Wireless Mesh Networks Security

Md. Asaduzzaman khan
Department of Computer Science and Engineering, Leading University, Sylhet, Bangladesh
Email: nepon_1979@yahoo.com

***Abstract*-Wireless mesh network has resolved the limitation of ad hoc networks which is ultimately improves the performance of Ad hoc networks. Security is a very important issue which can be resolve through proper management of network. The improvement of 802.11i security has greatly improved the network performance and increases the encryption and integrity security issues and threats and their counter measures. Attacks which can come on different layers are being discussed shortly in this paper. Security in wireless mesh network is still under consideration. Wireless mesh network are attracting more attention due to its enhanced features. Wireless mesh network topology and technology is being discussed in this paper. Finally security issues are discussed.**

***Keywords:* WMN Infrastructure, Network Management, Security issues of WMN, Mesh Routing.**

1 Introduction:

Wireless mesh networking is an attractive, emerging and new way of communication due to its low cost and its scalable wireless internetworking solutions for near future, which is the reason that it is becoming little popular communication sector. In all kind of networks security is one of the major factor for reliable and trusted communication. **[1]** WMNs have many advantages other wireless networks. For example it provides very simple settings, broadband capability and the inherent fault tolerance in case of network failures. Deployment of WMNs is very easy. It is dynamically self- configured and self organized with the existing nodes in the network by automatically establishing and maintaining mesh connectivity among the nodes so it brings reliable service coverage in the network. **[2]** Due to its cost effective solution it has been proposed in different networks. Mesh networks can be seen as one type of mobile ad hoc network (MANET). Data can be transmit to destination nodes by using multiple hops, and provides the backbone nodes that are generally not mobile. The IEEE 802.11 working group has provided many standards for communication and now they are more focusing on 802.11s standard due to its dynamic path configuration and topology learning. Wireless mesh networking is a way of routing the data, voice and instructions between the nodes. Sometimes WMNs provides local 802.11g access to clients and connects neighbors using 802.11a "backhaul" but not always because requirements varies like peak data rate and coverage range etc. **[2]** Nodes automatically establish an ad hoc network and maintain the connectivity due to that network provide dynamically self-organization and self-healing and self-configuration and selects the optimal path back to the "wired" network. WMNs consist of mesh routers and mesh clients. Mesh routers provide network access for both mesh and conventional clients. Mesh routers form the mesh backbone and provides the minimum mobility. It provides the same coverage as conventional routers do but with the lower transmission power. Usually it has multiple wireless interfaces but has similar hardware. **[3]**. It provides the additional routing functions for mesh networking. On the other hand mesh clients must have necessary mesh functions for behaving like mesh routers and for transmission of data in the network. They have only one wireless interface for connectivity. Gateway or bridge functions do not exists in these nodes. Clients are being interconnected via a wired backbone network with wireless access points in WLAN deployments so due to that wireless networks can have only a single hop of the end to end path. For connectivity clients must need to be within a single hop range of wireless access point. For achieving the more coverage they must have more number of fixed access points. In large scale the deployment of WLAN is very costly and time consuming as well **[8].**In contrast WMNs one can achieve wireless network coverage of large area without dedicated access points and without relying on wired backbone infrastructure. Mesh routers provides network access to wireless clients in WMNs and by involving multiple wireless hops communication between these mesh routers is achieved. Multiple mesh routers can serve as gateway for internet connectivity in mesh network or nodes. **[8]**

2 Wireless Mesh Networks:

The term WMNs describes wireless networks in which nodes can communicate directly or indirectly with one or more peer nodes. The word mesh describes that all nodes were connected to all other nodes directly but in most modern meshes it connects only a sub-set of nodes to each other. In WMNs we have two types of nodes:

