Survey on Attacks Pertaining to Wireless Mesh Networks and Approach towards Counter Measures

Sandeep Dalal
Assistant Professor,
Computer Science and Application
DCSA, Maharshi Dayanand
University, Rohtak

Seema Arya
M.Tech Scholar,
Computer Science and Application
DCSA, Maharshi Dayanand
University, Rohtak

ABSTRACT
Wireless Mesh Networks (WMN) is an integralbroadband wireless network who provides high bandwidth internet service to users. It is a kind of multi-hop network having many to many connections with the capability of dynamic sanify network topology WMN's utility network performance can cause a massive fall. Channel your physical security vulnerabilities, due to the dynamic changes of topology is a major challenging issue. Self –Configuration is a wireless mesh network self-organized nature make it vulnerable to various type of more attacks .In this paper we have discussed Some attacks that TCP / IP model are performed at different layers of security challenges, analyzing the counter remedies and protection mechanisms in place various attacks listed.

Some attacks that TCP / IP model, are performed at different layers of security challenges, analyzing the counter remedies and protection mechanisms in place various attacks listed.

Keywords
Wireless Mesh Networks, Wormhole attack, Grey Hole attack, Security, Attack, Challenges

1. INTRODUCTION
Wireless Mesh Networking is an emerge technology. A wireless Mesh Network originatesmesh nodes which form the backbone of the network[1].Nodes automatically configure network connectivity and dynamically reconfigure the network "self- build" and "self-healing" features are to maintain returns.Akyldiz [3] stated that WMNs are expand to retutation limitations and to improve the performance of Ad-hoc networks. Centralized management [2] need to be self-sufficient because of the relationship between the mesh nodes are removed .Various applications [4] of wireless mesh network as:

- Broadband home network
- Communityand vicinity networking
- Diligence Network
- Building Automation
- Transportation System
- Health and Medical System
- Security and Surveillance system
- Emergency disaster network
- Peer to peer communication

Security has become the main concern to provide secure communication. Various advantages of wireless mesh network such as:

- Simple Installation and Low Cost
- Nodes Self-connectivity
- Network flexibility
- Discovery of the newly added nodes

2. CHARACTERISTICSOF WMNs
Wireless Mesh Networks isdynamic, self-organization, self-configuration and self-healing characterized by flexible integration, rapid deployment, enabling easier maintenance,

Low costs, high scalability and reliable services. Network deployment and maintenance is greatly reduced complexity and the ability to organize their own [3].

Wireless Mesh networks consist of:

- Mesh Clients (MC): Minimal mobility
- Mesh Routers (MR): Static or Mobile in nature

WMNs are used to integrate different types of network like Internet, Cellular, Wi-Fi networks, Wi-Max, Sensor networks etc. Mainly three kind of wireless mesh networks can be defined:

a) Infrastructure WMNs mesh routers offer network services to the client users. The network has self-healing characteristics.

b) WMNs clients are ad-hoc networks formed by another client. None of dedicated routers or infrastructure exists so that the self-configuring client and client WMN routers act as traffic to be. WMNs have two other advantages of hybrid WMNs.

The development of this technology is to deal with the challenging security, architecture and protocol designed issues. It is still quite inadequate for deploying sizable wireless mesh networks has become important aspect

- Network Radio Range
- Network Capability
- Scalability
- Manageability and Security problem remains still open

Security is one of the tricky components that needs due attention. Various mechanisms used for providing security in WMNs are:

- Securing Routing
- MAC (Message Authentication Protocol)

- Intrusion Detection System
- Trust Management
- Key-Management.

