ISSN 2278-3091

**International Journal of Advanced Trends in Computer Science and Engineering**, Vol. 3 , No.1, Pages : 154– 160 (2014)
*Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India*

# CONTEMPORARY ATTACKS AND APPLICATIONS ON WIRELESS SENSOR NETWORKS

**Kodem Sree Gouri Varshini[1], Seelam Abigna Reddy[2], Kodem Sowmya[3]**

**1: III year student of Computer Science And Engineering, Mallaredddy Institute of Engineering And Technology, sgvkodem@gmail.com.**
**2: III year student of Computer Science And Engineering of Mallaredddy Institute of Engineering And Technology, abignareddy9@gmail.com.**
**3: III year student of Computer Science And Engineering of Mallaredddy Institute of Engineering And Technology, sowmi_199418@yahoo.com**.

## ABSTRACT:

**Wireless Sensor Networks are an active research area in computer science and telecommunication with crucial pool of knowledge not only for underlying networking applications, but also for security associated configurations. The surfacing of sensor networks as one of the dominant technology trends in the coming decades has posed numerous unique challenges to researchers. These WSNs consists of spatially scattered autonomous sensors for monitoring physical and environmental conditions. These networks are composed of hundreds or thousands of tiny sensor nodes, functioning autonomously, low power, self-organizing, low cost nodes and in many cases without access to renewable resources which are highly scattered. As these networks are highly distributed, there is a possibility of different types of attacks. So security plays a major role. In this paper we discuss several denial of service attacks of WSNs security and their defenses .We also discuss a wide range of applications on WSN.**

**Keywords:-Wireless Sensor Networks, Characteristics, Types of WSN, Attacks, Applications.**

## INTRODUCTION:

Wireless Sensor Networks refers to a heterogeneous system combining actuators and small devices called sensor nodes with general-purpose computing elements .These networks consists of low power, low cost and self - organizing nodes which are highly distributed either very close to it or inside the system. Sensor nodes consists of components like aggregation ,base station, data processing and communication[6].These networks mostly operate in uncontrolled area and public, so security is the major challenge in sensor applications. There are some traditional security mechanisms like authentication, symmetric key encryption & decryption and Public Key Infrastructure (PKI) cryptography [3,4,5].

Wireless Sensor Network (WSN) security differs from WIFI because:

1.WSN networks need to deliver real-time deterministic performance
2.WSN devices such as transmitters and valve positioners are constraint in computational capabilities (memory, CPU, bandwidth) and frequently battery powered
3.WSN devices are easily accessible because they are located in the field at fixed positions and often not tamper resistant.

ISSN 2278-3091

**International Journal of Advanced Trends in Computer Science and Engineering**, Vol. 3 , No.1, Pages : 154– 160 (2014)
*Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India*

**Characteristics of WSN[8]:**

1. Compact size
2. Memory space
3. Bandwidth
4. Physical Security
5. Power
6 .Unreliable Communication
7. Heterogeneity of nodes
8. Communication failure
9. Mobility of nodes

## TYPES OF WSN NETWORKS:

### A. Multimedia WSNs[11]:

In these types of WSN low cost sensor nodes are outfitted with microphones and cameras. These sensor nodes are positioned in a pre-planned manner to assurance coverage. There are some issues in these networks which are insist of high energy utilization, quality of service provisioning, high bandwidth, data processing and compression techniques, and cross layer design.

### B. Terrestrial WSNs[9]:

Here the nodes are circulated in a given area either in an ad hoc manner which means sensor nodes are indiscriminately placed into the target area by dropping it from plane, or in pre-planned manner which means nodes are placed according to the grid placement ,optimal placement ,2-d and 3-d placement models.
These sensor nodes are provided with an optional power source such as solar cells as battery power of these sensor nodes is boundless.

### C. Underground WSNs[10]:

Here sensor nodes should monitor underground conditions so they are buried in underground or in a cave or mine. The gathered information is forwarded from the sensor nodes to the base station by deploying sink nodes above the ground. Proper nodes are to selected that can assure reliable communication through soil, water, rock and other mineral resources which becomes more expensive than terrestrial WSNs.

### D. Underwater WSNs[10]:

Here sensor nodes and vehicles are placed underwater. Independent vehicles are used to gather the data from the sensor nodes. In these networks sparse deployment of nodes is done. Some important problems which comes under these networks while communicating are limited bandwidth, long propagation delay and signal fading issue.

## ATTACKS ON WSN NETWORKS:

Wireless Sensor Networks are power constraint networks, which have limited computational and energy resources. This makes them exposed enough to be attacked by any attacker deploying more resources than any individual node or base station, which may not be difficult job for the attacker. A typical sensor network uses broadcast or multicast, which compresses potentially hundreds of nodes. The broadcast nature of the transmission medium is the reason why wireless sensor networks are susceptible to security attacks. Denial of Service attack eradicates a network's range to satisfy its expected function.

