**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

*IJCSMC, Vol. 4, Issue. 6, June 2015, pg.260 – 265*

**REVIEW ARTICLE**

# A Review: DoS and DDoS Attacks

**Monika Malik, Dr. Yudhvir Singh**

**Department of Computer Science and Engineering, UIET, MDU University, Rohtak, Haryana, India**

***Abstract: Wireless sensor networks (WSNs) are a special type of Ad-hoc network. WSNs are easily subjected to intentional or unintentional attacks as compared to wired based networks. Denial of Service (DoS) attack is one of the main threats that the network is facing. DoS attack makes use of many hosts to send a lot of useless packets to the target in short time of invalid access which will consume the targets resources and causes outage of server operations. In this paper we will discuss various types of attacks on WSNs and emphasize on DoS attack. And will discuss smurf attack which is one of the DoS attack type.***

***KEYWORDS: WSNS, DoS, DDoS, ICMP, IP Address, Smurf Attack.***

## I. INTRODUCTION

Sensor networks are highly distributed networks of small, lightweight wireless nodes, deployed in large numbers to monitor the environment or system by the measurement of physical parameters such as temperature, pressure, or relative humidity [1]. The sensor nodes are similar to that of a computer with a processing unit, limited computational power, limited Memory, sensors, a communication device and a power source in form of a battery. In a typical application, a WSN is scattered in a region where it is meant to collect data through its sensor nodes. The sensors also have the ability to transmit and forward sensing data to the base station. Most modern WSNs are bi-directional, enabling two-way communication, which could collect sensing data from sensors to the base station as well as transfer commands from base station to end sensors. The development of WSNs is motivated by military applications such as battlefield surveillance; WSN are widely used in industrial environments, residential environments and wildlife environments etc. In this paper an overview on various WSN attacks are mentioned with a special mention on Denial of Service (DoS). The rest of the paper is as follows: the section 2 gives an overview of attacks on WSNs followed by section 3 which explains DoS and attack techniques and in section 4 comes the Distributed Denial of Service (DDoS) attack and smurf attack which is the type of DDoS attack and then conclusion in section 5.

## II. ATTACKS ON WIRELESS NETWORK

There are various types of attacks which effect WSNs very badly [2] [8] [9]. These attacks are classified differently which is based on their behaviour [4] [5], some are categorized as layer wise and other as type wise i.e. Active or Passive type wise etc. But here we discuss security attacks by categorizing mainly in 3 types. They are as follows:

**1. Attacks on network availability:** Adjusting the traditional encryption algorithms to fit within the wireless sensor network is not free, and will introduce some extra costs. Some approaches choose to modify the code to reuse as much code as possible. Some approaches try to make use of additional communication to achieve the same goal. What's more, some approaches force strict limitations on the data access, or propose an unsuitable scheme (such as a central point scheme) in order to simplify the algorithm. But all these approaches weaken the availability of a sensor and sensor network for the following reasons:

- Additional computation consumes additional energy. If no more energy exists, the data will no longer be available.
- Additional communication also consumes more energy. What's more, as communication increases so too does the chance of incurring a communication conflict.

• A single point failure will be introduced if using the central point scheme. This greatly threatens the availability of the network. The requirement of security not only affects the operation of the network, but also is highly important in maintaining the availability of the whole network.

The attacks on availability of WSN are often referred to as DoS [3] attacks.

**2. Attacks on secrecy and authentication:** Data confidentiality is the most important issue in network security. Every network with any security focus will typically address this problem first. In sensor networks, the confidentiality relates to the following

• A sensor network should not leak sensor readings to its neighbours. Especially in a military application, the data stored in the sensor node may be highly sensitive.

• In many applications nodes communicate highly sensitive data, e.g. key distribution; therefore it is extremely important to build a secure channel in a wireless sensor network.

• Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks.

Standard cryptographic techniques can protest the secrecy and authenticity of communication channels from outsider attacks such as eavesdropping, packet replay attacks etc

**3. Silent attack on service integrity**: With the implementation of confidentiality, an adversary may be unable to steal information. However, this doesn't mean the data is safe. The adversary can change the data, so as to send the sensor network into disarray. The goal of the attacker is to make the network accept a false data value. For example, an attacker compromises a sensor node and injects a false data value through that sensor node.

