IJDACR
ISSN: 2319-4863

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary Research
Website: www.ijdacr.com (Volume 4, Issue 4, November 2015)

A Review of Security Issues in Wireless Mesh Network

Deepshikha Yadav
Dept. of Computer Science & Engineering
Acropolis Technical Campus, Indore
Deepshikha.cs16@gmail.com

***Abstract*— Wireless mesh network (WMN) is a new wireless networking paradigm. Wireless mesh networks are a promising technology for offering ubiquitous Internet connectivity. Unlike traditional wireless networks, WMNs do not rely on any fixed infrastructure. One main challenge in design of these networks is their weakness to security attacks. In this paper, we investigate the major security issues for WMNs. We identify the new challenges and opportunities posed by this new networking environment and explore approaches to secure its communication.**

***Keywords* —Wireless Mesh Network, authentication, Security attacks.**

I. INTRODUCTION

A. Wireless Mess Network

A wireless mesh network (WMN) is a communications network made up of radio nodes organized in a mesh topology. Wireless mesh networks often consist of mesh clients, mesh routers and gateways. The mesh clients are often laptops, cell phones and other wireless devices while the mesh routers forward traffic to and from the gateways which may, but need not, connect to the Internet. The coverage area of the radio nodes working as a single network is sometimes called a mesh cloud. Access to this mesh cloud is dependent on the radio nodes working in harmony with each other to create a radio network. A mesh network is reliable and offers redundancy. When one node can no longer operate, the rest of the nodes can still communicate with each other, directly or through one or more intermediate nodes. The animation below illustrates how wireless mesh networks can self-form and self-heal. Wireless mesh networks can be implemented with various wireless technology including 802.11, 802.15, 802.16, cellular technologies or combinations of more than one type. A wireless mesh network can be seen as a special type of wireless ad-hoc network. A wireless mesh network often has a more planned configuration, and may be deployed to provide dynamic and cost effective connectivity over a certain geographic area. An ad-hoc network, on the other hand, is formed ad hoc when wireless devices come within communication range of each other. The mesh routers may be mobile, and be moved according to specific demands arising in the network. Often the mesh routers are not limited in terms of resources compared to other nodes in the network and thus can be exploited to perform more resource intensive functions. In this way, the wireless mesh network differs from an ad-hoc network, since these nodes are often constrained by resources.

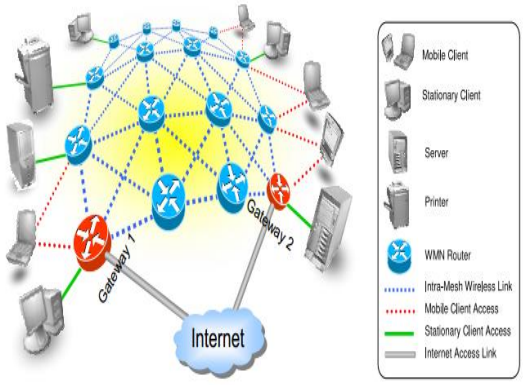

Figure 1.1: A wireless mesh network connecting several stationary and mobile clients to the Internet

B. Security Requirements of Wireless Mesh Network

Security Requirements to ensure the security of WMNs, the following major security objectives of any application have paramount importance.

- Confidentiality - It means that certain information is only accessible to those who are authorized to access it.
- Integrity - Integrity guarantees that a message being transferred is never corrupted. Integrity can be compromised mainly in the following

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary Research
Website: www.ijdacr.com (Volume 4, Issue 4, November 2015)

two ways: Malicious altering – A message could be removed, replayed or revised by an adversary by a malicious attacker. Accidental altering - Such as a transmission error, goals on the network which is regarded as malicious altering.

- Availability - Availability ensures the survivability of network services despite of denial of service (DoS) attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes make some of the network services unavailable.
- Authenticity - Authenticity is essentially, assurance that participants in communication are genuine and not impersonators.
- Non-repudiation - Non-repudiation ensures that the sender and the receiver of a message cannot deny that they have ever sent or received such a message. It is useful for detection and isolation of a node with some abnormal behavior.
- Authorization - Authorization is a process in which an entity is issued a credential by the trusted certificate authority. It is generally used to assign different access rights to different level of users.
- Anonymity -Anonymity means that all the information that can be used to identify the owner or the current user, should be kept private and not distributed to other communicating parties.

II. Threats and Vulnerabilities of Wireless Mesh Network

In this section, the main threats that violate the security criteria, which are generally known as security attacks, are analyzed.

