Volume 3, Issue 10, October 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Attacks on Wireless Sensor Networks: A Survey

Manisha, Gaurav Gupta
Department of Computer Science Engineering
Shoolini University, HP, India

Abstract- Wireless Sensor Network platforms are less expensive and more powerful having tiny electronic devices called Motes (sensor nodes). Wireless sensor networks enhance its popularity in military and health centric research areas; now it is also popular in industrial area. This paper describes the security requirements as WSNs are easily prone to more attacks than wired networks. This paper studies the security attacks in WSNs that are popular now days. This paper also elaborate the most popular attack i.e. wormhole attack and their countermeasures in the network layer.

Keywords-Wireless Sensor Networks, Attacks, Wormhole Attack, Sensor Nodes, Sinkhole attack

I. INTRODUCTION

Wireless sensor networks (WSN) [1, 3, and 4] are emerging as the most promising research area for the researchers over 15 past years [1]. Wireless sensor networks are categorized in four ways: Terrestrial WSNs, Underground WSNs, Underwater WSNs and multimedia WSNs. These wireless sensor networks have composed thousands of sensor nodes called Motes. These sensor nodes which act as autonomously are distributed over the region to analyse the hostile environment conditions [1, 4].

These sensor nodes communicate with each other via base station fig.1.

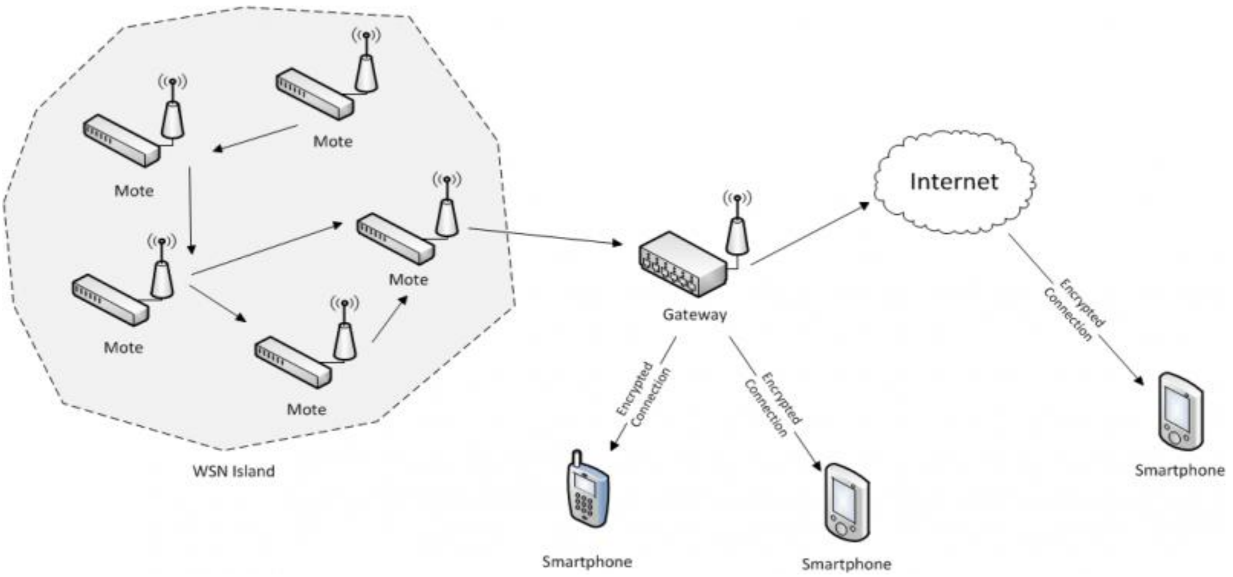


Fig1. Wireless sensor network

These tiny Sensors nodes (Motes) have transceivers, limited battery power, less memory and limited signalling capability as shown in fig 2.

