Volume 3, Issue 4, April 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Survey on Privacy Issues and Security Attacks in Wireless Mesh Networks

Ratika Sachdeva *
Student Masters of Technology
Department of CSE
Sri Guru Granth Sahib World University
Fatehgarh Sahib, Punjab, India

Aashima Singla
Student Masters of Technology
Department of CSE
Sri Guru Granth Sahib World University
Fatehgarh sahib, Punjab, India

Abstract-Wireless Mesh Networks (WMNs) is considered as a promising solution for offering self-healing, self-configuring capabilities, low-cost access in broadband services. Wireless mesh networks continue to receive significant interest in an existing new technology that has application in defence, metro-area Internet access, and transient networks (e.g.: disaster recovery, conventions). In this review paper, we review security issues, challenges, and attacks at physical layer, medium access control, and network layers wireless mesh backbone and access control in Wireless Mesh Network. In the wireless mesh network, there are number of an issue which affects the performance and efficiency.

Keywords- Wireless mesh network, security, attack, challenges, routing and medium access control.

I. Introduction

In recent years, **wireless mesh networks (WMNs)** received much attention and continue to research. Further new applications and services include broadband and wireless home internet access, health and medical systems, public safety and security surveillance systems and networking disaster and so on. [1]. WMNs consists of two-tier architecture, in the first architecture is made of wireless mesh routers (WMRs) which are basically PowerPC and Advance Risc Machines (ARM) and these mesh routers forming a self-organized backbone. Mesh routers are robust in terms of computation and continuous power supply and have communication capability. In second layer, it consists of wireless mesh clients (WMCs), which are basically end-user terminals. WMRs act as a APs (access point), APs needs to be connected with a fixed internet infrastructure to offer connectivity. APs provide the connectivity to any authorized WMC. Security is always a important step to manage WMNs. It is implementing with some encryption algorithms for tunneling such as IPSec to provide the safe virtual path along the shared networks. But still WMNs lack efficient and scalable security solutions because their security is easy to compromise due to nodes in the shared wireless medium, absence of proper infrastructure and dynamic change of topology. The key management is one of the most important tasks for networks security. The key mechanism becomes difficult for WMNs, because there is no trusted third party, no central authority. A self-organized was propose to distribute and mange the security keys. In this, certificates are stored and distribute among themselves. This observation leads to the challenges architecture: a self-organized spontaneous WMN architecture (as shown in Fig. 1).

