Denial of Service Attack in Wireless Data Network:A Survey

Rahul Sourav Singh
Assistant Professor,
Dept. of IT,
Sikkim Manipal
University Sikkim, India.

Ajay Prasad
Assistant Professor,
Dept. of IT,
Sikkim Manipal
University Sikkim, India.

Roselina Maria Moven ,
Dept. of CSE, University
of Engineering and
Management, Jaipur.

Hiren Kumar Deva Sarma
Dept. of IT, Sikkim Manipal
Institute of Technology,
Sikkim.

Abstract: Wireless networks is one of the dominant technology trends in this digital era. Due to the broadcast nature of wireless network, wireless air interface is open and accessible to all types of users, which turned to be a numerous unique challenges on their security to researchers. While the set of challenges in wireless networks are diverse, we focus on Denial of service attack in Wireless Network in this paper. Denial of Service (DoS) attack targets to degrade the efficient use of network resources and disrupts the essential services in the network. DoS attack could be considered as one of the major threats against Wireless Network security. First, we propose effects of DoS attack on Wireless Network. Further, various DoS attacks on different layers of TCP are proposed.

Keywords: Wireless networks, Security, Denial of Service (DoS), Availability, TCP model.

NOMENCLATURE

CA	COLLISION AVOIDANCE
CDMA	CODE DIVISION MULTIPLE ACESS
CSMA	CARRIER SENSE MULTIPLE ACCESS
CTS	CLEAR TO SEND
DoS	DENIAL OF SERVICE
FHSS	FREQUENCY HOPING SPREAD SPECTRUM
ICMP	INTERNET CONTROL MESSAGE PROTOCOL
IP	INTERNET PROTOCOL
MAC	MEDIA ACESS CONTROL
MITM	MAN IN THE MIDDLE
OFDMA	OTRHOGOONAL FREQUENCY DIVISION MULTIPLE ACESS
PHY	PHYSICAL LAYER
RTS	RIGHT TO SEND
TCP	TRANSMISSION CONTROL PROTOCOL
UDP	USER DATA PROTOCOL
WN	WIRELESS NETWORK

I. INTRODUCTION

During the last few decade wireless network gained popularity as compared to the wired network due to the infrastructure, services and ease of deployment. Wireless network adopt the protocol architecture called Transmission control protocol (TCP), which comprises of Application layer, Transport layer, Network layer, Medium Access Layer (MAC) and Physical Layer. Security threats are extremely vulnerable in all these protocol layers due to the open-air interface medium. For example, cryptography technique is used to achieve the security requirements, which includes data confidentiality, data authenticity, data integrity, data availability and data freshness. To ensure the genuineness or authenticity of a caller or receiver, wireless network uses some authentication approaches at different protocol layers. Explicitly, wireless networks are inclined to malicious attacks done by some internal or external malicious node, which includes denial of- service (DoS) attack, eavesdropping attack, spoofing attack, message falsification, injection attack, man-in the- middle (MITM) attack etc. The focus of this paper is to give an overview of DoS attack of a WN based on the TCP model.

II. SECURITY GOALS FOR WIRELESS NETWORK.

Wireless network has different type of architecture than a wired network, but exhibits a common characteristic, which are unique in both. Wireless nodes are always in threat of external malicious nodes so; wireless network should be able to protect the information traversing over the network and the resources from different types of attacks and misconducts of nodes [1] [2]. There are some of the important security objective, which are discussed below:

A. Data Confidentiality

One of the most important issue in network security is data confidentiality [3]. It keeps all the data and information secret from external nodes, which are not authorized to access the data. Only the intended receiver can understand and decode the message [4]. In a wireless network scenario, data confidentiality should fulfil the following requirements:

a. A node in the wireless network should not share data with its neighbor. Suppose for instance, in a domain like military application where an enemy has installed some of the infected nodes into the network. Data Confidentiality approaches will block them from accessing those data and information from the other nodes.