Below we discuss various attacks which come under above 3 categories:

### 1. Attacks on Network Availability

DoS come under this attack which affects different layers of WSNs as discussed below:

### Denial of Service Attacks

It occurs by the unintentional failure of nodes or malicious action. The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled [6]. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed [7] [10] [11]. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and desynchronization. There are different attacks of DoS which are discussed below in TABLE 1:

TABLE 1: VARIOUS ATTACKS OF DoS AT DIFFERENT LAYERS

| **Layer** | **Attack** | **Defenses** |
|---|---|---|
| Physical | Jamming | Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change |
| | Tampering | Tamper-proofing, hiding |
| Data link | Collision | Error Correction Coder |
| | Exhaustion | Rate Limitation |
| | Unfairness | Small Frames |
| Network layer | Spoofed routing information & selective forwarding | Egress filtering, authentication, monitoring |
| | Sinkhole | Redundancy Checking |
| | Sybil | Authentication, monitoring, redundancy |
| | Wormhole | Authentication, probing |
| | Hello Flood | Authentication, Packet leashes by using geographic and temporal info |
| | Acknowledgment Flooding | Authentication bidirectional link authentication verification |
| Transport | Flooding | Client puzzles |
| | Desynchronization | Authentication |
| Application | Path based DoS | Authentication and anti-replay protection |
| | Reprogramming attacks | |

### 2. Attacks on Secrecy and Authentication

There are different types of attacks under this category as discussed below in TABLE 1:

TABLE 2: VARIOUS ATTACKS OF SECRECY AND AUTHENTICATION

| **Attack** | **Working** | **Defenses** |
|---|---|---|
| Node replication attack | physically capture one node, collects all secret credentials, an adversary replicates the sensor node and deploys one or more clones of the compromised node into the network at strategic positions, damaging the whole network by carrying out many internal attacks. | limiting the order of deployment using symmetric polynomial for pair-wise key establishment and defined group-based deployment model |
| Attacks on privacy | Traffic analysis, eavesdropping on sensitive sensor (i.e. source location information) | Homomorphic encryption, Onion routing, schemes based on traffic entropy computation, group signature based anonymity schemes, use of Pseudonyms. |
| Eavesdropping and passive monitoring | Attackers monitor<br>the traffic in transmission on communication channels and collects data that can be analyzed to extract sensitive information. | Use of (i) anonymity mechanisms, (ii) flooding – probabilistic and phantom, and<br>(iii)Onion routing. |
| Traffic analysis | Intercepting and examining messages in order to deduce information from patterns in communication | rate monitoring attack, time correlation attack |
| Camouflage | insert their<br>node to attract the packets, then misroute<br>the packets, conducting the privacy analysis | Attack source identification, secure overlays |

### 3. Silent Attacks on Service Integrity

There are different types of attacks under this category as discussed below in TABLE 3:

TABLE 3: VARIOUS ATTACKS ON SERVICE INTEGRITY

| **Attack** | **Effect** | **Defenses** |
|---|---|---|
| Environment Tampering | High risk of apprehension if the network is under some kind of surveillance | Tamper-proofing, hiding |
| Node Displacement | The measurements which the node send to base station will be erroneous | Key Management, Encryption |
| Erroneous Data Value | changes the data, to make the network accept a false data value | Authentication, Digital Signature |

## III. DoS ATTACKS

In a DOS attack, a single computer and a single internet connection is used to exhaust the victim resources by flooding a server with packets. Below in Fig 1 DoS attack is shown on a single host:

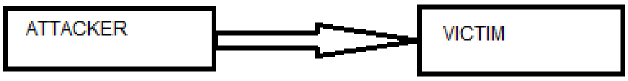

Fig 1: Denial of Service attack

### Attack Techniques

Many attack techniques can be used for DoS purpose as long as they can disable service, or downgrade service performance by exhausting resources for providing services. Although it is impossible to enumerate all existing attack techniques, we describe several representative network based and host based attacks in this section to illustrate attack principles [15].

**Network based attack**

Network-based denial-of-service attacks are one of the easiest types of attacks. It often requires a very little effort to fully consume resources on the target computer, or to starve the target computer of resources, even to cause critical services to fail or malfunction. Mainly DoS attacks try to send excessive amount of false packets in the network.

