
*Journal of Advances in Science and Technology*

*Vol. IV, No. VII, November-2012, ISSN 2230-9659*

# SECURITY IN WIRELESS MESH NETWORKS

www.ignited.in

*Journal of Advances in Science and Technology*
*Vol. IV, No. VII, November-2012, ISSN 2230-9659*

# Security in Wireless Mesh Networks

**Ritu Sharma[1] Dr. Prof. Deo Brat Ojha[2]**

[1]Research Scholar CMJ University, Shillong,Meghalaya, India

[2]Professor, R.K.G.I.T. , Ghaziabad, U.P.

***Abstract—Wireless Mesh Networks (WMNs) are currently the subject of much research. WMNs are not Mobile Ad Hoc Networks (MANETs); instead they are a superset of MANETs. WMNs may exist in the absence of a central infrastructure taking the form of a MANET. However on the other hand, they may exist as networks comprised of an infrastructure connecting extended ad hoc networks. One significant area of research within ad hoc networks is routing and in particular, the securing thereof. Owing to the characteristics of WMNs however, routing algorithms designed for ad hoc networks however may not always be applicable to WMNs.***

***Keywords—Wireless Mesh Networks, Ad Hoc Networks, Secure Routing.***

----------♦----------

## INTRODUCTION

NETWORKS have traditionally followed two paradigms: centralized and decentralized. Traditional wireless networks represent the centralized model where clients directly connect to an access point. Mobile Ad Hoc Networks (MANETs) on the other hand represent the decentralized model where clients themselves uphold the network in the absence of a central infrastructure. Wireless Mesh Networks (WMNs) are a means to merge these two paradigms into a single transparent network. A common scenario of WMNs is the existence of an infrastructure that is further extended by ad hoc sub-networks. Within the infrastructure component, dedicated hardware may be assigned for routing purposes; client nodes within the ad hoc network on the other hand are left to perform the routing responsibilities. Routing and security requirements should be treated differently when addressing different components within a WMN.

## II. ARCHITECTURES

WMNs generally fall under one of three categories [1]: Infrastructure mesh; Client mesh; or Hybrid mesh.

### *A. Infrastructure Mesh*

An infrastructure mesh in most cases is typically a mesh comprised of routing/access-point devices. The client nodes themselves do not form the mesh; instead they connect to the mesh like regular wireless clients. The routers form a mesh by connecting to one another and are responsible for routing client data. The data may travel via multiple router hops before reaching its final destination.

### *B. Client Mesh*

A client mesh resembles a MANET as there is no central infrastructure available to perform regular networking functions. The clients themselves perform these responsibilities and uphold the network connectivity.

### *C. Hybrid Mesh*

A hybrid mesh is simply a network that incorporates an infrastructure that is also extended by one, or many ad hoc networks. Hybrid meshes should be able to support regular wireless clients, wired clients via Ethernet bridging, and mesh clients. This introduces additional challenges in terms of protocol usage for the support of heterogeneity in the network. Hybrid mesh networks would probably be the most applicable model in a realistic environment.

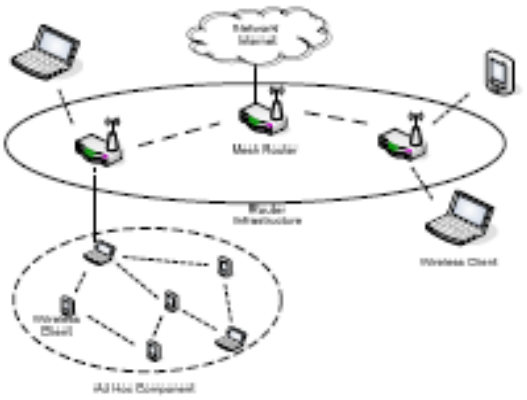

**Figure 1 - Hybrid Mesh**

## III. ROUTING AND SECURITY REQUIREMENTS

As already mentioned, a WMN may consist of an infrastructure component as well as many ad hoc (client mesh) networks. The routing and security requirements of these separate components may differ substantially due to different characteristics of the separate mesh components.

### *A. Routing Requirements*

Ad Hoc networks will generally consist of mobile devices such as PDAs, laptops, etc. These devices are generally limited with regard to battery and processing capabilities.

The following are requirements of the routing protocol used:

- Adaptation to changes in the network topology.
- Robustness to cope with link failures.
- Efficiency as to not over-consume resources.