* Corresponding author E-mail addresses: rss2016@outlook.com (R.S.Singh), ajay.prsd1@gmail.com (A.Prasad), rosemoven.rm@gmail.com (R.M.Moven), hirenkdsarma@gmail.com (H.K.D.Sarma).

978-1-5090-4724-6/17/$31.00 ©2017 IEEE

b. It is very important to establish and maintain confidentiality in the public information where node identities and secret keys are being distributed to establish a safe and secure communication among wireless network channels.

B. Data Integrity

Data Integrity refers to protecting the information from being modified by unauthorized parties [5] [6]. This mechanism ensures that message packet cannot be altered or edited by any adversary entity while communicated from the sender to the recipient in the wireless channel. To maintain data integrity, data confidentiality measures should be in place due to following reasons:

a. A malicious node present in the wireless network infuses false information.
b. Disarranged or uncontrolled conditions in wireless network channel cause damage or loss of information.

C. Data Availability

Information is useful if the right people can get to it at the right times [19]. Availability of data or information refers to guarantee that authorized parties are able to access the information whenever they needed even if there are any internal or external attacks suppose for example denial of service attack (DoS) [7]. Different researcher used different approaches for availability of data in wireless network. In some of the mechanisms, extra communication among nodes are being done and in some utilization of a central access control system to guarantee successful delivery of every message to its right recipient.

D. Authentication

Authentication guarantee that received packet comes from a legitimate user. Attack in the network is not of altering the packets in the network but also injecting fabricated packets in the network, so that receiver receives a malicious packet [8]. Therefore, data authentication validates the identity of users. Authenticity is checked either by symmetric or asymmetric mechanism where source node and destination node exchange some secret key to compute code called Message Authentication Code (MAC).

E. Data Freshness

Data freshness means that the data is current. In wireless network nodes sends data related to the environment, it is possible that an adversary retransmit the copy old data value. Therefore, it is very important to check whether the data is old or new. There are number of approach to get rid of these situation, one of the approach is to add the counter to the message packet or a random number. This approach can be used during encryption to maintain data freshness.

III. Denial of Service Attacks in different layers and counter measures:

Wireless networks are divided into different layers, and this layered architecture make it prone to many attack at different layers. Denial of Service is a form of such attack that affects different layer of OSI model. Wood and Stankovic [9] first proposed layer wise categorization of DoS attacks. Later, Raymond and Midkiff [10] enhanced the survey with some updated information. Here we study the Denial of Service attacks at different level of layered architecture of a Wireless network and the methods employed to counter such attacks

A. PHY Layer:

PHY Layer is the lowest layer of the Layered architecture of Wireless Network. PHY layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation, and data encryption [9]. There are two types of DoS attacks that can affect the PHY Layer:

- Tampering: Wireless network operates in distributed outdoor environment and thus it is prone to many attacks. A rogue access point can be added to a network without knowledge. These access points can create a very huge security concern. Such physical attacks cause irreversible damage. The rogue party can capture cryptographic keys and even tamper with the circuitry. Programs codes could be modified even. If the wireless network is unattended, it is very for the advisory to plug in an access point to one's network.

  Security Measures for tampering involves tamper proofing which involves:

  a. 802.1X Network Control Access can be used to authenticate the user every time they plug in the wireless network.
  b. Fault Tolerant Protocols designed to be resilient to such attacks.

- Jamming or interference: It means creating hindrance to one's network; the main aim is to generate intentional hindrance to communication between legitimate users [10]. Due to the nature of wireless communication, this is a very big challenge for the wireless network designer. Jamming of a network can be done using very less powerful devices such as Bluetooth headset, cordless phone or even a microwave oven. This make the communication difficult. Jamming attack can be further classified into:

  a. Constant Jamming, where the packets are corrupted while they are transmitted.
  b. Deceptive Jamming, where a bit stream is injected in the network continuously to make it look legal but flooding the communication link.
  c. Intermittent Jamming where advisory transmits jamming signal from time to time randomly to interfere the legitimate transmission and then sleeps.
  d. Reactive jamming, where the jamming is done when the adversary senses active communication in the network.

