A Theoretical Review on Multiple Security Threats In The Wireless Sensor Network

Ekta Singh Parihar[1], Khushboo Agarwal[2], Jaimala Jha[3]
[1, 2, 3] Dept of Computer Science & Engineering/ Information Technology
[1, 2, 3] Madhav Institute of Technology and Science, Gwalior, India

Abstract- *Wireless Sensor Networks perform has outstanding significance in many programs, which include battlefields surveillance, patient health monitoring, traffic manage, home automation, environmental remark and building intrusion surveillance Distributed Denial of Service (DDoS) flooding attacks are one in all of the maximum traffic for safety experts. DDoS flooding attacks are normally express tries to disrupt valid users' get right of access to to services. This paper presents an introduction of wireless sensor network, security in WSN and illustrate different techniques used to overcome attacks. we investigate the possibility of the DDoS flooding attack. Finally, we discuss the future research directions in this area.*

Keywords- WSN, Security Threats, WDM, Clustering

I. INTRODUCTION

WSN is dissimilar from a different popular wirelessly networks like wirelessly LAN and Bluetooth and cellular networks (n/w) in several method. WSN are planned for variety of monitoring usage. In this n/w (Fig.1) big no. of nodes occasionally takes atmosphere measurements data and transmits them to a middle data sink. With the development in wireless technology and embedded device technology, the capacity of the sensors is quite improved while their cost is lower. A WSN self-possessed thousands of sensor nodes with greatly shorter distance among adjoining nodes and low software data rate. WSN has additional eventuality to be disseminate in actual environments. In contemporary years WSN becomes rising area in wide variety of applications like health monitoring functions, environmental commentary, forecasting procedure, the sensors may also be deployed at quite a lot of places with specific usages and every have distinct capability to experience distinctive attributes like temperature, moisture, pressure humidity etc. But these sensors have confined power sources and likewise it is not fee strong to recharge the batteries. The batteries are often irreplaceable. Therefore, there lifetime will relies upon respective batteries of sensors. So the existence time of WSN can also be prolonged by using utilizing amazing energy balancing approaches [1].

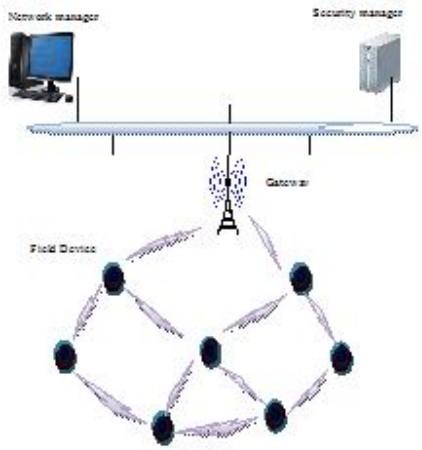

Fig.1 WSN Environment

II. CHALLENGES AND LIMITATIONS OF WSNS

In WSN sensor nodes have limited communiqué bandwidth, storage space and processing power. This gives rise to new and unique challenges in data management and information processing. In-n/w data method, for instance multicast, broadcast and data aggregation necessitate to be developed. Network lifetime is the key characteristics used for evaluating the performance of any sensor network. A span time of the n/w is determined thru residual Energy of the system, hence major and most vital challenge in WSN is the efficient exploit of Energy resources. Literature indicates the energy efficiency is offered in WSNs utilizing any of the next mechanisms: power conservation mechanism, Power conservation mechanism, energy efficient routing and vigor harvesting mechanism.

A. Energy aware routing

The object of routing in WSNs is to search and maintain routes in WSNs. Routing challenge with reference to WSNs are Node diffuse, Link heterogeneity, Data reporting model, Scalability, Energy consumption without losing accuracy, n/w dynamic transmission media, Coverage, Data aggregation, QoS, Connectivity [2].

