# A Review of Security Analysis in Wireless Mesh Networks

Jasleen Kaur[1], Dr. Om Prakash[2]
[1]*Research Scholar, Shri JJT University*
[2]*Associate Professor, MRIET Hyderabad*

***Abstract***—Wireless Mesh networks (WMNs) is among the self-systematize, self-configured and multi-hop wireless network that render wireless services to variant applications. These applications involve broadband home networking, community, transport system, security surveillance systems, health and medical system etc. used in personal, local campus and metropolitan areas. Due to dispersed nature of WMNs, it is vulnerable to various attacks. viz internal or external. Denial of service is among the recurrent types of attack in the wireless mesh networks. Due to extensive employment of broadband internet access, WMNs are more susceptible to Distributed Denial of service attack. In this paper, we propound different types of DDoS attacks in a network and encryption techniques (AES , RSA and DES) used that alleviate the upshot of DDoS attack in the network.

***Keywords***-DoS, LAN, WAN, MAN, DDOS

## I. INTRODUCTION

Network is a system that authorizes users to trade information at large distances by routers, servers, switches that are capable of sharing software and hardware resources. A network predominately comprises of wired and wireless technologies through which it communicate. Wired networks incorporate optical fiber ,coaxial cable or copper wires to form a twisted pair among users. In terms of a computer network, a network is defined as series of points or nodes, interconnected by communication paths for transmitting, receiving and exchanging data, voice and video traffic. Exchange of information materializes with the aid of switches and routers (Network devices) via various versions of protocols and algorithms. These endpoints may embrace cellular radio broadcast radio, microwave or satellite

## II. TYPES OF NETWORKS

Networks are categorized by extent of their domains. Local area networks (LAN- interconnects endpoints in a single domain). Wide area networks (WAN-interconnects multiple LANs), and metropolitan area networks (MAN-interconnect computer resources in a geographic area). Storage area networks (SAN-interconnect storage devices and resources). Network categorization based on span of topologies includes Wireless sensor networks (WSNs), which is a large scale network of small embedded devices, escorted by sensing, computational and communication capabilities. However in WSNs, the sensor nodes have constraints in terms of processing power, communication bandwidth and storage space which required very efficient resource utilization [1]. Mobile Ad-hoc networks (MANET) are a wireless ad-hoc network which is self configuring and accommodate network of mobile users connected via wireless links. It is one of the types of wireless network without having cumbersome infrastructure. Network topologies alter frequently as mobile nodes are free to move randomly, leading to network partition, route change and loss of information. Vehicular Ad-Hoc Network (VANET) is a subset of Mobile Ad-Hoc Network (MANET) that provides communication between vehicles and vehicles-road-side base stations with an aim of yielding efficient and safe transportation. A vehicle in VANET is considered to be an intelligent mobile node capable of communicating with its neighbors and other vehicles in the network [2]. Limitations include difficulties to manage networks and control congestion collision in network.

WMNs are gaining wide popularity due to their ability to integrate several networks in one network. It enhances reliability and improved performance over conventional wireless LANs [3].

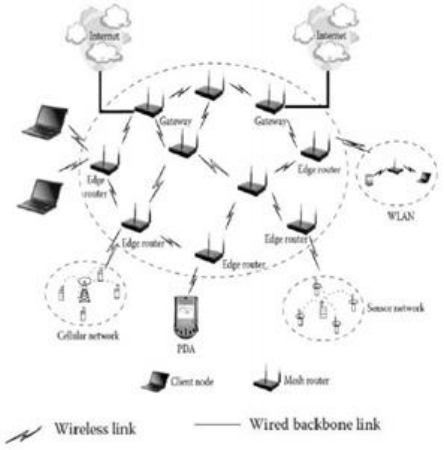


Fig 1: Wireless mesh network

## III. APPLICATION AND CHALLENGES IN WIRELESS MESH NETWORKS

WMN institute the concept of a peer-to-peer mesh topology with wireless communication between mesh routers. Assignable to the recent amelioration in research, WMNs, are desired numerous applications. These applications are as numerated below:

1. Home networking: Broadband home networking is a network of home appliances (personal computer, television, video recorder, video camera, washing machine, refrigerator

etc.) apprehended by WLAN technology. WMNs administer broadband connectivity between the home networking devices with the aid of single Internet connection through the gateway router.