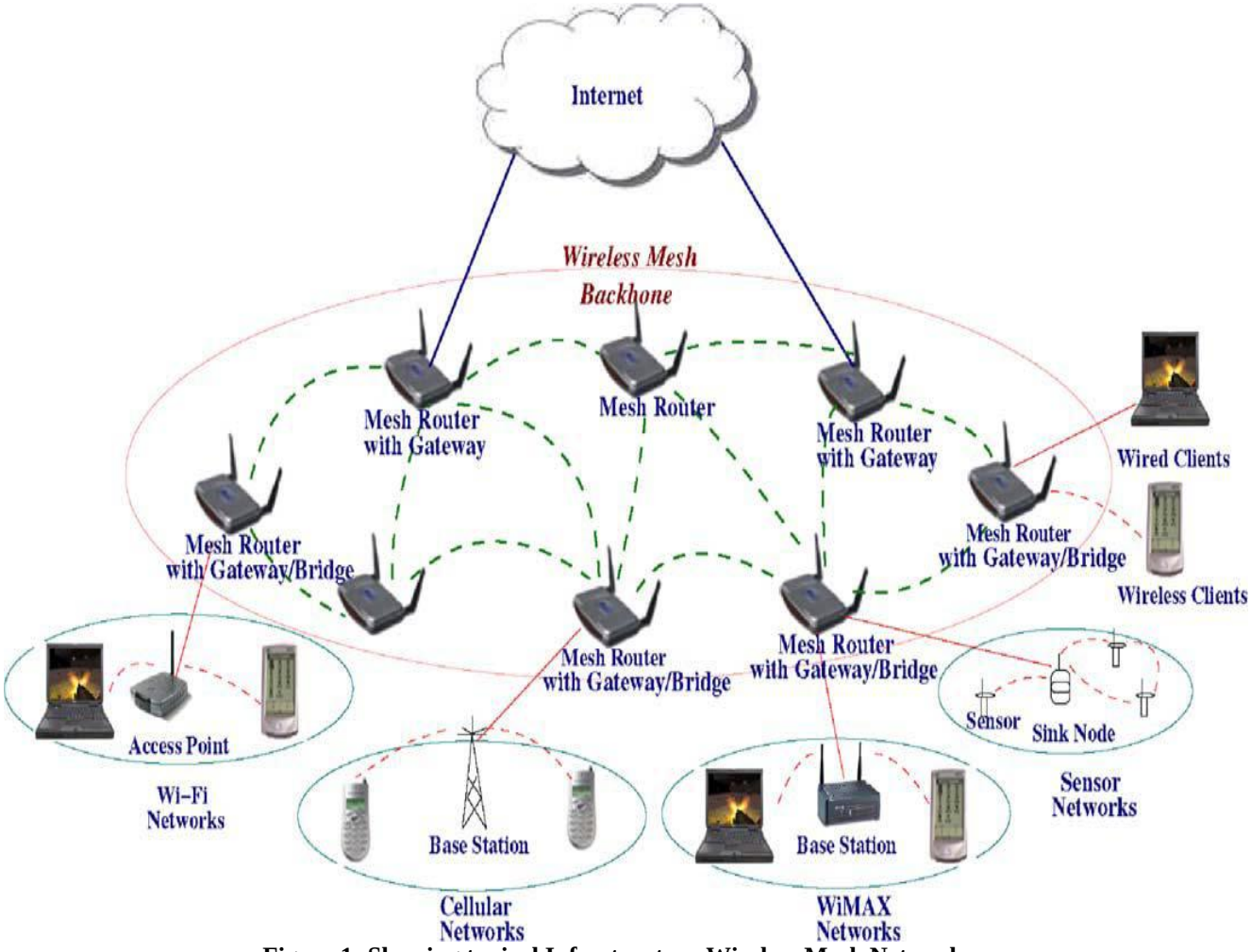

Figure 1: Showing typical Infrastructure Wireless Mesh Network

3. SECURITY REQUIREMENTS

A wireless mesh network security requirement can be classified as:

a. Data Validation: To ensure the data is originated from the exact source.

b. Data Privacy: Toensure that only authorized nodes can get the content of the messages.

c. Data Integrity: Toensure that any received message has not been modified or alterationby unauthorized parties to send.

d. Availability: Toensure that services offered by WSN or by a single node should be available while necessary.

e. Non Repudiation: To ensure a node which sends a packet to a destination node cannot disprove that the packets sent and received packets to the destination cannot deny.

