A Brief Review on Security and Privacy Issues in Wireless Mesh Networks

Priyanka Patel
Dept. of Computer Science Engineering
Acropolis Institute of Technology & Research,
Indore, M.P., India

Abhay Kothari, PhD
Dept. of Computer Science Engineering
Acropolis Institute of Technology & Research,
Indore, M.P.,India

ABSTRACT
In recent years wireless mesh networking has emerged as a promising technology to tackle the challenges of the next era of broadband services. It has offered the economical services in the field of medicine, defense, natural disasters and availability of Internet access in the remote areas etc. In this review paper, the fundamental security challenges and privacy concerns are analyzed. This paper also provides a brief detail about existing security architectures and technologies based on wireless mesh network.

General Terms
Wireless Mesh Network, Security, Attacks et. al.

Keywords
Wireless Mesh Network (WMN), Security Challenges, Privacy, Architectures and Broadband Services etc.

1. INTRODUCTION
In recent years, wireless mesh networks (WMNs) received much interest of eminent researchers. Its heterogeneous applications and services are widely used for health and medical systems, broadband services and for security based monitoring systems etc. [1] several architectures of WMNs have been proposed based on their features and applications [1], the widely accepted one is a three tier framework as represented in Fig. 1. At the lower level of this architecture there are the mesh clients (MCs) which or well known as the mobile users with inadequate mobility and resource. At the middle tier, a set of mesh routers (MRs) for interconnection of wireless back bone is used. MRs are used for connectivity to the existing MCs. At the top tier of this architecture there are a group of Internet gateways (IGWs) existed. A mesh network provides the multi-hop communication path between the MCs and MRs. However such multi-hop nature generates the lack of security, the dynamic topology and connectivity with the end users this will not only increase the routing overheads but also generate the vulnerability [2,3].

The popularity of Wireless Mesh Network has become widespread due to its last mile connectivity. Its design is secure and efficient for home networking, remote networking and community services. But due to its dependency on the intermediate nodes, its communication leads to several security concerns and vulnerabilities. By this dodges, the attacker can cause its performance and interrupt the network services like the dropout of packets. Therefore, it has become a serious issue to defend against the privacy attacks. In previous years, various protocols and architectures have been proposed for such vulnerable attacks. But most of them were specifically designed for MANETS Mobile Adhoc Networks (MANETs) and consequently such mechanisms do not satisfy the preliminary requirements of wireless mesh network. By looking at this, the prime objective of the paper is to highlight the security and privacy concerns by considering the security threats and vulnerabilities.

The paper is categorized as follows: Section II a brief review on security challenges. Section III discusses the existing attacks at different layers. Various protocols are reviewed in section IV. Finally, Section V gives the concluding remarks of the paper.

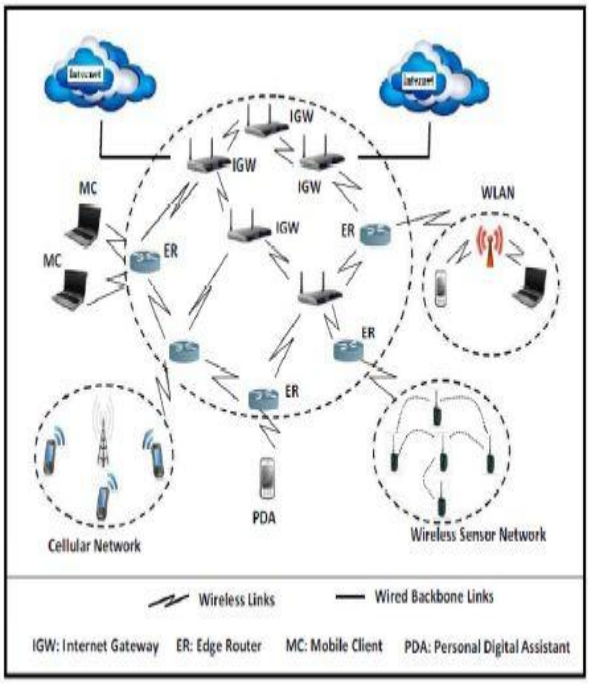

Fig 1: Three-tier Architecture of Wireless Mesh Network

2. FUNDAMENTAL SECURITY AND PRIVACY ISSUES IN WIRELESS MESH NETWORK
All The fundamental security issues are as follows [4, 5, 6, 7, 8, 9]:

i. Network traffic Authentication: While transferring the data from one node to another there may be interferences and the sensitive information can be leaked and acquired by the malicious users.
ii. Resource Heterogeneity: To improve the network performance, the heterogeneous resources can play a vital role but it is complex to make them adhered.