  Security measures that involves avoiding Jamming includes:

TABLE I:
SUMMARIZATION OF DOS ATTACKS IN PHY LAYER

PHY DoS Attacks	Characteristics	Security measure
Tampering	Unauthorized access to access points	a. 802.1X Network Control access. b. Fault Tolerance Protocols.
Jamming	Interruption of Legitimate Transmission	a. FHSS to transmit signal randomly. b. Detect and Reroute.

a. Frequency Hoping Spread spectrum technique where the signal is transmitted by randomly switching the carrier among many frequency channel. A pseudo random sequence is employed for the purpose, which is known to the both receiver and transmitter. Rapidly frequency hopping makes it difficult for the advisory to track the frequency used thus making jamming attack difficult to be performed in the network.

b. Employing protocols to detect offending signal and ether get it out of network or reroute.

B. MAC – Layer Attacks:

The MAC layer with intelligent control mechanisms like CSMA/CA, OFDMA, CDMA, etc enables multiple network nodes to access a shared medium. Each network node is installed with a NIC (Network Interface Controller) and has a unique MAC address. MAC address helps in uniquely identifying the user for authentication. Advisory tries to access the MAC layer and hinder the service it provides. There are various methods as listed below:

- Collison: When two or more nodes tries to transmit using same frequency simultaneously then collision occurs. As a result of collision, the packet is discarded and has to be resent. An adversary can create collision in network by targeting specific packets such as ACK control messages. If the adversary following the network traffic can transmit on a known frequency that some node in the targeted network is transmitting, thus resulting in collision. The packet will be rejected every time. This will result in exponential back off.
  Two major security measures are employed to overcome collision. They are listed below:

TABLE II:
SUMMARIZATION OF DOS ATTACKS IN MAC LAYER

MAC Layer DoS Attacks	Characteristic and Features	Security measure
Collision	Tracing targeting frequency and transmitting to create collision.	a. CSMA/CA b. Error correcting codes
Exhaustion through Network Injection	Injecting malicious network forged command to exhaust the network	a. Time Division Multiplexing. b. Rate limiting to the MAC admission control
Interrogation	Sending continuous RTS to CTS from a authorize user by impersonating as the target node.	a. Anti-replay protection. b. Link layer authentication. c. Jamming detection.

a. Back-off timers to determine when the network is free for devices to communicate, i.e. send packets follow CSMA/CA, a series of listening periods. These mechanisms have controls in place to prevent collisions in a controlled environment.
b. Use of error correcting codes.

- Exhaustion through Network Injection: Malicious node exhausts the systems like routers, switches by injecting malicious network reconfiguration command continuously in the network [11]. Even the node continuously keeps continuously transmitting or requesting over the channel. These leads to starvation of other nodes present in the network with respect to channel access and as huge number of networking commands are initiated, the network is paralyzed.
  Security measures to avoid such attack are listed below:
  a. Time division multiplexing; each node is allocated a time stamp for which it can transmit through the network.
  b. Rate limiting to the MAC admission control; the network can ignore excessive requests hence preventing the energy drain.

- Interrogation: IEEE 802.11 use RTS and CTS. An advisory can trace the interaction between two nodes prior to transmission and exhaust the node by continuously sending RTS messages to its legitimate CTS responses from authorize user by impersonating as the target node [12].
  Security measures taken to avoid such attack include
  a. Anti-replay protection; where the packets are sent and received only once.
  b. Link layer authentication; ensuring the packets are trusted between trusted parties only.
  c. Jamming detection; sleeping to counter stream of replayed messages.

C. *Network Layer*

In Network Layer IP is the principal protocol to deliver packages from SN to DN through the network. Attacks to Network Layer tries to exploit the drawbacks in IP. DoS in IP includes spoofing, selective forwarding and Smurf attack.