2. Disaster Management and Rescue Operations: WMNs are useful at places where spontaneous network connectivity is solicited, such as disaster management and emergency operations. During disasters like fire, flood, and earthquake, all the existing communication infrastructures might collapse. Consequently during the rescue operation, mesh routers can be installed at rescue team's vehicle and at different locations which form the high-bandwidth mesh backbone network.. Different communication interfaces at the mesh routers confer access to different mobile devices of network. This abets public users to communicate with others when they are in critical circumstances. These networks can be established in insignificant time, which makes the rescue operation more effective.

3. Military applications: Field operations in Military forces are wielding WMNs to connect their computers, system laptops etc.

4. Medical field: It enables clinicians to monitor patients remotely and render timely health information, reminders, and support thereby potentially extending the reach of health care by making it available anywhere, anytime.

There are prevalent challenges in wireless mesh network that are as follows:

1. Directional Antennas: Principally in WMNs, directional antennas are exploited which scale down the interferences between the simultaneous transmissions and also cut down the transmission power for long distance communications. Notwithstanding, directional antennas can significantly complicate the design of upper layers [4].

2. Mobility: WMNs are barely capable of supporting supplemental user mobility therefore it is mandatory for physical layer to support fast fading conditions associated with mobile users.

3. Authentication: Data is transferred amid the authenticated users in the network. Unauthorised users deferred services in the network.

4. Privacy: In WMNs, user data is to be secured from sniffing by eavesdroppers that degrade the performance of network. End to end encryption should be effective [4].

## IV. LITERATURE SURVAY

Ahmed E. A. A. & et. al. [6-7, 9] worked on unmanned aircraft systems. In this process there are many unmanned aircraft system and ground base stations are configured. These are responsible to create a UAS network and communication of data packets from one to another node. Ahmed investigated some problem during setup and operating this type of terminology. These problem cause high operating cost and maximize the time consumption of network communication.

Author also investigates the adaptive modulation effects on the network and their communication with this architecture using a small design of a game based on formulated potential for checking the performance and energy consumption of current scenario.

Various security issues in the wireless networks along with their some routing challenges were also considered. They also assume some attacks in the wireless networks. Attacks can degrade the performance of the network.

They stole information with many anonymous routes in the network. Different attacks are having their own way to perform degradation on the network. Some of them are working with some kind of clone node and other are working with by pushing a heavy load on the network. These types of attacks are known as DDos attacks. Dos attacks applied through a heavy load of request pushing on the server which will just to degrade the processing speed of the network. Various techniques are also there for prevent these type of attacks. Most common technique is encryption of data packets when data travel from intermediate node in the network or authentication scheme for the network node etc.

AggelikiSgora, & et. al. [8, 10] survey about mesh networks in wireless communication. The mesh network technology can save much more cost for communication as compare to other networks. It's a high speed network which can be combination of various other topologies. Due to their very flexible behavior it can be easy to adjustable in all the conditions and can provide much more satisfaction for their users. In future the mesh networks can be used as high speed communications in wireless mediums.

Author analyzes the fundamental security challenges in the wireless networks. It can degrade the performance of the network with less security. Attack can affect various parameters of the network as throughput, packet drop, and delay in communication.

DDoS attacks are among the most difficult problems in Wireless mesh networks. It occurs especially, when the target is the Web server. In a DDoS attack, the incoming traffic flooding the victim originates from many different sources. This attack occurs usually when multiple systems does not allow the target system to use the bandwidth or resources in the network. Thus multiple compromised systems is formed called a botnet. A botnet is a network of computers programmed to receive commands without the owners' knowledge. When a server is overloaded with connections, new connections can no longer be accepted. Therefore by blocking single source effectively makes it impossible to stop the attack in WMNs.