III. CHARACTERISTICS OF WSNS

Unlike customary WSN like MANETs, WSN has sole individuality as follows:

a) Dynamic Network Topology**:** n/w topology modify frequently as nodes can also be delete or become a member of, node failure, channel fading or energy depletion.
b) Application Specific: The design requirement of the network varies with required application.
c) Energy constrained**:** Nodes are moveable and are greatly limited in storage capacities and energy computation. This is the most important design consideration of WSN.
d) Self-configurable: Nodes are randomly deployed without careful planning. Once diffuse, nodes have to configure autonomous themselves into a communiqué n/w [3].

IV. ADVANTAGES OF WSNS

Because the type of utilization, WSNs have revolutionized the world around us. They are fitting critical part of our lives. Following is a list of the benefit of WSN

a) Robustness to Withstand Rough Environmental Conditions

As shrinking measurement of sensor nodes they've the capacity to keep up a correspondence through a lot of substances and likewise designed to withstand in harsh climate stipulations. WSNs can be utilized in a tremendous sort of functions in environment like wooded area fireplace detection or seismic monitoring.

b) Ease of Deployment

In a sensor n/w thousands or hundreds of nodes can be diffuse in dangerous or remote atmosphere. Since these nodes are little in economical and size, hundreds throwing or thousands of sensors from a plane over a dangerous or remote region permit extract data is such a way that could not have been likely otherwise.

c) Fault Tolerance

In WSN many sensor nodes are diffuse close to all other. They are able to overcome node failure, resultant of dead or destroyed nodes thru easy exploiting other routing path. For instance during war, if an enemy destroys a surveillance sensor node, this will not affect the entire n/w.

d) Ability to Cover Wide and Dangerous Areas

In many areas, infrastructure and economic conditions prevent wired networks from being used. For example, setting-up of a wired network on a battlefield would not be possible. WSN can fill this gap due to their lack of infrastructure and their low setup costs.

e) Self Configurable

When sensor nodes are deployed in the sensing field, they have the ability to self configure in network discovery and multihop broadcast in small amount of time.

f) Mobility of Nodes

In the previous few years, mobility nodes have been exploited to trace the event for permanent track. Recently developed Protocols and architectures are able to handle these real shifting to maintain further routing.

g) Unattended Operation

WSNs are able to work unattended with a purpose to bring about decreased working time and decrease the attempt that must be carried out to administrate those structures.This is helpful to manage industrial monitoring, control and home appliances etc.

h) Improved Lifetime

The sensor nodes are placed close to every node. They can be collection together. From this set only one node can be exploited in a round robin fashion to gather data and transmit to base station (BS). It will improve the span time.

i) Improved Accuracy

In WSNs, the intently placed sensor nodes sensing and amassing the data approximately the same occasion will result in better accuracy and decreased uncorrelated noise [4].

V. SECURITY GOALS

WSN are prone to many attacks when you consider that of broadcast nature of transmission medium, useful resource hindrance on sensor nodes and uncontrolled atmosphere. Where they are left unattended. Similar to another

communiqué system, WSNs have the subsequent common security aims:

A. Integrity: Make sure message has not been modify thru malicious nodes
B. Data Origin Authentication: authenticating are the message source;
C. Availability: Make sure desired service may be accessible whenever necessary In addition, WSNs have subsequent precise security aim:
D. Confidentiality: protecting secret info from illegal entities
E. Forward secrecy: prevent a node from decrypting any future secret messages later than it leaves the n/w.
F. Backward secrecy: Stopping a add node from decrypting any earlier than send secret message.
G. Survivability: Confer an some step of service in the attendance of failures or/and attacks –
H. Freshness: Make sure that the data is newest and no adversary can replay old messages
I. Scalability: supporting a huge no of nodes
J. Entity Authentication: authenticating the client/BS/node is really the entity whom it claim to be
K. Efficiency: processing, communiqué and storage restrictions on sensor nodes must be measured.

