IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Methodology For Securing Wireless Mash Network Against Denial-Of-Service Attack

SEEMA DEVI,[1] Dr. KALPNA MIDHA[2]
Student P.hd,[1] Assistant Professor[2]
Department of Computer Science
Shri Khushal Das University, Hanumangarh, India

Abstract: - Wireless mesh network is a multi-leap communication. All packets produce from source to goal node in leap by leap forwarding manner. To assure the genuineness of each node is much substantive and communication must be protected. WMN can be defined as an influential, self-concerned, self-construct, propagates wireless multi-leap network. WMN comprises of mesh routers (MRs), mesh clients (MCs) and gateways. When WMN is indexed the nodes will form a network automatically and lead off listening to broadcasting notification. Security has turn the leading pertain to provide protected communication between different mesh nodes. The objective is to study the mechanism Multilayer model for preventing WMNs, possibility of Denial of Service attack in WMNs networks and a high efficiency DoS attack detection algorithm**.**

Keywords: DoS (Denial of Service), Authorization, Security Mechanisms, IP Filter, WMNs etc.

INTRODUCTION:

Wireless mesh network is an open network that is fain of discrete types of migratory as well as static nodes. Wireless mesh network is prepared to similitude wide space redundancy pay. It assembles rapid internet services at less cost. It is a particular multi-leaps network which connects node to each other [1]. A WMN is established among with the connection of wireless entree way points installed for each local network users. Every network user sends data to the further node. The WMN infrastructure is consolidating because every node requires only deliver data to the further node. Mesh networking can be victimized to connect small businesses in rural neighborhoods and upstage areas for their affordable internet connection [2].

"***Denial of service***" that demote the WMN performance and extremely makes the network service scummy. Denials of Service (DoS) attacks are attacks against accessibility which seeks to prevent the decriminalize users from accessing the network. When authoritative users are not provided a requested service within a defined maximum waiting time it means that a DoS violation has occurred [3].

It is highest degree adverse and dangerous attack that can be launched on any layer of broadband Wireless network. The leading aim of a DoS attack is to abundance the network with service requests to the server. This can lead to server being unable to service all the requests thereby denying offering service to legitimate requests [4].

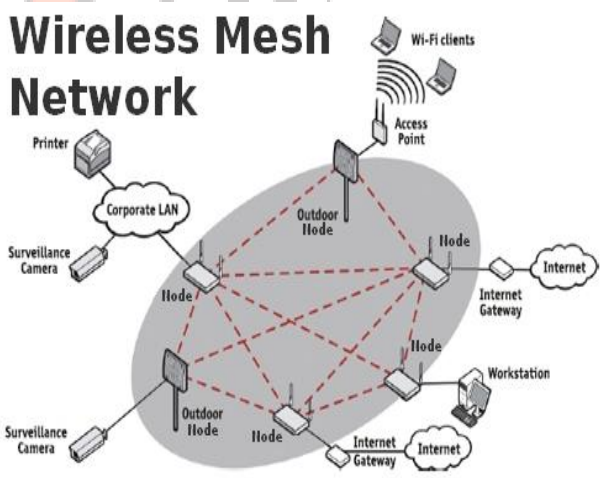

Figure 1. Wireless mesh network (WMN)

Divers applications of Wireless mesh network as [3]:

- Community and vicinage network
- Building Automation
- Transportation System
- Health and Medical System

- Security
- Surveillance system
- Emergency disaster network
- Peer to peer Communication

Network security threats in WMNs

Network security threats Categories of attacks could involve of reflexive observing of data communications discrimination by insiders, close-in attacks, and detrimental attacks from side to side service provider & vigorous network attacks [4]. Information systems & networks usually offer targets & must be resistant with in order to attack from full dimension of threat agents from intruders to nation-states [5]. System must be capable to restrict detriment & recovery from occurrence of attacks.

DENIALS of SERVICE (DoS):- Today DoS attacks are very general in the internet world [1]. Ascend tempo of so much attacks have created servers and network devices on the internet at higher danger then invariably. Expected equivalent intellect constitution and community bear huge servers and data on the internet are now making neat strategy and investiture to be protected and defend themselves adverse several cyber-attacks including service rejection.