- IP Spoofing: It employs impersonating an authenticate node in the network to hide the malicious node identity [13]. The target of the mentioned attack is the routing information of the network traffic. The attackers after spoofing a nodes id, alters or replay routing information to disrupt the network traffic. The advisory creates routing loops by attracting or repelling the network traffic to the node that it is impersonating thus causing network portioning and increase in end-to-end latency. In addition, it paralyzes the network by flooding it with forged IP packets while impersonating itself as an authenticate node present in the network.
  Security measures to counter such attacks are as follow:
  a. Appending MAC address every time the message is relayed, hence the receiver can verify for any alteration to the message.
  b. Inclusion of timestamp to counter replayed messages.
- Smurf Attack: A form of DoS attack to the network layer where the advisory with the spoofed node IP address sends huge number of ICMP messages to the node or groups of nodes it wants to affect [14] [15] [16]. The nodes have to respond to the ICMP requests upon receiving. The victim network gets flooded with huge number of ICMP requests and responds to this network. It results in huge traffic in communication network thus paralyzing the network.
  Security measures to avoid Smurf attack includes:
  a. Use of firewalls to reject malicious message request arriving from the forged network.
  b. Routers and individual nodes in the network configured such that it does not constantly respond to ICMP requests.

TABLE III:
SUMMARIZATION OF DOS ATTACKS IN NETWORK LAYER

Network Layer DoS attacks	Characteristics and Features	Security Measures
IP Spoofing	Impersonating IP address	a. MAC address appending b. Timestamp
Smurf Attack	Paralyzing the network by huge number of ICMP requests.	a. Firewalls to block malicious requests. b. Routers and nodes configured not to constantly respond to ICMP requests.
Selective Forwarding	Blocking some messages.	a. Use of multiple paths. b. Acknowledgement.

- Selective forwarding: In a wireless network, the nodes need to transfer the packet accurately. In selective forwarding the advisory impersonating as an authenticate node or hijacked node gain access to the data traffic through that node; comprises the communication by forwarding some messages received at the node and dropping the rest.
  Security measures to counter selective forwarding involves the following procedures:
  a. Using multiple paths instead of single path for data transmission.
  b. Use of acknowledgement to ensure the data are transfers as they are received.

D. *Transport Layer*

Transport layer provides end-to-end connection. There are two main ways to do so; unreliable data transfer through UDP protocol and reliable data transfer through TCP protocol. Both UDP and TCP suffers from vulnerabilities, which make them prone to attack.
The DoS attacks to transport layer includes the following attacks:

- Flooding: Both UDP and TCP suffer from flooding which is a kind of DoS attack. TCP flooding is also called ping flooding; where a huge number of ping requests are sent by attacker to the victim node or group of nodes, for example ICMP echo, on receiving which the nodes have to respond to the malicious node for example ICMP echo reply [17] [18].

TABLE IV:
SUMMARIZATION OF DOS ATTACKS IN TRANSPORT LAYER

Transport Layer DoS attacks	Characteristics and Features	Security measures.
Flooding: a. TCP Flooding b. UDP Flooding	a. Flooding the network with ping requests. b. Flooding the network with huge number of UDP packets	a. Limited response. b. Firewalls
De-Synchronization	Dropping Frames	Authentication of packets.

- Similarly, in UDP, flooding is done by sending huge number of packets to a victim node or group of nodes from the malicious node and the nodes on receiving the packets have to respond to it [19].
  In either of the cases the node at the receiving end get unavailable to other legitimate node in the network due to overwhelming incoming requests and reply to them.
  Security measures employed to counter such flooding attacks include:
  a. Limited response rate of UDP packets and TCP pings.
  b. Firewalls that filters the incoming request.
- De- Synchronization: In this attack, the adversary impersonating as a legitimate node repeatedly spoof messages to other nodes, so the nodes request for retransmission of missing frames. Nodes keep sending request continuously for missed packets through the network thus flooding the network with response resulting in huge traffic even paralyzing the network and the attacked node becomes unavailable for other legitimate node in the network.
  Security measures to counter de-synchronization attack includes:
  a. Authentication of packets before they are delivered to the end node.

