# A Review on Attacks in Wireless Sensor Networks

Prof. Anirudh A.Bhagwat*
Department of Computer Engineering
Smt. Radhikatai Pandav College of Engineering
Nagpur -440009, INDIA
*E-mail :anirudh.bhagwat2011@gmail.com*

Prof.Vinod W.Wankhede**
Department of Electronics & Telecomm Engineering
Smt. Radhikatai Pandav College of Engineering
Nagpur -440009, INDIA
*E-mail :vwwankhede@gmail.com*

***Abstract**:* - Security is important for many sensor network applications. Wireless sensor networks consist of many small, inexpensive devices that have constraints in coverage, bandwidth, storage resources, communications ability and processing power. Therefore security issues are a critical concern due to possible exposure to malicious activity and potential threats. As a result of the physical constraints in sensor nodes, traditional cryptographic techniques are not suitable to operate on such networks where security requirements are of crucial importance. This raises serious concerns on finding methods to protect sensor nodes from adversaries, to quickly segregate those that have been attacked, and allow the network to reform. A particularly harmful attack against sensor and ad hoc networks is known as the Sybil attack where a node illegitimately claims multiple identities..One practical limitation of structured peer-to- peer (P2P) networks is that they are frequently subject to Sybil attacks: malicious parties can compromise the network by generating and controlling large numbers of duplicate identities. In this paper we are discuss about various attacks comes in Wireless Sensor Network.

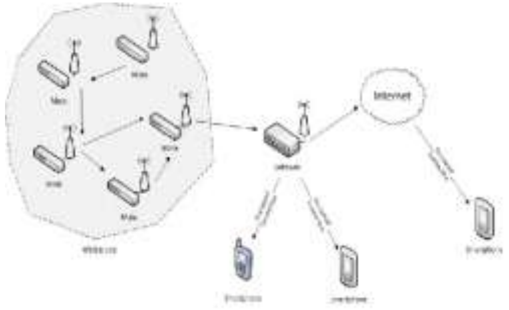
**Keywords**- *WSN, Security, Attacks-DOS, Wormhole, Sinkhole and Sybil*

*****

## I. INTRODUCTION

Wireless sensor networks have appeared as a technology that are being speedily adopted due to their flexibility and use in a variety of environments. A Wireless Sensor Network (WSN) is a collection of spatially organized wireless sensors by which to monitor various changes of eco-friendly conditions (e.g., forest fire, air pollutant concentration, and object moving) in a cooperative manner without relying on any underlying infrastructure support [1]. However, sensors consist of small, inexpensive devices or nodes that have severe limitations such as incomplete bandwidth, limited processing power, small battery life, less storage capability and are actually responsible to external threats[2].In most cases, the sensor nodes form a multi-hop has limitation in terms of calculation capability and energy reserves. The BS wants to collect the sensed information from the network[3]. One common way is to allow each sensor node to forward its reading to the BS, possibly via other in-between nodes. Finally, the BS processes the received data. However, this method is too expensive in terms of communication overhead.

Even with all the benefits that wireless sensor networks provide such as fast deployment and configuration, the limitations of the sensor nodes makes them extremely helpless to various security threats. These include attacks that target a specific node with endless communication in order to consume its limited battery life and also the physical liability of the sensor nodes within aggressive environment, e.g. a military battlefield. Unfortunately, a cryptographic techniques such as Public Key Infrastructure (PKI),this techniques widely used in traditional wired networks, is not appropriate to operate on sensor networks to enable secure data communication. In the proposed system we are implementing Security architecture for providing security for WSN against Sybil attack. A wireless sensor network is a special network which has many constraints compared to a traditional computer network. These constraints make it difficult to directly employ the existing security approaches to the area of wireless sensor networks. Therefore, to develop useful security mechanisms while borrowing the ideas from the current security techniques, it is necessary to know and understand these constraints. All security approaches require a certain amount of resources for the implementation, including data memory, code space, and energy to power the sensor.



Fg. Wireless Sensor Network

Limited Memory and Storage Space: A sensor is a tiny device with only a small amount of memory and storage space for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm. For example, one common sensor type (TelosB) has an 16-bit, 8 MHz RISC CPU with only 10K RAM, 48K program memory, and 1024K flash storage. With such a limitation, the software built for the sensor must also be quite small. The total code space of TinyOS, the de-facto standard operating system for wireless sensors, is approximately 4K [32], and the core scheduler occupies only 178 bytes. Therefore, the code size for the all security related code must also be small.