Various types of DOS attacks on different layers are discussed below:

### A. JAMMING:

This attack interrupts in physical layer of the WSN structure. There are two types of jamming. They are: intermittent jamming and constant jamming.

ISSN 2278-3091

**International Journal of Advanced Trends in Computer Science and Engineering**, Vol. 3 , No.1, Pages : 154– 160 (2014)
*Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India*

Intermittent jamming nodes can communicate data periodically but not continuously, where as constant jamming affects the complete obstruct of the whole network. Fig 1 shows the jamming attack.

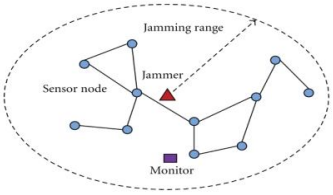


FIG 1: JAMMING

**B. COLLISION:**

This type of attack interrupts in data link layer. This attack occurs when any two nodes try to transmit the data at the same frequency at the same time. Attacker causes collisions in particular packets like ACK control messages. The effected packets are transferred again, increasing the energy, time, cost for transmission. Such an attack reduces the network flawlessness.

**C. EXHAUSTION:**

This attack interrupts in data link layer. This attack causes the retransmission of the message even when there no collision or late collision which dominates the power resources of the nodes[8].

**D: NEGLECT AND GREED ATTACK:**

This occurs at network layer[7]. When a packet is transferred from a sender to receiver there occur a number of other nodes through which the packet is routed before reaching to the final destination between both these nodes .This transferring of the packet is said to be successful only when the packet is entirely reached to its destination. Meanwhile, a node called malicious node can force multi-hopping in the network, either by splashing few packets or by routing the packets towards an erroneous node. This attack disturbs the behavior of adjoining nodes, which may not be capable of sending or receiving messages.

**E: UNFAIRNESS:**

This attack interrupts in data link layer. Protocols like MAC protocols at link layer administer the communications in networks by constraining precedence schemes for seamless correlation. It is possible to use these MAC protocols thus effecting the priority schemes which ultimately results in drop of in service[8].

**F: HOMING:**

This attack interrupts in the network layer. Here the attacker investigates the network traffic at the network layer to infer the geological area of cluster heads or base station neighboring nodes. It then implements some other attacks on these critical nodes, so as to physically wipe out them that further cause major obliteration to the network[8].

**G: SYBIL ATTACK:**

This attack occurs in physical layer and also in network layer. It is defined as a “malicious device unlawfully taking on multiple identities”, which generally effect the routing mechanism. These attacks are generally prevented by validation techniques[12].

**H: HELLO FLOOD ATTACK:**

This type of attack interrupts in network layer. Hello flood attack uses HELLO message to present itself to its adjoining nodes. It is one of the simplest attack in WSN in which attackers broadcast the hello packets with high transmission power to either sender or receiver. The nodes receives the messages and thinks that sender node is

ISSN 2278-3091

**International Journal of Advanced Trends in Computer Science and Engineering**, Vol. 3 , No.1, Pages : 154– 160 (2014)
*Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India*

nearest to them .Due to this data congestion occurs in the networks and thus complicates the data flow. Techniques like blocking are used to prevent Hello Flood attacks[8,12].Hello flood attack is shown in fig 2.

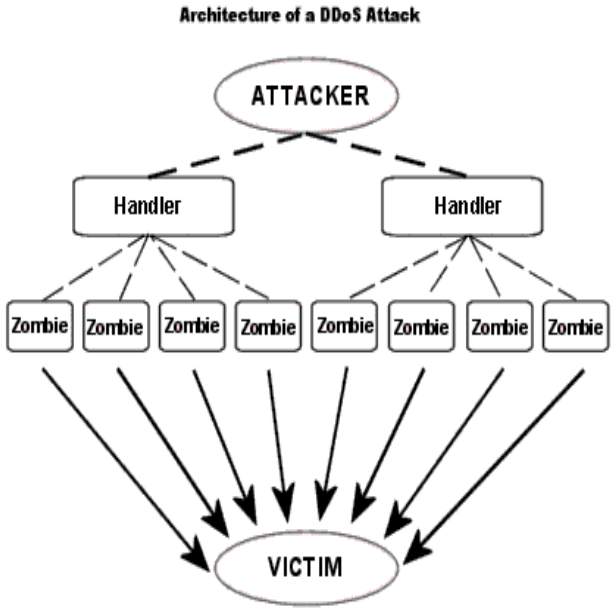


FIG 2: HELLO FLOOD ATTACK

**I: WORMHOLE ATTACK:**

This attack interrupts in network layer[13]. In this attack, a pair of awful nodes discovers a wormhole firstly at network layer. This attacker uses tunneling mechanism to establish himself between them by perplexing the routing protocol. Consider 'A' wants to send data by way of broadcasting before sending the data to find path. Attacker ☠ introduces himself as a node 'A' and sends acknowledgement to 'B' and then it sends data to 'A' that is received by ☠ and ☠ sends that data to 'A' by tunneling, hiding its own identity. In this case 'A' and 'B' are not in a single leap but they think they are in a one leap range. The attacker ☠ thus may destroy security by interruption, interception, modification and fabrication.

