Survey for Power Draining In Wireless Sensor Networks

Vinya Joshi Research Scholar –MTech Final Year
Sushila Devi Bansal College of Technology, Indore
vinyas.joshi@gmail.com

Deepak Sharma
Sushila Devi Bansal College of Technology, Indore
dsharma6@live.com

Abstract: Distributed Denial of Service (DDOS) attack is such kind of attack which aims to disrupt the network by draining resource capability. Here, Attacker communicates worthless messages formally known as false packet to increase network traffic and make target node busy in useless activity. The complete work observes that, DDOS attack does not require any study about network vulnerability.

The major challenge with mobile network is energy issue. Its life is directly proportional with battery capacity. Thus draining in battery energy directly degrades the life of node. This project observed it as severe problem and proposed a solution to overcome the problem of power draining due to DDOS attack. Subsequently, Power draining is the major thread; where attacker not only exhausts the network traffic but also degrades the life of node as well network. This paper aims to make survey to explore solution to overcome flooding attack in WSN.

Keywords: WSN, DDOS Attack, Flooding, AODV

1. INTRODUCTION

A Wireless Sensor Network is usually composed of hundreds or thousands of sensor nodes. These sensor nodes are often densely deployed in a sensor field and have the capability to collect data and route data back to a base station (BS). A sensor consists of four basic parts: a sensing unit, a processing unit, a transceiver unit, and a power unit. It may also have additional application-dependent components such as a location finding system, power generator, and mobilize as shown in Figure 1.1.

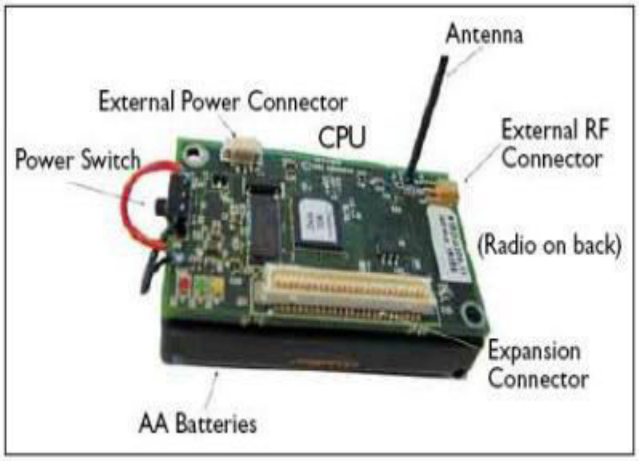


Figure 1: Units of Sensor Nodes [3]

Sensing units are usually composed of two subunits: sensors and analog-to-digital converters (ADCs). The ADCs convert the analog signals produced by the sensors to digital signals based on the observed phenomenon. The processing unit, which is generally associated with a small storage unit, manages the procedures that make the sensor node collaborate with the other nodes. A transceiver unit connects the node to the network. One of the most important units is the power unit. A power unit may be finite (e.g., a single battery) or may be supported by power scavenging devices (e.g., solar cells). Most of the sensor network routing techniques and sensing tasks require knowledge of location, which is provided by a location finding system. Finally, a mobilize may sometimes be needed to move the sensor node, depending on the application [2].

The major concentration of routing protocols is finding efficient route in the network and do not measure about vulnerability of selected path. Work determines the need to develop secure routing protocol to perform safe and efficient routing process. There are many security threat may affect the network performance such as denial of service, black hole, sinkhole etc. They not only saturate the network communication but may compromise the packet information with negative objective.

2. RELATED WORK

In recent years, in the field of wireless communication and networking considerable advancements have been experienced. WSNs have become very popular. Ad hoc is derived from Latin, meaning “for this purpose” meaning temporary. “Mobile Ad hoc Networks” as the name reflects is a temporary deployed mobile wireless network.

WSN is a multi-hop, temporary, self-organizing system made up of a group of portable electronic equipments with wireless transmitter and Receiver. This collection of mobile nodes may operate in isolation, or may have gateways to interface with a fixed network. An ad-hoc network uses no centralized administration.