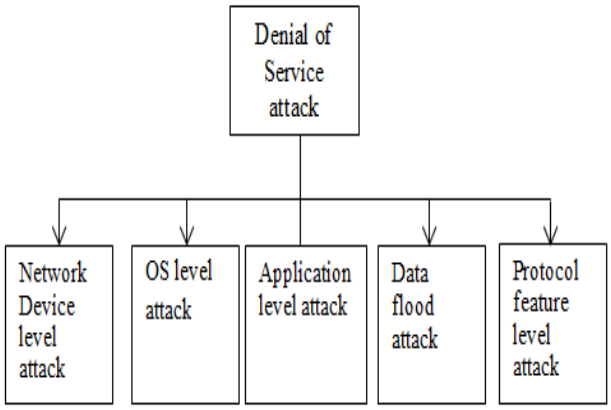

Figure2. Type of DoS Attack

On the network mechanism level attack certain hardware devices like router targets on the network. An attack has been inserted by exploiting some software worms or hardware resource exposure [6]. In the victim device the OS is used to launch the DOS attack to attack the exposure (OS) level of the operating system [9]. In application attack glitch or exposure in the operations are discovered to feat them for dos attack. Port scanning is very common in this scene to identify open ports of a remote application [6]. In the data flood attack objectives are relation capability of a remote host or compatibility of a network [7]. Congestion is furnished by the aggressor among dupe to exhaust connectivity or compatibility resources. So that normal services are refuse or disgrace for requests of legitimize users. In protocol lineament attacks impuissance of some protocol aspects are used to feat them for inserting DoS attack.

Proposed Model for Denial of Service Attack

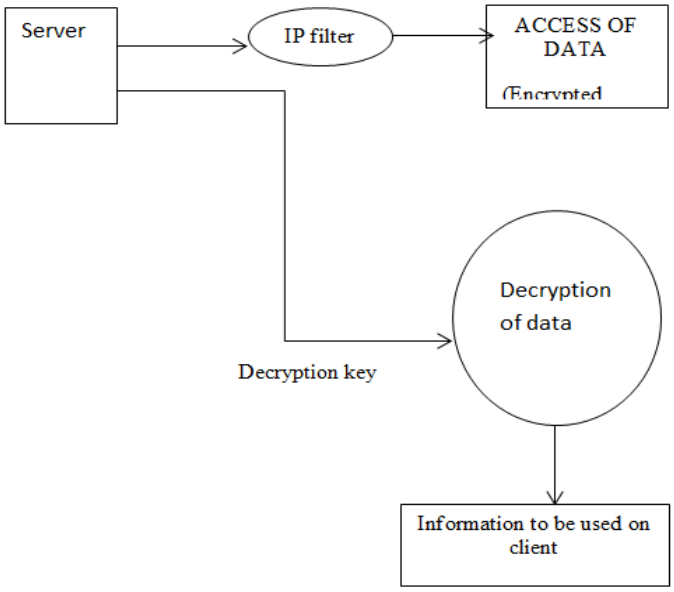

Figure3. Proposed model for DoS

IP filter is used to refuse unauthenticated transmission of packets from server to client [11]. It enhances the network security by customizing existing encryption techniques. The loopholes of existing security mechanisms & enhance security of network.

Socket server & corresponding client to prevent unauthentic access during data transmission to make use of more complex key during encryption & decryption to develop user interface to make client server communication. Cryptography method is used to encrypt and decrypt the client data.

Cryptography refers to the use of techniques like microdots a nd word-

image integration to conceal information during storage or tr ansmission. **Confidentiality**: - It recognizes that only participants (Sender & Receiver) should be able to approach message [7].

- **Unity**: - Subject matter of message should not be changed. If this has been altered then this has been called type of modification attack.
- **Non-repudiation**:- There has been situation where sender changed over subject matter of message & after that he decline that he had not sent message.
- **Authentication**: - Both sender & receiver have to examine certification to each other.

