International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 01, January-2017

Security in Wireless Sensor Networks: DoS Perspective

Zafar Iqbal Khan, Mohammad Mazhar Afzal
Department of Computer Science & Engineering
Glocal University, India

***Abstract* - Wireless Sensor Network (WSN) is being used in a wide range of applications primarily for detecting, recording and communication physical world events in a real-time environment. Events recorded by sensors are accumulated and subsequently communicated to some special nodes of high computational capabilities known as Base Station or simply BS. Communication among nodes, between nodes and accumulating nodes, between nodes and base stations are predominantly wireless, which carries inherent weaknesses of wireless communication, augmented with very little computational resources, these nodes become more vulnerable for various types of attack. DoS/DDoS has wide area of application for real time event detection. The sensing capability of a WSN requires sensor nodes as a part of it. The sensor nodes are with limited resources and power. This makes a WSN vulnerable to many kinds of attacks. Denial of Service (DoS) attack is one of them. Each layer has different type of DoS attack. Tackling this attack requires knowledge of types of DoS as well as various defense mechanisms applied to overcome them. In this report, an introduction to DoS attack along with various countermeasures has been discussed.**

Keywords: Wireless Sensor Networks, DoS, DDoS +3,

1. INTRODUCTION

Wireless Sensor Networks aka WSNs are essentially clusters of computing nodes usually tiny, low power attached to some electro-mechanical devices assigned some special task and vigilant about some specific events deployed in variety of places of this physical world. Their numbers in clusters may vary from few to few thousands [1].

These nodes may have some micro controllers of limited processing power, tiny memory, a radio transceiver with inbuilt antenna or a link to external one and an interface to single or may be some times multiple sensors used for sensing changes in surrounding physical environment [2]. They are only solution available for some very hard difficult to reach places where normal wired network can't be laid e.g. Rotating machinery, furnaces, narrow and deep excavation, many exploratory works, monitoring some specific event in weather like temperature, pressure, long time taking processes etc. Unlike normal networks these nodes are application specific, their structure, cost, longevity, accuracy all depends upon their deployment and purpose, nonetheless all have more or less same structure [3].

Mode of communication also vary from deployment to deployment, sometimes any single node may directly send data to base station and on the other hand they may send data collectively simply or adding more and more dimension to data being sent. Similar to their miniaturization communication may also depends up on sophistication of application [4]. Ranging from simple star topology in a trivial WSN, communication may be multi-hop mesh in some sophisticated WSNs. This topology may be self-organizing, self-healing, having dynamic network configuration to cope with node failures and malfunctioning, ability to withstand bad environmental conditions.

Power backup remained a exploratory part of WSNs as power consumption for different type of WSNs greatly vary from each other, depending upon application use, no. of quantities being sensed power also varies [5]. While miniaturized dry cell batteries are mostly used, non conventional modes of energy are also having substantial share in WSNs, also known as Energy-Harvesting, which can be of any form like Ambient-radiation sources, Fluid flow, Photovoltaic, Piezoelectric, Pyroelectric, Thermoelectrics, Electrostatic, Magnetic induction, Atmospheric pressure changes and Meta-material etc.

1.1Application Areas of Wireless Sensor Networks

Design and work flexibility has unfolded seamless integration opportunities for wireless sensor networks into traditional networks as well as new horizons of novel applications. Most of the time WSNs are designated for some sort of monitoring, recording and communicating accumulated information to some base node for further processing. Some of the prominent application areas of WSNs are-

1.1.1 Terrestrial monitoring: WSNs has found place in military annals for monitoring border incursions and other civilian uses like gas pipe-line monitoring etc.
1.1.2 Health care monitoring: WSNs can be used for medical appliances of both types viz. wearables and implants
1.1.3 Environment care monitoring: WSNs use in environment care include Air pollution monitoring, Forest fire detection, Landslide detection, Water quality monitoring, Natural disaster prevention.
1.1.4 Industrial monitoring: Machine health monitoring, Data center monitoring, Data logging, Waste water monitoring, Structural health monitoring

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 01, January-2017

1.2 WSN Architecture

As wireless sensor network has a cluster of may be thousand sensing units which demands low cost of individual unit, they are deployed in geographically hostile environments. A typical WSN architecture has following components.