VI. APPLICATIONS

There are broad reasons for WSN, relating to Great Duck (bird creature perception on great Duck island), Cattle Herding, Bathymetry, Glacier Monitoring, Cold Chain Management, ZebraNet, Grape monitoring, Rescue of Avalanche Victims, principal signal Monitoring, power monitoring, elements assembly, tracking military Vehicles, Ocean Water Monitoring, and Self- healing Mine discipline and Sniper Localization. According to areas of deployment WSN applications can be categorized as the following fields: military, environmental, industrial, location oriented, public Security oriented, car, airport oriented, agricultural, and emergency dealing with, scientific and oceanic. Medical and military rationalization are two of the as a rule protection-oriented usage discipline of WSN. Military sensing networks are designed to realize and acquire as so much understanding as viable about enemy actions, explosions, and different phenomena. Traditionally, wirelessly sensors nodes are integrated with manipulate, communiqué, computing, intelligence, surveillance, navy command, reconnaissance and concentrating on methods. Examples of military WSN applications are battlefield surveillance, steering systems for shrewd missiles, detection of attacks with the aid of weapons of mass destruction together with nuclear, biological, or chemical, and other monitoring applications. Due to the nature of the military, it is apparent that those applications could not be mounted without appropriate security assurance. Not too long ago, many medical programs are geared up with an enormous quantity of tiny, non-invasive sensors, located on or virtually the sufferer's body, for health monitoring functions. Such systems are being applied to measure numerous physiological values include Electrocardiogram, Blood Oxygen degree, Blood strain, activity cognizance, and lots of others., and are to be had in lots of extraordinary varieties, including wrist wearable, ambulatory instruments and as a part of biomedical intelligent clothes. The term of body sensor network (BSN) is conied to represent this kind of applications. A no of intelligent physiological sensors is integrated into a wearable wirelessly body sensor n/w, that can be exploited for computer aid rehabilitation and even early detection of medical conditions. Such functions mean that outpatients may be monitored from their homes, liberating space in hospital beds. As physiological patient data is legally required to be saved exclusive, the implemented network have got to invoke a strong protection protocol [5].

VII. SECURITY REQUIREMENTS

The purpose of security services in WSNs is to guard the resources and information from misbehavior and attacks. The security necessities in WSNs comprise:

- Availability: which ensure that the favored community services are to be had even in the presence of DOS attacks.
- Authentication: which make certain that the communiqué from one node to exceptional node is genuine, that is, a malicious node can't masquerade as a trusted on n/w node.
- Confidentiality: which make sure that a given message can't be understand thru anyone another than the desired receiver.
- Integrity: which make sure that a message transmits from one node to different is not modified thru malicious middle nodes.
- No repudiation: which signify that a node can't deny transmits a message it has before transmits.
- Forward secrecy: A sensor must now not be able to learn any future messages after it leaves the community.
- Authorization: Which make sure that simplest licensed sensors will also be concerned in supplying understanding to network services.
- Backward secrecy: A joining sensor will have to no longer be ready to read any beforehand transmitted message. The safety services in WSNs are commonly founded on cryptography. Nevertheless, because of the

constraints in WSNs, many already present secure algorithms will not be practical for use [6].

VIII. ATTACKS ON WSN AND THEIR MITIGATION

The security breaches arise principally within the form of Interruption (breakdown of communique hyperlinks), Interception (unauthorized access of WSN), change (exchange of data through unauthorized entry) and fabrication (Addition of false data via unauthorized accesses).

a) Denial of service (DOS)

This type of attack results into making busy the resources to their deliberate users. As an instance node "A" sends request to node "B" for communication and node "B" sends renowned to node "A" however, „A" continues on sending request to "B" always. As a result "B" is not able to communicate with any other nodes and thus becomes unavailable to all of them. Dos attack might also arise at link layer thru jamming (thru broadcasting mechanism) and/or tampering (amendment or fabrication) of the packet. In link Layer it's with the aid of producing collision info, exhaustion of assets and unfairness in use of networks. In network layer, it happens via neglecting and the greediness of packets ensuing into direction failure. Most of DOS attacks could also be avoided by using robust authentication and identification mechanisms.

b) Attack of information in transit

In case of WSN most commonly each and every node reports changes to a cluster head or BS just for data above some threshold data in send might be spoofed, replayed, alter vanished or once more. This kind of attack may be prevented thru authentication and data aggregation method.

c) Sybil attack

In this attack the attacker gets unlawfully several individuality on one node. Thru this, the attacker typically affects the routing mechanism. Sybil attacks are usually prevented thru validation method.

