International Journal of Emerging Engineering Research and Technology
Volume 4, Issue 1, January 2016, PP 96-99
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

# Issues and Attacks – A Security Threat to Wsn: An Analogy

**Sonali Joyce Lobo[1], Sumana K R[2]**

[1]*Information Science & Engineering, National Institute of Engineering, Mysuru, India*
[2]*Computer Science & Engineering, National Institute of Engineering, Mysuru, India*

## ABSTRACT

Computer network is a group of computing devices like computers which are connected together and these devices communicate or exchange the information through links. One such type of network is wireless sensor networks. Wireless sensor networks consist of sensor nodes connected in some fashion. These nodes detect various environmental conditions such as temperature, sound and so on. Attacks have become serious security threats that wireless sensor networks have to overcome. These attacks lead to energy inefficiency. There are various types of security attacks that a wireless sensor network has to overcome. Blackhole attack and power consumption attack are also among the types of security attacks. This paper is a survey paper which consists of a survey on avoidance of the attacks mentioned above and an effort to reduce the power consumption and increase the energy efficiency.

**Keywords:** Computer Networks, Wireless Sensor Networks, Power Consumption, Energy Efficiency, Blackhole attack

## INTRODUCTION

Computer Networks (CN) are the networks which consists of one, few or enormous devices which are connected in some fashion. These computing devices communicate using links. The links can be in the form of a cable or wireless media. The devices that communicate in the network are referred to as nodes. These nodes communicate through various communication protocols such as Transmission control protocol referred to as TCP or User Datagram Protocols referred to as UDP. These protocols are named as transfer control protocols.

CN's have various concepts called as clustering. In this clustering concept, clusters are formed. Clustering is normally used in huge networks. This huge network is divided into small group of nodes. And each group formed as such is called as a cluster. Each cluster consists of cluster head and cluster members (CM). Cluster head is the chief of the cluster formed and all other member in the group formed are the cluster members. Cluster head acts as the chief and collects the data obtained from the CM's.

Wireless sensor network (WSN) is also a type of CN. These type of networks consists of various low power sensor nodes can be in tens, hundreds, thousands and so on in number and are in distributed form. These nodes are meant for keeping track of environmental conditions like sound pressure temperature and so on. These nodes communicate data with one another and send it to a location called as base station. WSN's also makes use of the clustering concept mentioned above. The chief nodes collect the data from its members and send the data to the base station. Power constraint is one of the main challenges of wireless sensor networks. As the sensor nodes are low-powered, care has to be taken on their power constraint. If care is not taken on the above mentioned constraint, then it might lead to battery or power drainage, and leads to death of the nodes.

Security is also one of the important issue. Security attacks are the main cause of security issues. For solving these issues concern has to be taken towards avoiding and preventing security attacks. There are various types of security attacks like blackhole attack, greyhole attack, denial of sleep attacks, flooding attacks, jamming attacks and so on.

***Address for correspondence:***

sonalijoycelobo@gmail.com

Some of these attacks lead to power exhaustion which leads to power drainage and also leads to death of sensor nodes. This survey paper mainly concentrates or goes through the research of avoiding the power exhaustion and also avoidance and prevention of blackhole attack.

Blackhole attack is an attack where in a node keeps hold of the data with itself and doesn't even try to send it to the correct receiver. In this type of security attack a router or any node gets compromised due to various causes. One of such cause is denial of service attack. Here a node drops the data and doesn't send it further. Because of this attack the receiver won't receive the data that it was supposed to receive. This type of attack must be avoided.

In addition to blackhole attack there are various other attacks that causes power exhaustion one of such attacks is denial of sleep attack. Denial of sleep attack is a type of attack where a node denies to go to a state called as sleep state, thus loses its power or the power gets drained, and this leads to the death of the node. Here one such node acts as an anti-node(AN) and sends incorrect preamble packet to the receiver, in case the receiver could not make out the difference between the correct preamble or the fake preamble packets then it receives and processes further packets from the antinodes which are incorrect data packets and loses its power. Here the main aim of the AN is to generate incorrect preamble packets and to make the receiver drain its power completely and makes the receiver to die. This is one of the serious type of attacks that has to be avoided as it leads to energy inefficiency, and which also reduces the lifetime of WSN's.

Rest of this survey paper is organized or arranged in following way, first is the literature survey which describes the research work that is already completed in the field of Wireless Sensor Networks, second is the Issues and Merit's Summary which gives the merits and issues of each work, and then is the conclusion and finally the references.

## LITERATURE SURVEY

### 1.1. Fighting Insomnia: A Secure Wake-up Scheme for Wireless Sensor Networks [1]

This paper mainly concentrates on avoiding Denial of Service attacks in particular sleep deprivation attack. According to this paper sensor node can switch between two states. The two states are active state and sleep state. When the sensors are in active state they consume higher amount of energy. Sensors in the sleep state consume lesser amount of energy. SDA requires a node to be in the active state continuously communicating with other node, thus leads to loss of energy which results in death of the sensor nodes. This paper proposes concept of wake up radio which is secure and it acts as a watchman and activates a node only when it receives a secure token. Firstly, sender sends the secure token to the recipient then both of them communicate using main radio.

### 1.2. A Secure Scheme for Power Exhausting Attacks in Wireless Sensor Networks [2]

Denial of sleep attack is a type of attack which avoids a node from going to sleep mode. DeOS attack not only avoids a node from going to sleep state but also makes it process the packets continuously from the anti-node. The job of this node is to continuously send the fake packets to the receiver. If the receiver cannot make out the difference between the real and the fake one, it processes the packet which leads to unnecessary delay in processing of packets which is directly proportional to reduction of its power. This paper aims at avoiding the above mentioned attack.