Triple Layer Security:-

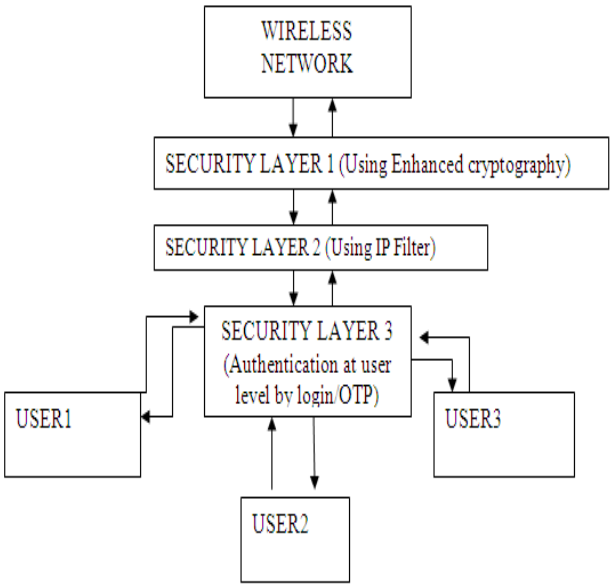

Figure4. Triple layer Security

In proposed model there would be triple layered security

1. Security layer 1 would be commissioned cryptography algorithm of AES to boost security.
2. Security layer 2 would drop packets from unauthentic IP addresses.
3. Security layer 3 would authenticate user by providing login password security at application layer.
4. Security would be enhanced using one time password also that becomes useless after using one time.
5. In this way we would secure wireless network from external attacks & authentic access.

OTP GENERATION: One time password would be generated randomly by Math.random() function in java. Each & every time complex OTP number could be generated to be used during decryption [12].

IP Filter: Centralized database of IP address would be created on centralized server & decryption request from authentic IP would be accepted. If IP has been not found in database or its status has been 0 then Decryption would not be allowed.

Conclusion:-

We have enhanced security by enhancing encryption algorithm. Here we have also defined our own ports for server and client & defined new rules for encryption and decryption & involved multiple layer of security like IP Filter & OTP code this would definitely improve security mechanism within Wireless computing environment. Our security mechanism would first prevent hacker to access data within unauthenticated way & restrict them to understand data.

Future Analysis could be made on different network and topology. Additional security layers may be added to enhance security.

REFERENCES

1. Ian F. Akyildiz, Xudong Wang , Weilin Wang “Wireless mesh Networks: A survey” Computer Network 2005; 47(4): 445-487.
2. monika, Denial of service attacks in wireless MESH NETWORK. IJCTIS, 2012. 3(3): p. 7.
3. Peter mill and Tim grance, “The NIST Definition of Cloud Computing”, 2011, National Institute of Standards and Technology, Gaitherbsburg,MD 20899-8930, NIST Special Publication 800-145.
4. Misra, S., et al., An adaptive learning routing protocol for the prevention of distributed denial of service attacks in wireless mesh networks. Computers & Mathematics with Applications, 2010.
   60(2): p. 294-306.
5. Peng T, Leckie C, Rammamohanarao K. Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Computing Surveys.2007; 39(1).
6. Haggerty J, Shi Q, Merabti M. Early detection and prevention of denial-of-service attacks: A novel mechanism with propagated traced-back attack blocking. IEEE Journal on Selected Areas in Communications. 2005; 23(10), pp.1994–2002
7. Mathew R, Katkar V. Survey of Low Rate DoS Attack Detection Mechanisms. ICWET’11 Proceedings of the International Conference and Workshop on Emerging Trends in Technology. 2011. University, Mumbai,India , pp. 955-958
8. Pointcheval D,Boyen X, *Strong Cryptography from Weak Secrets*, (Stellenbosch, South Africa), D. Bernstein and T. Lange Eds., Springer-Verlag, 6055, pp. 297–315.
9. Haggerty J, Shi Q, Merabti M. Early detection and prevention of denial-of-service attacks: A novel mechanism with propagated traced-back attack blocking. IEEE Journal on Selected Areas in Communications. 2005; 23(10), pp.1994–2002
10. Mathew R, Katkar V. Survey of Low Rate DoS Attack Detection Mechanisms. ICWET’11 Proceedings of the International Conference and Workshop on Emerging Trends in Technology. 2011. University, Mumbai,India , pp. 955-958
11. Pointcheval D,Boyen X, *Strong Cryptography from Weak Secrets*, (Stellenbosch, South Africa), D. Bernstein and T. Lange Eds., Springer-Verlag, 6055, pp. 297–315.

12. Peng T, Leckie C, Rammamohanarao K. Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Computing Surveys.2007; 39(1).