1.2.1 Nodes

Irrespective of deployment and application type, a node is basic unit of any Wireless Sensor Network. Node has four basic units.

a) Sensing Unit: it is the core of sensor networks, responsible for capturing event of interest from physical world. It has two sub units
   1. Sensors: these are circuits which incorporate various electro-mechanical phenomenons for producing electrical pulses as event of interest takes place in outer physical world.
   2. Analog to Digital Converters (ADC): Electrical pulses generated by sensor are fed to ADCs to obtain digital signals

b) Processing Unit: Processing unit takes care of temporarily storing data, transforming data in the form required by applications, encryptions etc.

c) Transceiver Unit: Supported by external or internal antenna, Transceiver units is responsible for connecting nodes to network.

d) Power Unit: This unit is responsible for power backups of nodes primarily by batteries, sometimes compensated by non conventional energy sources viz. Solar cell, Ambient-radiation sources, Fluid flow, Photovoltaic, Piezoelectric, Pyroelectric, Thermoelectrics, Electrostatic, Magnetic induction, Atmospheric pressure changes and Meta-material etc.

e) Location Unit (Optional): Some applications required location of sensor as well for specific uses, this unit is responsible for determining location of sensor node

f) Mobilizing Unit (Optional): Some specific recording activities require movement of sensor with time, this unit takes care of movement and type of movement.

1.2.2 Base Station

It is usually a special node with high computational capabilities and connectivity to send data collected so for, for further processing via an Internet link.

Fig. 1 shows a typical Wireless Sensor Network

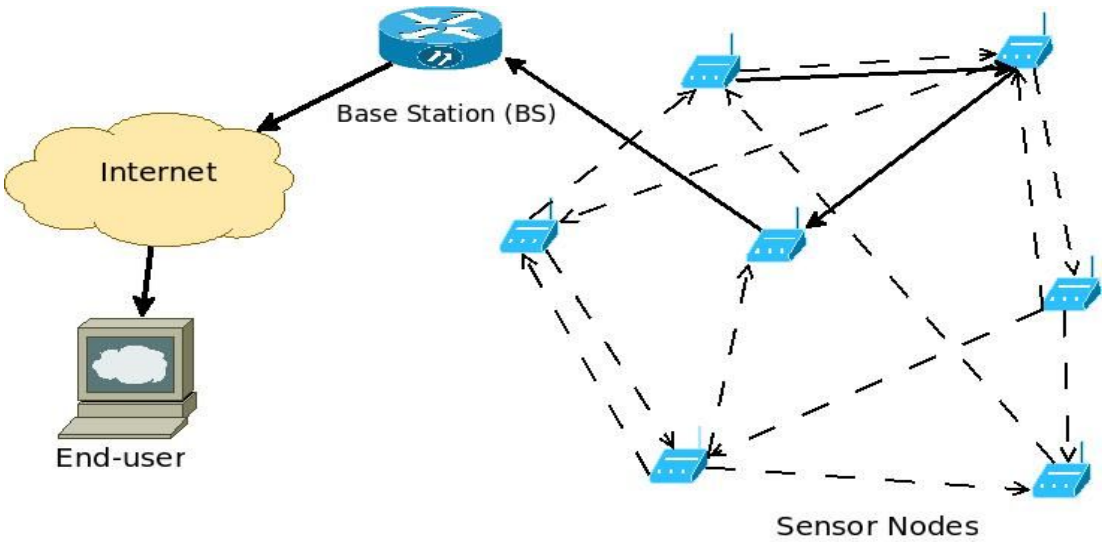

Fig. 1: Wireless Sensor Network

2. Security Issues in Wireless Sensor Networks

WSNs' architectural constraints make them vulnerable for different types of security threats. Most prominent architectural constraints are limited computing power, unattended operational modes, unreliable communication channel respectively [6]

2.1 Limited computing power WSN has to operate into hazardous environment, because of the deployment conditions processing power and memory could not be raised beyond certain limits although lot more computing power has been added in recent past but still it's a problem to look into.

2.2 Unattended operational modes WSNs work relentlessly without human interaction which is an essential feature of WSNs as often they have to work is spatially sparse hazardous and sometimes hostile environments. This mode of working provides a basis to launch various attacks.