4. SECURITY CHALLENGES IN WMNS

WMNs completely for some reasons it is difficult to be protected. These security challenges are as below:

a) Multihop Nature: Multihop [11] to delay in detection and treatment is intended for attacks. Moreover since the majority of the one-hop out protection schemes are proposed for the network, one of them being attacked are not sufficient to protect the WMN.

b) Multisystem security:[11] WMNs include various wireless technologies, such as IEEE 802.15, IEEE 802.16, IEEE 802.11 etc. A safety network is needed but it's not easy to provide in the networks.

c) Multitier Security system: [11] Security is needs to be protected not only the client nodes but also the mesh routers and as well as the mesh clients and mesh routers.

d) We expected [10] the node is being compromise due to lack of physical security. Therefore the system outside the network from malicious attacks launched from inside the network is vulnerable to attacks.

e) WMN has memory and computational constraints [10], the security are not applied to conventional schemes.

f) Shared wireless links: [12] since a single radio channel is usedby mesh clients to send and receive

data packets eavesdropping or the replay attacks like MAC layer are possibleto be back.

g) Dearth of association: [12] Due to the ad hoc nature of WMNchange the trust relationship among nodes.

h) Physical Risk: [12] The lack of physical security node is likely to settle.

i) Resource Avail: [12] Security are not suitable for traditional plans WMNs because of lake of computational constraints and memory.

5. SECURITY ATTACKS

Security services to avoid an attack and attempt to breach system security policies. Security attacks can be classified by their nature, scope, behavior and the targeted layer by the attacker as shown in Figure 2. [5]

Passive attacks (without any data modification) attacks and unrest imposed on network resources based on active (modification of data) attacks are classified. Eavesdropping and traffic inspection are passive attacks whereas masquerade modification of messages replay and abandonment are active attacks. The attack can be classified as external or internal based on the person starting the attack. External attacks are launched from the intruders who are not legitimate users and their objective is to degrade the network performance are starting from. Denial of Service (DoS) is such kind of attack. Internal attack is introduced by malicious or selfish nodes. Depending on the behaviorof rational attackers (some advantages in rule of quality or price) or malicious attackers can be classified as:

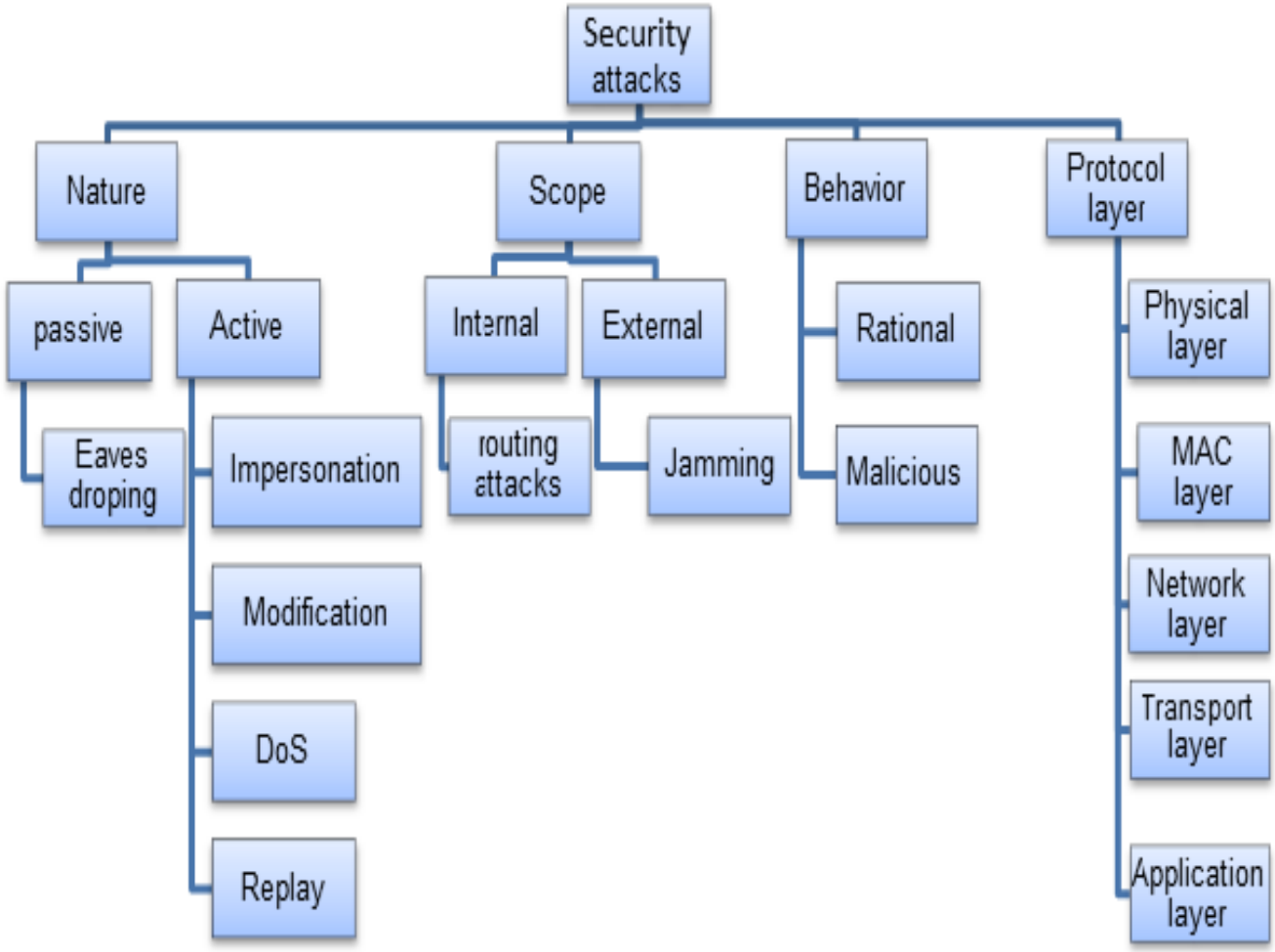

Figure 2: Various types of Attacks

6. ATTACKS ON PROTOCOL LAYER

The attacks might appear in Physical layer, MAC layer, Network layer, Transport layer and Application layers of the protocol stack.