The major disadvantageous of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are difficult to remove in the network. These attacker advantages cause challenges for defense mechanisms. Thus result in closing a website for periods of time.

## V. TYPES OF DDOS ATTACKS

DDoS attacks can be broadly divided into three categories:

1. Volume Based Attacks: The Volume based attack abstain target system from using bandwidth in the network and

its magnitude is measured in bits per second (Bps). It involves UDP floods, ICMP floods, and other spoofed-packet floods.

2. Protocol Based Attacks: Protocol Based attack consumes an actual server resource, or those of intermediate communication equipment, such as firewalls and load balancers, and is measured in Packets per second. It comprises SYN floods, fragmented packet attacks, Ping of Death and Smurf DDos etc.

3. Application Layer Attacks: Application layer attack Comprised of innocent requests that is composed on the server whose sole goal is to crash the web server, and magnitude is measured in requests per second. It includes low-and-slow attacks and GET/POST floods. Some catastrophic types of DDoS attacks include:

a. UDP Flood Attack

User Datagram Protocol flood attack is essentially a session less or connectionless computer networking protocol. This flood occurs when an attacker sends an IP packet containing UDP datagrams with the purpose of slowing down the victim to the point from where victim could no longer handle valid connections. This activity shut down host resources, and could ultimately lead to inaccessibility.

b. ICMP (Ping) Flood Attack

Internet Control Message Protocol is akin to UDP flood attack. It is radically an error-reporting protocol network device used to generate error messages to the source IP address. ICMP could create and send messages to source IP address. It results in ICMP echo requests which overload the victim with large no. of requests. Thus, victim expends all its resources responding until it could no longer process valid network traffic.

This type of attack consumes both outgoing and incoming bandwidth, with victim's server often attempting to respond with ICMP Echo reply packets ultimately resulting in significant overall system slowdown.

c. SYN Flood Attack

A SYN flood is a denomination of denial-of-service attack. It includes attacker sending a succession of SYN requests to target's system in an attempt to consume enough server resources. This emanate in system unresponsive to traffic. Thus new connections are forbidden eventually resulting in denial of service.

d. Ping of Death

Ping of Death is a genre of Denial of Service attack where attempts are made to crash, destabilize and freeze the targeted computer or service via malformed or oversized packets manoeuvring a simple ping command. Overflow memory buffers, causes denial of service for legitimate packets.

e. Sybil Attack

In peer-to-peer network, computer bank on assumptions of identity, where each computer represents a single identity. Sybil attack is a type where a node in a network claims multiple identities. This attack emerges when an insecure computer is hijacked to plea multiple identities. Here the node fakes multiple identities and claims itself to be a distinct nodes on the network though it is just a single malicious node. The sybil attack hampers the routing protocols by creating false links between a honest and a malicious node. The attack can have detrimental effects on resource allocation, misbehaviour detection, disrupting communication by stealing information and voting techniques in the wireless networks.

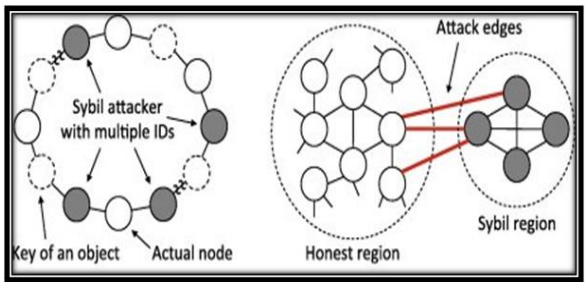


Fig 2: Sybil attack

The above figure shows Sybil attack. Here the wireless mesh networks are equally prone to network partitioning attacks and routing loop attack. In network partitioning attack, the malicious nodes collude together to disrupt the routing tables in such a way that the network is divided into non-connected partitions resulting in denial of service for certain network portion. Routing loop attacks affect the packet forwarding capability of the network. When the packets are forwarded to these fake nodes, the malicious node, that created the identities, processes these packets. Thus creating multiple identities, this attack degrades the performance of wireless mesh networks.