Power Limitation : Energy is the biggest constraint to wireless sensor capabilities. We assume that once sensor nodes are deployed in a sensor network, they cannot be easily replaced (high operating cost) or recharged (high cost of sensors). Therefore, the battery charge taken with them to the field must be conserved to extend the life of the individual sensor node and the entire sensor network. When implementing a cryptographic function or protocol within a sensor node, the energy impact of the added security code must be considered. When adding security to a sensor node, we are interested in the impact that security has on the lifespan of a sensor (i.e., its battery life). The extra power consumed by sensor nodes due to security is related to the processing required for security functions (e.g., encryption, decryption, signing data, verifying signatures), the energy required to transmit the security related data or overhead (e.g., initialization vectors needed for encryption/decryption), and the energy required to store security parameters in a secure manner (e.g., cryptographic key storage).

## 2. LITREATURE REVIEW

Authors discussed in [2] Due to the severe physical constraints in sensor nodes, traditional cryptographic mechanisms are not suitable to deal with such potential security threats. This paper proposes a secure lightweight architecture that takes account of the constraints of sensor networks. With the use of a base station, a hierarchical network topology is formed that enables end-to-end communication between sensor nodes with the aid of intermediary nodes where necessary. The architecture also supports the detection and isolation of aberrant nodes.

In this paper [4] authors focused on intrusion vdetection is defined as a mechanism for a WSN to detect the existence of inappropriate, incorrect, or anomalous moving attackers. For this purpose, it is a fundamental issue to characterize the WSN parameters such as node density and sensing range in terms of a desirable detection probability. Authors consider this issue according to two WSN models: homogeneous and heterogeneous WSN. Furthermore, we derive the detection probability by considering two sensing models: single-sensing detection and multiple-sensing detection. In addition, we discuss the network connectivity and broadcast reachability, which are necessary conditions to ensure the corresponding detection probability in a WSN.

In this paper [5], authors introduce the *wormhole attack*, As mobile ad hoc network applications are deployed, security emerges as a central requirement. a severe attack in ad hoc networks that is particularly challenging to defend against. The wormhole attack is possible even if the attacker has not compromised any hosts, and even if all communication provides authenticity and confidentiality .In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them there into the network.

Due to practical limitation of structured peer-to-peer (P2P) networks is that they are frequently subject to Sybil attacks: malicious parties can compromise the network by generating and controlling large numbers of shadow identities. In this paper [8], authors proposed an admission control system that mitigates Sybil attacks by adaptively constructing a hierarchy of cooperative peers. The admission control system vets joining nodes via client puzzles. A node wishing to join the network is serially challenged by the nodes from a leaf to the root of the hierarchy. Nodes completing the puzzles of all nodes in the chain are provided a cryptographic proof of the vetted identity.

In this paper [10] authors proposed a secure lightweight architecture for providing security because Wireless sensor networks consist of many small, inexpensive devices that have constraints in coverage, bandwidth, storage resources, communications ability and processing power. Therefore security issues are a critical concern due to possible exposure to malicious activity and potential threats. The (ASLAN) takes account of the constraints of sensor networks. With the aid of a base station, a hierarchical network topology is formed allowing end-to-end communication between sensor nodes. ASLAN also supports identifying and isolating aberrant sensor nodes.

The Author Ashwini D. Khairkar Deepak D Kshirsagar Sandeep Kumar Talked about issues of existing IDS i.e. low false positive rate, low false negative rate and information over-burden. Creators displays a suggestion of utilizing Semantic Web and Ontology ideas to characterize a way to deal with break down Security logs with the objective to recognize possible security issues. It separates semantic relations between PC assaults and interruptions in an Interruption Location Framework[11]. Philosophy gives to empower, reuse of space learning and it is also less demanding to comprehend and overhaul legacy information. The fundamental segments of cosmology are classes , relations , maxims , properties and cases . Metaphysics is utilized for demonstrating information from particular domains furthermore permits deductions to find understood learning in these. Cosmology can be useful for enhancing the characterization of the assaults happened and the distinguishing proof of related events. An ontological representation of information gives numerous advantages over straightforward string matching.