**J: BLACKHOLE/ SINKHOLE ATTACK:**

This attack interrupts in the network layer. In this attack, attacker places himself in a network with high potential resources with high processing power and high band width, by which is always creates shortest path. As a result, all the data passes through attacker's node.

**K: ACKNOWLEDGEMENT SPOOFING:**

This type of attack is introduced in the network layer on routing algorithms that needs transferring of acknowledgement messages. An attacker may eavesdrop packet transference from its adjoining nodes and swindle the acknowledgement, there by sending wrong information to the nodes[8].

**L: NODE REPLICATION ATTACK:**

A unique ID is present for every sensor node in a network, which can be duplicated by an attacker and is assigned to a new supplementary malicious node in the network. This assures that the node is in the network and it can lead to a variety of calamitous effects to the sensor network. Packets can be misrouted, missed or modified by using the replicated node which results in wrong information of packet, loss of connection, data loss and high end-to-end latency. Malicious node can get right to the sensitive information and thus can damage the network[8].

**M: PHYSICAL ATTACKS:**

ISSN 2278-3091

**International Journal of Advanced Trends in Computer Science and Engineering**, Vol. 3 , No.1, Pages : 154– 160 (2014)
*Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India*

This occurs in physical layer. These attacks give the adversary the endowment to reconstruct the nodes and thus the network functioning at the physical layer. The attacker can extract source code which ultimately provides attacker the information about the network that can alter the code to get admittance into the network. Various types of physical attacks are discussed in the below table[6].

| ATTACKS | THREAT |
|---|---|
| Signal/radio jamming | Availability, integrity |
| Device tampering attack, node capturing attack | Availability, integrity, authenticity, confidentiality |
| Path-Based DOS | Availability, authenticity |
| Node outage | Availability, integrity |
| Eavesdropping | Confidentiality |

**N: VOLUMETRIC ATTACK:**

The largest attacks reported to Arbor were in the 60 Gbps range for the last 2 years. The size of volumetric attacks increased dramatically, those focused on consuming the bandwidth of a target network or service. There are several respondents which experienced DDoS attacks that surpassed the 100 Gbps mark. Arbor noted that the customers of the respondents were the main targets of volumetric DDoS attacks, but Sockrider said the communications of network and service providers is coming under larger threat, with 17% of these reported attacks hitting those targets, compared to 11% in the previous year. The large-scale attacks, with the largest verified attack it has seen clocking in at 245 Gbps .

## APPLICATIONS ON WSN:

WSNs have found application in a vast range of different domains, scenarios and discipline. WSN researchers have also realized the application specificity of the domain; it is incredibly difficult, if not impossible, to find an application-independent solution to most WSN problems. Hence, research into WSNs dictates the adoption of an application-centric design process.
Here are the applications of the wireless sensor networks:

**1.INDUSTRIAL CONTROL & MONITORING:**

ISSN 2278-3091

**International Journal of Advanced Trends in Computer Science and Engineering**, Vol. 3 , No.1, Pages : 154– 160 (2014)
*Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India*

WSNs can be used in industries for the condition of manufacturing equipment or to be used to monitor manufacturing process. For example, chemical plants or oil refiners can use sensors to monitor the condition of their miles of pipelines. These sensors are used to alert in case of any failure occurred.

**2. MILITARY OR BORDER SURVEILLANCE:**

WSNs are becoming an integral part of military command, control, communication, intelligence systems and mainly used because it is difficult to deploy a communication infrastructure in the theatre of operation, e.g., in a battlefield. Sensors can be deployed in a battle field to monitor the presence of forces and vehicles, and track their movements, enabling close surveillance of opposing forces. The installation of a centralized infrastructure, apart from being time consuming, would become a vulnerable network solution.

**3. DETECTION AND PREVENTION OF FOREST FIRES:**

A network of Sensor Nodes can be installed in a forest to detect when a fire has started. After installing the WSN, the network can also acquire the daily values for temperature and relative humidity in order to determine the likelihood of the fire in each zone under surveillance. And then the alarm indicating the status of fire and the probability and the area information is send using WSNs.