It is essential to recognize a Sybil attack and transcript its hazards. Since Sybil attack is a harmful attack in distributed peer-to-peer systems therefore almost all such systems are based on a common assumption that each participating entity controls exactly one identity.

Sybil attack was first exposed in distributed computing applications where the redundancy in the system was exploited by creating multiple identities and controlling the considerable system resources. In the networking scenario, a number of services like packet forwarding, routing and collaborative security mechanisms could be disrupted by the adversary using sybil attack.

## VI. ENCRYPTION TECHNIQUES IN WIRELESS MESH NETWORKS

The prime motive to use these wireless mesh networks is in physical security systems where they can potentially improve mobile communications, communications with remote locations, temporary communications, and others applications. Since these physical security systems may employ a mobile WMN to transport sensitive or classified information, end-to-end encryption working within a very dynamic WMN is

paradoxical. End-to-end encryption techniques are required when the path through the wireless network changes. Encryption algorithms play a vital role in wireless mesh network security systems. However, these algorithms consume a significant amount of computing resources such as CPU time and packet size.

For implementing encryption algorithm following steps are adhered to -

1. Decomposition of a speech signal in sub-frame, each frame is represented by an index.
2. Encrypting data with inversion and random permutation algorithm, which gives the permutation indexes.
3. Encrypting these indexes with various end to end algorithms. - Used to decrypt the signal.

Many encryption algorithms are widely available and are used in information security. They can be categorized into Symmetric (private) and Asymmetric (public) keys Encryption. In Symmetric keys encryption or secret key encryption, only single key is used to encrypt and decrypt data. DES utilizes one 64-bits key. Triple DES (3DES) requires three 64- bits keys. While AES uses various (128,192,256) bits keys

Various encryption techniques are as follows:

1. .RSA-Stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first described it in 1978. It is an asymmetric cryptographic algorithm, used by modern day computers to encrypt and decrypt messages. RSA involves a public key and private key. The public key can be known to everyone. It is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key. In the case of RSA, the public key operations are quick operations when the exponent is relatively modest (typically 65537), while the private key operations are three orders of magnitude slower. The RSA algorithm can be employed for both public key encryption and digital signatures. Its security is contingent to the difficulty of factoring large integers.

For example: Party A can send an encrypted message to party B without any prior exchange of secret keys. A just uses B's public key to encrypt the message and B decrypts it using the private key, which only he knows. RSA is furthermore used to sign a message, so A can sign a message employing their private key and B can verify it drawing A's public key.

The RSA is pressed into service for different communication networks in order to ensure data confidentiality, higher data security and an enhanced computing process speed. In wireless mesh networks, this algorithm is used in Bluetooth devices which entail an increased security by enlargement of the utilization area. Moreover the user uses maximum acceptable length for encryption key and algorithm complexity, which increases the computing speed and security degree.

2. DES The Data Encryption Standard (DES) is a symmetric-key block cipher published by National Institute of Standards and Technology (NIST). It is a symmetric-key algorithm for the encryption of electronic data. DES is implementation of a Feistel Cipher. It applies 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit. DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not utilized by the encryption algorithm. By using a 64-bit key which gives a 64-bit block of plain text as input and gives an output in the form of a 64-bit block of cipher text. DES operates on blocks of balanced size by employing permutations and substitutions in the algorithm. Since DES has 64-bit rounds, therefore the main algorithm is repeated 16 times to produce the cipher text. However it has been noted that the number of rounds are always exponentially proportional to the time required. Security of the algorithm increases exponentially when the number of rounds increases which means security is maximized automatically when the number of rounds is more. The encryption process consists of two permutations are also called as initial and final permutations and in addition sixteen feistal rounds. Each Round with two elements consists of mixer and swapper. It is also called as invertible. The decryption algorithm should be identical to the encryption algorithm in a reverse order. But in case of DES cipher, the encryption algorithm is so well designed, that the decryption algorithm is identical to the encryption algorithm only with the sub keys applied in the reverse order. Feistel structure makes encryption and decryption processes.