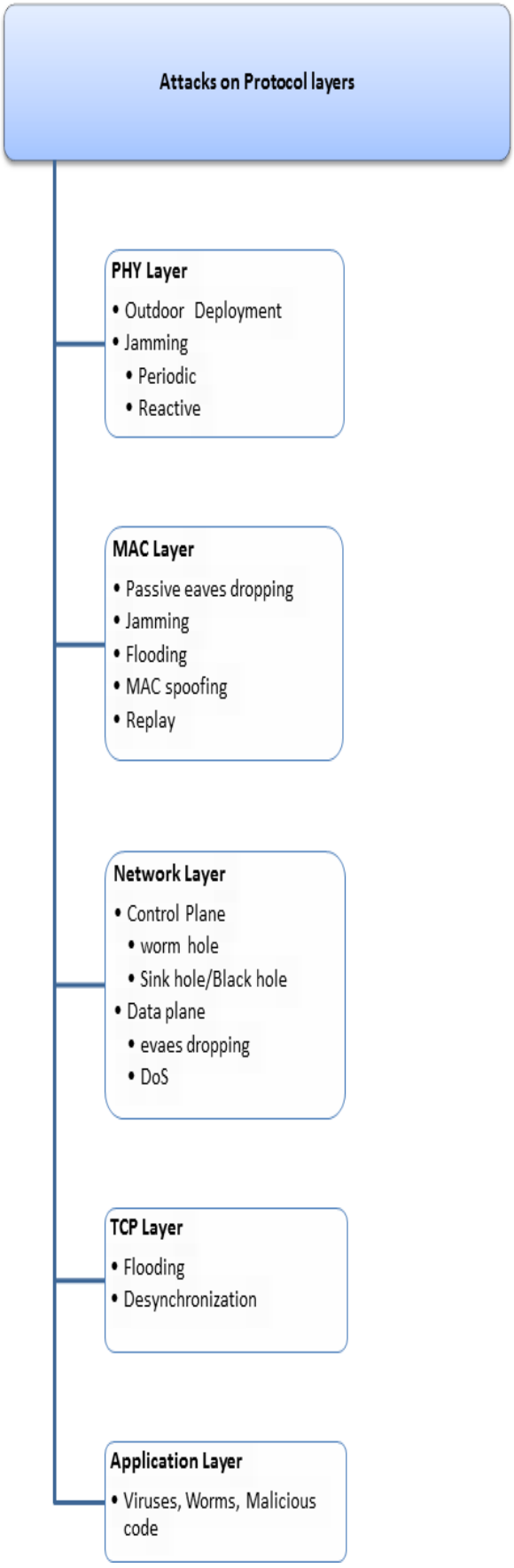

Figure 3: Attacks on Different Protocol Layers

6.1 Security Attacks at the Physical Layer of WMNs

There WMNs first physical layer consists of different types of attacks. An attacker could destroy external hardware just the routers are installed in the outdoor area. Such vulnerable routers arean attacker can easily extract the information. The pinpoint jamming, jamming at time, reactive jammingattacks can be applied inphysical layer [13]. In pinpoint jamming attack attacker transmits the constant noise. In periodic jamming attack (or scrambling attack) an attacker sends a small periodic signal. Inlast reactive jamming attack whenever a node detects that an attacker has started a transmission signal transmit an attacker.

6.2 Security Attacks in the MAC Layer of WMNs

Many types of attacks are possible in the MAC layer and consist of the following:

a. Passive Eavesdropping: WMNs nature of broadcasting the transmission it falls within the transmission range of the attacker passive communication nodes is possible to launch the eavesdropping. It can be launchedin internal nodes and external nodes. Internal eavesdropping by malicious intermediate nodes keeps copy the data and forward to any nodes in the network without further knowledge [14].

b. Flooding Attack: An attacker sends many messages to its neighboring nodes to control several MAC. Due tothefairness of the medium is physically abused [15].

c. MAC Spoofing: If an attacker tries to change the MAC address of the frame is broadcast.

d. Jamming Attack: Jamming attacks are also possible inMAC layer.

6.3 Security attacks in the Network layer of WMNs.

Many attacks on the network layerare also possible. These attacks are further classified in two groups:

Control Plane: Control Plane or (routing) to focus on the routing functionality of the network. Control Plane attacks aredistinguished as below:

1. Rushing Attacks:On-demand routing protocols an attacker sends multiple routing packets beyond the network in a short intervalof time to keep nodes busy.
2. Routing Table Overflow:the new routes are being created by an attacker enough to escape routes with the intention of making fictitious nodes attempts to build new roads.
3. Wormhole Attack:In this attackmalicious attacker to convince two nodes use the path or colludes with more malicious node is during the installation of a tunnel. A wormhole attack using an successful communication medium.Once the victim nodes enter the malicious nodes in the way of routing nodes the malicious node begins droppingpackets.

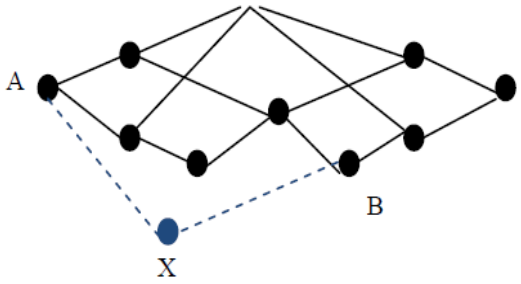

Fig. 4 Wormhole Attack

4. Sinkhole (or Blackhole) Attack:In this attack a malicious packet forwarding nodes begins to explain to its neighboring nodes. That packet to advance the most optimum node. A vicinage node began to forward packets malicious node packets are forwarded by the neighboring nodes goes.

