenario, security in WSN is one of the major issue.WSN are vulnerable to different types of attacks due to various constraints such as low battery power, less memory, and associated low energy. These attacks lead to decrease in performance of the network, decrease in packet delivery rate. Sybil attack is one of the attacks in which a node forms its multiple identities in the network and thus leads to decrease in performance of the network. Balachandran Nitish et.al discussed various techniques to mitigate Sybil attacks such as trusted certification, resource testing, privilege attenuation, RSSI scheme, random key distribution. By detecting this attack performance of the network can be increased. Also packet drop can be reduced.

Keywords: Wireless sensor networks, Sybil attack, WSN security, security threats, various attacks

I. INTRODUCTION

Wireless sensor networks(WSN) is a collection of sensing devices that communicate wirelessly in which each device can sense, process, and talk to its peers. A sensing node has basic components: a central processing unit, a radio transceiver, and a sensor array. Nodes are normally battery-powered.

In Wireless Sensor Networks, number of wireless sensors uses radio link to communicate with each other. In today's scenario Wireless Sensor Networks are being used for vehicle tracking, detecting vehicular movements, measuring pressure, humidity, scientific explorations. There is a probability of occurring various types of attacks in Wireless Sensor Networks. Each layer of OSI model faces different type of attack. While employing major security for these attacks Wireless Sensor Networks faces major challenges such as size of sensors, memory processing power, various tasks expected from sensors.

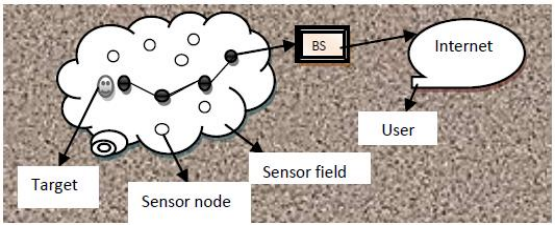

Figure 1 architecture of WSN

A. Security requirements in Wireless Sensor networks

The major security requirements in Wireless Sensor Networks are to provide confidentiality, integrity, authenticity in the presence of available resources. Providing security is a major challenge in wireless sensor networks due to factors such as resource limitation on sensor nodes, size and density of networks. All messages need to be encrypted and authenticated to provide security in wireless sensor networks. Following may be the security requirements:

Authentication:-

Authentication is necessary during the exchange of sensitive information in network. The receiver nodes always need to ensure that the data is originated from correct sender.

Integrity:-

Integrity ensures that during the data exchange any adversary may not change the data i.e data is not altered. For example new fragment of data may be added to the packet by some malicious node.

Confidentiality:-

Confidentiality is extremely essential as the nodes may exchange highly sensitive data as in military applications. To achieve it we may use various cryptographic techniques.

Self Organization:-

Wireless sensor networks must organize themselves according to the environment as in Wireless sensor networks no fixed infrastructure is available due to random deployment of nodes.

Scalability: Scalability means that if network size grows, it should not increase the chances of node compromise should not increase communication overhead. It should allow nodes to be added in network after the deployment as well.

B. Security threats on network layer in wireless sensor networks

Sybil attack:- In Sybil attack malicious nodes pretends to be multiple nodes by taking multiple identities. [Jetter Oliver, et al.(2010)] In peer to peer systems, due to lack of central authorization authority these systems are vulnerable to these attacks. [Yu Haifeng et. al(2008)] Sybil guard protocol can be used as a defense against Sybil attacks which bounds the number of Sybil nodes accepted. To limit the effect of Sybil attacks effectively they use distributed approach. Sybil attack is major challenge in facebook social networking sites.

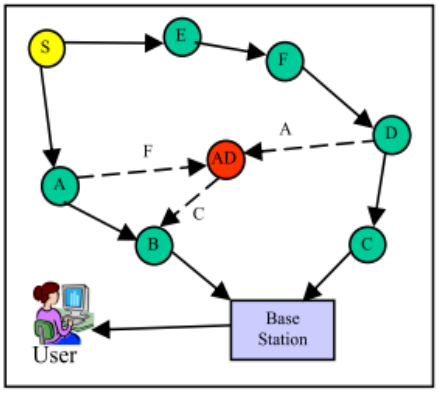

Figure 2 Sybil attack

(i) Wormhole attack:-

In this attack, attacker receives packet at one point in the network and tunnels them to another point in the network. To detect this attack they use mechanism of packet leashes which can be further divided into geographical and temporal leashes that are used to restrict the maximum transmission distance of a packet. In this, node with out of band communication links show themselves as neighbors by recording packets and then replaying them. [Naït-Abdesselam Farid et al.(2008)] Use OLSR protocol to detect this attack in suspicious links.