In [1 In [13] author focuses on distinguishing interruptions practices in WLANs among information clustering procedures. Creators first investigate the security vulnerabilities of 802.11 and abridge the system traffic, measurements that are critical to demonstrate the security of remote systems. Based on the metric considered we propose a bunching based interruption location approach and assess it on a certifiable vast remote system traffic dataset. In this work the remote follows were converted into information records that can be utilized for bunching. An effective online K-implies clustering calculation was utilized to bunch the information into groups. Meddling groups are then determined by separation based heuristics. The adequacy of the grouping based remote intrusion recognition technique has been approved by the consequences of our contextual investigation of an expansive wireless system.

## II. TYPES OF ATTACKS

DOS ATTACK- Denial of Service (DOS) attack is created by the unintentional failure of nodes or malicious action. A DOS attack is an opponent's attempt to exhaust the resources available to its genuine users.[4]To launch DOS attacks at the physical layer Jamming is also widely used. Radio frequency jamming can be working to enter the transmitted signal band. An opponent can utilize jamming signals (thereby disturbing the communications) to make the attacked nodes suffer from DOS in a specific region. DOS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DOS attacks in different layers might be performed. At physical layer the DOS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and resynchronization. The mechanisms to prevent DOS attacks include payment for network resources, pushback, strong authentication and identification of traffic.

WORMHOLE ATTACK- In a wormhole attack, an attacker accepts packets at one point in the network, "channels" them to another point in the network, and then reiterations them into the network from that point. For channel distances extended than the normal wireless transmission range of a single hop, it is simple for the attacker to make the channeled packet reach with better metric than a normal multi hop route [5]. A simple example of this wormhole attack is a one node situated between two other nodes sending messages between the two of them. However, they more commonly include two distant malicious nodes planning to minimize their distance from each other by communicating packets along an out-of-bound channel available only to the attacker. The wormhole attack is particularly dangerous against many ad hoc network routing protocols in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of (and, thus a neighbor of) that node. For example, when used against an on-demand routing protocol such as dynamic source routing (DSR) or ad hoc on-demand distance vector (AODV) , a powerful application of the wormhole attack can be mounted by tunneling each ROUTE REQUEST packet directly to the destination target node of the REQUEST. When the destination node's neighbors hear this REQUEST packet, they will follow normal routing protocol processing to rebroadcast that copy of the REQUEST, and then discard without processing all other received ROUTE REQUEST packets originating from this same route discovery. This ttack, thus, prevents any routes other than through the wormhole from being discovered, and if the attacker is near the initiator of the route discovery, this attack can even prevent routes more than two hops long from being discovered.

SINKHOLE ATTACK -In the sinkhole attack, the opponent node create a sink immediate the nodes. Sinkhole attacks make compromised nodes by spoofing all the information of routing protocols and make a false optimal path which is highly attractive and manipulate all the neighboring nodes to choose that false path which is nearby the compromised nodes. By creating sink, the opponent may drop all packets in the network and change the topology of network [6]. Since all the nodes communicate with each other via base station, the opponent simply create a high quality route to the base station and move all the traffic on it. Other attacks, eavesdropping, selective forwarding and traffic spoofing ad black holes can be permitted by sinkhole attack. Geo-routing protocols are resistant to sinkhole, because of naturally routed traffic through the physical location of sinkhole, which makes difficult to lure it and elsewhere to create it.

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 subtasks and redundancy of information. In such a situation, a node can pretend to be more than one node using the identities of other legitimate nodes (Figure 1). This type of attack where a node forges the identities of more than one node is the Sybil attack [7]. Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts toachieve. Sybil attack can be performed for attacking the distributed storage, routing mechanism, data aggregation, voting, fair resource allocation and misbehavior detection. Basically, any peer-to-peer network (especially wireless ad hoc networks) is vulnerable to Sybil attack. However, as WSNs can have some sort of base stations or gateways, this attack could be prevented using efficient protocols. Without a logically centralized authority, Sybil attacks are always possible except under extreme and unrealistic assumptions of resource parity and coordination among entities. However, detection of Sybil nodes in anetwork is not so easy.