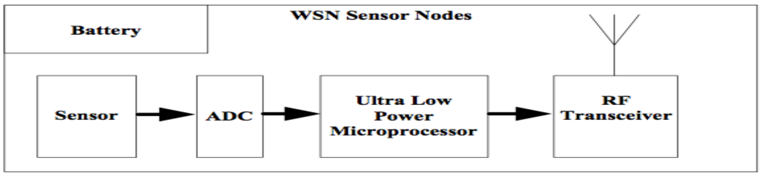


Fig2. Sensor nodes in WSN

With rapid development, there are many applications where autonomous nodes (Motes) are deployed to interact with environment and to cooperatively pass their data through network to the main location [1, 2, 5]. The development of wireless sensor networks was concerned by battlefield surveillance; now these networks are developed in industrial process monitoring and control, machine health monitoring and so on.

Wireless sensor nodes have insecure wireless communication are easily vulnerable by threats. Reliable and secure communication, as a main aspect of any wireless networking environment, is an especially significant challenge in wireless networks. The mission critical nature of sensor nodes imposed many attacks such as:

1. Attacks on authentication
2. Attacks on data integrity.
3. Attacks on data availability.

The deployment of sensor nodes may have intelligent adversaries intending to subvert damage or hijack message exchanged in the network. This may leads to degrade performance in the network and change the overall topology of network. Hence, Security is the important and critical issue in the wireless networks due to its operating nature. It is a fundamental concern in order to provide protected and authenticated communication between sensor nodes [1, 2, 5]. Various researches had been completed on the security of sensor nodes in the wireless sensor networks. This paper is organized as: section II represents the security requirements in wireless networks. Section III represents the constraints in WSNs. Section IV represents the attacks in Wireless networks and their countermeasures. Section V represents conclusion of this paper.

II. SECURITY REQUIREMENTS[8]

In wireless sensor networks, physical security of sensor nodes is not granted as they are usually deployed in hostile environments. Therefore, attackers can easily compromise sensor nodes and use them to degrade the network's performance. Wireless sensor networks exhibit many unique characteristics and imposing various security services. These security services protected information and resources from the attackers.

TABLE I. The main Security Requirements (CAIFASO) in Wireless Sensor Networks [8, 5]

Security requirements	Description
Data confidentiality	• Data that are passed over the network should be confidential. Public sensor information like sensor identities and public keys should be encrypted by using cryptographic method. Sensor readings should not be leaked to its neighbours.
Data availability	• It ensures that resources and data should be easily available to the sensor nodes. Different approaches have been proposed to achieve this goal.
Data integrity	• The data may be altered by attackers as it is traverse among sensor nodes. So, integrity control should be implemented to ensure that traversed data should not be altered until it reaches to its original recipients.
Data freshness	• Data freshness refers that data should be updated up to time. No old messages should be convey among sensor nodes. This requirement is especially important when there are shared-key strategies employed in the design
Authenticity	• Authentication is required for many administrative tasks. Various authentication mechanisms such as cryptography, shared keys digital signature and so on must ensure that data used in decision making process comes from legitimate and authorized nodes.
Self-Organization	• Nodes in wireless network should be feasible in order to be self-healing and self-organizing in any difficult situations. If self-organization is lacking in a sensor network, the damage resulting from an attack or even the hazardous • Environment may be devastating. Several key distribution approaches implemented to achieve this feature inn wireless sensor networks.

III. CONSTRAINTS IN WIRELESS SENSOR NETWORKS[9,19]

Wireless sensor network considered as a special type of adhoc networks composed of large no. of sensor nodes. These nodes have several resources constraints such as memory limitations, restricted energy, unattended operations, and high latency of communication. Due to these constraints, the adversary causes serious threats to degrade the performance of network and also difficult to implement the conventional security mechanisms in WSNs [1, 2]. In order to optimize the conventional security mechanisms, it is necessary to be aware about the constraints of sensor nodes.
These constraints are explained as [19]:

A. Memory restriction

Sensor nodes which are compact in size, have limited memory space. Memory is of two ways for sensor nodes: RAM and flash memory. RAM is used to store the computational result, application program [3]. Flash memory generally includes downloading application code. It is difficult to employ high loaded security mechanisms in this limited memory space. It causes serious memory overhead problem in WSNS- TelosB- has a 16-bit, 8 MHz RISC CPU with only 10K RAM, 48K program memory, and 1024K flash storage. The current security algorithms are therefore, infeasible in these sensors [19].

