NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696
VOLUME 3, ISSUE 12, Dec.-2016

WIRELESS MESS & AD HOC NETWORK STUDY AND CHALLENGES

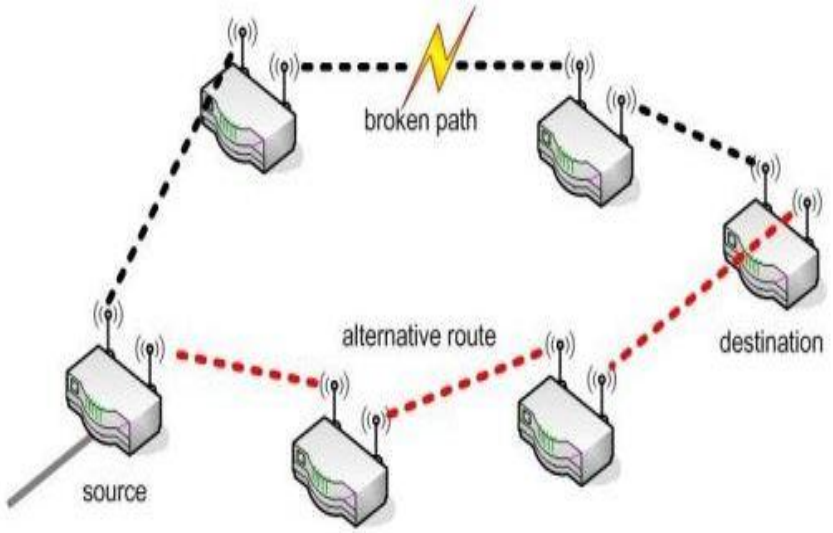
ANKUSH SHARMA
Lecturer in Computer Application Department,
Aryabhatta International College of Technical Education, Ajmer
Email-ankushsharma_31@yahoo.com

ABSTRACT
In the recent time, there will be an increasing need to provide application platforms such as internet deployment for areas without infrastructure, wireless video streaming between moving objects, data exchange between office equipment etc. These applications can be solved with the help of wireless ad hoc networks that can be realized e.g., with Wi-Fi protocols. The question arises, what theoretical throughput different wireless standards can achieve, and how much the throughput will decrease when data has to be transferred over several hops. This is a technology that enables un tethered wireless networking environments where there is no wired or cellular infrastructure. Wireless Ad hoc Networks since then is a fast developing research area with a vast spectrum of applications. Wireless sensor network systems enable the reliable monitoring of a variety of environments for both civil and military applications
This paper provides an overview of wireless technologies which can be used in ad hoc scenarios, their limitations and applications involved in this mechanism.

KEYWORDS: wireless, network, multihop, mess, attacks, security.

INTRODUCTION
Today wireless networks are used daily by millions of people. We use this technology for wireless Internet access with our laptop, for data transfer between phones, and even to play multiplayer games with portable game consoles. However, hardly any of these wireless networks operate in ad hoc mode. These kinds of networks have many advantages over wired networks: ad hoc networks do not require infrastructure, they can be deployed instantly and they are highly flexible.
A wireless ad hoc network is a collection of independent nodes or stations which communicate with each other by creating a multihop radio network. A network where nodes are all connected to each other can be called mesh network. Every node of a wireless ad hoc network is a user terminal and a router at the same time. The management of the network is distributed between all nodes. Therefore, it is extremely necessary to have efficient routing algorithms which make it possible to exchange data over paths consisting of multiple nodes, in other words hopping over multiple nodes. This approach is called multihop transmission. An important feature of mesh networks is the ability of self-healing. The network can still function when a node fails or a path gets congested. In that case, nodes can discover different routing paths and the data can be transmitted along an alternative path. Redundancy makes a mesh network very reliable. The decentralized structure makes ad hoc networks suitable for applications where a centralized structure could be unreliable. Another advantage is the better scalability of ad hoc networks in contrast to centralized wired networks. Ad hoc networks can be easily extended with further nodes at any point in the network. Adding more nodes to the network enables to choose more alternative paths. This also increases the capacity of the network. Wireless ad hoc networks abandon the usage of cables to wire neighboring nodes.