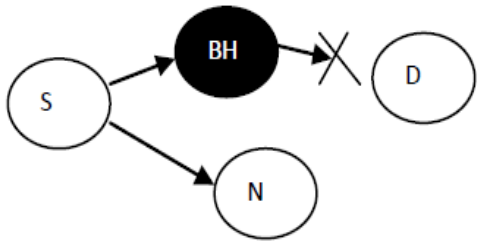

Fig. 5 Black hole Attack

5. Grey Hole Attack: Grey Hole attack is a variation of sinkhole attack [16]. During this attack they will not drop the entire packet just selective packet drop [13].
6. Location Disclosure Attack:During this attack structure or network node reveal information about the location [17].

Data Control Attack: Data control (or path forwarding) network attacks target path forwarding functionalities. Thesetypes of attacks are initiated by the nodes in the network abuse. Bansal et. al.[18] divided into two groupsselfish nodes and malicious nodes. A greedy node tries to disturb the operation of a selfish node network; even in the operating costs of the other nodes is concerned about his performance. Eavesdropping is a simple way to control theattack.

6.4 Security Attacks in the Transport Layer of WMNs

An attacker might target the transport layer. Flood attacks are possible in the transport layer and desynchronization. In flooding attacks malicious node to reach a maximum limit to the resource requirements can request a new connection. In desynchronization attack a malicious node may repeatedly fake themessages to request the retransmission of the frame so that the host can fail.

6.5 Security Attacks in the Application Layer of WMN

Application layer attacks viruses as well as concern in wireless networks, malicious code, denial of the application, worms etc.

7. PHYSICAL SECURITY THREATS[10]

- Conventional wireless network deploymentswere within physical and administrative control of the director or agency of an enterprise environment.Outdoor wireless mesh networks mesh access points need to be out of the operator's physical control. Physical device security poses more challenges for outdoor deployment. Wirelessmesh access points, lighting positions are moving awayor external buildings, an environment where the deployment of a wide area network that is not under the control the operator of the physical and administrators, such devices could be several thousand.
- Wirednetwork access points thatrequired network connectivity.Wired network access points sometimes media backhaul which can expose sensitive wirednetwork connections is required.
- Battery fatigue attack 'sleep deprivation attack' is known as a realthreat and simple denial ofservice attacks more dangerous. Attack on CPU count maydeny the availability of the denial of service while batteryexhaustion can cripple the victim.

Security of user privacy is a very notable issue in wireless network communication. However it is difficult toensuring privacy of the users.

To realizethe message are protected within the network as there are not many security solutions or machine which guarantee that knowledge authorized parties themselves [19].

Table1.WMN of a communication protocol stack and their potential security vulnerabilities in different layers of the system presents a summary of the different types.

Table 1: Various Types of Vulnerabilities and their Defense Mechanisms

LAYER	ATTACKS	DEFENCE MECHANISMS
Physical	Jamming	Spread-spectrum, prior messaging, lower duty cycle, fieldmapping, change mode
MAC	Collision	Error-correction code
	Exhaustion	Rate limitation
	Unfairness	Small frame
Network	Forged routing information & selective forwarding	Egress filtering, confirmation, monitoring

	Sinkhole	Surfiet check
	Sybil	Confirmation, surveillance, surfiet
	Wormhole	Authentication, probing
	Hello Flood	Confirmation, Geographic and temporalinformation by using packet leashes
	Ack. Flooding	Confirmation, bi-directional linkconfirmation, verification
Transport	SYN, Flooding, Desynchronization	Client puzzles, SSL-TLS confirmation, EAP
Application	Logic errors, Buffer overflow	Application confirmation, affiance computing, Antivirus.
Privacy	Traffic analysis, Data privacy and locationprivacy attack	Holomorphic encryption , onion routing , traffic plans based on entropy calculations , the Group signed Anonymity based plans , using pseudonyms

8. POSSIBLE COUNTER MEASURES[10]

DoS in any form against any network are regarded asa serious attack. Broadband wireless network the results of different DoS attacks vary with the natureand type of DoS attack. If start against a singlenode either to exhaust its battery to separate it fromthe network operation. Selfish mesh router attack inWMN and wicked BS attacks are used to make servicesunavailable to a target area in wireless broadbandnetworks.