B. Restricted Energy

As energy play an important role in lifespan of sensor node. In WSNs, sensor nodes employ limited power and they are easily destroyed.

C. High Latency of Communication

Due to network congestion, the problem of greater latency in communication occurred in WSNs [3]. This high latency achieve critical problem of synchronization in security mechanisms that rely on critical reports and key distribution.

D. Unattended Operations

Some sensor nodes are unattended for a long period of time as they are spatial distributed on remote region. Some of the major caveats to unattended Motes are [3]:

a. Due to the deployment of senor nodes in adversary environment, WSNs faces serious physical attacks that are not easily removed and detected.
b. Remote management make impossible to detect physical tampering and battery replacement and nodes may not have friendly interact with other once deployed.

IV. ATTACKS AND THEIR COUNTERMEASURES IN WIRELESS SENSOR NETWORKS

The above constraints may tend to increase serious attacks on different layers in WSNs. Some of the layered based attacks are explained as:

A. Physical Layer Attacks[2,3,6,7,15]

Physical layer is responsible for bit transmission and signal monitoring, frequency selection and soon. Physical layer attacks are categorized as active attacks and passive attacks. Adversaries can do many attacks on it as all upper layer functioning rely on it. Some of the major attacks are:

Jamming: it is the most popular attack that conducts on physical layer by attackers. It simply provides disruption in the availability of transmission media. With device jamming its surrounding sensors, adversaries can disrupt the entire sensor network by deploying enough number of such devices. To defence this attack, use channel hoping and spread spectrum techniques for radio communication. Algorithms statically analysing the receive signal strength indicator values and the packet delivery ratio techniques can reliably identify all four types of jamming [2, 3].

Device tempering: Attackers can easily damage or modify sensor physically and stop all services that are in progress. To defence this attack, temper proofing approach has been introduced. Various algorithms such as self-destruction (node vaporizes their memory contents and this can prevent any leakage information.) and fault tolerance method [2, 3].

B. MAC Layer Attacks[2]

As wireless channel is open, many adversaries can affect the MAC layer by conducting serious attacks. Sensors rely on this layer to coordinate their transmission to share the wireless channel fairly. MAC protocols have special significance that it helps in maintaining the communication resources effectively. Adversaries can forge MAC layer identification and masquerades other entities for the various purposes. Two attacks are introduced in this layer such as traffic manipulation and identity spoofing. In the first attack, attacker can create collisions and unfairness by disobeying the coordinate rules which can further lead traffic distortion. The second attack is responsible to spoofing the MAC layer identities. Due to broadcast in nature, MAC identities such as certificates are open to all its nodes, attackers can easily act as a legitimate node by tracing the legitimate nodes' identity and take over the whole network. To defence these attacks, many approaches have been presented by researchers such as identity protection-to protect the identities from adversaries, Cryptography based mechanisms and other authentication mechanisms have been implemented. In addition to authentication, others security measures also exist such as code attestation, sequence checking and position verification. These countermeasures are responsible to detect the malicious nodes by validating the code.

C. Network Layer Attacks[2,3,5,7,16]

The responsibility of network layer is to locate destination and to find out the secure path for exchanging control packets among nodes. Various routing protocols exist that are quite simple and easy to implement. Due to this, attackers can easily fail the communication in WSNs by modifying the routing information. Network layer attacks are the most popular attacks in WSNs. Adversaries can gain access to routing paths and redirect the traffic, or distribute false information to mislead routing direction, selectively forwarding packets through certain sensors, etc.