- **Ping of death:** The ping of death attack sends oversized ICMP datagram's (encapsulated in IP packets) to the victim node. The Ping command makes use of the ICMP echo request and echo reply messages and it is commonly used to determine whether the remote host is alive. However in a ping of death attack ping causes the remote system to hang, reboot or even crash.
- **Teardrop attack:** Whenever data is sent over the internet, it is fragmented at the source system and reassembled at the destination system.
- **SYN - flood attack:** In SYN flooding attack, several SYN packets with an invalid source IP address are sent to the target host. When the target system receives those SYN packets, it tries to respond to each system with a SYN/ACK packet but as all the source IP addresses are invalid the target system goes into wait state for ACK message to receive from the source.
- **UDP - flood attack:** Two UDP services: echo (which echos back any character received) and chargen (which generates character) were used in the past for network testing and are enabled by default on most systems. These services can be used to start DoS by connecting the chargen to echo ports on the same or another machine and generating large amounts of network traffic.
- **Land attack:** A land attack is similar to SYN attack, the only difference is that instead of including an invalid IP address, the SYN packet includes the IP address of the target system itself. Consequently an infinite loop is created within the target system, which ultimately hangs and crashes the victim system.
- **Smurf attack:** It Broadcasts ICMP packets with victim's spoofed source IP and causes all hosts on the network to reply to the ICMP request, results significant traffic to the victim's node.

**Host Based Attack**

Besides misusing network protocols, attackers can also launch DoS attacks via exploiting vulnerabilities in target's applications and systems. Different from network based attacks, this type of attacks are application specific, i.e.,

- Exploiting particular algorithms
- Memory structure
- Authentication protocols etc.

Attacks can be launched either from a single host as a conventional intrusion or from a number of hosts as a network based DDoS attack. The traffic of host based attacks may not be as high as network based attacks, because application flaws and deficiencies can easily crash applications or consume a tremendous amount of computer resources.

## IV. DDoS ATTACKS

On the other hand DDOS attacks multiple computers and multiple internet connections are used which are distributed globally to make an attack. In this situation the victim will be flooded with the packets send from many hundreds and thousands of sources [16].

A Distributed Denial of Service Attack is composed of four elements, as shown in Fig 2.

• The real attacker.

• The handlers or masters, which are compromised hosts with a special program running on them, capable of controlling multiple agents.

• The attack daemon agents or zombie hosts, who are compromised hosts that are running a special program and are responsible for generating a stream of packets towards the intended victim. Those machines are commonly external to the victims own network, to avoid efficient response from the victim, and external to the network of the attacker, to avoid liability if the attack is traced back.

• A victim or target host.

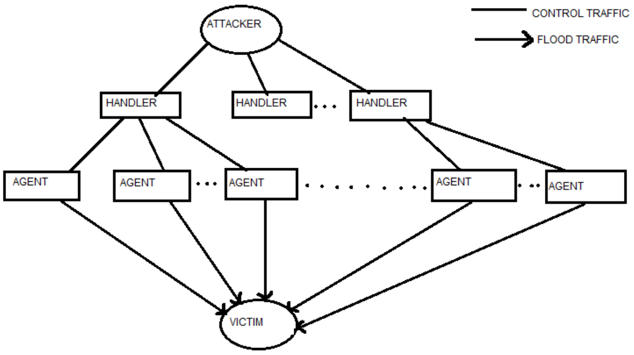

Fig 2: Distributed Dos

DDoS attacks can be divided into three main categories as shown in Fig 3:
1. **Volume based attacks: -** These include ICMP floods, UDP floods and other spoofed packet attacks. The main goal of the attacker is to consume the bandwidth of the victim's site. The magnitude of the attack is measured in bits per second (Bps).
2. **Protocol based attacks**: - These include SYN floods, fragmented packet attacks, Ping of death, Smurf attack and more. The main goal of the attacker is to consume actual server resources, such as firewall. The magnitude of the attack is measured in Packets per second.
3. **Application layer based attack**: - These include attacks like Zero-day attack, Slowloris etc. the main goal of the attacker is to target the Apache, Windows or open BSD vulnerabilities and more.