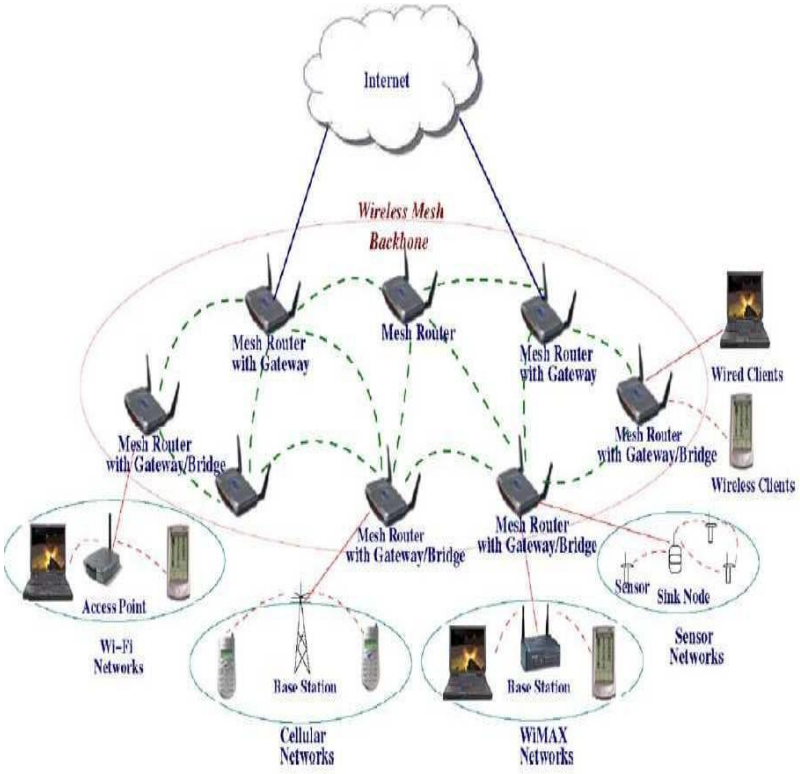

Figure 1: Infrastructure of WMN **[5]**

Both type of nodes can operates as a host and router as well. Packets are being forward on behalf of other nodes that may not be within direct wireless transmission range of their destinations. **[4]**

2.1 Mesh Routers

Mesh routers are mainly stationary devices. Through multi-hop technology they can achieve the same coverage as a conventional router do but with much less power. They have additional routing functions that support mesh networking. **[2]** Its greatly helps the users by connecting them with wireless mesh routers through Ethernet even though they do not have wireless NICs, so user can be always online, anywhere and anytime. Through gateway or bridge functions they integrate with different existing wireless networks such as cellular, wireless-fidelity (Wi-Fi) 802.11 a,b,g and 802.11n. **[4]**

Mesh clients can be mobile or stationary as well. Mesh clients have necessary mesh functions and they can acts as a router but they do not have gateway or bridge functionality. They only have one wireless interface. We have large variety of devices that can acts as mesh clients. **[3]**

3 Characteristics of WMNs:

Wireless mesh networks are multi hop networks and provides much coverage range. Like if one node is failed or turns off then through other nodes message can be transmitted to destination nodes that function provides the redundancy in the mesh network. They have capability of self healing and self forming and self organization and provide support for Ad Hoc Networking. As we have multi-hoping so it achieves higher throughput, and more efficient frequency re-use. They provide low cost for installation because the reduction of the number of access points to

internet so the main advantages of WMNs is that easiness of deployment. Multiple type of network access like support for internet and p2p communication as well. Provide compatibility with existing wireless networks like WiMax, Wi-Fi, cellular networks. It has flexible network architecture.

3.1 Difference between WMNs and Ad hoc Networks

The comparison of WMNs and Ad hoc networks is discussed and summarized as below:-

3.1.1 Wireless infrastructure/backbone

The WMNs consist of wireless backbone with mesh routers, WMNs provides large coverage, connectivity, and robustness. On the other hand the coverage of ad hoc networks depends on contributions of end users, which may not be reliable.

3.1.2 Integration

Through gateway or bridge functions WMNs enables the integration of various existing networks such as Wi-Fi (802.11a, b, g, n), the Internet, cellular and sensor networks.