1. Routing Protocol Threats

Wireless mesh networks may be susceptible to routing protocol threats and route disruption attacks. Many of these threats require packet injection with a specialized knowledge of the routing protocol; however, these threats are unique to wireless mesh networks and are summarized below:

- Black-hole. An attacker creates forged packets to impersonate a valid mesh node and subsequently drop packets, where attacking packets involve advertising routes as low-cost.
- Grey-hole. An attacker creates forged packets to attack and selectively drops, routes or inspects network traffic.
- Worm-hole. Routing control messages are replayed from one network location to another, which can severely disrupt routing.
- Route error injection. An attacker disrupts routing by injecting forged route error message to break mesh links. Relative to the other routing attacks, this attack conceivably has high exploitability because it does not require detailed knowledge of the routing protocol state model. The risk associated with these threats depends on the routing technology or mesh network architecture.

2. Spoofing Of Wireless Infrastructure

Attacker used an “evil twin” or “man-in-the-middle” attack to execute an information disclosure threat. In an enterprise deployment, such attacks were mitigated using EAP methods that allow mutual authentication between a client and the infrastructure

- Denial-of-service attack- A DoS attack could be launched at any layer of the network. For instance, on the physical and media access control layers, an adversary could employ jamming signal to interfere with communication on physical channels. On the network layer, an adversary could interrupt the routing protocol and disconnect the network. On the higher layers, an adversary could bring down high-level services. One such target of an adversary is the key management service, which is an essential service for any security framework.
- Something-of-Death Attack- While protocols serve a specific purpose, there is always the danger that bad implementations open yet another door for DoS attacks where a malicious attacker sends forged and mal-formed frames with the intention of crashing the AP under attack.
- Theft-of-Service Attack-An attacker could steal valid user credentials or performs paid-user session hijacking (e.g., “freeloading”). Many Wi-Fi systems use a service gateway or captive portal to secure paid access – a captive portal uses SSL-secured Web page. After authentication, the captive portal authorizes the client to network access by registering the valid client MAC and IP addresses in the gateway. Alternatively, malicious users could relay traffic across the mesh network without traversing a network gateway (e.g., peer-to-peer traffic across the mesh backhaul). These attacks do not represent any new threats for

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary Research
Website: www.ijdacr.com (Volume 4, Issue 4, November 2015)

mesh networks relative to existing Wi-Fi hotspot services.

- Node Deprivation Attack-In node deprivation attack, the attackers target a single node and isolate it from taking part in the normal network operations. In WMN and IEEE 802.11, the nodes first authenticate itself with the mesh router or AP, and needs to de-authenticate [1] it if the node has no more desire to use the network resources. The attacker could spoof the de-authentication message on behalf of the target node to stop it from using the network resources.
- Authorization Flooding on Backbone Devices-WMN and IEEE 802.11 nodes use Probe request frames to discover a wireless network, if a wireless network exist then the AP respond with Probe response frame. The clients select that AP which provides the strongest signal to it. Here the attacker could spoof a flood of probe request frames presenting a lot of nodes searching for wireless network, which could seriously overload the AP or wireless mesh router. If the load exceeds, the threshold value will cause the AP or wireless mesh router to stop responding and may create service unavailability.

3. Physical Security Threats

Conventional wireless network deployments were within an enterprise environment with physical and administrator control of the operator or agency. Outdoor wireless mesh networks require that the mesh access points be outside the physical control of the operator. Outdoor deployment poses more challenges for physical device security. Wireless mesh access points are mounted remotely on light posts or externally on buildings, where a wide-area deployment may have several thousand such devices in an environment that is not within the physical and administrator control of the network operator. Wired mesh access points require network connectivity. Wired network access points sometimes require wired media backhaul, which may expose sensitive network connections.

- Battery Exhaustion-Battery exhaustion attack also known as ‘sleep deprivation attack’ is a real threat and is more hazardous than simple denial of service attacks. Attack on CPU computation may deny the availability of the service while battery exhaustion can disable the victim.

III. RECOMMENDATIONS

Offering recommendations can often provide a false sense of security, as threats are difficult to anticipate and may often exploit previously unknown vulnerabilities. Securing wireless networks must always be treated carefully, mainly due to the inherent trust disparity in a wireless network.