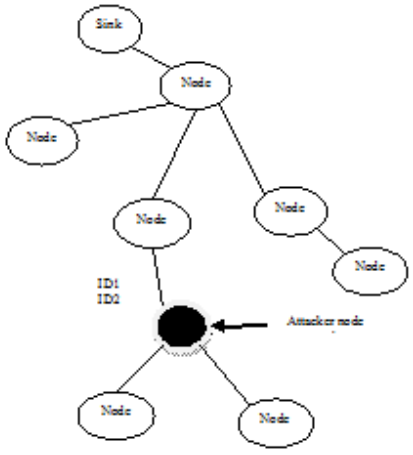

Fig.2 Sybil attack

d) Black hole/Sinkhole Attack

In this kind of attack, attacker places himself in an n/w with highest ability resources (highest processing power and maximum band width) by which it continually creates shortest direction. As a result, all data passes thru attacker's node.

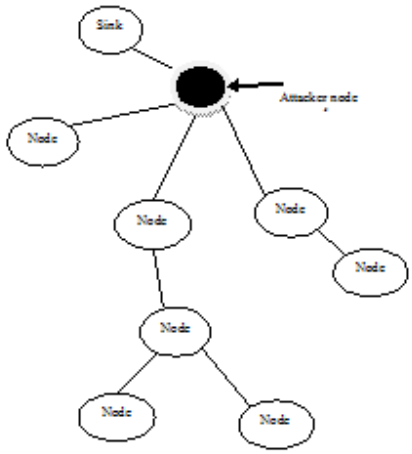

Fig.3 Blackhole/S sinkhole Attack

e) 'Hello flood' Attack

In WSN, This is an essay attack in that attacker broadcasts HELLO packets with highest transmission power to source or destination. The nodes receiving the messages assume that the sender node is nearest to them and sends packets by this node. Thru this attack congestion occur in the n/w. This is a exact kind of DOS. Blocking method are exploited to prevent Hello Flood attacks.

f) Wormhole attack

On this assortment of attack, the attacker utilizes burrowing instrument to set up himself between them by means of muddled the routing protocol. Figure 4 demonstrate the design of wormhole attack let „Y‟ desires to send data by mode of propagation before sending the data to get the path. However the "Y" acquaint himself as a node "X" and an attacker sends acknowledgement to "Y". "Y" sends data to " X" and "X" sends that facts to attacker and attacker gets the data by "X‟ . the data acquistius by means of attacker to "X" by tunneling, hiding its personal identification. In this case "X" and "Y" are not in a single hop but they believe that they are in a one hop range. Thus, security may dissipate by an attacker intervention, interception, revisal and creation[7].

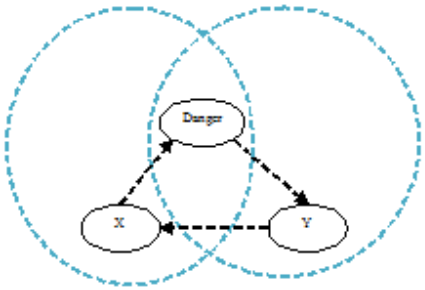

Fig.4 Wormhole Attack

IX. DISTRIBUTED DENIAL OF SERVICE ATTACK

DOS attacks are outlined as attacks which are launched via a collection of malicious entities closer to a victim, with the intention of incapacitating it from offering additional provider to reliable purchasers. The ambitions of the attack are executed through exploiting both system/protocol-stage vulnerabilities, or by means of forcing the sufferer to undertake computationally intensive tasks, in simple word DDOS attack attempt to unnecessarily consume network resource and decrease network performance. DOS attack with flooding not only creates congestion but also consume battery life. As a single victim node may be centered with overwhelming range of incoming requests from a couple of ends of the network. The attacker nodes can either be respectable but compromised nodes working in the community, or be a laptop-class adversary, i.e. an adversary with higher capabilities, utilizing solid identities to generate a tremendous set of reliable packets for overwhelming the sufferer node. It is assumed that no pre-hand information is to be had to elude in the direction of central (abilities victims) nodes in the community. For this reason, an adversary have got to have statement capabilities for a targeted interval of time to establish on the primary nodes within the network. Intelligent group of adversary will launch the DDOS attacks from many ends of the n/w thus as to avoid being detected thru a detection module observing traffic from a single point of origin in the network. A DDOS attacks may be classified into two categories which are Direct Attack and Reflector Attacks. These threats can ateriorly sorted as Flooding, Ping of Death, Smurf Attack and Flooding on Victim's Link [8].