IV. CONCLUSION

Security plays a vital role while developing wireless network application hence it becomes important to study and analyze the attacks and the security measures related to wireless network. In this paper, we have surveyed on the different dos attacks in the different layers of wireless network architecture and its effects on communication. DoS attacks are categorized as

A) Destructive -that is they destroy the functionality one of the way by which this is achieved is by changing the configuration information
B) Resource consuming- that is they consume the scarce and limited resources of the device.
C) Bandwidth consuming-they consume high bandwidths; network devices with low bandwidths may suffer from high bandwidth consumption.

We have discussed in details the existing protocols and the methods that can be employed in overcoming these attacks in wireless networks. The different layers of wireless network architecture and the dos attacks related to each layer is analyzed. We have started with the physical layer, which is lowest layer of the wireless network architecture, the DoS attack related to the layer are Tampering and Jamming, are described and related security measures are discussed. The next layer is the MAC layer and DoS attacks related to the following layer are Collision, Exhaustion through network and Interrogation; the characteristics and security measures of each of these attacks has been analyzed. Thirdly, we have the network layer and the DoS attacks related to it are IP Spoofing, Smurf attack and Selective Forwarding; and security measures likes firewalls to block malicious requests and timestamp are discussed. Lastly, we have the transport layer and the DoS attacks related to it are Flooding; which is further characterized into two types; TCP flooding and UDP flooding; and De-synchronization are surveyed. In spite of employing security measures such as TDM, firewall, re-routing, authentication of packages, Fault tolerance protocols and many more, still there are open challenges that are to be addressed regarding DoS attack. Among many, there are these two types of security challenges opened for further research as discussed below:

- Mixed DoS wireless attack where different algorithms are to be employed to secure the system from different DoS attacks happening simultaneously.
- Cross Layer, wireless security design, where single security protocols should be strong enough to overcome DoS attacks at different layers.

REFERENCES

[1] D. Ma and G. Tsudik, “Security and privacy in emerging wireless networks,” IEEE Wireless Communications, vol. 17, no. 5, pp. 12-21, October 2010

[2] H. Kumar, D. Sarma, and A. Kar, “Security threats in wireless sensor networks,” IEEE Aerospace and Electronic Systems Magazine, vol. 23, no. 6, pp. 39-45, June 2008.

[3] Y. Wei, K. Zengy and P. Mohapatra, “Adaptive wireless channel probing for shared key generation,” in Proceedings of The 30th Annual IEEE International Conference on Computer Communications (INFOCOM 2011), Shanghai, China, April 2011

[4] W. Stalling, Cryptography and network security: Principles and Practices, Third Edition, NJ: PrenticeCHall, January 2010.

[5] X. Lin, “CAT: Building couples to early detect node compromise attack in wireless sensor networks,” Proceedings of The 2009 IEEE Global Telecommunications Conference, Honolulu, USA, December 2009.

[6] E. Shi amd A. Perrig, “Designing secure sensor networks,” IEEE Wireless Communications, vol. 11, no. 6, pp. 38-43, December 2004

[7] A. D. Wood and J. A. Stankovic, “Denial of service in sensor networks,” IEEE Computer, vol. 35, no. 10, pp. 54-62, October 2002.

[8] Y. Jiang, C. Lin, X. Shen, and M. Shi, “Mutual authentication and key exchange protocols for roaming services in wireless mobile networks,” IEEE Transactions on Wireless Communications, vol. 5, no. 9, pp. 25692577, Septermber 2006.