1. Dos Attacks and Possible Countermeasures

DoS in any form against any network, is regarded as a severe attack. The results of different DoS attacks on broadband wireless networks vary with the nature and type of DoS attack. If launched against a single node either to exhaust its battery or to isolate it from the network operations. Selfish mesh router attack in WMN and rogue BS attack is used to make services unavailable for a target area in wireless broadband networks. Some possible countermeasure needs to be investigated to overcome it to some extent are:

- Cognitive radios implementation at physical layer needs to be investigated to handle the jamming and scrambling kind of attacks, which are common in all the broadband networks.
- Current encryption mechanisms used in these broadband networks are WEP, DES, and AES, which are vulnerable to eavesdropping kind of attack. Improved and efficient encryption mechanisms needs to be proposed exclusively for each of the broadband technology, as successful eavesdropping later on facilitate the attackers to launch DoS attacks.
- Intrusion detection mechanism can be used to detect and respond to most of the network layer threats particularly for WMN environment.
- A location detection mechanism based on the signal strength needs to be devised for the AP and wireless mesh router with the ability to identify a malicious node for flooding probe request and de-authentication kinds of attacks, same mechanism can be used for the IEEE 802.16 network to identify fake registration request flooding.
- Improved routing protocols are desirable particularly for the multi-hop WMN.

2. Cryptography & Digital Signatures

If the nodes can produce digital signatures and check them; then the solution is straight forward. While one node can verify the other nodes signature using public key cryptography, both nodes will establish a common secret key, using imprinting

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary Research
Website: www.ijdacr.com (Volume 4, Issue 4, November 2015)

techniques, and will be able to accept messages protected by secret key. But many of the nodes in a WMN have computation and battery constraints due to which the verification process, which includes public key cryptography, may not be implemented. However, Elliptic Curve Cryptography (ECC) provides some energy and computation efficient techniques in implementing cryptographic algorithm, which can be suitable for mobile clients.

3. Pair-Wise Key Sharing

In WMNs, symmetric cryptography is possible as it requires less computation than asymmetric cryptographic techniques. Or a better solution would be using the Diffie-Hellman (D-H) key exchange. Diffie-Hellman (D-H) key exchange is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish shared keys over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

4. Secure Routing to achieve availability

Routing protocols should be robust against both dynamically changing topology and malicious attacks. There are two sources of threats to routing protocols. The first comes from external attackers. The second and also the more severe kind of threats come from compromised nodes, which might advertise incorrect routing information to other nodes. To protect from such attacks we can exploit certain properties of WMNs to achieve secure routing. Like, Multipath routing takes advantage of multiple routes in an efficient way without message retransmission. The basic idea is to transmit redundant information through additional routes for error detection and correction. Even if certain routes are compromised, the receiver may still be able to validate messages.

IV. CONCLUSION

In summary, the major security requirements, threats and vulnerability to WMN security are analyzed and to conclude few defense mechanisms are discussed. This paper can be used to give a baseline for building a tight security for WMNs.

REFERENCES

[1] Miguel Elias M. Campista, Pedro Miguel Esposito, Igor M. Moraes, Luis Henrique M.K. Costa, Otto Carlos M. B. Duarte, “Routing Metrics and Protocols for Wireless Mesh Networks”, Network, IEEE, 22(1):6-12, 2008.

[2] Maltz, David B. Johnson and David A., “Dynamic Source Routing in AdHoc Wireless Networks”, In Imielinski and Korth, editors, Mobile Computing, volume 353. Kluwer Academic Publishers, 1996.

[3] Royer, E.M. Perkins, C.E.,“An Implementation Study of AODV Routing Protocol”, In Wireless Communications and Networking Conference, 2000. WCNC, pages 1003 – 1008 vol.3 IEEE 2000.

[4] Yaling Yang, Jun Wang,“Design Guidelines for Routing Metrics in Multihop Wireless Networks”, In IEEE INFOCOM - The 27th Conference on Computer Communications, pages 1615-1623. IEEE. 2008.

[5] Manolis Genetzakis, Vasilios A. Siris,“Contention-Aware Routing Metric for Multi-Rate Multi-Radio Mesh Networks”, In 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, pages 242-250. IEEE. 2008.

[6] Hongkun Li, Yu Cheng, Chi Zhou, Weihua Zhuang,“Minimizing End-to-End Delay: ANovel Routing Metric for Multi-Radio Wireless Mesh Networks”, InIEEE INFOCOM the 28th Conference on Computer Communications, pages46-54. IEEE. 2009.

[7] Jonathan Guerin, Marius Portmann and Asad Pirzada,“Routing Metrics formulti radioWireless Mesh Networks”, In Telecommunication Networks andApplications Conference,pages 343 - 348. 2007.