Nodes in WSN are equipped with portable communication devices. These nodes may vary in size and capabilities. They could be small sensors with very limited computation, communication, and energy capabilities. Or there may be larger more powerful nodes such as laptops or even vehicles that are equipped with communication and computation devices. In WSNs nodes may be deployed in large numbers and can typically have a large span. The nodes could be distributed in the network either randomly or in a fixed grid.

To understand the concept and impact of power draining on wireless sensor networks, work consider certain research work which is explain below:

Zubair A. Baig[1] proposed a solution where it concludes that Distributed Denial of Service attack is most popular attack for power draining. They also discussed about various attack models and impact. They designed pattern recognition problem to detect DDOS attack. Proposed method improve performance on basis of timely and energy-efficient manner.

Jaydeep Sen [2] explore that there is a need to develop dynamic and intelligent security approaches to enhance protection level and reduce security overhead. Opportunistic approach attains the encryption base for varying levels of channel knowledge. They also study of various design constraints in Wireless Sensor Network i.e. Power, Memory & Processing are major design constraints.

Furthermore, they also explore the various threats like DDOS attack, Black-hole Attack, Jamming Attack etc.

Sriram Nandha Premnath & Sneha Kumar Kasera [3] proposed a advanced DDOS attack They also propose a special attack named as SDP Attack (Service Discovery Protocol based attack) to make Heavy Power Drain on node.SDP sends new service request similar to SYN Flooding to create conjunction and overwhelming the nodes. SDP attack effectively make it inoperable and reducing the battery life by as much as 97%.

Thomas Martin at el [4] observed the Impact of Service request power attacks and Benign power attacks and explain the study of Power drain due to DDOS attack

Routing protocol is use to determine the route from source to destination. To understand the routing protocol and attack impact complete work consider AODV as routing protocol and SYN Flooding technique for DDOS attack.

3. AD HOC ON-DEMAND DISTANCE VECTOR (AODV) ROUTING PROTOCOL

AODV is a reactive routing protocol designed for ad hoc wireless networks. In AODV routes to connect two nodes are obtained only when it is required i.e. on demand. AODV routing algorithm is specially suited for dynamic self-configured networks like WSN. AODV provides loop free routes along with route management for broken links. Bandwidth requirement of mobile nodes in AODV is comparatively less than other protocols as AODV does not require periodic route advertisements.

AODV uses symmetric links between communicating nodes. Nodes which are communicating or intermediate nodes on active route only maintain routing information. Nodes which do lie on active path need not maintain routing information and does not exchange routing table periodically. Furthermore, routes are discovered and maintained between two nodes only when they need to communicate or if they are acting as the intermediate node supporting in communication.

The AODV algorithm’s primary objectives are as follows:

1. Initiate route discovery only when necessary.
2. Periodic exchanges utilized only for local connectivity management and not for general topology maintenance.
3. Sharing the local connectivity information with only those neighbouring nodes which may need the information.

For route discovery AODV uses broadcast mechanise. Instead of using source routing, routing strategy used in AODV is to establish route entries dynamically at intermediate nodes. This kind of routing serves networks with large number of nodes by saving overhead required by source routes in each data packet.

Similar to DSDV, a destination sequence number is used. Each node keeps an increasing sequence number to ensure freshness of routes.