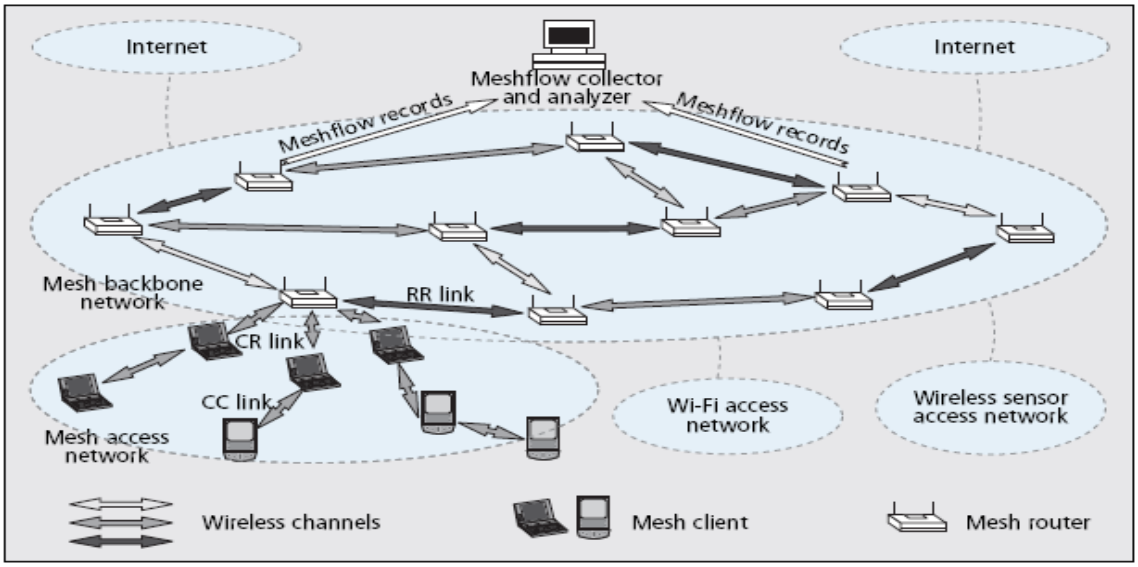

Fig. 1 Infrastructure of Wireless Mesh Network [18]

II .SECURITY ISSUES AND CHALLENGES IN Wmns

A. Security Issues in WMNs

The key issues are as below:

1) *Availability:* Group of nodes in the mesh network infrastructure is suggested in our proposal, where mesh network functionalities are assigned to specific nodes, thus it helps to enhance the network availability.
2) *Heterogeneity:* This approach takes the advantage of heterogeneous resources of each node, exploiting the nodes capacity to execute network functionalities.
3) *Self-organization:* We offer WMNs architecture with a mechanism that is dynamically self-organized and coherent integration of nodes.
4) *Authenticity of network traffic:* In the lack of authenticity, malicious user can masquerade a node, and gain the unauthorized access to resources and sensitive information and interfere with the data transferring of other nodes.
5) *Authorization:* It is a process in which different access rights are assigning to different levels of users by the trusted certificate authority.
6) *Integrity:* In this process it ensures that the data cannot alter without being detected and can be compromised either by chance or caused by misbehaving users.
7) *Access Control:* It guarantees that only authorized user can perform authorized actions.
8) *Confidentiality:* It guarantees that the information is only available to those who have been authorized to access it.
9) *Accountability:* Accountability aims are to detect the malicious users, sometimes it is necessary to deny network access to them via revoking, so that malicious users can be ejected.

B. Security Challenges in WMNs

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

1) *Multihop Nature:* Multihop aims to delays the detection and treatment of the attacks. Also, since the majority of the exited security schemes are proposed for one-hop networks, render them not enough to protect a WMN from being attacked.
2) *Multisystem security:* WMNs involves various wireless technologies, such as IEEE 802.15, IEEE 802.16, IEEE 802.11 etc. A security mechanism is needed but it is not easy to provide in all networks.
3) *Multitier System Security:* Security is needed not only between the client nodes, but also between the mesh routers and as well as among the mesh clients and mesh routers.

III. Public Safety And Disaster Recovery Communications

The purpose of the network communication infrastructure in disaster situation is to maintain the typical hierarchical command and control structure. We have four different types of communication networks for the public safety and disaster recovery applications (as shown in fig.2):

A. Personal Area Networks (PANs)

Personal Area Networks is used for communication among various devices for example fire fighters supervise their statistical, oxygen tank status or geological locations.

B. Incident Area Networks (IANs)

An incident area network is a temporary network. It is created for the duration of a particular incident. An IAN is required when fixed infrastructure networks are not available at the particular incident scene, because they are destroyed. The first responders share the crucial data and coordinated their efforts.

C. Jurisdiction Area Networks (JANs)

Jurisdiction area networks are permanent networks. They are mostly installed by the municipalities or public safety agencies for providing the wide area communication for the purpose of crisis and failure situations. JAN is used for communications network for first responders for all data. It is also used for voice traffic that the Incident area network doesn't handle. The first responders clients are connect to the JAN by an IAN. Clients can also communicate directly by one or more JANs. (as fig 2. illustrates its working).

D. Extended Area Networks (EANs)

Extended area network offers the wide area connectivity. It provides the connectivity among local, state and countrywide public safety networks.

IV. SECURITY ATTACKS IN Wmns

Security attacks depend on the various factors. It depends on the nature, the behaviour or the protocols that are used on the different layers. Furthermore, the attacks can be classify, based on method of the attacker to use to accomplish their motive, is on impersonation, fabrication, modification, Denial of Service (DoS) and other attacks. Glass et. al. in outline the attacks at the different layers of WMN protocol stack is defined (in Table I).

