Study on Security Protocols in Wireless Sensor Networks

C.Dhivya Devi [#1], B.Santhi* [2]
#Computer Science & Engineering, School of Computing,
SASTRAUNIVERSITY,Tirumalaisamudram, Thanjavur - 613401.Tamilnadu, India.
1 divyamtech89@gmail.com
*Computer Science & Engineering, School of Computing,
SASTRAUNIVERSITY,Tirumalaisamudram, Thanjavur - 613401.Tamilnadu, India.
2 shanthi@cse.sastra.edu

***Abstract*— The extremely undefendable to attacks which is being composed of hundreds and thousands of tiny sensory nodes with less energy, memory and power is the existence of wireless sensor network. The area covered by WSN application has raised the level of security to the adoption and consumption of sensor networks without any interrupts throughout the wide area of occurrence. Sensor networks are interacting with very sensitive data and deployed in hostile unattended environments, where the security issues should be concentrated to attain their potential. This paper lights a torch on security of WSN and different attacks in it and mainly focuses on the effect of Denial of Service (DoS) attacks, which is caused by a flood attack where there is a composition of many illegitimate nodes sits inside the network can produce traffic and dampen the security of WSN. On behalf of the security aspects, this paper also has concentrating on the anatomy of security protocols.**

Keyword- Denial of Service, Adversary, Security, Throughput, Flooding attack, Routing protocols.

I. Introduction

WSN is a substantive part of the network, popped out with a smatter application such as medical applications, environmental pollution detection, agribusiness etc., Even there is a presence of confinements over characteristics like battery power, low energy consumption which calls for a lot of care to keep off network’s life time reduction profiting from security issues in wireless sensor networks.

To get the better of performance in WSN, it is a mandate thing to provide a good path. Here this paper heels on flooding attack which would have done by constructing a path , since the wireless sensor networks has invested on various kinds of attack.

To demonstrate the data flooding attack, an illegal node create a route to the prey node and starts sending an enormous incorrect data packets to the prey node through that route. Because of this action, definitely the attack will bring down the functioning level of the network to an unexpected situation. Here the security issues should be considered over a given network for the creation of goodly environment in wireless sensor networks.

In this paper composition, Section II and III focalises the goals of the security which insisted on the wireless sensor networks along with the attacks where it have been classified on the basis of general categories respectively. The position of attacks on routing protocol have been illustrated along with a keen look on flooding attack by keeping it as major work in Section 4 whereas Section 5 concludes this paper.

II. WSN Security goals

Security goals guarantee the Confidentiality, Integrity, Authenticity, Availability and Freshness of data.

A. *Confidentiality*:

Confidentiality means bounding the data access and revealing only to authorize users and preventing from unauthorized folks. Data Confidentiality [1, 4, 5, 14, 15, 16] is obtained in WSN with the help of the following statements:

1. Data should be restricted within the network.
2. Secure Connection for key management.
3. Keys should be convertable with respect to the layered attacks.

B. *Integrity*:

Integrity [1, 4, 5, 14, 16] means trusting the data resources. It has two types

- Data integrity
- Source integrity

Data integrity means refers to the data is not altered by an accident or any malicious activity. Source integrity means data is only originated from the trusted person or source.

Integrity actually means the concept of validity, which includes preservation not corruption of data during transmission or reception.

C. *Authenticity*:

Authenticity [1, 4, 5, 14, 16] allows the receiver to maintain the origin of data which involves more than one proof of identity. It may be a password or a key known only the user.

D. *Non-repudiation*:

The sender cannot falsely refuse transmission of information. It can be achieved through digital signature which is a function of unique identifier for each individual similar to a written signature. [1, 16].

E. *Availability*:

Availability [5, 14, 16] refers to the availability of data resources. Data should be available always to the legal users throughout the network even if there occurs internal or external failures, faults, errors or attacks.

F. *Freshness*:

Data freshness [1, 5, 14] assures that the data received during exchange is raw and no opponent has used it. In wireless sensor network the data’s are not transferred with a given time interval, so we must guarantee that it is fresh. To achieve this nonce or time stamp are used. It consists of two types. Weak freshness provides a little order for the data’s so delay cannot be calculated, whereas strong freshness provides a general order and allows the calculation of delays.