Network layer attacks can be categorized as:

C.I. Selective Forwarding Packet [2, 3, 9, 6]

As its name suggest, the attackers tries to directly forward packages towards a certain node in order to remove the packages' importance. The attackers selectively send the information of the sensor nodes and also discard the information from sensor nodes. However, it is conceivable an adversary overhearing a flow passing through neighboring nodes might be able to emulate selective forwarding by jamming or causing a collision on each forwarded packet of interest. To defense this, multi path routing can be used with random selection of path and braided paths which do not have two consecutive links. Other approaches such as observing nodes behavior, listening channel and use acknowledgement mechanisms have been introduced.

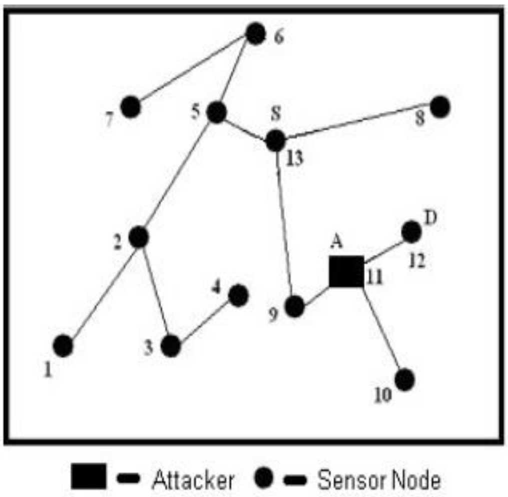
C.II. False Routing Path [2]

False routing attacks enforced in three types of attacks which can be used to place the adversary in route and disrupt the network functionalities as:

i. *Overflowing routing tables*: attackers can inject the void routing information in the networks that will eventually occupy the majority of routing table space on normal nodes. This can lead the overflow problem I the routing table. For example. In fig3. a) represents the topology and routing table before this attack. If A was a normal node, then S can communicate with D node. And if A was attacker then it sends the wrong routing information about nonexistent nodes and there is no path between S and D nodes. b) represents the wrong topology and routing table after this attack.

ii. *Routing table poisoning*: malicious nodes modify the routing updates before sending and receiving the messages inside the network and make “poison”. This attack will direct traffic in the wrong path and may result in congestion and also tends to increase further attacks in the network.

iii. *Cache poisoning:* the adversary can poison the cache by using similar techniques as in routing table poisoning.



Destination	Path	Destination	Path
5	13→5	7	13→5→6→7
2	13→5→2	8	13→8
3	13→5→2→3	9	13→9
4	13→5→2→3→4	11	13→9→11
1	13→5→2→1	12	13→9→11→12
6	13→5→6	10	13→9→11→10

Fig.3 (a) Topology and routing table before attack

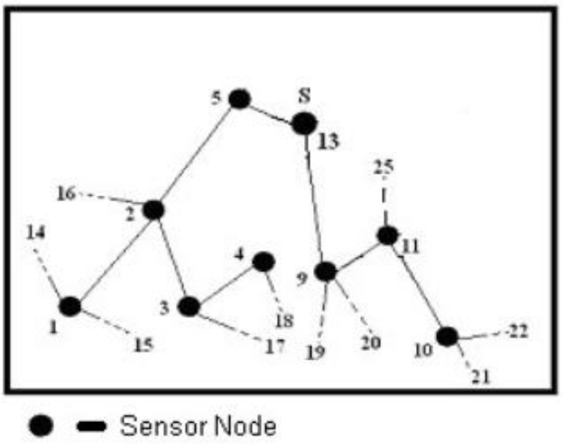


Fig.3 (b) Topology and routing table after attack

Destination	Path	Destination	Path
14	13→5→2→1→4	11	13→9→11
15	13→5→2→1→15	10	13→9→11→10
16	13→5→2→16	20	13→9→20
17	13→5→2→3→17	21	13→9→11→10→21
18	13→5→2→3→4→18	22	13→9→11→10→22
19	13→9→19	25	13→9→11→25

C.III. Wormhole Attack [2, 3, 1,]

Wormhole attack is most complicated attack in WSNs which is hardly to detect. Wormhole attack has two or more adversaries (established tunnel and high bandwidth, power resources). A.A. Pirazada and McDonald concluded that the wormhole attack poses three ways [17]:

i. Tunneling the messages above the network layer.

ii. Long range tunnel using high power transmitters.

iii. Creation of tunnel via wired infrastructure.