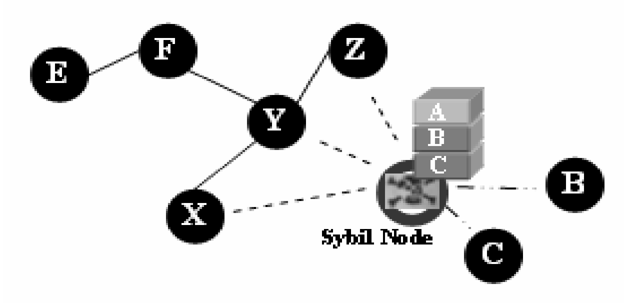


Fig. sybil Attack

## III.SUMMARY AND CONCLUSION:

In this survey paper we surveyed about security in wireless sensor networks. In a sensor networks sensors consist of small, inexpensive devices or nodes that have severe constraints such as partial bandwidth, partial processing power, small battery life, small storage capability and are actually liable to external threats. We are in progress by explaining why security issues come from Sybil attacks in wireless sensors networks & also planning to come up with a new secure architecture that provide security for Wireless Sensor Network.

## REFERENCES

[1] Yun Wang, Xiaodong Wang, Bin Xie, Demin Wang and Dharma P. Agrawal, *"Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks",* IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 7, NO. 6, JUNE 2008

[2] Michael Collins, SimonDobson, Paddy Nixon,"*A Lightweight Secure Architecture for Wireless Sensor Networks*",INT. J. INTERNET TECHNOLOGY AND SECURED TRANSACTIONS, VOL. X, NO.X, 2008

[3] Sankardas Roy, Mauro Conti, Sanjeev Setia, and Sushil Jajodia, "*Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact*" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 4, APRIL 2014

[4] Yi-sheng shiu and Shih yu chang, Hsiao-chun wu, Scott c.-h. Huang, Hsiao-hwa Chen, "Physical layer security inWireless networks: a tutorial", IEEE WIRELESS COMMUNICATIONS APRIL 2011

[5] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Wormhole Attacks in Wireless Networks"IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006.

[6] Manisha, Gaurav Gupta, "Attacks on Wireless Sensor Networks: A Survey", International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 10, October 2013 ISSN: 2277 128X.

[7] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong"Security in Wireless Sensor Networks: Issues and Challenges", ISBN 89-5519-129-4 - 1043 - Feb. 20-22, 2006 ICACT2006

[8] Hosam Rowaihy, William Enck, Patrick McDaniel, and Thomas La Porta,"Limiting Sybil Attacks in Structured P2P Networks".

[9] Manjuprasad B,Andhe Dharani"Simple Secure Protocol for Wireless Sensor Networks", 2014 World Congress on Computing and Communication Technologies

[10] Michael Collins, Simon Dobson, Paddy Nixon,"Securing Wireless Sensor Networks: Introducing ASLAN - A Secure Lightweight Architecture for WSNs"INTERNATIONAL JOURNAL ON ADVANCES IN INTERNET TECHNOLOGY, VOL 2 NO 1, YEAR 2009.

[11] Ashwini D. Khairkar Deepak D Kshirsagar Sandeep Kumar, "Ontology for Detection of Web Attacks", *International Conference on Communication Systems and Network Technologies 2013*

[12] G.V.Pradeep Kumar Dr. D Krishna Reddy, "An Agent based Intrusion detection system for wireless network with Artificial Immune System (AIS) and Negative Clone Selection"

[13] Shi Zhong, Taghi M. Khoshgoftaar and Shyarn V. Nath, "A Clustering Approach to Wireless Network Intrusion Detection", IEEE Proceedings of the 17th *IEEE International Conference on Tools with Artificial Intelligence (ICTAL'OS) 2005*

[14] James Newsome, laine Shi ,Dawn Song , Adrian Perrig ," The Sybil Attack in Sensor Networks: Analysis & Defenses", IPSN'04,April26–27,2004,Berkeley,California,USA

[15] Kamlesh Gupta, Sanjay Silakari , JUET, Guna, UIT, RGPV,"ECC over RSA for Asymmetric Encryption:AReview",IJCSI International Journal of Comput er Science Issues, Vol. 8, Issue 3, No. 2, May 2011 ISSN (O nline): 1694-0814

[16] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", *IEEE Transactions On Industrial Electronics*, Vol. 60, No. 3, March 2013