A. DoS attacks and possible Counter Measures[10]

Needs to beinvestigated to overcome it to some extent are these:

- Cognitive radios implementation at physicallayer needs to be investigating to handle the jammingand scrambling kind of attacks, all of which are commonin the broadband networks.
- The current encryption mechanisms used in broadband networks WEP, DES, and AES, whichare vulnerable to attacks like eavesdropping.Improved and efficient encryption mechanisms needto be proposed exclusively for each broadbandtechnology as the successful eavesdropping facility attackers to launch DoS attacks.
- Intrusion detection mechanism todetect and respond especially for the network layerapprehend particularly for WMN environment.
- Location detection mechanism is basis on signal strength and AP test request spate of the attacks and de-authentication type with the ability to identify malicious node mesh wireless router needs to be ready, the same system IEEE 802.16 networks can be used to identify fake registration request floods.
- Improve routing protocols specifically for multi-hop WMNs are desired.

B. Cryptography & Digital Signatures[10]

Nodes can produce digital signatures and checkthem then solution is straight forward. The use of public key cryptography a node can verify the signature of the other nodes, the two nodes will establish a common secret key signs technology access, and protected by the secret key messages will be able to accept. But many of the nodes in a WMN havecomputation and lack of battery verification actionthat includes public key cryptography may not beimplemented. However Elliptic Curve Cryptography(ECC) [20] provides some energy and computationefficient techniques in implement cryptographicalgorithm which may be deserve for mobile customers.

C. Pair-Wise Key Sharing [10]

In WMNs symmetric cryptography is possible because of the asymmetric cryptographic technique require less computation.A better solution Diffie-Hellman (D-H) key exchange to be used [21].Diffie-Hellman(D-H) key interchange is a cryptographicprotocol that allowing two parties that have no priorknowledge of each other both parties commonly establish an unsecured communications channel that allows shared key. The key is a symmetric key cipher to encrypt communications using the later can be used.

D. Secure Routing[10]

To achieve availability both dynamically changing topology and routing protocol must be robust against malicious attacks. There are two sources ofthreats to routing protocols. First comefromexternal attackers and the secondmoreserious types of threats also come from compromisednodes; incorrect routing information may be advertised to other nodes. To prevent suchattacks we can utilize certain properties of WMNs toachieve safe routing. Like Multipath routing [22]takes advantage of multiple routes in an efficient mannerwithout message retransmission. The original idea for error detection and correction through additional routes to transmit information is unnecessary. Even ifsome route compromised the receiver maystill be able to validate messages.

9. CONCLUSION

WMNs are able to provide seamless connectivity to the nature of self-healing system. WMNs successful implementation of secure conventional and enhanced security protocols required. Thwarting all security to prevent attacks on the network layer and above all security measures to maintain security is

impossible. So far, the proposed security measures introduced in the various layers are not the solution for a variety of attacks. Network layer security attacks can be caused by events in the lower layers is caused. This is necessary to secure a cross-layer approach WMNs. The major security requirements threats and security risks are analyzed WMNs and finally some security mechanism are discussed.

10. REFERENCES

[1] Ho Ting Cheng, Hai Jiang and Weihua Zhuang , "Distributed medium access control for wireless mesh networks" , Wirel. Commun. Mob. Comput. 2006;:845–864 Published online in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/wcm.445.

[2] Shin-Ming Cheng, Phone Lin, Di-Wei Huang and Shun-Ren Yang, "A Study on Distributed/Centralized Scheduling for Wireless Mesh Networks", IWCMC'06, July 3–6, pp 599-604, 2006, Vancouver, British Columbia, Canada.

[3] F. Akylidz, X. Wang and W. Wang, "Wireless Mesh Networks: A Survey" Comput. Net, vol. 47 no. 4, 445-487, 2005.

[4] Xiang Xu, Xianjie Wu, Zhi Yu. 2010. Application of Wireless Mesh Network in Campus Network. Second International Conference on Communication systems Networks and applications. pp.245-247.