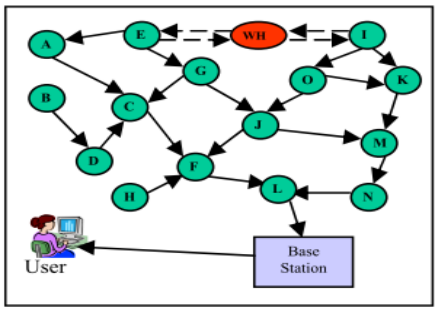

Figure 3Wormhole

(ii) Flood attack:-

In this attack large numbers of requests are send by malicious clients in order to create congestion to the target server. [Argyraki Katerina et al.(2009)] AITF (Active Internet Traffic Monitoring) is a defense mechanism against this attack which enables malicious clients to stop sending packets and asks each source for policy by its own internet service provider (ISP).[Yatagai Takeshi et.al(2007)]Example- HTTP-GET flood attack in which malicious node send large number of requests to web server

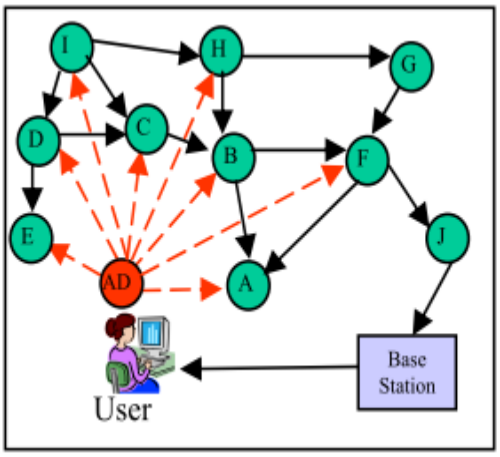

Figure 4 Flood attack

(iii) Sinkhole attack:-

In sinkhole attack, a node is placed at centre that attracts all the traffic moving from base station through sensor nodes. In this attacker creates a sinkhole usually near the base station where it attracts the whole traffic. Wireless sensor networks are susceptible to this attack as they use specialized communication patterns for transmission [Mohantany Prabhudutta et.al].

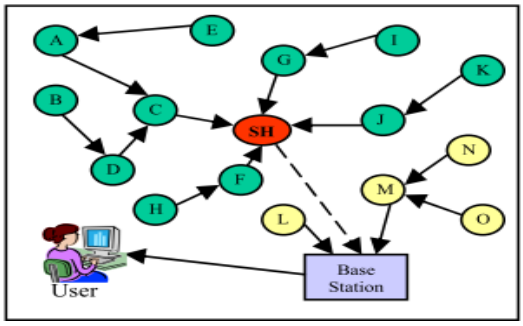

Figure 5 Sinkhole attack

(iv) Selective forwarding attack :-

Multi-hop mode of communication is commonly preferred in wireless sensor network data gathering protocols. Multi-hop networks assume that participating nodes will faithfully forward and receive messages [Mohantany Prabhudutta et al.]. However a malicious node may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. This attack can be detected if packet sequence numbers are checked properly and continuously in a conjunction free network. Addition of data packet sequence number in packet header can reduce this attack.

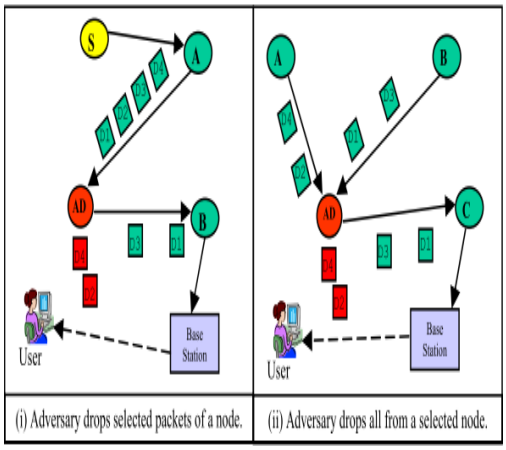

Figure 6 Selective Forwarding attack

II. PREVIOUS WORKS:

Khan Pathan Al-Sakib et al., (2006) discuss basic security schemes in WSN such as cryptography, steganography. They [4] discuss various security attacks in WSN such as Sybil attack, wormhole attack, sinkhole attack, HELLO flood attack, denial of service. Singh Saurabh, et al.(2011) discuss various applications of WSN[11] such as military applications, health applications, scientific applications, environment applications, area monitoring and various security requirements such as integrity, confidentiality, authenticity, scalability in WSN. Pramod A.V, et al., (2012) discussed an approach to detect Sybil attack the Wireless Sensor Network (WSN). They represent a protocol for two cases: single node observer and[8] multiple node observer in which they use passid of every node entering, use the concept of affinity between nodes, use the time bucket to observe the behaviour of each node.

III. PROPOSED WORK

A. Research Methodology:

Under the proposed work, the single node that wishes to detect the presence of a Sybil attacker in the network will record the identities of all other nodes it hears broadcasting after a series of time intervals[Piro Chris et.al(2006)]. A complete record of all data transferred may not be needed. There will be a time bucket known as observation period that will be long enough to capture the likely behaviour of all normal node that includes normal data flow, regular HELLO messages and other periodic route requests for nodes that have data to send[Pramod A.V et.al (2012)].