2.3 Unreliable communication channels pose biggest threat to WSNs, as WSN sends data collected from physical surroundings for further processing into some meaningful information or knowledge through wireless media which is inherently susceptible to security of data e.g. confidentiality, integrity and availability.

Furthermore since WSNs work in Ad-hoc mode location accuracy is also a sought feature.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 01, January-2017

3. LITERATURE REVIEW

B.Yu proposed a simple approach for detection of forwarding attacks based up on some intermediary nodes or checkpoints. We begin with selecting some random nodes along the path as checkpoints, which on receiving data packets initiates acknowledgment process from upper level. Upon not receiving appropriate amount of packets, checkpoints issues warning messages to source nodes so that corresponding malicious node detection and prevention measures could be started. An apparent drawback of this strategy is that nodes have to continuously send acknowledgment which may results in power exhaustion of nodes and increases network cost [8].

Jiang proposes a method based on level of mutual trust and packet loss to detect Grey hole attack. A statistical record is maintained at intermediate nodes for data packed received and sent, which after certain period of time communicated to base stations (BS), while sensed data is transmitted over a designated path. According to received statistical report base station determines trust level of nodes and packet lost, consequently decision is made about if there is an attack taking place in network [9].

Yu and Xiao in, came up with an scheme which incorporates multi-hop acknowledgements, each node in designated path is responsible for detecting malicious nodes, if a nodes detects any malicious node in its communication link it immediately sends alarm packets to source and base stations [10].

Sophia Kaplantzis et al. brought a centralized intrusion detection mechanism which utilizes Support Vector Machines (SVM) and sliding windows to detect presence of Black hole and Grey holes in the network. Being a centralized solution, all computation required for detection of malicious nodes are performed at the base station which provide nodes freedom of overheads of lengthy computations required for detecting malicious nodes and they can works as usual as if there is no attack and preserve their energy [11].

Brown and Xiaojiang gave an idea about formation of clusters viz. Heterogeneous Sensor Network (HSN) for detection of Grey holes, consisting few powerful high-end sensors or H-sensors and large number of low-end sensors or L-sensors. When deployed cluster formation takes place having H-sensor as cluster head [12].

Xin, etal. Proposed a defense mechanism based on neighbor monitors for mitigation of Grey hole attack. In this approach neighboring nodes act as Monitoring nodes also, monitoring nodes keep check on data packets being forwarded by neighbors and resends packets when saw selective dropping [13].

Zurina Mohd Hanapi et al came up with an idea of using dynamic window stateless routing protocol DWSIGF which is resilience to black hole, wormhole and selective forwarding attack caused by the CTS rushing attack. Even without inserting any security mechanism inside the routing protocol, the dynamic window secured implicit geographic forwarding (DWSIGF) still promise a good defense against black hole attack with good network performance [14].

Deng-yin ZHANG et al. proposed a embedding watermarks into data packets. Base stations on receiving such watermarked data packets, deciphers them and by analyzing packet loss rate from received data decides about attack and type of attack whether there is black hole, grey whole or worm hole present in the network [15].

4. SECURITY OBJECTIVES

Although security objectives depends upon WSN deployment and their function, data gathering and sharing among nodes and BS, nonetheless some major milestones with this regards are as following.

4.1 General Security Requirements

4.1.1 Confidentiality: To ensure that data transported by nodes are received only by intended systems or node only, no other node can have this.

4.1.2 Integrity: To ensure that data delivered to intended node is in its original form as send by sender node, and is free from alteration during the transportation.
4.1.3Availability: To ensure that network resources are available to node as needed by nodes and in the magnitude needed by nodes.

4.2 Application Specific Requirements

As deployment of WSNs are application specific, some added application specific requirement may also exist in the system e.g.

4.2.1 Temporal accuracy: Some times WSNs are used to measure temporal quantities e.g. temperature, pressure, seismic activities etc. which requires latest data values to be send to BS.
4.2.2 Authentication: There should be some authentication mechanism for mission critical WSNs to ensure data sending node is who, it is conveying, it is. This is necessary to make sure that a adversary node cannot masquerade as a genuine node.