III. Different Attacks in WSN

There is a rapid increment of vulnerability in the WSN due to the placement of nodes in an unattended and dangerous or unfriendly environment since the nodes are not safe inside the region. Though the reaction can be overwhelm by taking the security concepts into account which plays a vital role in the WSN.

Attacks on WSN is can be classified into active attacks and passive attacks. Fig. 1. shows the general categorization of attacks.

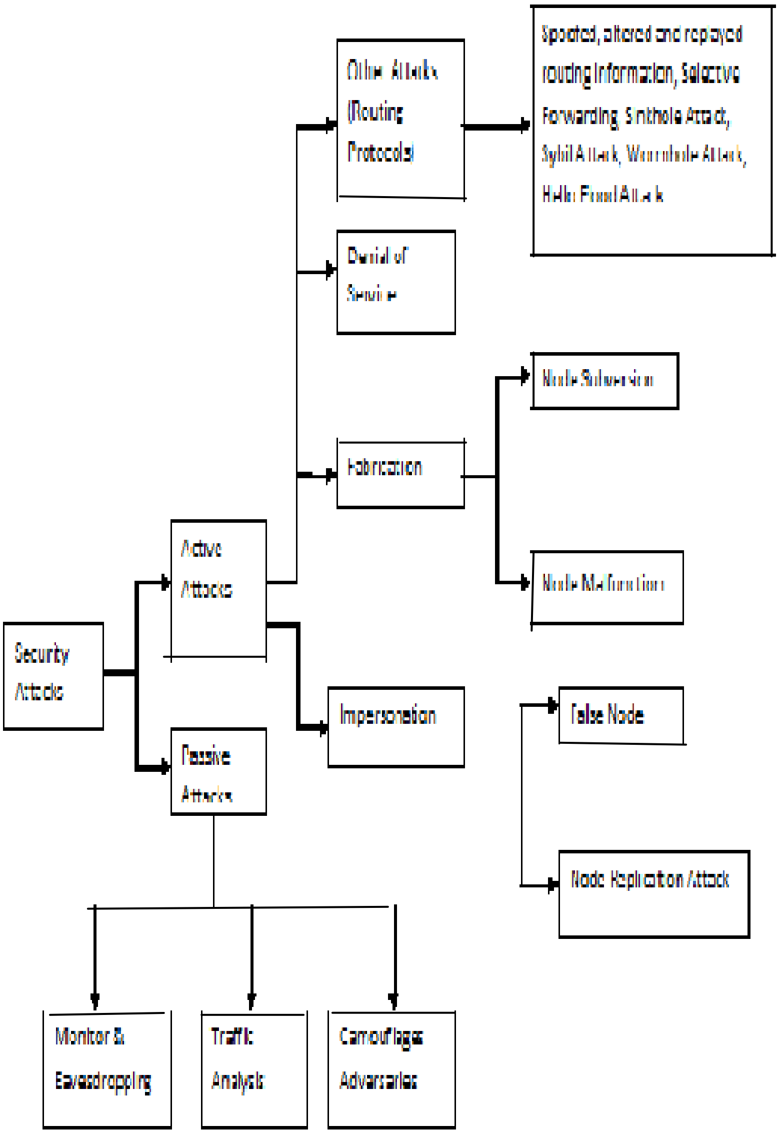

Fig. 1. General Categorization of Security Attack

A. *Passive Attacks*:

A passive attack defines in [16, 12] which holds the data switched over in the network without interrupting the operation of the communication.

1) *Monitor and Eavesdropping*:

The frequently used attack to privacy is the Monitor & Eavesdropping. Here, the adversary who could easily bring out the communication message by spying to the data. The Eavesdropping can act efficaciously against the privacy protection. [12]

2) *Traffic Analysis*:

Communication patterns is used to analyse and left over with a eminent possible actions even though after the transferred messages have been encoded, which can be used further by an adversary who have the ability to bring the harmful effects to the network. [12]

3) *Camouflage Adversaries*:

One can repelled and enter the network area by inserting the node or comparing with the other nodes to cover in the network. Then these nodes can change him as a legal node and starts to get attracted towards the packets will leads to misrouting of packets in the network. [12]

B. Active Attacks :

The active attacks in [16, 12] states that the unauthorized attackers involves information suspension, alteration assembling the data packets during the effective communication. The types of active attacks are as follows:

1) *Routing Attacks in sensor networks*:

The routing attacks present in the network layer with the following list of attacks.