A. Security Attacks at the Physical Layer of WMNs

There are different types of attacks at the first physical layer of WMNs. An attacker may destroy the external hardware, simply routers are installed at the external area. Such routers are sensitive, an

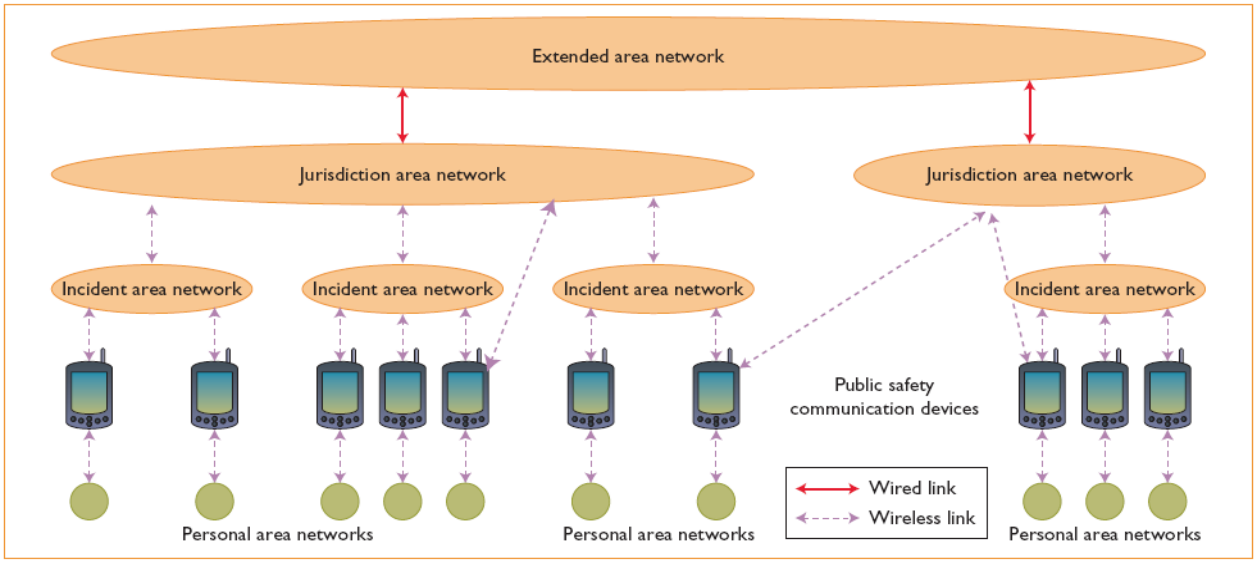

Fig. 2. General architecture of public safety communication networks [1]

attacker can easily extract the information from them. The trivial jamming, periodic jamming, reactive jamming attacks are may be applied in the physical layer [9]. In trivial jamming attack, attacker transmits the noise continuously. In periodic jamming attack (or scrambling attack), an attacker sends a short signal periodically. In last reactive jamming attack, whenever an attacker detects that a node has begin a transmission, an attacker transmits a signal.

B. Security Attacks at the MAC Layer of WMNs

Different attacks are possible at MAC layer of the WMNs and these consist of:

1) Passive Eavesdropping: The Nature of the WMNs is broadcasting the transmission, it is possible for attacker to launch the passive eaves dropping within the transmission range of the communication nodes. It can be launched in internal as well as external nodes. In internal eavesdropping by the malicious intermediate nodes keep the copy of data and forward to any nodes in the network without knowledge [6].

2) Flooding Attack: An attacker sends many MAC control messages to its neighbour nodes. Due to this, the fairness of the medium is physically abused [10].

3) MAC Spoofing: An attacker tries to change the MAC address during transmission of frames.