[9] Raymond, D. R. and Midkiff, S. F. (2008). Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. IEEE Pervasive Computing, January-March 2008, pp 74-81.

[10] A. Mpitziopoulos, “A survey on jamming attacks and countermeasures in WSNs,” IEEE Communications Surveys & Tutorials, vol. 11, no. 4, pp. 42-56, December 2009.

[11] J. Park and S. Kasera, “Securing Ad Hoc wireless networks against data injection attacks using f rewalls,” Proceedings of The 2007 IEEE Wireless Communications and Networking Conference, Honkong, China, April 2007.

[12] X. Du, H. Chen, "Security in Wireless Sensor Networks", IEEE Wireless Communications, 2008

[13] Computer Emergency Response Team (CERT), “CERT advisory: IP spoof ng attacks and hijacked terminal connections,” January 1995, available on-line at http://www.cert.org/advisories/CA-1995-01.html.

[14] N. Hastings and P. McLean, “TCP/IP spoof ng fundamentals,” Proceedings of The 1996 IEEE Fifteenth Annual International Phoenix Conference on Computers and Communications, Arizona, USA, March 1996.

[15] B. Harrisa and R. Hunt, “TCP/IP security threats and attack methods,” Computer Communications, vol. 22, no. 10, pp. 885-897, June 1999

[16] F. El-Moussa, N. Linge, and M. Hope, “Active router approach to defeating denial-of-service attacks in networks,” IET Communications, vol. 1, no. 1, pp. 55-63, February 2007.

[17] C. Schuba, et al., “Analysis of a denial of service attack on TCP,” Proceedings of The 1997 IEEE Symposium on Security and Privacy, Oakland, USA, May 1997.

[18] A. Kuzmanovic and E. W. Knightly, “Low-rate TCP-targeted denial of service attacks and counter strategies,” IEEE/ACM Transactions on Networking, vol. 14, no. 4, pp. 683-696, August 2006.

[19] R. Chang, “Defending against f ooding-based distributed denial-ofservice attacks: A tutorial,” IEEE Communications Magazine, vol. 40, no. 10, pp. 42-51, October 2002.

[20] Arun Malik, Gaurav Raj and Isha, (2013). DoS Attacks on TCP/IP Layers in WSN. IJCNS, vol. 1, no. 2, 2013, pp 40-45.

[21] I"Wireless security threat taxonomy,". Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society 18-20 June 2003 Page(s):76 – 83.

[22] "Wireless security's future,". Security & Privacy Magazine, IEEE Volume 1, Issue 4, July-Aug. 2003 Page(s):68 – 72.

[23] Radomir Prodanovi and Dejan Simi, “A survey of wireless security”, Journal of Computing and Information Technology – CIT 15, 2007, 3, pp – 237–255.

[24] Mansoor Ahmed Khan, Aamir Hasan, “Pseudo Random Number Based Authentication To Counter Denial of Service Attacks on 802.11 “, WCON Conference, Surabaya, Indonesia, IEEE Xplore, 2008.

[25] Deng, J., Han, R., and Mishra, S. (2005). Defending against Path-based DoS Attacks in Wireless Sensor Networks. ACM SASN’05, November 7, 2005, Alexandria, Virginia, USA,pp 89-96.

[26] By Yulong Zou, Senior Member IEEE, Jia Zhu, Xianbin Wang, Senior Member IEEE, and Lajos Hanzo, Fellow IEEE,A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. Accpeted for approvl 23rd April 2016.

[27] Y. Jiang, C. Lin, X. Shen, and M. Shi, “Mutual authentication and key exchange protocols for roaming services in wireless mobile networks,” IEEE Transactions on Wireless Communications, vol. 5, no. 9, pp. 25692577, Septermber 2006.

[28] H. Huang, N. Ahmed, P. Karthik, “On a new type of denial of service attack in wireless networks: The distributed jammer network,” IEEE Transactions on Wireless Communications, vol. 10, no. 7, pp. 23162324, July 2011.