X. WSN TECHNIQUES

a) WDM

The schematic of a fiber sensor network using optical power supply with WDM technique. There are two laser diodes (LDs) with a wavelength of 1.5μm and 1.3 μm in a monitoring station. The light from these LDs are combined by a WDM coupler, transmitted through an optical fiber, and split by a 1xN optical splitter. Optically driven nodes are located at the ends of the optical fiber branches. In this study, we developed two types of nodes. One is a wired sensor node that controls semiconductor-based wired sensors. The other is a wireless node that communicates with a wireless sensor. Both nodes have a WDM coupler that separates the incident light into the wavelengths of 1.5 μm and 1.3 μm. The 1.5-μm light is lead to an InGaAs PV cell, which generates electrical power to drive the node. Since the output voltage from the PV cell is as low as 0.4 V, it is boosted to 5V by a booster circuit [9].

b) Clustering

Clustering is one of the techniques that can be used to meet the challenges in WSN. In clustering, sensor nodes are endue into less significant groups called clusters. In each cluster, a CH is designated. The records from the sensor node is exceeded to the CH in every cluster; the CH forwards it to the base station or sink.

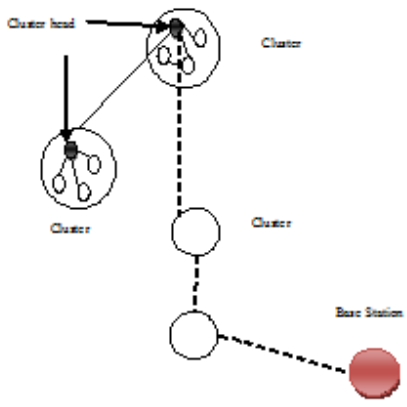

Fig.5 Clustering

The cluster based agency of the sensor nodes leads to a two level hierarchy, in which CH is the higher stage and the sensor node the low degree. The base station is the data

processing centre where the give up person get admission to records. Clustering affords universal device scalability, increase network lifetime and energy efficiency. In addition in the cluster the direction setup is localized, network topology is stabilized and the CH can agenda activities within the cluster [10].

c) LAD Localization Anomaly Detection

A scheme named Localization Anomaly Detection (LAD) is proposed by Due to detect anchor node outliers in the localization process for WSNs. The scheme attempts to identify the outliers and perform compromise resistant localization without remove the malicious anchors from the network. LAD takes advantage of the deployment understanding this is available in lots of sensor networks applications. When sensor nodes are deployed in groups, every node follows two-dimensional Gaussian distribution, which is centered on the deployment factor of the node's group. It uses the known deployment information and the group membership of neighbor sensor nodes to check whether the computed position of the unknown nodes is consistent with the known deployment knowledge. If it is inconsistent, LAD will report an outlier. Three metrics are proposed to degree the diploma of inconsistency among an unknown nodes derived location and its commentary; the metrics are Difference metric Add-all metric and Probability metric. For each metric, they obtain a threshold through training. If the rank of discrepancy increase such threshold, they declare that the localization results are incompatible with the observation, For that motive an alarm may be raised. They have evaluated LAD approach, inclusive of its tolerance to malicious attacks, fake positive rates, detection charges, etc. The simulation effects show that even if the outlier detection thresholds are not optimally selected, the technique still has a excessive detection fee and low false alarm charge for large localization errors. This makes it a great candidate for localization outlier detection. In addition to being effective in detection assaults in opposition to the localization, LAD have to also resist in opposition to assaults at the outlier detection scheme itself. As a whole lot as adversaries want to attacks localization schemes, they may attack the detection scheme if they recognize any such scheme is deployed; there are a number of attacks the adversaries can release. Therefore, the authors have developed a mathematical framework to model those attacks, and this model is used in their simulation-based evaluation to generate attacks. The results display that the proposed detection scheme is tremendously resilient towards attacks that can reason large harm [11].