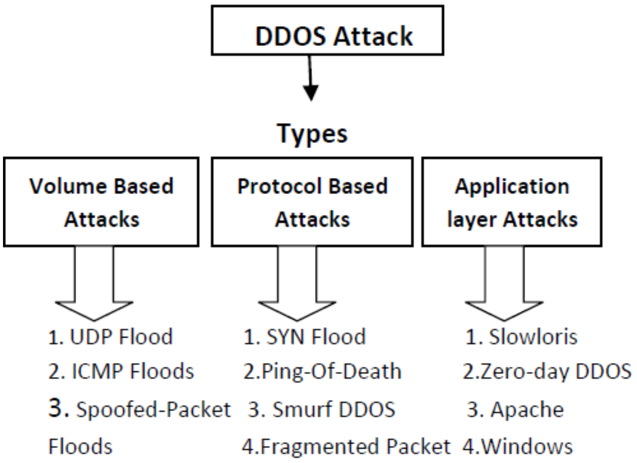

Fig 3: Distributed DoS attack classification.

### Smurf Attack

A smurf attack is a Distributed Denial of Service (DDoS) network based attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source Internet Protocol (IP) are broadcast to a computer network using an IP Broadcast address [12]. The attacker uses a program called smurf to cause the attacked part of a network to become inoperable. Most devices on the network will, by default, respond to this by sending a reply to source IP address. The ICMP is used by network nodes and their administrators to exchange information about the state of the network. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic. This can slow down the victim's computer to the point where it becomes impossible to work on [13].
Smurf attack can be devastating, both to the victim network and to the network(s) used to amplify the attack. An ICMP smurf attack is a brute force attack on the direct broadcast feature that is built in to the IP protocol. The players in this type of DoS attack include the following:

- The hacker
- The intermediary (also known as the amplifier)
- The victim

In most scenarios the attacker spoofs the IP source address as the IP of the intended victim to the intermediary network broadcast address. Every host on the intermediary network replies, flooding the victim and the intermediary network with network traffic. Result: Performance may be degraded such that the victim, the victim and intermediary networks become congested and unusable [14]. The working of Smurf attack is shown below in Fig 4:

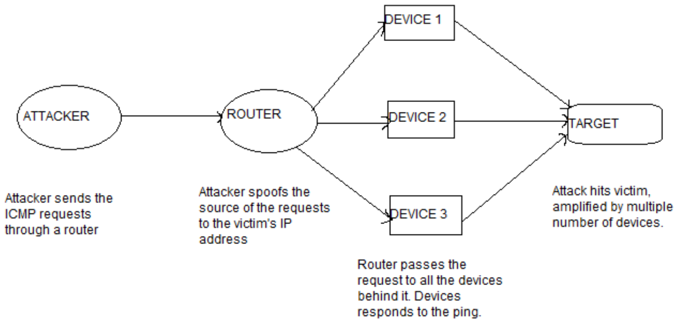
ATTACKER
ROUTER
DEVICE 1
DEVICE 2
DEVICE 3
TARGET
Attacker sends the ICMP requests through a router
Attacker spoofs the source of the requests to the victim's IP address
Router passes the request to all the devices behind it. Devices responds to the ping.
Attack hits victim, amplified by multiple number of devices.

Fig 4: Smurf attack.

**Working of Smurf Attack**

**Step1:** Victim IP address is to be identified by the attacker.
**Step2:** Intermediary site is to be identified by attacker which helps in amplifying attack.
**Step3:** Large amount of traffic will be sent by attacker to the broadcast address at particular intermediary sites.
**Step4:** These intermediaries will provide broadcast to all hosts which are there in a subnet.
**Step5**: Hosts will reply to network.

## V. CONCLUSION

We have studied various attacks on WSNs; these attacks collapse the entire systems and networks. DOS and DDOS attacks are done to affect the resources like bandwidth, server, and disk space or processor time. This paper gives the information about the Smurf attack which is the protocol (ICMP) based DDOS attack undertaken by the attacker using IP Spoofing technique. Future work will be focussed on detecting and preventing smurf attack.

## REFERENCES

[1] Shio Kumar Singh, M P Singh, and D K Singh "A Survey on Network Security and Attack Defense Mechanis for Wireless Sensor Networks" *International Journal of Computer Trends and Technology (IJCTT), May to June Issue 2011.*

[2] M.J. Karmel Mary Belinda and C. Suresh Gnana Dhas, "A Study of Security in Wireless Sensor Networks", *MASAUM Journal of Reviews and Surveys*, Sept. 2009, vol. 1, Issue 1, pp. 91-95.