**4. HEALTH CARE MONITORING:**

WSNs can be used to monitor the patient for their long time surveillance, by monitoring the ill patients and elders at home by reducing expenditures. There are two types of medical applications i.e., wearable and implanted. Wearable devices are used on the body surface of a human or just at close proximity of the user. The implantable medical devices are those that are inserted inside human body. WSNs are used to form a so called Body Area Network (BAN), which consists of several sensors placed close to the human body measuring signals such as heart beat rate or breathe rate and collect information about an individual's health, fitness, and energy.

**4. DATA LOGGING:**

Wireless sensor networks are also used for the collection of data for monitoring of environmental information, this can be as simple as the monitoring of the temperature in a fridge to the level of water in overflow tanks in nuclear power plants. The statistical information can then be used to show how systems have been working. The advantage of WSNs over conventional loggers is the "live" data feed that is possible.

**5. INTELLIGENT BUILDINGS (OR BRIDGES):**

WSNs are used in the construction of the buildings, bridges, flyovers, embankments, tunnels .They are used to reduce energy wastage by proper humidity, ventilation, air conditioning (HVAC) control. They need measurements about room occupancy, temperature, air flow. WSNs are also used to monitor mechanical stress after earthquakes.

**6. RADIATION PREVENTION:**

WSNs are used to help authorities and security forces to measure the levels of radiation of the affected zones without compromising the life of the workers.

**7. AUTOMOBILE APPLICATIONS:**

A modern automobile has about 8km of cables to connect hundreds of sensors [1]. WSNs allow not only to reduce the volume and weight required by the cabling, but also the deployment of sensors with more freedom.

**8. ENVIRONMENTAL CONDITIONAL MONITORING:**

WSN applications in this area include monitoring the environmental conditions affecting crops or livestock, monitoring temperature, humidity and lighting in office buildings, and so on. These monitoring modules could even be combined with actuator modules which can control, for example, the amount of fertilizer in the soil, or the amount of cooling or heating in a building, based on distributed sensor measurements.

## CONCLUSION:

In this paper we presented an idea on introduction of WSN and also discussed about characteristics of WSN and its various types. We proposed recent attacks on WSN and applications of WSN. As there are wide range of applications on WSN security plays a crucial role so we give an open problem to design a sensor network routing protocol that satisfies proposed attacks of WSN.

## REFERENCES:

[1] Y.Zou, K.Chakrabarty,"Sensor Deployment and target localization based on virtual forces",INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and

Communication Societies IEEE, Volume:2, pages:1293-1303,April 2003.

[2] Jan Steffan, Ludger Fiege, Mariano Cilia Alejandro Buchman,"Scoping in Wireless Sensor Networks", 2nd Workshop on middleware for pervasive and Ad-Hoc Computing Tornoto, Canada ,2004 ACM 1-58113-951-9

[3] Xiao Chen, Jawad Drissi, "An Efficient Key Management Scheme In Hierarchical Sensor Networks", IEEE MASS 2005 Workshop-WSN05.

[4] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Network: Issues and Challenges", Feb 20-22,2006 ICACT2006.

[5] Woo Kwon Koo, HGH\waseong Lee, Yong Ho Kim, Dong Hoon Lee, "Implementation and Analysis of New Lightweight Cryptographic Algorithm Suitable For Wireless Sensor Networks", International Conference on Information Security and Assurance, 2008.

[6] Rina Bhattacharya,"A Comparative Study of Physical attacks on Wireless Sensor Networks:, IJRET, vol. 2, issue 1, pp. 72-74, jan 2013

[7] Jaydip Sen, Security and Privacy Challenges in Cognitive Wireless Sensor Network, Dec 2012.

[8] M.Yasik Malik, "An Outline Security in Wireless Sensor Networks and Energy Efficiency: Protocols, Routing and Management DOI.

[9] I.F. Akyildiz, W. Su, Y.Sankarasubramaniam, E. Cayirci, "A survey on sensor networks", IEEE Communications Magazine 40.

[10] I.F. Akyildiz, E.P. Stuntebeck, "Wireless underground sensor networks: research challenges", Ad-Hoc Networks

[11] Kriti Jain, Upasana Bahuguna, "Survey on Wireless Sensor Network", IJSTM, Vol. 3 Issue 2

[12] Pooja , Manisha, Dr. Yudhvir Singh, "Security Issues and Sybil Attack in Wireless Sensor Networks", International Journal of P2P Network Trends and Technology, vol. 3, issue 1

[13] C. Karlof, D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", In Proc. of the 1st IEEE Int. Workshop on Sensor Network Protocols and Applications (SNPA'03)