a. *Spoofed, altered & replayed routing information*:

The most outstanding attack on routing is to alter, spoof, or just replay routing information is known as false routing information [2, 4, 5, 10, 12, 14, 15, 16]. Malicious nodes simply,

- Drop data packets quietly
- Modify data content
- Generate false error messages
- Traffic redirections

b. *Selective forwarding*:

A venomous node which behaves like black hole can compromise the other nodes by creating an illusion that it is still active by forwarding only selective packets and that data can be routed via it. Introducing redundancy to the network in the form of multi-path routing will reduce the effort of selective forwarding attack in the WSN. [1, 2, 4, 5, 8, 10, 12, 14, 15]

c. *Sinkhole attack*:

In the sinkhole attack, the adversary's aim is to decoy nearly all the traffic from a particular area through a compromised node, creating a false sinkhole with the adversary at the centre. If the enemy node does not introduce itself as the sink, the node closer to the sink will make more interruptions in the network because the traffic absorbed by enemy node will be more. [1, 2, 4, 5, 8, 10, 12, 15, 16].

d. *Sybil attack*:

Node replicates itself and involves their existence in the different locations. In other words it is defined as a "malicious device illegitimately taking on multiple identifiers". The existence of this attack is at physical layer, data link layer and network layer.

The solution for Sybil attack is to verify the identities of participating nodes by having each node share a unique key with the base station. Two neighbouring nodes then communicate with each other using a shared key to encrypt and verify the link between them [1, 2, 4, 5, 8, 10, 12, 14, 15].

e. *Wormhole attack*:

In the wormhole attack, an adversary burrows messages over a low latency link which have been received in one part of the network and plays back them in a different part. Wormhole attack is very difficult to detect because it uses out-of-bound channel to route packets. An adversary records packets or bits from whatever location in the mesh that can perforate them to another location and conveys them into the network [1, 2, 4, 5, 8, 10, 14, 15, 16].

f. *Hello Flood attack*:

It is a novel attack against sensor networks. The unidirectional connections between nodes are highly utilized by this attack. Nodes broadcast hello packets with the help of routing protocols to announce themselves to their neighbours and a node inviting such a data packets may assure that it rests inside the (normal) radio range of the sender. Hello flood attack will taken part in the network layer [1, 4, 8, 10, 14, 15, 16].

This attack will increases the delay since the messages are need to be routed mulit-hop to their parent nodes. The avoidance of this attack can easily be avoided by verifying the bi-directionality of a link through identity verification protocol before taking action based on the information received over the link.

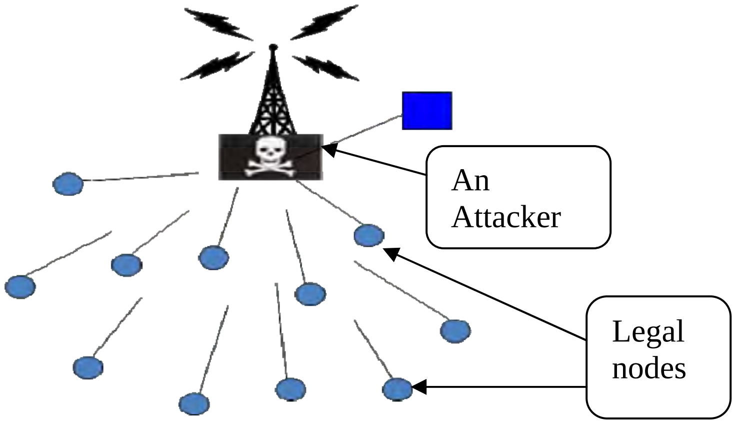

Fig. 2. Illustration of Hello Flood attack

2) *Denial of service attacks*:

It is an event that belittles or eradicates a network's capacity to perform its expected function. Its act as a path for the adversary to subvert, disrupt or destroy a network. Black hole, resource exhalant, sinkhole, wormhole, flooding, routing loops are the different types of DoS [3, 8, 10, 12, 14].

3) *Node subversion*:

An intruder may expose all the encryption information, secret keys and algorithm by captivating a true node in the network. The adversary use the true node itself as an attacker to launch an inside attack [3, 8, 12].

4) *Node malfunction*:

A malfunctioning node will generate the incorrect data which could expose the integrity of sensor networks by including dropping data packets at a high rate, denying packet forwarding requests. This will affect the performance of the network. [3, 12].