iii. Dynamicity & Self-organization: The WMNs architecture should be dynamic and self-organized while integrating the nodes.
iv. User Authorization: Assignment of access rights at various levels of users is a critical task.
v. Confidentiality: It is mandatory to share the information with the authorized users only.
vi. Accountability: It is the fundamental requirement while detecting the malicious users.
vii. Network Availability: To enhance the network availability, the mesh network functionalities should be assigned to specific nodes.
viii. Integrity: In this mechanism the content of data cannot be shared or altered by misbehaving users.
ix. Access Control: It ensures to give access to the authorized users only.
x. Non-repudiation: To ensure that the neither the sender nor the receiver deny that they have ever sent or received the message.

3. SECURITY ATTACKS IN WIRELESS MESH NETWORK

Security attacks depend on capability and behavior of the protocols deployed in various layers. Such attacks are classified based on the various methodologies of the attacks. In Table I various threats are represented at their corresponding layers [10].

Table I. Security Attacks in Wireless Mesh Network

Layer	Security Attacks
Physical	Signal Jamming
Data link	Man in the Middle Attack, Flooding, Logical Jamming, Unfairness
Network	Spoofed routing, Wormhole, Flooding
Transport	Session Hijacking, Spoofing, De-synchronization
Application	Buffer overflows, Privilege intensification, Privacy and location breaching

Table II. Study of Security Protocols in Wireless Mesh Network

S.No.	Layer	Name of Protocol	Features
1	Data Link	SDES [11]	i) stream cipher-based cryptosystem ii) It is robust against key compromise
2	Data Link	MobiSEC [12]	i) It is an efficient scheme to provide secure authentication and control in WMNs ii) It doesn't work better with the issues like message confidentiality, message integrity & replay attacks
3	Data Link	R-hash [13]	i) This scheme uses a hash function-based mechanism to prevent the misbehaviour at MAC layer
4	Network	ARIADNE [14]	i) On-demand routing protocol ii) Uses clock synchronization and secret key between the pair of nodes.
5	Network	SRP [15]	i) On-demand routing protocol ii) Deploy security association between source & destination node.
6	Network	SAODV [16]	i) On-demand routing protocol ii) It uses an online key management scheme.
7	Network	SEAD [17]	i) Table-driven routing approach is used in this scheme.
8	Network	ARAN [18]	i) On-demand routing protocol ii)It uses the policy of online certification authorization.
9	Network	SMT [19]	i) On-demand routing protocol ii) It used public key cryptography technique.
10	Transport	ARSA [20]	i) It used the feature of multiple trust domains managed by an individual broker
11	Transport	AKES [21]	i) It uses distributed authenticated key establishment scheme.
12	Transport	SLAB [22]	i) It uses localized authentication approach while providing tolerable security protections against the heterogeneous vulnerabilities
13	Application	PEACE [23]	i) three-tiers is used with the gateways while establishing the connection to the Internet at the uppermost level.
14	Application	SAT [24,25]	i) A hierarchical identity-based cryptographic structure is used to achieve the trade-offs between security and privacy

4. STUDY OF PROTOCOLS IN WIRELESS MESH NETWORK COMMUNICATION

This section elaborates various security mechanisms to preserve against the attacks. Such techniques are used at different layers such as physical, data link, network, transport & application layer. A review on protocol with their salient features is described in Table II.

5. CONCLUSIONS

In this paper, the fundamental key security issues and challenges of Wireless Mesh Networks are discussed. Various security attacks at different layers are analyzed. Most of the attacks are much harder to offset the existing network secrets and protocols are completely in the knowledge of attackers. To prevent from such attacked various security schemes and protocols are identified and elaborated with their features and functionality. However, the existing security approaches are very much effective to a particular layer only. Therefore, still there is a lack of mechanisms to prevent from attacks in various layers of the protocol. By overcome such limitations, WMNs can play a vital role in the area of Safety and Disaster Recovery Communication during the natural hazards.

