DDOS Attack in WSN: A Survey

Syed Faizan¹, Zahid Mushtaq², Irfan Rashid³

¹Department of CSE, SSM College of Engg and Tech, Baramulla, India
²Department of CSE, SSM College of Engg and Tech, Baramulla, India
³Department of CSE, SSM College of Engg and Tech, Baramulla, India

Syedfaizaan81@gmail.com; Er.zahid00@gmail.com; Samirfan@gmail.com

ABSTRACT—Wireless Sensor Networks (WSNs) is collection of large number of sensor nodes which are of limited capabilities, to collect sensitive information. With the advancement of this technology, one of the major concerns these days is of security. There are so many attacks possible on WSN, in Distributed-Denial of Service (DDOS) attacks, malicious nodes adapts many attacks such as flooding attack, black hole attack and warm hole attack, to halt the overall functioning of network. The risks are even more when we talk about military and industrial applications. Furthermore in WSN there are so many constraints like limited battery power, low capabilities of nodes etc. To present a security model that will consider these constraints and provide security is a major challenge these days. There are many mechanisms which are proposed by researchers to detect or defend from this DDOS attack. In this paper we will review these approaches on basis of various parameters.

Keywords --- Wireless Sensor Networks (WSNs), Sensor nodes, Security, DDOS attack.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) consists of small sensor nodes communicated through radio links. They are used in many applications like (agriculture, health, home, industrial, and military) for monitoring and data collection purpose. Its main advantage is that it is easy to deploy in harsh environments, where infrastructure is difficult to deploy. In many applications (like military, medical and industrial) security is very crucial requirement. Due to so many limitations in WSNs, the traditional security methods cannot be directly implemented. There limitations include limited battery power, power to communicate and compute. Furthermore the area for deployment of WSNs may be public locations, where intruder can physically take over sensor nodes and take all information. Moreover due to energy failures some nodes may die, or new nodes can join the network and the channel used for communication is very insecure. Hence more efficient security approaches are required which consider all these constraints.

Rest of the paper is organized as, Section II includes WSNs Architecture, Section III defines Attacks in WSNs. Section IV, gives the related work. Finally the section V gives the conclusion.

II. WSN ARCHITECTURE

Wireless Sensor Network (WSN) mainly contains one or few Base Station (BS) or Sink and hundreds or thousands of sensor nodes. Sensors have limited capacity whereas base stations are having more capabilities and are used to communicate with other networks. Sensor nodes are deployed at random, and responsible for data collection, whereas base stations are responsible for data aggregation and management of the network. BS sends aggregated data through internet to the user(Fig 1).
III. ATTACKS IN WSN

WSN is susceptible to so many attacks, because of broadcasting nature of network. The main security services of network are: Integrity, Authentication, Confidentiality, Availability, Access Control etc.

- Integrity: This service ensures that whatever is sent is same as whatever is received, i.e. is not being modified.
- Authentication: It ensures that the sender is same what it claims to be.
- Confidentiality: It ensures that the contents of message are understandable to only intended entities.
- Availability: This service ensures that services should be available to authorized members.
- Access Control: Access should be given only to authorized nodes.

In addition to these services efficiency and scalability are also the requirements. WSNs are vulnerable to so many security threats called Attacks.

A. Passive Attacks
In Passive Attacks intruder will listen to the channel or monitor the traffic but will not disrupt the communication between sender and receiver. Hence Passive attacks are hard to detect. It can further classify into:

1. Data Disclosure: In this attack intruder may harm to the privacy of information i.e. disclosure of information to unauthorized users.
2. Traffic Analysis: If actual information is in non-readable form, then attacker may analyze the traffic and try to find other aspects such as, type of information, frequency of messages transferred etc.

B. Active Attacks
In these attacks, an attacker can modify the information or disrupt the communications between the sender and the receiver. These attacks are more dangerous than passive attacks. Denial of Service is one type of Active attack. In this paper we will further focus on DOS attack.

1. Denial of Service (DOS): Denial of Service Attack (implemented by attacker by targeting the scheme of routing) occurs due to the failure of nodes unintentionally and also due to malicious action. In DoS attack, the resources available at the victim node are exhausted by receiving unnecessary packets which are not meant or entitled for that node. DoS attack is not only for adversary nodes but also for those events which dismisses the capability of network to provide services. In Wireless Sensor Network (WSN), various types of DoS attacks occur at each layer like jamming and tampering at physical layer, exhaustion, collision and unfairness at link layer, black holes, misdirection etc at network layer. At transport layer, DoS attacks occur due to de-synchronization and malicious flooding. So, to overcome all these DoS attacks a mechanism is included which contain pushback, authentication, network resources and identification of traffic.

IV. CONCLUSION

Wireless Sensor Network is sensitive to so many security threats. DoS attacks are much easier to launch in WSN. In this paper we defined various security services, attacks possible in ad-hoc WSN. The main focus is to study various types of DoS attacks, and techniques to prevent from these attacks. Many security techniques are invented in WSN, but it is still vulnerable to so many DoS attacks. Most techniques suffer from false alarms and high consumption of energy. As in WSN less consumption of battery power is very crucial, in order to enhance network lifetime. In future we improve the techniques which will have low false alarm problem and less energy consumption.
ACKNOWLEDGEMENT

Words are not just enough to express our gratitude but we take this opportunity to express our profound sense of gratitude and respect to all those who helped us throughout the duration of this paper. First of all we are very thankful to our HOD Yasmeen Bhat for her regular support and guidance. We are also very thankful to Allah for providing us such a great opportunity. We feel privileged to offer our sincere thanks and deep sense of gratitude to our college for expressing confidence in us by letting us work on a paper of this magnitude and providing support, help & encouragement in implementing this paper.

REFERENCES