3.1.3 Dedicated routing and configuration

For these functionalities the WMNs contain mesh routers and in ad-hoc networks, end-user devices perform routing and configuration functionalities for all other nodes or users. In WMNs we do not have much load on end-user devices. **[4]**

3.1.4 Multiple Radios

In WMNs mesh routers may have multiple radios for performing and access functionalities. Routing and configuration are performed between mesh routers which improve the capacity of network and in Ad hoc we have one radio for all functions which works on the same channel**. [6]**

3.1.5 Mobility

The network topology changed dynamically in Ad hoc networks because we have high mobile networks and it depends on the movement of uses. On the other hand, WMNs have fixed nodes and they provide relatively static mobility, and their network mobility is relatively low as compare to ad-hoc networks. **[6]**

3.1.6 Application Scenario

WMNs are being used in military and civilian applications as well due to their permanent and semi permanent devices but in the other hand in ad hoc mostly ad-hoc networks are temporary so they cannot be used for both purposes. WMNs are used in many other applications as well like broadband home networking, community and neighborhood networking, enterprise networking, metropolitan area networking, transportation systems, health and medical systems and in security and surveillance systems. **[5]**

3.2 Technology of WMNs

It is a communications network model that works in the same way as the wired internet works. We have more than one possible pathway between each node for communication. In mesh network architecture we have multiple possible connections for every other node which improves on point-to-point and point to-multi-point like centralized hub and spoke topologies.

3.2.1 Mesh Routing

For Wireless mesh routing multiple technologies are being used that proactively and reactively determine traffic paths within the radio network. On demand a route is being established to a destination by using reactive routing protocol but the proactive routing protocol are often based on link state for finding the routing paths irrespective of the path usage or demand. Combination of reactive or proactive mechanisms is used in vast numbers of different routing protocols. Mostly the implementation of ad-hoc networks is based on hybrid on-demand and link-state routing protocols. **[12]**

3.2.2 Point to Point

Point to point provides high performance, high speed interconnections and dedicated connection between the nodes. It is very simplest form of wireless communications that enables two nodes for communication with each other. It is not highly scalable and relatively it can be deployed quickly.

3.2.3 Point to Multipoint

In this type of topology we have more than one connection for a single node. By using multiple nodes a connection is being established between base station and other nodes. When a new user wants to enter in the existing network it can easily do that but user must be in the range of base station and subscriber requires only equipment for deployment at the user end, so this solution is best suited for backhaul operations like connection to main central site. **[7]**

3.2.4 Multipoint to Multipoint

Data is routed between different nodes for the destination so for that a routed mesh topology is created for that purpose. Multiple access routers are deployed for maximum coverage and for high

density, so all routers perform the functions for data through the network over multiple hops. **[7]** User can join network anytime, anywhere in the entire mesh does not matter that the user is going to be connect through wireless or wired.

4 Securities in Wireless Mesh Networks

Security issues and the potential of WMNs are cannot be ignored. In WMNs the understanding and properly addressing of these problems and challenges is very necessary. Due to dynamic change of network topology, distributed network architecture and shared wireless mediums WMNs lacks in security solutions. Attacks can occur on different protocol layers which can harm the network traffic and data. In wireless mesh there are different types of architecture which may uses different approaches for wireless mesh security purpose. **[9]**

4.1 Basic Prevention

The primary issues which are very necessary for privacy preventions are as follows:-

4.1.1 Data Confidentiality

Its main purpose to prevent from eavesdropping and protect the data against the attacks .It is controlled by intermediate mesh routers. The algorithm by which one can protect the data from misbehaviors is message encryption.

4.1.2 Traffic Confidentiality

Traffic confidentiality is quite difficult to prevent against the attacks. For traffic confidentiality users must know that to whom they are communicating and their traffic patterns must be followed by the communicators. It is usually occurred by the attackers at mesh routers while traffic transfer. By following the key distribution mechanism WMNs can overcome on this type of attacks. **[10]**

4.2 Mesh Security

802.11s is a standard which will be followed in future for all kind of commercial mesh products. Right now mesh products are using different approaches for security and many of them may be derived from existing ad-hoc security mechanisms. 802.11s is a standard which will be based primarily on 802.11i security mechanisms.

Security Goals

In any application these are the general goals and need to be considered to overcome on the security. These goals are not application specific. In WMN application there are same basic threats which are also common for other application. e.g:-Wired and wireless networks. An attacker can intercept, modify, delayed, replayed, the message. Attacker can insert the new message in the network.

4.2.1 Confidentiality

In this the whole path should be protected and message should not be altered during the communication. Users must know each other for secure communication. The message and data information should not be disclosed. The data is only revealed to the intentional users.