XI. LITERATURE SURVEY

Shital Patila et al. [2016] in this paper, An immune method is proposed for the DoS attack on WSN to be able to give a boost to the accuracy expense of assault prevention, curb the false alarm rate and capable to respect exclusive Dos attacks. WSN has extensive applications in knowledge gathering and knowledge transmission via wireless networks. Because of the weaknesses within the WSN, the sensor nodes are liable to most of the safety threats. DoS attack is most standard attack on these sensor nodes. Some attack prevention systems must be used in opposition to DoS attacks. There are different techniques to prevent DoS attack in WSN [12].

Kanchan Kaushal et al. [2016] in this paper, they illustrate a kind of method recognition of DDOS attack in WSN for the detection of DDOS attack. It will detect the attack on early stages so that data loss can be prevented and more energy can be reserved after the prevention of attacks. Efficiency of this scheme has been obvious on the foundation of throughput, packet supply ratio, no. Of packets flooded and last energy of the n/w [13].

Raksha Upadhyaya et al. [2015] in this paper, we define a explanation to prevent WSN from DDOS attack exploiting dynamic source routing (DSR). Energy of concerned nodes has been exploited for prevention and detection of attack. Qualnet 5.2 simulator is exploited for execution of the define explanation. unwrap WSN nature build it susceptible to external threats. So many security threats as DOS, sinkhole and black hole etc. may possess the n/w presentation. DDOS attacks are described as attacks which are launched thru a collection of malicious entities towards a node or group of nodes [14].

Megha Dubey et al. [2015] this paper is proposed routing protocol is implemented and simulated in NS2 network simulation environment. As a way to simulate the routing efficiency utilizing two one-of-a-kind network scenarios the efficiency is compared. And the comparative efficiency learn is carried out in phrases of packet delivery ratio, throughput, end to finish lengthen and vigor consumption. The acquired consequences express the valuable performance with reverence to the usual routing protocol [15].

Varsha Nigam et al. [2014] on this paper, they describe a profile depend protection scheme PPS security design against DDOS attack. This ruler of attacks is flooding entrée quantity of needless packets in n/w thru which the n/w bandwidth is consumed thru which data delivery in n/w are affected. Our major objective is evoke the effect of DDOS attack in n/w and distinguish the node or nodes which strike the n/w performance. The profile depend security approach are verify the profile of all node in n/w and only the attacker is a

node which swamped the unneeded packets in n/w then PPS has block the appearance of attacker. The execution of network is deliberate on the basis of performance metrics like routing load, throughput etc [16].

Almir Davis et al. [2012] A WSN comprise of spatially distributed autonomous sensors which cooperatively atmosphere circumstances or monitor physical, like as sound, vibration, pressure, motion, or pollutants, temperature, at dissimilar locality. Current advance in lowest-power highest-integrated electronics, advances in micro-electro-mechanical systems (MEMS), quick increase in the kind and value of available sensors, and advancement in communication have permissible WSNs to get an extraordinary expansion in commercial, industrial and military applications. In sequence to improve know WSNs, we seem at their n/w architectures. We categorize current WSN architectures into exact set depend on WSN conduct and data flow features. Obtainable architectures are define and existing along with their recompense and weakness. The accessible architectures are also assess in word of mostly ordinary WSN performance parameters e.g lifetime of n/w, reliability, QoS, fidelity, scalability, modularity, latency, and ease of deployment [17].

Jiawei Chen et al. [2011] In this paper, introducing a key chain distribution idea where the BS pass the sole method key chains to the source all the storage, computation burden and time interval on the source can be decrease, with good security recital for the sole-way key chain. The simulation specify which the newest method can solve the drawback which a powerful source with largest memory resource is necessary in the basic MSP method, As a result, our method is extra at ease and has wider applicable vicinity than the fundamental MSP strategy in the WSN [18].