4) Jamming Attack: Jamming attacks are also possible at MAC layer. Seth and Gankotiya [9] consider some jamming attacks, and these are unprompted clear to send (CTS) attack, reactive request to send (RTS) jamming attack and CTS corrupt jamming. In CTS corrupt jamming, on the basis of receipt RTS, an attacker transmits noise during the CTS response. In RTS jamming attack, whenever attacker detects the RTS message, it disrupts the RTS message by immediately beginning of a transmission.

C. Security Attacks at the Network Layer of WMNs

Several attacks are also possible at the network layer. These attacks are further divided into two groups:

1) Control Plane

Control Plane or (routing) focus on the routing functionality of the network. The Control Plane attacks are distinguished as below:

- *Rushing Attacks:*
  In on-demand routing protocols, an attacker sends a many routing packets across the network in a short interval of time for keeping nodes busy.
- *Routing Table Overflow:*
  An attacker attempts to build routes to imaginary nodes with intention to create sufficient routes to avoid new routes from being created.
- *Wormhole Attack:*
  In this attack, attacker convince the nodes to use the malicious path and if two or more malicious nodes collude together during this by establishing a tunnel. A wormhole attack using an efficient communication medium. Once, the victim node enters the malicious nodes in the routing path, the malicious nodes starts dropping packets.
- *Sinkhole (or Blackhole) Attack:*
  In this attack, a malicious node starts convincing to its neighbour nodes for forwarding packets. That is the "most optimal" node for forwarding the packets. When a neighbour node begins to forward the packet, then malicious node drops the packets which are forwarded by the neighbouring nodes.
- *Greyhole Attack:*
  A greyhole attack is a variation of sinkhole attack [5]. During this attack, they will not drop all the packets but they just drop the selective packets [9].

- *Location Disclosure Attack:*
  During this attack, it reveals the structure or information about the location of nodes in the network [14].

2) Data Control Attacks

Data control plane (or path forwarding) attacks target path forwarding functionalities of the network. These types of attacks are launched by misbehaving nodes in the network. Bansal et. al.[15] divided into two groups: selfish nodes and malicious nodes. A selfish node is concerned about its performance even at the operating cost of other nodes, while a greedy node tries to disturb the operation network. The simple way is to control the attack is eavesdropping.

D. Security Attacks at the Transport Layer of WMNs

An attacker could target the transport layer. The possible attacks at the transport layer are flooding and desynchronization. In the flooding attack, a malicious node may make new connection requests for resources requirements reach a maximum limit. In desynchronization attack, a malicious node may repeatedly spoof the messages, so that host to request the retransmission of missed frames.

E. Security Attacks at the Application Layer of WMNs

This layer attacks are only concern with the virus, malicious codes, application abuses, worms etc. in the wireless networks.

Table I WIRELESS SECURITY RISKS [23]

Protocols Layer	**Threats**
Application Layer	Logic errors, privilege escalation, buffer overflows
Transport Layer	Session hijacking, DNS spoofing, traffic injection
Network Layer	Rushing attacks, misrouting, Grey/worm/black holes
Data-link Layer	Virtual jamming, man-in-the-middle, traffic flooding
Physical Layer	Device tampering, collision jamming

V. Conclusion

In this paper, we have discussed the main security issues and challenges in Wireless Mesh Networks. We concluded that security attacks at different layers, while most attacks are much harder to counter because the challenger is aware of the network secrets and protocols. These adversaries are detected by behavioral metrics such as per-packet status. However, these metrics cannot detect attacks of selective nature, where high-value packets are targeted. An attacker drops only few packets, due to congestion or poor wireless congestion. However, current security approaches may be effective to a particular layer, but still lack of mechanism to prevent from attack in different protocol layers. These limitations in WMNs can be overcome, and WMNs play an important role in Public Safety and Disaster Recovery Communications.

References

[1] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless Mesh Networks: A Survey," Computer Networks *J. (Elsevier)*, vol. 47, Mar. 2005, pp. 445C–487.

[2] R. Malik, M. Mittal, I. Batra, and C. Kiran, "Wireless Mesh Networks (WMN)", International Journal of Computer Applications, vol. 1, no. 23, 2011, pp 68-76.