4.2.2 Availability

Insurance of authorized user actions can be done for secure communication. Provide the reliable delivery of data to the destination node. Protect the message and data against DoS (Denial of Service)

4.2.3 Authentication

In WMNs authentication is very important because of change of shared medium. A proper mechanism should be followed for data sending and receiving. Users must know each other because it very necessary for reliable transmission of data. If user will not follow the any process then data may be infected or fabricated by anybody else which cause the problem in the network transmission.

4.2.4 Authorization

Users have the right to amend the data. If anybody wants to perform any task then there should be a proper process which ensures that the person have right to perform that task.

4.2.5 Accounting

If a user is using any service then there should be a process or method through which measurement of used resources can be done for billing information of specific user.

4.2.6 Integrity

Users cannot modify the data without having proper right to perform that task. If a user do not have right to perform any task then he/she cannot modify or change the message.

4.2.7 Access Control

User should ensure that only authorized actions can be performed, like if one cannot have authorization of changing the message then that user must be communicate with administrator for performing that task which he/she wants to perform.

4.3 Security Challenges

Many challenges can be seen in WMNs due to its dynamic change in the network. Physical security of nodes is also a big considerable issue which can also be caused of network failure. New challenges are mostly seen because of multi-hop wireless communication. If administrator wants to apply statically security configuration it will not be sufficient for the network because of users frequently joining and leaving the mesh network. For mesh router and mesh clients same security solutions will not work because they have a lot of different characteristics such as mobility and power constraints. **[11]**

5 Conclusions

The ability of self healing and self organization is key factor in WMNs which reduces the network complexity and maintenance. Provides the backbone ability through which a user can connect to internet any where any time. WMNs are a promising technology for next generation wireless networking. WMNs have enhanced the capability and reliability of ad hoc networks. There are still many problems in WMNs which needs to be improved. The existing approaches are effective at specific layers but there is still need to have a comprehensive mechanism which can prevent from the attacks at protocol layers. For self healing and self organization WMNs still requires an inclusive protocol.

The main focus of this paper is to provide right recommendation and direction towards security enhancement. The security solutions used in Wireless LANs are not getting ready for WMNs. Cryptography, key management; WEP and TKIP are considerable solutions which are available right now for WMNs devices. IEEE task group defines 802.11s which is a pre draft for wireless mesh networks. In near future it can be deployed with its full functionality. Right now 802.11s is using the techniques of 802.11i. There are still many research problems in WMNs but it is most promising technologies for next-generation wireless networking.

REFERENCES:

[1] Siddiqui, M.S. Amin, S.O. Choong Seon Hong. "An Efficient Mechanism for Network Management in Wireless Mesh Network." ICACT 10th International Conference, Feb. 2008.

[2] [8] Ian F. Akyildiz, Xudong Wang, Weilin Wang, "Wireless mesh networks: A Survey" 1st January 2005.

[3] Anastasios, D. Khalil, K. "IEEE 802.11sWireless Mesh Networks" Dept. of Communication Systems, Lund University, Sweden.

[4] Omar Villavicencio-Calderon. "wireless mesh networks: performance analysis and enhancements." university of puerto rico mayag uez campus, 2008.

[5] Hamid, Zara; Khan, Shoab A., "An Augmented Security Protocol for WirelessMAN Mesh Networks," *Communications and Information Technologies, 2006. ISCIT '06. International Symposium on* , vol., no., pp.861-865, Oct. 18 2006-Sept. 20 2006

[6] Carlo Alberto Boano and Md. Sakhawat Hossen. "VoIP over Wireless Mesh Networks: Implications and Challenges," May 1, 2008.

[7] White Paper "Wireless Mesh Technology: Connecting the new millennium". IJIS Institute Briefing Paper.

[9] A.Gerkis ''A Survey of Wireless Mesh Networking Security Technology and Threats''. September 2006.

[10] Ian F. Akyildiz, Xudong Wang, ''Security in Wireless Mesh Networks''.December 19, 2006

[11] Yan Zhang, Jijun Luo, Honglin Hu, 'Wireless Mesh Networking architectures protocols and standards '.

[12] Guangsong Li, An Identity-Based Security Architecture for Wireless Mesh Networks. 2007.