XII. CONCLUSION

WSNs are susceptible to massive collection of security threats due to their exploitation in an unwrap and insecure atmosphere. In many applications, the WSNs have become a promising aspect. A variety of attacks can threaten the sensor networks in the absence of proper security techniques. In this paper, we converse about different protection techniques, which used for defense in WSNs. we relevant a all-inclusive survey of different attcks instead of DDoS attacks, detection techniques.

REFERENCES

[1] Ankita " A Survey on Wireless Sensor Network based Approaches" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 4, April 2014 ISSN: 2277 128X.

[2] Vinay Kumar , Sanjeev Jain and Sudarshan Tiwari "Energy Efficient Clustering Algorithms in Wireless Sensor Networks: A Survey" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011 ISSN (Online): 1694-0814.

[3] Heena Dhawan, Sandeep Waraich " A Comparative Study on LEACH Routing Protocol and its Variants in Wireless Sensor Networks: A Survey" International Journal of Computer Applications (0975 – 8887) Volume 95– No.8, June 2014.

[4] SANJEEV KUMAR GUPTA, POONAM SINHA "Overview of Wireless Sensor Network: A Survey" International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 1, January 2014.

[5] Zhijun Li and Guang Gong "A Survey on Security in Wireless Sensor Networks"2010.

[6] Rajkumar, Sunitha K R and Dr.H.G.Chandrakanth "A Survey on Security Attacks in Wireless Sensor Network" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622.

[7] Abhishek Pandey, R.C. Tripathi "A Survey on Wireless Sensor Networks Security" International Journal of Computer Applications (0975 – 8887) Volume 3 – No.2, June 2010.

[8] Raksha Upadhyay, Salman Khan, Harendra Tripathi, Uma Rathore Bhatt "Detection and Prevention of DDOS Attack in WSN for AODV and DSR using Battery Drain" 2015 IEEE.

[9] [9]Yosuke Tanaka, Shuhei Kobayashi, Akimasa Shiomichi, and Takashi Kurokawa "Low power fiber sensor network deploying both wired and wireless sensors using optical power supply with WDM technique" 978-1-5090-1906-9/16/$31.00 ©2016 IEEE.

[10] [10]Savitha M, Shantala Devi Patil "A Survey on Clustering Techniques in Wireless Sensor Networks" International Conference on Advances in Computer and Communication Engineering (ACCE-2014), Volume 4, Special Issue 1, April 2014), (ISSN 2250-2459.

[11] Hala Abukhalaf, Jianxin Wang and Shigeng Zhang "Outlier Detection Techniques for Localization in Wireless Sensor Networks: A Survey" International Journal of Future Generation Communication and Networking Vol. 8, No. 6 (2015), pp. 99-114.

[12] Shital Patila, Sangita Chaudharib," DoS attack prevention technique in Wireless Sensor Networks" ScienceDirect, International Conference on Communication, Computing and Virtualization 2016.

[13] Kanchan Kaushal, Varsha Sahni "Early Detection of DDoS Attack in WSN" International Journal of Computer Applications (0975 – 8887) Volume 134 – No.13, January 2016.

[14] Raksha Upadhyaya, Uma Rathore Bhatta , Harendra Tripathi "DDOS Attack Aware DSR Routing Protocol in WSN" ScienceDirect, International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur.

[15] Megha Dubey , Prof Mayank Bhatt , Prof Rajat Bhandari "Prevention of DDOS Attack in Wireless sensor network using secure routing" International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 2, February 2015.

[16] Varsha Nigam, Saurabh Jain and Dr. Kavita Burse "Profile based Scheme against DDoS Attack in WSN" Fourth International Conference on Communication Systems and Network Technologies 2014 IEEE.

[17] Almir Davis, Hwa Chang, "A SURVEY OF WIRELESS SENSOR NETWORK ARCHITECTURES" IJCSES Vol.3, No.6, December 2012.

[18] Jiawei Chen "Broadcast Authentication Protocol Scheme Based on DBP-MSP and Safe Routing in WSN against DDoS Attacks" 2011 IEEE.