5) *False node*:

A false node involves in appending the illegal node in the network which created by an adversary and starts pushing t he malicious data which results to a communication bottleneck, false location claims and bring the network performance to the lower level. [3, 8, 12].

6) *Node replication attack*:

Node replication attack is defined as an attacker may add-on the malicious node into the network by imitating the identity of a true existing sensor node. That node will starts to create a problem to a WSN in various ways including message corruption, injection of fake data, deviating the packets direction to other nodes and so on.[3, 12]

IV. ANALYSIS

The perspective view and analysis of flood attack by different authors in different papers have been listed in the TABLE I with the brief descriptions as follows.

TABLE I
Analysis of Methods

S.No	Author name	Method
1.	Revathi et al.:[13]	Extended DSR is implemented in ad hoc network.
2.	Virendra Pal singh et al:[9]	Detection of hello flood attack on signal strength and client puzzle method.
3.	Mohamed M.Ibrahim et al:[11]	REHIDAN algorithm to identify flooding attacker nodes.
4.	H.Kim et al.:[7]	PDM novel Period based Defense Mechanism.
5.	Vuanyuan Zhang and Wassim Znaidi [6]	Multi path ACK scheme

DESCRIPTIONS:

The brief descriptions for the methods listed on above table are as follows:

Method 1:

Dynamic Source Routing uses source routing rather than on the routing table at each intermediary device. In[13], the author have considered the neighbouring nodes as strangers, acquaintances and friends with different threshold values by implementing the algorithm in both RREQ flooding attack and DATA flooding attack using the extended DSR protocol.

The following Fig. 3., shows the performance analysis(evaluation) of throughput by varying the parameters such as number of malicious nodes, number of connections and mobility of nodes excluding the measurement of time, using extended DSR rather than regular DSR.

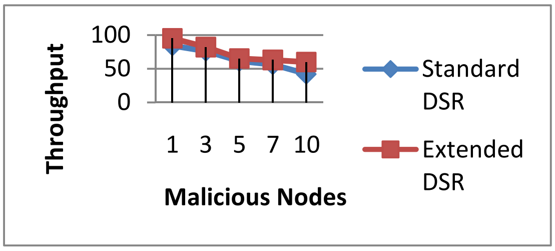

Fig. 3. Malicious nodes Vs Throughput

Method 2:

The authors have considered some primary assumption such as all sensor nodes are homogeneous, communicating within a fixed radio range which knows the fixed signal strength along with a time threshold, to detect the hello flood attack which is grounded on signal strength and client puzzles method in [9]. He uses the two ray propagation model to calculate the signal strength.

If the node receives hello message, have the signal strength equal to that of fixed strength, then it comes under stranger or a friend. Short client puzzles that need less computational and battery power is highly suitable to check the validity of suspicious nodes. The difficulty of puzzles can be made using Dynamic policy technique allotted to the strangers based on the number of hello messages sent.

Method 3:

The Ad hoc On- Demand Distance Vector Routing protocol have the ability to forward the data packets in dynamic network topology, but it could not address all the possible attacks. To overcome the above problem, the Real-time Host Intrusion Detection for Ad hoc Networks (REHIDAN) algorithm is used in [11], to minimize the effectiveness of the attacks. Intrusion detection approach having the functions like Monitoring, analysing, assessing, recognizing, and tracking are examined by author. The REHIDAN algorithm in [11], uses the idea of neighbour suppression algorithm isolating through which, the attacker is isolated from the neighbour nodes. It is implemented, with OPNET.

Method 4:

The main concept of Period based Defense Mechanism (PDM) in [7], is data flooding attack , where the adversary itself first set up the path to all the nodes and starts to send useless packets along the path. The path cut off mechanism is used as a defense against data flooding attack. FAP is not able to distinguish burst traffic from attack traffic.

Method 5:

The main aim of network coding in [6], is to find optimal information dissemination in the network where two information flows are identified. It is intrinsically resistant to selective forwarding adversaries that drop packet in the data flow, due to its multipath nature. Multi-hop multi-stream unicast routing protocol, gradient based routing protocol are used for implementation.