[3] A.D. Wood, J. Stankovic, "Denial of service in sensor network", *IEEE Computer Magazine*, vol. 5, no. 10, Oct. 2002, pp. 54-62.

[4] Ritu Sharma, Yogesh Chaba, and Yudhbir Singh, "Analysis of Security Protocols in Wireless Sensor Network", International Journal of Advanced Networking and Applications, Aug. 2010, vol. 2, Issue 2, pp. 707-713.

[5] Xiuli Ren, Haibin Yu, "Security Mechanisms for Wireless Sensor Networks", *International Journal of Computer Science and Network security (IJCSNS)*, March 2006, vol. 6, no. 3, pp. 155-161.

[6] Nagarathna C.R, Chinnaswamy C.N **"***The Technique to detect and avoid the Denial of Service Attacks in Wireless Sensor Networks"***,** International Journal of Research in Engineering and Technology (IJRET), Volume: 03 Issue: 05, May-2014.

[7] R.Ragupathy, Rajendra Sharma" Detecting Denial of Service Attacks by Analysing Network Traffic *in Wireless Networks", International Journal of Grid Distribution Computing*, Vol.7, no.3 (2014), pp.103-112.

[8] K.Venkatraman, J.Vijay Daniel and G.Murugaboopathi "Various Attacks in Wireless Sensor Network: Survey", *International Journal of Soft Computing and Engineering (IJSCE)*, ISSN: 2231-2307, Volume-3, Issue-1, March 2013.

[9] Nusrat Fatema, Remus Brad *"*Attacks and Counterattacks on Wireless Sensor Networks"*, International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC)*, Vol.4, No.6, December 2013.

[10] A.D. Wood, J.A. Stankovic, (2002) "*Denial of Service in Sensor Networks*," Computer, vol. 35, no. 10, 2002, pp. 54– 62.

[11] David R. Raymond, Scott F. Midkiff,(2008) "Denial-of- Service in Wireless Sensor Networks: Attacks and Defenses," *IEEE Pervasive Computing*, vol. 7, no. 1, 2008, pp. 74-81.

[12] Sandeep, Rajneet "A Study of DOS & DDOS – Smurf Attack and Preventive Measures", *International Journal of Computer Science and Information Technology Research,* ISSN 2348-120X (online) Vol. 2, Issue 4, pp: (312-317), Month: October - December 2014.

[13] Kavita Choudhary, Meenakshi, Shilpa ( ITM University, Gurgoan, Haryana, India) "Smurf Attack: Attacks using ICMP" *IJCST*, Vol.2, Issue 1, March 2011 (ISSN:2229-4333).

[14] Sandeep, Rajneet, "A Study of DOS & DDOS – Smurf Attack and Preventive Measures", *International Journal of Computer Science and Information Technology Research* ISSN 2348-120X , Vol. 2, Issue 4, pp: (312-317), Month: October - December 2014.

[15] Saurabh Ratnaparkhi, Anup Bhange **"**Protecting Against Distributed Denial of Service Attacks and its Classification: A Network Security Issue" *International Journal of Advanced Research in Computer Science and Software Engineering 3(1),* January - 2013, pp. 392-397.

[16] Wesam Bhaya, Mehdi Ebady Manaa" Review Clustering Mechanisms of Distributed Denial of Service Attacks"*, Journal of Computer Science* 10 (10): 2037-2046, 2014
ISSN: 1549-3636.

[17] B. B. Gupta, R. C. Joshi, and Manoj Misra, " Distributed Denial of Service Prevention Techniques", *International Journal of Computer and Electrical Engineering (IJCEE)*, Vol. 2, No. 2, April, 2010 1793-8163.

[18] Dr. Shahriar Mohammadi, Hossein Jadidoleslamy, "A Comparison of Link Layer Attacks on Wireless Sensors Network." *International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC)* Vol.3, No.1, pg 35-56, 2011.

[19] Sunil Gupta, Harsh K Verma, A L Sangal "Security Attacks & Prerequisite for Wireless Sensor Networks", *International Journal of Engineering and Advanced Technology (IJEAT)* ISSN: 2249 – 8958, Volume-2, Issue-5, June 2013.

[20] F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks‖", *IEEE Communications Magazine*, Vol. 40, No. 8, pp. 102-114, August 2002.