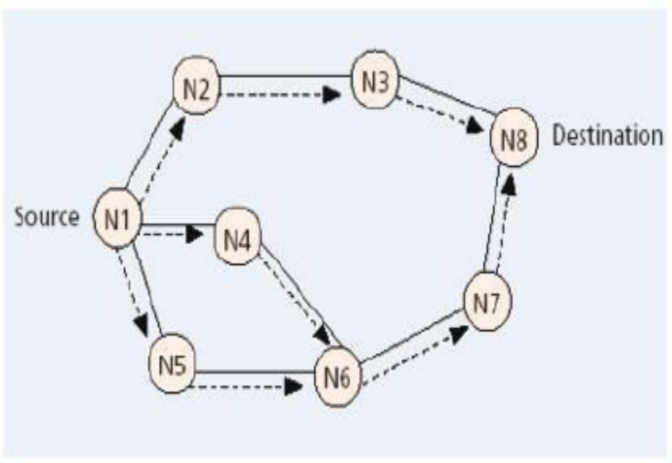
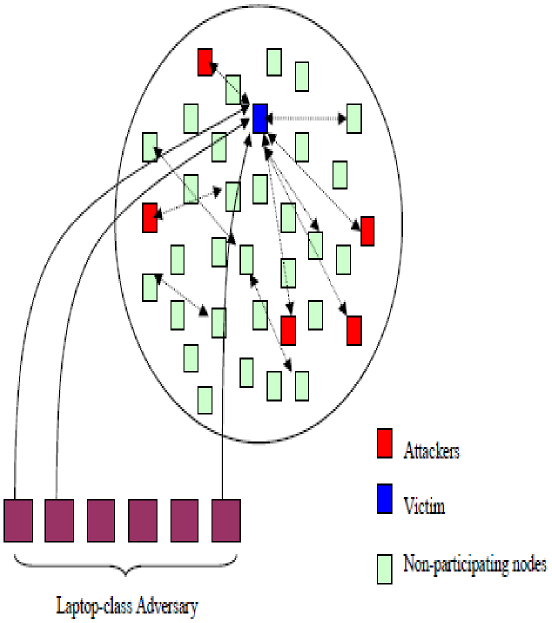


Figure 1. Path discovery in AODV (Deng *et al.*, 2002)

4. DISTRIBUTED DENIAL OF SERVICE ATTACK

Denial of service attacks are defined as attacks that are launched by a set of malicious entities towards a victim, with the aim of incapacitating it from providing further service to legitimate clients. The objectives of the attack are achieved by exploiting either system/protocol-level vulnerabilities, or by forcing the victim to undertake computationally intensive tasks, such as exponentiation large integers for applications.

As can be seen from 2, a single victim node may be targeted with overwhelming number of incoming requests from multiple ends of the network. The attacker nodes can either be legitimate but compromised nodes operating in the network, or be a laptop-class adversary, i.e. an adversary with higher capabilities, using forged identities to generate a large set of legitimate packets for overwhelming the victim node. It is assumed that no pre-hand information is available to elude towards critical (potential victims) nodes in the network. Therefore, an adversary must have observation capabilities for a certain period of time to identify on the critical nodes in the network. Intelligent set of adversaries will launch the distributed denial of service attacks from multiple ends of the network so as to avoid being detected by a detection module observing traffic from a single point of origin in the network.