In wormhole attack, adversary may create a high quality between and move the whole traffic on it. The adversary received messages from one section of network and tunnels these messages over a low latency link and replays them to the other section of network instead to original destination as shown in fig.4.

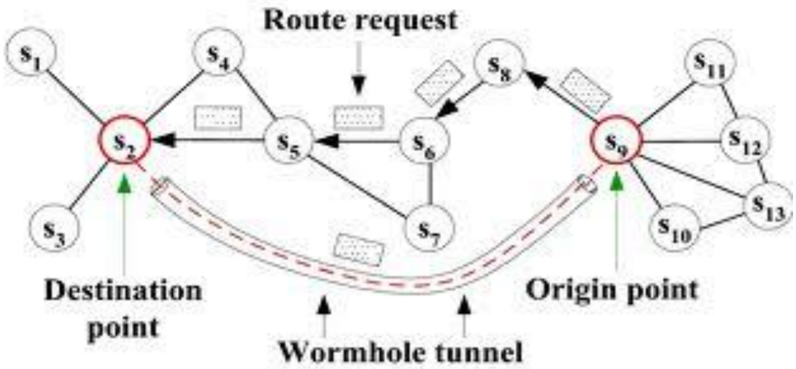


Fig.4. A Scenario of Wormhole Attack

Wormhole attack can be used to exploit the routing race conditions (refers that when a node take some actions based on the first instance of messages it receives and subsequently ignores later instances of that messages) and more effective even if any authentication and encryption mechanism used. Wormhole attack is the combination of various attacks such as black hole attack, sinkhole attack and eavesdropping.

D.I. Black hole Attack [2, 3, 6, 9, 10, 16]

As black hole absorbs all things in it, this attack also swallows all messages in it before receiving. It is the simplest attacks in WSNs. By refusing to forward any message he receives, the attacker will affect all the traffic flowing through it and may result to break the communication channel to the base station and rest of WSNs and degrade the performance of whole network [3]. If compromised node does not introduce itself as a sink, closer to the sink, makes more interruptions in the network by absorbing the more traffic as shown in fig.5.

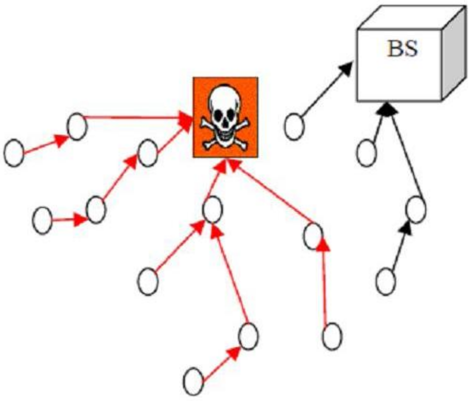


Fig.5. Black Hole Attack

To defence this, may approaches are introduced such as geographic forwarding (Motes are aware of their neighbouring nodes' coordinates and send messages according to geographical positions) and resistive routing protocol (use of systematic rerouting, this attack can be overcome and detected).

D.II. Sinkhole Attack [2, 3, 6, 9, 7, 16]

As the name suggests, the adversary create a sink nearby 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 adversary may drop all packets in the network and modify the topology of network. Since all the nodes communicate with each other via base station, the adversary 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 empowered 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.