### 1.3. Energy Prediction based Trust Management in Hierarchical Sensor Networks [3]

Generally, Trust indicates the level confidence on an object or a person. Trust Management is managing the level of trust or level of confidence. This paper proposes an energy prediction based scheme which avoids the anti-node becoming cluster heads. This scheme is also used to detect the Denial of service attacks. Here the trust value of each node is calculated. Cluster head evaluates the trust value of each node. Based on the trust value highest trusted node is chosen as a vice head node (VIHE). VIHE evaluates the trust value of the cluster head. This paper also involves calculation of trust value at the Base Station. This paper places its focus on avoiding flooding attacks particularly hello flood attacks.

### 1.4. Detection and Prevention Mechanism for Blackhole Attack in Wireless Sensor Network [4]

This paper achieves detection and prevention of Blackhole attack. Blackhole attack is a particular type of DOS attack. This attack programs nodes to block the packets within itself and will not allow them to send the data to the receiver. This paper proposes a mechanism to prevent these attacks using the technique called as clustering. Clustering is a technique wherein a set of nodes a particular node is chosen to be a cluster head. All other nodes are cluster members.

### 1.5. Wireless Sensor Networks: Routing Protocols and Security Issues [5]

This paper describes various challenges of wireless sensor networks which includes limited power management, security issue, scalability, mobility, lack of resources and so on. It also describes about various threats that will have serious impacts on wireless sensor networks some of which are flooding attack which leads to energy wastage and in turn leads to energy inefficiency, selective forwarding attack which is slight variation of blackhole attack, Sybil attack, wormhole attacks & so on. This paper basically concentrates providing secure communication during routing.

## ISSUES AND MERITS OF SURVEYED PAPERS

**Table1.** *Issues and Merits Summary*

| **Issues and Merit's Summary** | | |
|---|---|---|
| **Paper Titles** | **Merits** | **Issues** |
| Fighting Insomnia: A Secure Wake-up Scheme for Wireless Sensor Networks. | Avoidance of deprivation of sleep attacks. | A more secure scheme such as hashing could be used. |
| A Secure Scheme for Power Exhausting Attacks in Wireless Sensor Networks. | Avoidance of power exhaustion attacks. | Concentrates on solving only power exhaustion attacks, and doesn't take any measures to check whether the chief or head of the cluster is compromised and is sending the data to the base station. |
| Energy Prediction based Trust Management in Hierarchical Sensor Networks. | Avoidance of hello flood attacks. | Aims only on avoidance of anti-node becoming a cluster head, but it doesn't aim at avoiding other attacks like power exhaustion and blackhole attacks. |

## CONCLUSION

This paper is the survey of various researches done in the field of wireless sensor networks to solve either blackhole attack, or to reduce the power consumption by avoiding attacks caused due to the anti-node. The survey of existing system reveals that, it tries to increase the energy efficiency, and also increases the lifetime of WSN's. Measures have to be taken in resolving the drawbacks, and increasing the network efficiency by securing the network.

## REFERENCES

[1] C.-T. Hsueh, C.-Y. Wen and Y.-C. Ouyang, "A secure scheme for power exhausting attacks in wireless sensor networks", Ubiquitous and Future Networks(ICUFN) 3rd international conference, pp. 258-263, 2011.

[2] Ching-Tsung Hsueh, Chih-Yu Wen, Yen-Chieh Ouyang, "A Secure Scheme Against Power Exhausting Attacks in Hierarchical Wireless Sensor Networks", Sensors Journal, IEEE, pp. 3590-3602, 2015.

[3] Wen Shen; Guangjie Han, Mengli Cheng, Chuan Zhu, Gang Hu," Energy Prediction Based trust management in hierarchical wireless sensor networks", computer applications and system modelling, pp. V12-453-V12-456 , 2010.

[4] Wazid M, Katal A,Singh Sachan R, Goudar R.H, Singh D.P, "Detection and prevention mechanism for blackhole attack in Wireless sensor networks", 2013 international conference,

communication and signal processing, pp.576-581, 2013.

[5] Anjali, Shikha, Sharma M, " Wireless Sensor Networks: Routing Protocols and Security Issues", Computing Communication and Networking Technologies (ICCCNT), 2014 International Conference, PP.1-5

## AUTHORS' BIOGRAPHY

**Sonali Joyce Lobo,** is pursuing MTech 2nd year in Computer Networks and Engineering course under the department of Information Science and Engineering at National Institute of Engineering, Mysuru, Karnataka, India. Completed B.E in Computer Science and Engineering at St. Joseph Engineering College, Mangaluru, Karnataka, India. Research interest is Wireless Sensor Networks domain.

**Prof. Sumana K. R,** is currently working as Assistant Professor and pursuing her Phd degree at National Institute of Engineering, Mysuru, Karnataka, India. She has a total of 12 years of experience as a professor. She has 4 years of experience as a lecturer at Vidya Vardhaka College of Engineering, Mysuru, Karnataka, India. She has completed her B.E and M.Tech degree at Vidya Vardhaka College of Engineering, Sri Jayachamarajendra College of Engineering respectively located in Mysuru, Karnataka India. Her Research Interest is Biomedical Signal Processing for Smart Traffic.