[8] Bellman Ford Algorithm. Wikipedia.org. [Online] 2010.en.wikipedia.org/wiki/Bellman-Ford_algorithm.

[9] T. M. Mitchell, Machine Learning: McGraw-Hill, 1997.

[10] Z. Ghahramani, "Unsupervised Learning," ed: University College London, September 2004.

[11] R. S. Sutton and A. G. Barto, Reinforcement learning: An Introduction: The MIT Press, 1998.

[12] L. P. Kaelbling, et al., "Reinforcement Learning: A Survey," Journal of artificial intelligence Research, vol. 4, pp. 237-285, May. 1996.

[13] R. Poor, “Wireless mesh networks”, Sensors, February 2003.

[14] R. Poor, “Wireless mesh links everyday devices”, Electronic Engineering Times, 5 July 2004.

[15] I.F.Akyildiz, I.H.Kasimoglu, “Wireless sensor and actor networks: research challenges”, Ad Hoc Networks 2, pp.351-367, 2004.

[16] I.F.Akyildiz, O.B.Akan, “ARC for real-time traffic: ARC: the analytical rate control scheme for real-time traffic in wireless networks”, IEE/ACM Transactions on Networking 12 (4), pp.634-644, 2004.

[17] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, “Wireless sensor networks: a survey”, Computer Networks 38 (4) (2002) 393–422.

[18] C. Perkins, E. Belding-Royer, S. Das, “Ad hoc on-demand distance vector (AODV) routing”, IETF RFC 3561, July 2003.

[19] Ritu Malik, Meenakshi Mittal, Isha Batra and Chander Kiran, “Article: Wireless Mesh Networks (WMN)”, International Journal of Computer Applications 1(23):66–74, February 2010.

[20] Longjam Velentina Devi, Sheeba Parveen and Prof. Rizwan Beg, “Standard Activities of Wireless Mesh Networks”, International Journal of Computer Applications 12(10), pp.12-16, January 2011.

[21] Jaydip Sen , “Secure Routing in Wireless Mesh Networks, Wireless Mesh Networks, Nobuo Funabiki

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary Research
Website: www.ijdacr.com (Volume 4, Issue 4, November 2015)

(Ed.), InTech. Available from: http://www.intechopen.com/articles/show/title/secure-routing-in-wireless-mesh-networks, 2011.

[22] John Paul M. Torregoza,Won-Joo Hwang, "Multi-channel Multi- Tranciever Routing Protocol for Wireless Mesh Network", in: IEEE Communications magazine, pp. 484–487, 2007.

[23] J. Jun, M.L. Sichitiu, "The nominal capacity of wireless mesh networks", IEEE Wireless Communications 10 (5)pp. 8–14,2003.

[24] S. Tierney, Mesh Networks, whitepaper of communitynetworking.org.

[25] R. Draves, J. Padhye, B. Zill, "Routing in multi-radio,multi-hop wireless mesh networks", in: ACM Annual International Conference on Mobile Computing and Networking (MOBICOM), pp. 114–128, 2004.

[26] Mesh Networking Forum, "Building the business case for implementation of wireless mesh networks", Mesh Networking Forum 2004, San Francisco, CA, October 2004.

[27] Mesh Networks Inc. Scalable routing technology. Available from: <http://www.meshnetworks.com/pages/technology/msr_atp_overview.htm>.

[28] Mesh Networks Inc; www.meshnetworks.com.

[29] Microsoft Mesh Networks. Available from: <http://research.microsoft.com/mesh/>.

[30] Theodore S. Rappaport, "Wireless Communications, Principles and Practice", 2nd edition, pp.643, 2003.

[31] T.-S. Jou, D.E. Eastlake, ESS MESH Network Study Group Meeting Minutes, May 2004.

[32] J. Beutel J. "Metrics for Sensor Network Platforms", in Proc. ACM Workshop on Real-World Wireless Sensor Networks (REALWSN'06), June2006.

[33] A. Forster and A. L. Murphy, "Balancing Energy Expenditure in WSNs through Reinforcement Learning: A Study," in Proc. of the 1st Int. Workshopon Energy in Wireless Sensor Networks (WEWSN), 2008.

[34] Anna Forstery, Amy L. Murphyz, Jochen Schiller and Kirsten Terfloth, "An Efficient Implementation of Reinforcement Learning Based Routing on Real WSN Hardware", IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2008.