Wormhole facilitates a variety of attacks against key establishment and routing protocols. It can affect network functionality, data aggregation and clustering protocols. This attack can be launched without using the encryption mechanism or compromising any legitimate node in the network. In simple words, wormhole attack is most popular and complicated attack that causes hazards damage in the network.

There is a lot of work that has been implemented in order to curb the wormhole attack and poses two methods such as wormhole detection method(introduce various routing mechanisms to detect the wormhole attack by using any simulation process) and wormhole prevention(to remove wormhole completely from the network by developing various methodologies).

Table II. LITRATURE SURVEY ON THE WORMHOLE ATTACK DETECTION MECHANISMS [10, 11, 12, 13, 14, 17, 18]

Methods	Description	Problem
Packet leashes proposed by Y. Hu. A. Perring and D.B Johnson	• Prevent packets from travelling farther than radio transmission range. • Overcome the wormhole attack by restricting the maximum distance of transmission by using time synchronization • Two ways: temporal leash(ensure that packets should be upper bound on its lifetime) and geographical leash(ensure that the recipient of the packet is within a certain range of sender)	• Need Highly synchronized clocks • Need information about nodes' location and all nodes must have loosely synchronized clocks. • Limited applicability in WSNs.
Wang's approach (end-to-end location information)	• Each node appends its location and time to a packet it is forwarding and uses authentication code to secure the information.	• End nodes left to do all verification
SECTOR by Capkun et al	• Uses a distance bounding algorithm to determine the distance between two communicating nodes. • Do not require any clock synchronization or location information	
MDS-VOW by Wang	• Method for graphically visualizing the occurrence of wormhole in static sensor networks by reconstructing the layout of the sensors using multidimensional scaling.	• Requires a central controller and thus not readily suitable for decentralized networks
LAGNS(location aware guard nodes) by L. Lazes	• Inherit the guard node to detect the message flow between nodes. • Use guard property and communication range constraints property	
SAM(simple scheme based on statistical analysis) by N. Song	• Calculate the difference between most frequently appeared link and the second most frequently appeared link in the set of all obtained routes. • Maximum relative frequency and difference are much higher under wormhole attack than in normal system.	
RTT(round trip time) by Zaw Tun and Aung htein Maw	• Does not require any special hardware or synchronized clocks. • To calculate the round time between successive nodes and their neighbours nodes • Consists three phases: ▪ To construct neighbour list for each node ▪ To find the route between sources to destination node ▪ To find the location of wormhole link to make any necessary action.	• Memory and bandwidth overhead.
Distributed detection method by Dezun Dong	• Relies solely on network connectivity information. • Based on Local topology.	

Transmission time based detection mechanism	• It consists three phases: ▪ Grid formation phase(sensor nodes are arranged in grid form and identify the location of node) ▪ Construction of neighbour list(broadcasts neighbour request message and reply message between neighbour nodes and calculating the time between REQ and REP of neighbour nodes) Detection (to detect the wormhole attack by comparing the transmission time of suspected nodes with legitimate nodes) • Based on the assumption that if transmission time of suspected nodes is greater than legitimate nodes, then it leads wormhole attack in the routing path	• Memory overhead Energy consumption • Bandwidth overhead.

V. CONCLUSIONS

Wireless sensor networks have gained much popularity over past few years. Due to its operating nature and openness in wireless channel, security is the most challenging aspects in it. The survey of wireless networks security is vast with various attack models and counter measures proposed by researchers. We have elaborated different attacks that spoil the functioning of the network and degrade the performance of network. Among the various attacks of different layers, wormhole attack, combination of others attacks, is the most popular attack because of its complex nature and hard to detect. Wormhole attacks can significantly degrade the network performance and threaten network security. Various countermeasures have been done for the detection of wormhole attack as above explained. Hopefully by reading this paper, the readers can have a better view on security requirements with attacks and their countermeasures at network layer in WSNs.