[3] K. Ren, S. Yu, W. Lou, and Y. Zhang, "PEACE: A Novel Privacy-Enhanced Yet Accountable Security Framework for Metropolitan Wireless Mesh Networks", IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 2, 2010, pp. 203-215.

[4] A. O. Durahim, E. Savaş, "A-MAKE: An Efficient, Anonymous and Accountable Authentication Framework for WMNs", In the Proceedings of the 5th International Conference on Internet Monitoring and Protection (ICIMP), Barcelona, Spain, 2010, pp. 54-59.

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

[6] 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.

[7] I. Akyildiz and X. Wang, "Wireless Mesh Networks (Advanced Texts in Communications and Networking", John Wiley & Sons Ltd. ISBN: 978-0-040-03256-5,2009.

[8] M. O. Pervaiz, M. Cardei and J. Wu, "Routing Security in Ad Hoc Networks", Network Security, Editors S. C.-H. Huang, D. MacCallum, D.- Z. Du, Springer, ISBN: 978-0-387-73820-8, 2010.

[9] 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.

[10] 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.

[11] L. Lazos and M. Krunz, "Selective Jamming/Dropping Insider Attacks in Wireless Mesh Networks", IEEE Network,vol. 25, no.1, 2011, pp. 30-34.

[12] D. Divyaand S. Kumar, "Security Challenges in Multihop Wireless Mesh Networks–A Survey", Information Security and Digital Forensics, D. Weerasinghe (Ed) , Springer Berlin Heidelberg, ISBN: 978-3-642-11530-1,2010.

[13] H. Redwan and K. Ki-Hyung, "Survey of Security Requirements, Attacks and Network Integration in Wireless Mesh Networks", In the Proceedings of the 2008 New Technologies, Mobility and Security Conference (NTMS 2008), Tangier, Morocco, 2008, pp. 1-5.

[14] 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.

[15] 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.

[16] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks", IEEE Communications Surveys & Tutorials, vol. 8, no. 2, 2006, pp. 2-23.

[17] H Yang, H Luo, F Ye, S Lu, and L Zhang, "Security in mobile ad hoc networks: challenges and solutions", IEEE Wireless Communications, vol. 11, no. 1, February 2004, pp. 38 – 47.

[18] Feiyi Huang, Yang Yang, Liwen He, "A Flow-Based Network Monitoring Framework for Wireless Mesh Networks", IEEE Wireless Communication, October 2007.

[19] Aggeliki Sgora, Dimitrios D. Vergados, P.Chatzimisios, "A Survey on Security and Privacy Issues in Wireless Mesh Networks", 2012.

[20] Loukas Lazos, Marwan Krunz, "Selective Jamming/Dropping Insider Attacks in Wireless Mesh Networks", IEEE Network, January February 2011.

[21] Lucio Studer Ferreira, MD De Amorim, L Iannone, L Berlemann Luis M. Correia, "Opportunistic Management of Spontaneous and Heterogeneous Wireless Mesh Networks", IEEE Wireless Communications, April 2010.

[22] Marjus Portmann, Asad Amir Pirzada, "Wireless Mesh Networks for Public Safety and Crisis Management Applications", IEEE Computer Society, 1089-7801/2008 IEEE.

[23] S. Glass, M. Portmann, and V. Muthukkumarasamy, "Securing Wireless Mesh Networking", IEEE Internet Computing, vol. 12, no. 4, 2008, pp. 30-36.

[24] S. M. Glass, V. Muthukkumurasamy and M. Portmann, "Detecting Man-in-the-Middle and Wormhole Attacks in Wireless Mesh Networks," In the Proccedings of the International Conference on Advanced Information Networking and Applications (AINA '09), Bradford, UK, 2009.

[25] F. Martignon, S. Paris, A. Capone, "DSA-Mesh: a Distributed Security Architecture for Wireless Mesh Networks, Wiley Security and Communication Networks, vol. 4, no. 3, 2011, pp. 242-256.