This characteristic makes them very flexible. Usually distances between neighboring nodes remain short. But it is also possible to use these networks for longer distances. Ad hoc networks can maintain the signal strength by splitting a longer distance into a series of shorter hops. Intermediate nodes can make routing choices based on their knowledge of the network.



Ability of self-healing in a wireless mesh network

WIRELESS MESH NETWORKS (WMNS) OVERVIEW

A WMN, consists of mesh clients and mesh routers. Mesh routers have minimal mobility and form the mesh backbone for mesh clients. Furthermore, in order to further improve the flexibility of mesh networking, a mesh router is usually equipped with multiple wireless interfaces built on either the same or different wireless access technologies. In addition, the bridge/gateway functionalities that exist in mesh routers enable the integration with other networks. Also, WMNs are characterized by infrequent topology changes and rare node failures.

WMNs can be classified depending on the architecture in infrastructure /backbone WMNs, client WMNs and Hybrid WMNs. In infrastructure WMNs mesh clients can join the network only through the mesh routers. In client WMNs mesh nodes constitute the actual network while in Hybrid WMNs mesh client may join the mesh network either by connected to the mesh backbone or among each other.

Through the different configurations WMNs can be easily used to build up large scale wireless networks. For that reason, IEEE has established several working groups with aim to develop their mesh standards with coverage ranging from a Personal Area Network (PAN) to a Metropolitan Area Network (MAN), as it can be seen from Table I. Also, several companies are developing their proprietary WMN solutions.

SECURITY CHALLENGES AND ISSUES IN WMNS

A. SECURITY CHALLENGES AND CONSTRAINTS IN WMNS

A WMN is exposed to the same basic threats common for both wired and wireless networks, therefore the messages in such networks can be intercepted, and modified, delayed, replayed, or new messages can be inserted. However, WMNs are more difficult to be fully protected for the following reasons:

[1] Multihop Nature: Multihopping delays the detection and treatment of the attacks. Also, since the majority of the existed security schemes are developed for one-hop networks, render them insufficient to protect a WMN from being attacked.

- **Multitier System security**: In such networks security is needed not only between the client nodes, but also between mesh clients and mesh routers, as well as among mesh routers.
- **Multisystem security:** Since the WMNs involve the interoperability of different wireless technologies, such as IEEE 802.15, IEEE 802.11, IEEE 802.16, etc. a security mechanism is needed so that inter-network communications can be provided seamlessly without compromising security in all networks.
- Siddiqui and Hong and Gao et al. also describe the constraints that should be considered in WMNs or in other system with mobile clients such as PDAs, cell-phones etc. These are:
- **Central Processing Unit (CPU):** the total computing power on the end nodes is very limited, so large computations on them are slow.
- **Battery:** the total power capacity is very limited and so it is not desirable to use the device for high range computations and transmissions.
- **Mobility:** nodes can be mobile, which can produce latency in the convergence of the network and the handover to the networks.
- **Bandwidth:** bandwidth in amongst the mobile nodes is also limited.
- **Scalability:** the current wireless networks act poorly, when the networks enlarged in both aspects of members and computation.

In addition, the fact that usually the mesh devices are relatively cheap devices with limited physical security makes them potential targets for node capture and compromise.
Zang and Fang highlighted the three different levels, where security requirements of WMNs should be identified: infrastructure, network access and application. Although Infrastructure security and application security are goals that can be easily achieved network access security is not an easy task due to the multihop nature of the WMNS and their dynamic network topology. For that reason in this paper we mainly focus our attention on network access security issues and countermeasures.