3. AES-The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six times faster than triple DES. The features of AES are as numerated below:

a. Symmetric key symmetric block cipher 128-bit data, 128/192/256-bit keys Stronger and faster than Triple-DES

b. Provide full specification and design details. Software implementable in C and Java

c. AES is an iterative rather than Feistel cipher. It is based on ‘substitution–permutation network’. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

This algorithm provides the secure transmission in wireless mesh networks in order to acquire the specified communication delays at low energy cost by dynamically adapting transmission power and routing decisions. AES algorithm also prevents information and communication systems from illicit delivery and modification, message authentication and identification is examined through certified mechanisms. The messages transmitted from the various nodes over a wireless mesh networks is authenticated by the receiver. The sender uses the encryption algorithm to send a message to the receiver, through unsecured channel, and the receiver uses the decryption algorithm to decipher the received message.

## VII. CLASSIFICATION IN WMNs

1. SUPPORT VECTOR MACHINE (SVM) Support vector machines (SVMs) are a set of supervised learning methods exploited for classification, regression and outliers' detection. It is a sort of statistical learning theory, which is on the basis of the principle of structural risk minimization. Support vector machine is adapted to network intrusion detection in wireless mesh networks.

The advantages of support vector machines are:

(a) Effective in high dimensional spaces.

(b) Effective in cases where number of dimensions is greater than the number of samples.

SVM possess numerous advantages in solving small sample size, nonlinear and high dimensional pattern recognition problem. The principles of SVM and binary tree are introduced in detail and applied in network security in wireless mesh networks.

SVM hold higher Classification precision, better generalization performance and less learning and test time, especially to get a better assessment performance under small samples. It leverages a flexible representation of the class boundaries and implements automatic complexity control to condense over fitting.

Furthermore, it oft-times has superior generalization performance and the same algorithm solves a variety of problems with little tuning, which makes SVM suitable for dynamic environment. It imparts idea to evaluate the similarity of vehicle driving patterns, and then employ SVM classifiers to distinguish the malicious nodes. It is a new intelligent learning method; that will provide solution for sundry future problems, essentially the choice of Kernel function and its parameters, the optimization of training algorithm and multi-classification algorithm.

2. ARTIFICAL NEURAL NETWORK Artificial Intelligence plays a paramount role in wireless communication. It possesses ability to learn things and adapt itself according to input and ascertain output. For an instance if we apply ANN on CRN then we achieve maximum performance and maximum utilization of wireless communication.

In Wireless mesh networks, the eminent character of a routing protocol is to find a way to establish connection between an end user and one of the gateways, as quick as possible, considering links status. This path should be optimized from the traffic distribution and path distance point. Artificial intelligence is used for path optimization. Distribution of local routing information and routing table updates is realized by mobile agents. In this modus operandi, network should have a simple means of routing information delivery and thus for effective user traffic support.

The networking infrastructure of wireless mesh networks (WMNs) is decentralized and relatively simple, but they can display reliable functioning performance while having adept redundancy. With the utilization of artificial neural networks, WMNs provide Internet access for fixed and mobile wireless devices. In urban and rural areas they provide users with high-bandwidth networks over a specific coverage area.

The employment of artificial neural networks (NNs) delivers minimum delay and blocking probability. In that way, it is imperative to prefer the route in accordance with the requirements of future subscribers and their traffic, with minimum possible number of rerouting and the optimal load balance of the entire network.

## VII. CONCLUSION

Security is an exceptionally crucial concern in wireless mesh networks. Distributed Denial-of-Service attack (DDoS) is one of the major attack-occurs when an attacker continually bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection messages, failure messages and/or other commands. This refrain legitimate users to ride on the network and may even cause the network to crash. This attack elevates critical threat to WMNs as it could be established without a hitch by an intruder via spoofed source traffic.