V. Conclusion

Security in WSN is vital to maintain the good performance of the entire wireless network. Many authors survey work has been studied. In particular, this article have concentrated on the Hello flood attack which relies on the network layer to briefly illustrate the methods and protocols that have been implemented in different papers from the different perspective view of different authors which will take the performance of the network to the next higher level. Our future is based on the mobility of the nodes along with the time measure to exclude the adversary from the network through the identification of the malicious nodes via signal strength comparison. The client puzzle method is used for each node, based on the number of hello messages sent and the difficulty of puzzle can be adjusted by applying the Dynamic policy technique which increases the throughput of the network by considering different routing protocol at different aspects to achieve the suspected output from the performance of the network.

References

[1] Jalil Jabari Lotf, Seyed Hossein Hosseininazhad Ghazani, “Security and Common Attacks Against Network Layer In Wireless Sensor Networks”, J. Basic. Appl. Sci. Res., 2(2) pp. 1926-1932, 2012.

[2] Dimple Juneja, Atul Sharma, and A.K. Sharma, ” Wireless Sensor Network Security Researchand Challenges: A Backdrop”, HPAGC, CCIS 169, pp. 406–416, 2011.

[3] S.H. Jokhio, I.A. Jokhio, and A.H. Kemp,” Node Capture Attack Detection And Defence In Wireless Sensor Networks”, IET Wirel. Sens. Syst , Vol. 2, Iss. 3, pp. 161–169 2012.

[4] Saurabh Singh, Dr. Harsh Kumar Verma ,”Security For Wireless Sensor Network “, International Journal On Computer Science And Engineering (IJCSE) Vol. 3 No. 6 pp. 2303-2399 June 2011.

[5] Suraj Sharma And Sanjay Kumar Jena,” A Survey On Secure Hierarchical Routing Protocols In Wireless Sensor Networks”, ICCCS’11 February 12-14, pp. 146-151, Rourkela, Odisha, India, ACM 2011.

[6] Yuanyuan Zhang, Wassim Znaidi, C´Edric Lauradoux And Marine Minier,“ Flooding Attacks Against Network Coding And Countermeasures “, pp. 305-309, IEEE 2011.

[7] Hyojin Kim, Ramachandra Bhargav Chitti, And Jooseok Song,” Novel Defense Mechanism Against Data Flooding Attacks In Wireless Ad Hoc Networks”, IEEE Transactions On Consumer Electronics, Vol. 56, No. 2, pp. 579-582 May 2010.

[8] Kalpana Sharma, M K Ghose, “Wireless Sensor Networks: An Overview On Its Security Threats,” IJCA Special Issue On “Mobile Ad-Hoc Networks”Manets, pp. 42-45, 2010.

[9] Virendra Pal Singh, Sweta Jain And Jyoti Singhai, ”Hello Flood Attack And Its Countermeasures In Wireless Sensor Networks”, IJCSI International Journal Of Computer Science Issues, Vol. 7, Issue 3, No 11, pp. 23-27, May 2010.

[10] Hemanta Kumar Kalita And Avijit Kar,” Wireless Sensor Network Security Analysis”, International Journal Of Next-Generation Networks (IJNGN), Vol.1, No.1, pp. 1-10, December 2009.

[11] Mohamed M. Ibrahim, Nayera Sadek, Mohamed EI-Banna “Prevention Of Flooding Attack In Wireless Adhoc AODV-Based Networks Using Real-Time Host Intrusion Detection” pp. 1-5 IEEE 2009.

[12] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, ”A Survey Of Attacks, Security Mechanisms And Challenges In Wireless Sensor Networks”, (IJCSIS) International Journal Of Computer Science And Information Security,Vol. 4, No. 1 & 2, 2009.

[13] Revathi Venkataraman, M. Pushpalatha, Rishav Khemka, T. Rama Rao,” Prevention Of Flooding Attacks In Mobile Ad Hoc Networks”, International Conference On Advances In Computing, Communication And Control (ICAC3) pp. 525-529, 2009.

[14] Xiangqian Chen, Kia Makki, Kang Yen, And Niki Pissinou, “ Sensor Network Security: A Survey”, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 11, NO. 2, SECOND QUARTER pp. 52-57, 2009.

[15] Xiaojiang Du And Yang Xiao,” A Survey On Sensor Network Security” pp. 403-421, 2007.

[16] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, ” A SURVEY OF ATTACKS AND COUNTERMEASURES IN MOBILE AD HOC NETWORKS” , In Wireless Network Security, pp.103-135, 2007.