5 SECURITY THREATS IN WSNS

5.1Types of Threats: Attacker used a number of techniques to sabotage WSN, a broad classification is given here in Fig.2 and in Table 1

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 01, January-2017

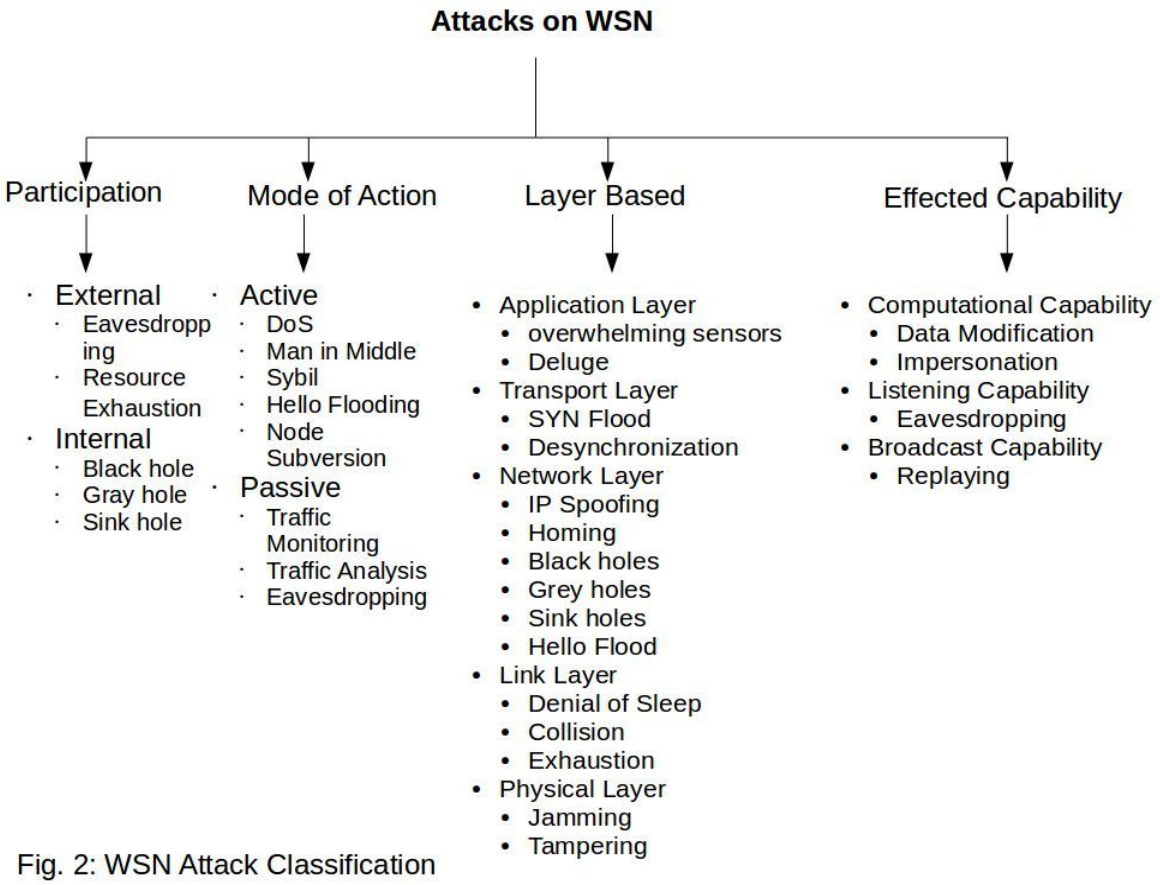

Fig. 2: WSN Attack Classification

Table 1: Classification of attacks on the basis of Confidentiality, Integrity and Availability

Property	Attack
Confidentiality	Traffic Monitoring
	Eavesdropping
	Traffic Analysis
	Spoofiing
	Man in Middle
Integrity	Fabrication
	Tampering
	Session Hijacking
	Repudiation
	Black hole
Availability	Grey hole
	Worm hole
	Exhaustion
	Jamming