[5] Thillaikarasi, Mary Saira Bhanu, A Survey of Secure Routing Protocols for Wireless Mesh Networks; International Journal of Computer Applications (0975 – 8887) Volume 97– No.6, July 2014

[6] Monika Department of computer science, "Denial of Service Attacks in Wireless Mesh Networks", International Journal of Computer Science and Information Technologies, Vol. 3 (3), 2012, pp 4516-4522

[7] Sachin Dev Kanawat, Pankaj Singh Parihar, "Attacks in Wireless Networks", International Journal of Smart Sensors and Adhoc Networks, Volume-1, Issue-1, 2011

[8] V.S.Shankar Sriram, Ashish Pratap Singh, G.Sahoo, "Methodology for Securing Wireless LANs Against Wormhole Attack", International Journal of Recent Trends in Engineering, Issue. 1, Vol. 1, May 2009

[9] Yongguang Zhang and Wenke Lee, "Security in Mobile Ad-Hoc Networks," In Book Ad Hoc Networks Technologies and Protocols, Springer, 2005.

[10] Dr. M.S.Aswal1, Paramjeet Rawat2, Tarun Kumar, Threats and Vulnerabilities in Wireless Mesh Networks, International Journal of Recent Trends in Engineering, Vol 2, No. 4, November 2009

[11] Ratika Sachdeva, Aashima Singla, Survey on Privacy Issues and Security Attacks in WirelessMesh Networks, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013 ISSN: 2277 128X

[12] Anil Kumar Gankotiya1, Gurdit Sing, SahilSeth2. Attacks and their Counter Measures in Wireless Mesh Networks. Available: htttp://www.csjournals.com/IJITKM/Special.

[13] S. Seth, and A. Gankotiya, "Denial of Service Attacks and Detection Methods in Wireless Mesh Networks", In the Proceedings of the 2010 International Conference on Recent Trends in Information, Telecommunication and Computing (ITC 2010), Koshi, Kerala, 2010 , pp. 238 – 240.

[14] A. Naveed, S. S. Kanhere, and S. K. Jha, "Attacks and Security Mechanisms Security in Wireless Mesh Networks", Ed (Y. Zhang), Auerbach Publications, ISBN: 978-0-8493-8250-5, 2009.

[15] H. Moustafa, U. Javaid. T. M. Rasheed, S. M. Senouci and D. Meddour, "A Panorama on Wireless Mesh Networks: Architectures, Applications and Technical Challenges", In the Proceedings of the First International Workshop on Wireless mesh: moving towards applications (WIMESHNETs „06) , Waterloo, Canada, 2006.

[16] Y. Zhang, J. Luo and H. Hu, " Wireless Mesh Networking: Architectures, Protocols and Standards", Auerbach Publications, ISBN: 978-0- 8493-7399-2, 2006.

[17] B. Wu, J. Chen, and J.Wu, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks Wireless Network Security", Y. Xiao, X. S. Shen, D.-Z. Du (Ed.), Springer, ISBN: 978-0-387-33112-6978-0-387-33112-6, 2007.

[18] D. Bansal, S. Sofat, and A. K. Gankotiya, "Selfish MAC Misbehaviour Detection in Wireless Mesh Networks", In the Proceedings of 2010 International Conference on Advances in Computer Engineering (ACE 2010), Bangalore, Karnataka, India, 2010, pp. 130-133.

[19] H. Moustafa, "Providing authentication, trust, and privacy in wireless mesh networks", book chapter in: Security in Wireless Mesh Networks. Y.Zhang et al. (eds.), pp. 261-295, CRC Press, USA, 2007.

[20] M. Aydos, T. Tanýk, Ç. K. Koç, "High-SpeedImplementation of an ECC-based WirelessAuthentication Protocol on an ARM Microprocessor", IEE Pro.: Comms, Oct., 2001, pp 273-279.

[21] W. Diffie, M. Hellman, "New Directions in Cryptography", IEEE Trans., on IT, Nov, 1976, pp.644-654.

[22] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Efficient Security Mechanisms for Routing Protocols. In Proceedings of the 2003 Symposium on Network and Distributed Systems Security (NDSS '03), February 2003.