A DDOS attack may classified into two category which are

1. Direct Attack
    1. SYN Flooding
    2. Ping of Death
    3. Smurf Attack

2. Reflector Attacks
    1. Flooding on Victim's Link

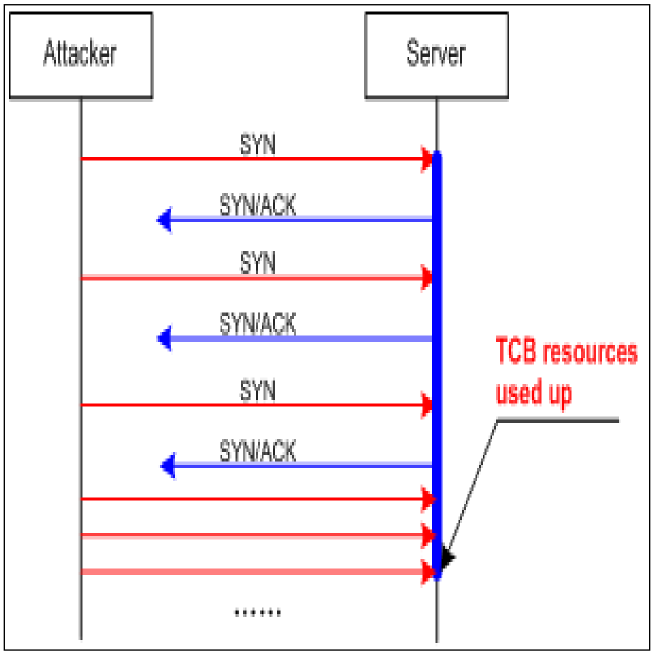


Figure 4: SYN Flooding

5. PROBLEM DOMAIN

The AODV routing protocol is a popular reactive routing protocol in wireless networks, but AODV routing protocol designed for better performance of the network not for security of node, secure protocols are generally designed to have features such as authentication, integrity, confidentiality and non-repudiation. For security purpose AODV have vulnerabilities and it is easily manipulate by malicious node to destroy its network routing.

The open nature of wireless medium also makes it easy for outsider attackers to interfere and interrupt the legitimate traffic. This concept classifies the attacks into two broad categories, namely Passive and Active attacks. In Passive attack, the adversary only eavesdrop upon the packets content, while packets may get dropped or altered on way in case of Active attacks. Wormhole attack is one of the Denial of Service attacks effective on the network layer, that can affect network routing, data aggregation and location based wireless security. DDOS attack does not require scanning network vulnerability; instead it uses SYS Flooding and bulk messaging to create intentional power draining in sensor networks.

The complete work determine that, there is need to develop a scheme to avoid power draining problem in WSN using DSR to sustain node life and improve the network performance over DDOS attack.

The major problems with AODV are:-

- In-Secure Routing: No Security measurement or policy associated with AODV routing protocol.
- Incredibly prone for external security threats due to use of large scale network
- Major Targeted for disruption of network using overwhelming power consumption
- Need to develop security policy to maintain network life as it deserve.

6. CONCLUSION

The complete work concludes that there is need to develop a security scheme to detect and prevent sensor network from useless conjunction and service utilization to avoid power drain. The proposed solution will help to sustain node life as they deserve.

References

1. Sriram Nandha Premnath, Sneha Kumar Kasera, “Battery-Draining-Denial-of-Service Attack on Bluetooth Devices”, Project Report School of Computing University of Utah ,2012

2. Jaydip Sen, “A Survey on Wireless Sensor Network Security”, In proceedings,

International Jouenal of Communication Networks and Information Security (IJICNIS), Vol 1, No 2, Augest-2009.

3. Jayan Krishnaswami, “Denial-of-Service Attacks on Battery Powered Mobile Computers ”, Master of Science in Electrical Engineering, Virginia Polytechnic Institute and State University, Blacksburg, Virginia.

4. Maneesha V. Ramesh, “Real-time Wireless Sensor Network for Landslide Detection”, In *Third International Conference on Sensor Technologies and Applications,* 09 IEEE-Computer Society of India.

5. R.balakrishna, U.Rajeshwar Rao, N. Geetahanjali, “Performance issues on AODV And AOMDV for MANETs*”, International journal of Computer Science and Information (IJCSIT),* vol. 1 (2), 2010,pp. 38-43.

6. Miss Morli Panday,Ashish Kr. Shriwastava, “A Review on security Issues of AODV routing protocol for MANETs”, *IOSR Journal of Computer Engineering(IOSR-JCE)*, e-ISSN:2278-0661, p-ISSN:2278-8727 vol. 14, Issue 5 (Sep. - Oct. 2013), pp.127-134.

7. Sangwan,A., Sindhu,D., Singh, K., “A Review of various security protocols in Wireless Sensor Network”, *IJCTA, ISSN:2229-6093*, vol. 2 (4), july-august-2011, pp.790-797.

8. Zubair A. Baig, “Distributed Denial of Service Attack Detection in Wireless Sensor Networks”, Report of Doctor of Philosophy at Monash University January, 2008