After a sufficient observation period, which consists of a number of buckets, the clustering of nodes will be done to determine Sybil nodes. The length of the observation period depends on the amount of mobility within the network; highly mobile networks need fewer intervals than more static networks. Then various clusters of the nodes will be formed using k means clustering. After different clusters will be found, DFS algorithm will be used to find cluster with maximum connected components. The one with maximum connected components will be taken as a Sybil attacker.

B. SOLOTION:

Due to various resource constraints in WSN, they suffer from different types of attacks and Sybil attack is one among these attacks on network layer a has different composition from other attacks. Sybil attack can disrupt various operations such as data aggregation, fair resource allocation scheme, misbehaviour detection and routing mechanisms in a network. In Sybil attack, a node multiplies its identities and thereby decreases the performance of the network, increase packet drop, decrease throughput of the network. Piro Chris (2006)

discussed that Sybil attack can occur in a distributed system that operates without a central authority to verify the identities of each communicating entity. The proposed technique will detect the Sybil attack and than the behaviour of WSN will be analysed with and without attack and the performance of the system will be analysed.

IV. CONCLUSION

Due to various resource constraints in WSN, they suffer from different types of attacks and Sybil attack is one among these attacks on network layer a has different composition from other attacks. Sybil attack can disrupt various operations such as data aggregation, fair resource allocation scheme, misbehavior detection and routing mechanisms in a network. In Sybil attack, a node multiplies its identities and thereby decreases the performance of the network, increase packet drop, decrease throughput of the network.

The proposed technique will detect the Sybil attack and then the behaviour of WSN will be analysed with and without attack and the performance of the system will be analysed. This research is helpful to analysis the behaviour of WSN without any attack in WSN after the deployment of WSN without any attack.

REFERENCES

[1] Argyraki Katerina, Cheriton David R. (2009), "*Scalable Network-Layer Defense Against Internet Bandwidth-Flooding Attacks"* IEEE/ACM TRANSACTIONS ON NETWORKING ,pp. 1284-1297.

[2] Balachandran Nitish, Sanyal Sugata (2012)"*A Review of Techniques to Mitigate Sybil Attacks*" IntJ advanced networking and applications, pp.1514-1518.

[3] Jetter Oliver, Dinger Jochen, Hartenstein Hannes (2010) "*Quantitative Analysis of the Sybil Attack and Effective Sybil Resistance in Peer-to-Peer Systems*" IEEE , pp.1-6.

[4] Khan Pathan Al-Sakib , Lee Hyung-Woo , Hong Choong Seon .(2006) *"Security in Wireless Sensor Networks: Issues and Challenges"* ICACT, pp. 1043-1048.

[5] Maraiya Kiran, Kant Kamal, Gupta Nitin(2011)" *Application based Study on Wireless Sensor Network"* International Journal of Computer Applications, pp. 9-15.

[6] Mohantany Prabhudutta, , Panigrahi Sangram, Sarma Nityananda and Sankar Satapathy SIiddhartha (2005 - 2010)"*Security issues in wireless sensor network data gathering protocols: A survey*" Journal of Theoretical and Applied Information Technology JATIT, pp. 14-27.

[7] Naït-Abdesselam Farid, Bensaou Brahim, Taleb Tarik (2008), "*Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks"* IEEE Communications Magazine, pp. 127-133.

[8] Pramod A.V , Azeem Abdul, Prakash M. OM (2012) "*Detecting the Sybil Attack in Wireless Sensor Network*" International Journal of Computers & Technology , pp. 158-161.

[9] Piro Chris, Shields Clay , Levine Brian Neil(2006), "*Detecting the Sybil Attack in Mobile Ad hoc Networks*" IEEE, pp. 1-6.

[10] Sharmila S., Umamaheswari G (2012)"*Detection of Sybil attack in mobile wireless sensor network*" [IJESAT] INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE & ADVANCED TECHNOLOGY, pp. 256 – 262.

[11] Singh Saurabh, Dr. Verma Harsh Kumar .(2011) "*Security For Wireless Sensor Network*" International Journal on Computer Science and Engineering (IJCSE), pp. 2393-2399.

[12] Yatagai Takeshi,. Isohara Takamasa, and Sasase Iwao (2007) "*Detection of HTTP-GET flood Attack Based on Analysis of Page Access Behavior"* PACRIM'07 , pp. 232-235.

[13] Yu Haifeng, Kaminsky Michael, Gibbons Phillip B. , Flaxman Abraham D.(2008). *"SybilGaurd: Defending against Sybil attack via social networks"* IEEE/ACM TRANSACTIONS ON NETWORKING, pp. 576-589.

Author Description

Heena Sharma, Research Scholar, Done B.TECH (CSE) from L.L.R.I.E.T, (PTU). Now doing M.Tech(CSE) from L.L.R.I.E.T (PTU), Punjab, India, Research area is Data Mining.

Co-Author Description

Awan Dhawan, Research Scholar, Done B.TECH (ECE) from RIMT-Maharaja Aggrasen Engineering College (**RIMT-MAEC**), mandi gobindgarh. Now doing M.Tech(ECE) from Al-Falah School of Engineering & Technology (AFSET), India,