SECURITY ATTACKS IN WMNS

Security attacks may be classified based on several factors, like the nature, the scope, the behavior, or the protocol layer the attacker target. First, depending on whether the operation of the network is disrupted or not, the attacks may be distinguished on active and passive attacks. An active attack is conducted to intentionally disrupt the network operation, while a passive attack intends to steal information and to eavesdrop on the communication within the network. Passive attacks would compromise confidentiality and active attacks would result in violating availability, integrity, authentication, and non-repudiation. Active attacks can be further divided into internal (or insider) and external (or outsider) attacks.
External attacks are conducted by attackers that do not participate in the mesh topology usually by jamming the communication or injecting erroneous information. Internal attacks are conducted by members of the mesh network and for that reason are more severe threats, since they are not as easy to prevent as external ones.
An attack also can be rational or malicious. In a rational attack, the adversary misbehaves only if misbehaving may worth something in terms of price, obtained quality of service or resource saving; otherwise it is characterized as malicious.

Moreover, the attacks can be classified, based on method the attacker use to accomplish their goal, on impersonation, modification, fabrication, replay and Denial of Service (DoS) attacks. In impersonation attacks, an adversary attempts to assume the identity of a legitimate node of the WMN in order to consume its resources or to disrupt the network operation. Modification attacks target on the illegally modification of the contents of the messages, while fabrication attacks aim on consuming the network resources or the disruption of the network operation by generating false routing messages. Finally, in replay attacks (or man-in-the-middle attacks), the attackers retransmit data in order to produce an unauthorized effect, e.g. to convince mesh nodes to use a malicious path through legitimate means, while DoS attacks target on preventing legitimate mesh nodes to use the network services.

CONCLUSION

Wireless Mesh Networks is now a day a very popular technology for providing IP services due to its fast, easy and inexpensive network deployment. However, due to their characteristics, such as the open medium, the dynamic network topology, the multihop nature, and the lack of concentration points where traffic can be analyzed, WMNs pose new challenges in achieving security.

In this paper, we provided a detailed analysis of the fundamental security challenges and constrains of these networks. Furthermore, we classified the possible attacks based on several factors, like the nature, the scope, the behavior or the protocol layer the attacker target. We have also surveyed several defense methods exclusively for WMNs, including intrusion prevention, detection, and response mechanisms found in the literature.

Although security in WMNs has attracted many researchers and many intrusion prevention, detection and response mechanisms may be found in the literature the question about which is the best solution still remain answered, since each of them focus on specific attacks and requirements.

REFERENCES

1) X. H. Wang, M. Iqbal and X. Zhou, "*Design and Implementation of a Dual-Radio Wireless Mesh Network Testbed for Healthcare", In the Proceedings of the International Conference on Technology and Applications in Biomedicine, (ITAB 2008), Ioannina, Greece, 2008, pp. 300-304.*

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) A. Sgora, D. D. Vergados, and P. Chatzimisios, *"IEEE 802.11s wireless mesh networks: Challenges and Perspectives", In the Proceedings of the 1st International Conference on Mobile Lightweight Wireless Systems (Mobilight '09), Athens, Greece, 18-20 May 2009.*

4) M. S. Siddiqui, C. S. Hong, *"Security Issues in Wireless Mesh Networks", In the Proceedings of the International Conference on Multimedia and Ubiquitous Engineering (MUE'07) , Seoul,Korea, 2007, pp. 717 – 722.*

5) N. Nandiraju, D. Nandiraju, L. Santhanam, B. He, J. Wang, and D. P. Agrawal, *"Wireless Mesh Networks: Current Challenges and Future Directions of Web-In-The-Sky", IEEE Wireless Communications, vol. 14, no. 4, 2007, pp. 79-89.*

6) 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.*

7) I. F. Akyildiz, X. Wang, and W. Wang, *"Wireless Mesh Networks: a survey", Computer Networks, vol. 47, no. 4. 2005, pp. 445-487.*

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