References

[1] Rohit Tiwari, Monika Kohli, "*Security Aspects for Wireless Sensor Network"* International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 8, October – 2012

[2] Kai Xing †, Shyaam Sundhar Rajamadam Srinivasan †, Manny Rivera †, Jiang Li ‡, Xiuzhen Cheng †, *"Attacks and Countermeasures in Sensor Networks: A Survey*", NETWORK SECURITY Scott Huang, David MacCallum, and Ding Zhu Du (Eds.) pp. – - –c2005 Springer

[3] 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)1926-1932, 2012 © 2012, TextRoad Publication, ISSN 2090-4304, Journal of Basic and Applied Scientific Research

[4] Tanveer Zia and Albert Zomaya, "*Security Issues in Wireless Sensor Networks*"

[5] Adrian Perrig, John Stankovic, David Wagner, "*Security in Wireless Sensor Networks*" Communications of the ACM, Page53-57, year 2004

[6] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "*Security in Wireless Sensor Networks: Issues and Challenges*", International conference on Advanced Computing Technologies, Page1043-1045, year 2006

[7] Zinaida BENENSON a, 1, Peter M. CHOLEWINSKI b, Felix C. FREILING a, "*Vulnerabilities and Attacks in Wireless Sensor Networks".*

[8] Wireless Sensor Network Security, *"A Survey John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin* Chaudhary", Security in Distributed, Grid, and Pervasive Computing Yang Xiao, (Eds.) pp. – - –°c 2006 Auerbach Publications, CRC Press

[9] Chris Karlof *, David Wagner, "*Secure routing in wireless sensor networks: attacks and countermeasures*", Ad Hoc Networks 1 (2003) 293–315

[10] Priya Maidamwar and Nekita Chavhan, "*A SURVEY ON SECURITY ISSUES TO DETECT WORMHOLE ATTACK IN WIRELESS SENSOR NETWORK",* International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 4, October 2012

[11] Xiaopei Lu, Dezun Dong, and Xiangke Liao, *"MDS-Based Wormhole Detection Using Local Topology in Wireless Sensor Networks",* Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2012, Article ID 145702, 9 pages doi:10.1155/2012/145702

[12] Majid Meghdadi, Suat Ozdemir and Inan Giiler (2011*),"A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Network"*, IETE Technical review, Vol.28, Issue.2, PP89-102

[13] Marianne Azer, Magdy, El-Soudani, Sherif El-Kassas (2009)," *A Full Image of the Wormhole Attacks towards Introducing Complex Wormhole Attacks in Wireless AdHoc Networks*", International journal of Computer Science and Information Security, Vol.1, No.1, PP 41-52

[14] Fan-rui KONG†1, Chun-wen LI1, 3, Qing-qing DING2, Guang-zhao CUI3, Bing-yi CUI4, "*WAPN: a distributed wormhole attack detection approach for wireless sensor networks"*, Journal of Zhejiang University SCIENCE a ISSN 1673-565X (Print); ISSN 1862-1775 (Online)

[15] Rina Bhattacharya, "*A Comparative Study of Physical Attacks on Wireless Sensor Networks*", *IJRET,* vol. 2, issue 1, pp. 72-74, Jan 2013

[16] Atul Yadav, 2Mangesh Gosavi , 3Parag Joshi, *"Study of Network Layer Attacks and Countermeasures in Wireless Sensor Network"*, International Journal of Computer Science and Network (IJCSN) Volume 1, Issue 4, August 2012 www.ijcsn.org ISSN 2277-5420

[17] Zaw Tun and Aung Htein Maw, *"Wormhole detection in Wireless Sensor Networks*", World Academy of Science, Engineering and technology 46 2008

[18] S.Sharmila and G.Uamaheshwari, "*Transmission Time Based Detection of Wormhole Attack in Wireless Sensor Networks"*, Special Issue of International Journal of Computer Applications (0975-8887) on IPRC, August 2012.

[19] Jaydip Sen, *"A Survey on Wireless Sensor Network Security",* International Journal of Communication Networks and Information Security (IJCNIS) Vol. 1, No. 2, August 2009