6. 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] A. A. Franklin and C. S. R. Murthy, "An introduction to wireless mesh networks", book chapter in: Security in Wireless Mesh Networks, Y. Zhang et al. (eds.), CRC Press, USA, pp. 3 – 44. 2007.

[3] 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.

[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] 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.

[9] D. Bansal, S. Sofat, P. Pathak, S. Bhoot, "Detecting MAC Misbehavior Switching Attacks in Wireless Mesh Networks", International Journal of Computer Applications, vol. 26, no.5, July 2011, pp. 55-62.

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

[11] H. S. Soliman and M. Omari, "Application of synchronous dynamic encryption system in mobile wireless domains", in Proceedings of the 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks (Q2SWinet'05), Montreal, Quebec, Canada, pp. 24-30, 2005, ACM Press.

[12] F. Martignon, S. Paris, and A. Capone, "MobiSEC: a novel security architecture for wireless mesh networks", in Proceedings of the 4th ACM Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet'08), pp. 35-42, Vancouver, Canada, 2008.

[13] J. Konorski and M. Kurant, "Application of a hash function to discourage MAC-layer misbehaviour in wireless LANS", in Journal of Telecommunications and Information Technology, vol 2, pp. 38-46, 2004.

[14] Y.-C. Hu, A, Perrig, and D. Johnson, "Ariadne: a secure on-demand routing protocol for ad hoc networks", in Proceedings of ACM Annual International Conference on Mobile Computing (MobiCom'02), pp. 21 – 38, Atlanta, GA, USA, September 2002.

[15] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks", in Proceedings of the SCS Communication Networks and Distributed Systems Modelling and Simulation Conference (CNDS'02), San Antonio, TX, USA, pp. 27-31, January 2002.

[16] M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols", in Proceedings of the 1st ACM Workshop on Wireless Security (WiSe'02), Atlanta, GA, USA, pp. 1-10, September 2002. ACM Press.

[17] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks", in Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02), Callicoon, NY, USA, pp. 3 – 13, June 2002.

[18] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, and E.M. Belding-Royer, "A secure routing protocol for ad hoc networks", in Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP'02), Paris, France, pp. 78 – 87, November 2002.

[19] P. Papadimitratos and Z.J. Haas, "Secure data transmission in mobile ad hoc networks", in Proceedings of the 2nd ACM Workshop on Wireless Security (WiSe'03), San Diego, CA, USA, pp. 41-50, September 2003.

[20] Y. Zhang and Y. Fang, "ARSA: an attack-resilient security architecture for multihop wireless mesh networks", IEEE Journal of Selected Areas in Communication, vol 24, no 10, pp. 1916–1928, 2006.

[21] B. He, S. Joshi, D. P. Agrawal, and D. Sun, "An efficient authenticated key establishment scheme for wireless mesh networks", in Proceedings of IEEE Global Telecommunications Conference (GLOBECOM'10), pp. 1-5, Miami, Florida, USA, 2010.

[22] H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "SLAB: A secure localized authentication and billing scheme for

wireless mesh networks", IEEE Transactions on Wireless Communications, vol 7, no 10, pp. 3858–3868, October 2008.

[23] K. Ren, S. Yu, W. Lou, and Y. Zhang, "PEACE: a novel privacy-enhanced yet accountable security framework for metropolitan wireless mesh networks", in IEEE Transactions on Parallel and Distributed Systems, vol 21, no 2, pp. 203–215, February 2010.

[24] J. Sun, C. Zhang, Y. Fang, "A security architecture achieving anonymity and traceability in wireless mesh networks", in Proceedings of the 27th IEEE International Conference on Computer Communications (IEEE INFOCOM'08), pp. 1687–1695, April 2008.

[25] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "SAT: A security architecture achieving anonymity and traceability in wireless mesh networks", IEEE Transactions on Dependable and Secure Computing, vol 8, no 2, pp. 295–307, March 2011.