5.2 Denial of Services (DoS) Attack in WSN

A Denial of service attack is an explicit attempt to deprive the legitimate user from services or data. Few of the tactics used widely to achieve this outpouring the target system with requests, such that it cannot respond to legitimate traffic consequently legitimate user can't avail the services or data, hence system appears unavailable to him. The basic types of attack are: consumption of bandwidth or consumption of processor time, obstructing the communication between two nodes, disruption of service to a specific system or node, disruption of routing information, disruption of physical components etc. When attacked, performance of Wireless Sensor Networks degrades gradually or it may come to complete halt. If deployed for mission critical application this may have devastating effect, catastrophe caused by this unavailability may result in human life, monetary losses, production and trade loss etc [7].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 01, January-2017

5.3 Mode of Operation

Mode of operation of DoS in whatever form it may take, adopts following three methodologies viz.

a. Consumption of limited or scares resources(network bandwidth, memory)

b. Alteration or destruction of configuration information.

c. Physical destruction of network components.

5.4 Types of DoS in WSN

Al though most of the DoS attacks which are possible in traditional networks or MANETs are also possible in WSNs except few e.g. SMURF. Some prominent DoS attacks in WSNs are as given below.

5.4.1 Jamming: Jamming is Physical Layer attack. Its working is very simple, adversary node keep on transmitting or transmit frequently, radio waves of identical frequency but of different amplitude which target node is listening. This causes destructive interference on node subsequently they are no more able to listen and hence Jammed.

5.4.2 Node Destruction or Tampering: It is also a physical layer attack where we assume that any how attacker has access to mote or node and he may extract invaluable information from node such as sensed data, encryption key etc. because of the deployment conditions and cost involved nodes usually are not tamper proof.

5.4.3 Denial of Sleep: It is a Data Link Layer attack which prevents dormant state of node transmitters, a condition for which they are not built for. As radio transceiver requires a lot of energy from mote(node), a node under this attack goes off line very soon disruption network proper operation.

5.4.4 Spoofing: Spoofing is a network layer attack. In any network environment, routing table information is a soft target and it is mostly attacked, altered, deleted, introduction of routing loops takes place while it is being shared between nodes. Attacker manipulates it in such a way to add routing loops, attract network traffic to some targeted node or to distract traffic from some specific nodes.

5.4.5 Hello Floods: It is a network layer attack which exploits the fact that many protocols are using HELLO packets to ascertain about nodes in their radio communication range. An adversary with powerful radio transceiver initiates HELLO and subsequently broadcast a superior route (less hop) to BS. nodes assumes it is their neighbor and start transmitting towards this new route although it may be out of reach.

5.4.6 Black Hole: This is a Network layer attack where compromised node broadcast superior route to Base Station (BS) and when other node send data packets to it, it simply drops them. This behavior of consuming all packets borrow it name black hole.

5.4.7 Grey Hole or Selective Forward: This is also a network layer attack and a special case of black hole attack where malicious mote behaves differently at different time. It may drop all packet for some time and then start behaving normally and then after certain period of time again start behaving abruptly. It may also drop packets destined for certain addresses and forward remaining packet normally.

5.4.8 Worm Hole: This is a network layer attack also known as tunneling. Any two compromised nodes not in vicinity setup an off the track connection and broadcast promising route to lure neighboring nodes send their data packet through this connection, after receiving packets they simple consume it.

5.4.9 SYN Flood: This is one of the commonly used mechanisms to launch DOS attack. SYN Flood is a Transport Layer attack, which exploits the simplicity of routing protocol, in a wireless sensor network environment, a node sends SYN packet, in response Server sends SYN and ACK and waits for ACK from client and hence keeps the socket open. This is exploited by adversaries, they send enormous amount of SYN packets from Spoofed IP and keep server waiting for ACK from spoofed IP, which never comes and eventually resource drains.

5.4.10 De Synchronization: It is a Transport layer attack where malicious node disrupts an active connection between nodes by sending forged packets. These forged packets have control flags having message to desynchronize the endpoints so as they may retransmit data.

5.4.11 Path based DoS: It is an Application Layer attack where an malicious node overwhelms sensor node from distance by injection spurious packets (replayed packets) which floods the multi hop communication path between two nodes. Nodes involved are stripped off bandwidth and battery power.