Routing protocols generally fall into two categories [2]:

proactive and reactive protocols. Proactive protocols are table-driven and involve nodes storing routing information about neighbours inside local routing tables. In general terms, nodes periodically broadcast routing information to keep the routing tables up-to-date. Reactive (on-demand) protocols involve a sender node establishing a route on- demand only when data is needed to be sent. Proactive protocols have the advantage of routes being available immediately when a message is needed to be sent. The disadvantage of proactive protocols is the additional overhead of keeping the routing tables up-to-date; this is problematic within ad hoc networks where nodes are typically constrained in terms of battery and processing capabilities. Reactive protocols are more suited for use within ad hoc networks due to the establishment of routes only when they are needed and hence requiring less overhead. As already mentioned, WMNs may consist of a routing infrastructure/backbone responsible for routing client data, as shown in figure 1. The nodes making up the router backbone will most likely differ considerably to that of

client devices in an ad hoc network. Infrastructure nodes will most likely have a lesser constraint on battery and processing power and will also most likely be less mobile than the client devices. The difference in characteristics between infrastructure and ad hoc nodes is evidence that routing protocols designed for ad hoc networks cannot in all cases be suitable for wireless mesh networks. A solution may be to use separate routing protocols for the different components of the network, resembling the internet architecture. A proactive routing protocol is better suited for use within a routing infrastructure; routing devices are better equipped to handle the additional overhead and the advantage is the immediate availability of routes amongst the backbone. A reactive protocol on the other hand is most suitable for use within any ad hoc sub-networks present in the WMN.

### *B. Security Requirements*

Most existing ad hoc routing protocols have been designed with performance as a priority and thus have neglected to incorporate a significant amount of security in the protocol. The following are requirements of a secure routing protocol:

- Authenticating the sources of routing information as well as all nodes involved in a multi-hop routing path.
- Integrity of routing information to prevent tampering or corruption of routing data.
- Confidentiality is less important but may be used to prevent passive eavesdropping.

Many routing protocols have been adapted to provide secure routing [3, 4, 5]. The problem with many existing secure routing protocols is the unrealistic assumptions they place on the operating environment. In [4], it is assumed that nodes in the network are loosely synchronized; in a heterogeneous environment with mobile devices, this assumption is not realistic [2]. In [3], a central Certification Authority (CA) is assumed, and in [5], security associations a priori between each sender and receiver are assumed. The previous assumptions are clearly unrealistic within use of an open ad hoc network not under the control of a single administrative domain. A comprehensive summary of secure ad hoc routing and their assumptions is given in [2]. Many of these secure routing protocols however may be well suited for use amongst routers in a router backbone. It is most likely that a router infrastructure will be arranged under a single administrative domain, therefore assumptions relying on prior secret keys or security assumptions may not be a restrictive issue. The use of more powerful cryptographic techniques such as asymmetric cryptography also may not be a problem for the router devices which may not suffer from power and processing constraints as apposed to ad hoc mobile devices.

## IV. FUTURE RESEARCH AREAS

Hybrid routing protocols rely on the use of both proactive and reactive routing protocols to achieve routing within the network. The Zone Routing Protocol (ZRP) [6] is a hybrid which utilizes both proactive and reactive routing protocols. ZRP is not an actual implementation; rather it is a framework. Nodes using ZRP are arranged into zones; nodes will use a proactive routing component for routing amongst nodes in the same zone. A reactive routing

protocol is used for inter-zone communication and for route discovery and maintenance. One possible area of research is the use of hybrid routing in WMNs and the potential to develop a security framework for its use. Another potential area for further research is secure multi-path routing for ad hoc networks. The majority of routing protocols used for ad hoc networks establish a single path between sender and receiver; multi-path protocols on the other hand make use of multiple paths simultaneously to improve load-balancing and robustness against link failures. A greater amount of research regarding security has been undertaken for the more commonly used single-path routing protocols; hence there is scope for further research regarding security within multi-path routing protocols for ad hoc networks.

## REFERENCES

[1] Akyildiz, I. F., Wang, X., and Wang, W. 2005. Wireless mesh networks: a survey. *Comput. Netw. ISDN Syst.* 47, 4 (Mar. 2005), 445-487. DOI= http://dx.doi.org/10.1016/j.comnet.2004.12.001

[2] Patroklos G. Argyroudis, Donal O' Mahony, "Secure Routing for Mobile Ad hoc Networks". IEEE Communications Surveys and Tutorials, vol. 7, no. 3, pp 2-21, 2005.

[3] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields and E.M. Royer, "A Secure Routing Protocol for Ad hoc Networks", *Proc. 10th IEEE Int'l. Conf. Network Protocols (ICNP'02)*, IEEE Press, 2002, pp. 78-87.

[4] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks," *Proc. 8th ACM Int'l. Conf. Mobile Computing and Networking (Mobicom'02)*, Atlanta, Georgia, September 2002, pp. 12-23.

[5] P. Papadimitratos, and Z.J. Haas, "Secure Routing for Mobile Ad hoc Networks," *Proc. Communication Networks and Distributed Systems, Modeling and Simulation Conf. (CNDS'02)*, San Antonio, Texas, January 2002, pp. 27-31.

[6] Nicklas Beijar, "Zone Routing Protocol (ZRP)". www.netlab.tkk.fi/opetus/s38030/k02/Papers/08-Nicklas.pdf