Thus diverse encryption algorithms and artificial intelligence techniques are employed in the wireless mesh networks. These methods aid in enhancing the security of the network by utilizing possible accepted security keys.

Using access to all the keying and authentication information, performance of WMNs is augmented. It is evident that the literal potential of WMN cannot be exploited without considering and adequately addressing the internal as well as the external security circumstances.

## VIII. REFERENCES

[1]. Vinay Kumar[1], Sanjeev Jain[2] and Sudarshan Tiwari (sept 2011) "Energy Efficient Clustering Algorithms in Wireless Sensor Networks: A Survey" international journal of computer science, ISSN: 1694-0814, Vol no: 8, Issue:5, page no.:259-268.

[2]. Divya Chadha, Reena ( March 2015) , "Vehicular Ad hoc Network (VANETs): A Review" International Journal of Innovative Research in Computer and Communication Engineering, Issn: 2320-9801, Vol no: 3, Issue:3, page no.; 2339-2346

[3]. Abdul Nasser A. Moh **,** Borhanuddin Mohd. ( Nov 2015) " Optimum QoS Resource Allocation Algorithm for Video Traffic over Wireless Mesh Networks based on IEEE 802.11s", IEEE 12th Malaysia International Conference on Communications (MICC), Kuching, Malaysia, isbn: 978-1-5090-0020-3, page no: 102-106.

[4]. Jubil Jose, Rigi C.R, ( Feb , 2014) "Wireless mesh networks: issues and challenges", International journal of computer Science and mobile computing, issn: 2320-088X, Vol. 3, issue .2, page no-831-833

[5]. Ms. Ankita Umale, 2, Ms. Priyanka Fulare , ( 2014), "Comparative Study of Symmetric Encryption techniques for Mobile Data Caching in WMN", International Journal Of Engineering And Science, ISSN: 2319 – 1805, Vol:3, issue :3, page no.- 7-12.

[6]. Abdulla, Ahmed EAA, ZubairMdFadlullah, Hiroki Nishiyama, Nei Kato, Fumie Ono, and RyuMiura. (2015) "Toward fair maximization of energy efficiency in multiple uas-aided networks: a game-theoretic methodology." *IEEE Transactions on Wireless Communications* 14, Vol :1, page no.- 305-316

[7]. Yih-Chun, Hu, and Adrian Perrig.(2004) "A survey of secure wireless ad hoc routing." *IEEE Security & Privacy* 2, Vol: 3, page no.-28-39.

[8]. Yih-Chun, Hu, and Adrian Perrig.(2004) "A survey of secure wireless ad hoc routing." *IEEE Security & Privacy* 2, no. 3 :28-39.

[9]. Sgora, Aggeliki, Dimitrios D. Vergados, and P. Chatzimisios.(2013) "A survey on security and privacy issues in wireless mesh networks." *Security and Communication Networks*

[10]. Sbeiti, Mohamad, NiklasGoddemeier, Daniel Behnke, and Christian Wietfeld. "PASER: Secure and Efficient Routing Approach for Airborne Mesh Networks.(2016)" *IEEE Transactions on Wireless Communications* 15, no. 3 : 1950-1964.

[11]. Akilarasu, G., and S. Mercy Shalinie. (2016), "Wormhole-free routing and DoS attack defense in wireless mesh networks." *Wireless Networks* : 1-10

[12]. Moh, Abdul Nasser A., and MohdBorhanuddin.(2015), "Optimum QoS resource allocation algorithm for video traffic over wireless mesh networks based on IEEE 802.11 s." In *Communications (MICC), 2015 IEEE 12th Malaysia International Conference on*, pp. 102-106. IEEE.

[13]. Wang, Jin, Kejie Lu, Jianping Wang, Junda Zhu, and ChunmingQiao.(2016), "ULNC: An Untraceable Linear Network Coding Mechanism for Mobile Devices in Wireless Mesh Networks." *IEEE Transactions on Vehicular Technology* 65, no. 9: 7621-7633.