6. CONCLUSION

A Wireless Sensor Network are used widely in Military, Industry and Civilian purposes for variety of uses. WSNs suffer from a number of security threats ranging from physical perturbation and ransacking to various software and network related attacks. While few of them pose threats neutralized easily others on the other hand cast devastating effect on public security, integrity and production in different aspect. In article presented here we have discussed the security requirement, security objectives and security challenges of wireless sensor networks. While security requirements may differ from deployment to deployment, security objective are almost same for every deployment. Security challenges may also vary from application to application. A lot of research work has been done to make WSN secure, while physical security could not be guaranteed because of working environment constrained of the node, network security could be assured by taking certain precautionary measures. A number attacks on WSN and their working principles have been

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 01, January-2017

discussed. We have focused ourselves to DoS in different forms here. A lot of research has been undertaken for prevention and mitigation of DoS but still a lot more is remaining. As attackers are taking benefit of advancement in technology and camouflaging day by day, defense mechanism also requires sophisticated use of advance technologies for detection, mitigation and prevention of attacks on wireless sensor networks.

7. Acknowledgement: We would like to acknowledge Almighty Allah by whose mercy this work was possible, I am also indebted to all my friends and colleagues for their extended hand and specially Dr. Tariq Ahamad Ahanger for his continuous guidance, support and inspiration during accomplishment of this work.

REFERENCES

[1] M. Al Ameen, J. Liu, and K. Kwak, "Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications," J. Med. Syst., vol. 36, no. 1, pp. 93–101, 2012.

[2] J. gu Song, S. Jung, J. H. Kim, D. Il Seo, and S. Kim, "Research on a Denial of Service (DoS) detection system based on global interdependent behaviors in a sensor network environment," Sensors (Switzerland), vol. 10, no. 11, pp. 10376–10386, 2010.

[3] K. CHELLI, "Security Issues in Wireless Sensor Networks," Proc. World Congr. Eng., vol. 1, 2015.

[4] A. More and V. Raisinghani, "A survey on energy efficient coverage protocols in wireless sensor networks," J. King Saud Univ. - Comput. Inf. Sci., 2016.

[5] J. gu Song, S. Jung, J. H. Kim, D. Il Seo, and S. Kim, "Research on a Denial of Service (DoS) detection system based on global interdependent behaviors in a sensor network environment," Sensors (Switzerland), vol. 10, no. 11, pp. 10376–10386, 2010

[6] T. Zia and A. Zomaya, "Security issues in wireless sensor networks," … Networks Commun. 2006. ICSNC'06 …, vol. 2, no. 1, pp. 106–115, 2006.

[7] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses," IEEE Pervasive Comput., vol. 7, no. 1, pp. 74–81, 2008.

[8] B Yu, B Xiao. "Detecting selective forwarding attacks in wireless sensor networks". In: Proe. of the 20th International Parallel and Distributed Processing Symposium, RhodesIsland, Greeee, 2006,1218 1230

[9] Jiang changyong, Zhang jianming. "The selective forwarding attacks detection in WSNs". Computer Engineering, 2009, 35(21):140-143

[10] Bo Yu and Bin Xiao. Detecting selective forwarding attacks in wireless sensor networks. In Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International, page 8 pp., 2006

[11] Sophia Kaplantzis , Alistair Shilton , Nallasamy Mani , Y. Ahmet S,ekercio glu ," Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Support Vector Machines", intelligent sensors, sensor networks and information ,3rd international conference ,pg 335 – 340,ISSNIP 2007 .

[12] Jeremy Brown and Xiaojiang Du. Detection of selective forwarding attacks in heterogeneous sensor networks. In ICC, pages 1583–1587, 2008.

[13] Wang Xin-sheng, Zhan Yong-zhao, Xiong Shu-ming, and Wang Liangmin. Lightweight defense scheme against selective forwarding attacks in wireless sensor networks. pages 226 –232, oct. 2009.

[14] Zurina Mohd Hanapi, Mahmod Ismail and Kasmiran Jumari, Priority and Random Selection for Dynamic Window Secured Implicit Geographic Routing in Wireless Sensor Network", American Journal of Engineering and Applied Sciences 2 (2): 494- 500, 2009

[15] Deng-yin ZHANGa, Chao Xub, Lin Siyuan "Detecting Selective Forwarding attacks in WSNs using Watermark