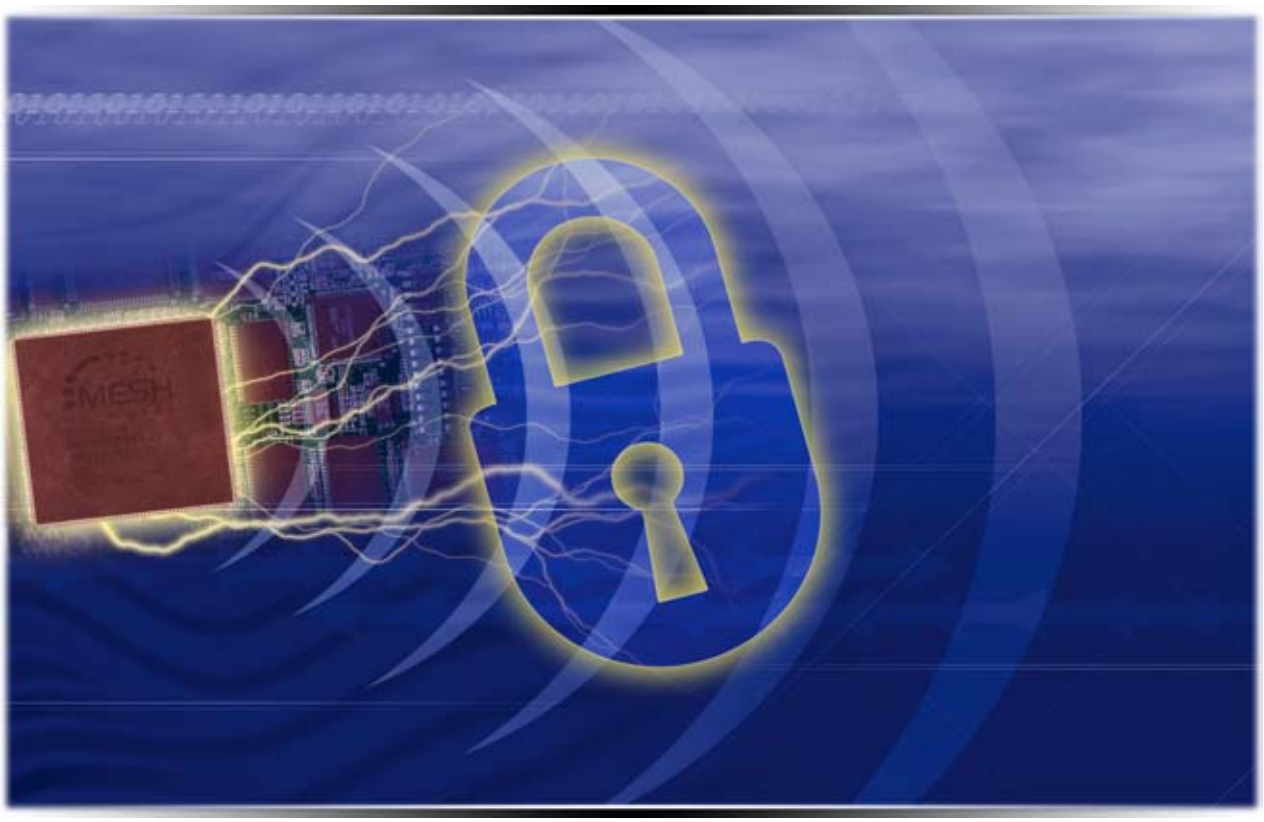
SECURITY ISSUES & SOLUTIONS IN MOBILE AD HOC NETWORKS



MeshNetworks, Inc.
Maitland, Florida

Introduction

Wireless communications networks present security challenges that extend beyond those of wired networks. However, with good technology and practices, the risks to the network, subscriber, and data content, can be minimized.

Security Issues In A Wireless Network

The Security issues faced in a wireless network are well known and understood. In general, these issues can be grouped into the following categories:

- **Insertion of Unauthorized Terminals or Network Devices** – including cloned or stolen user devices and fraudulent network access elements.
- **Interception & Monitoring of Wireless Traffic** - including the capturing of user names, addresses and passwords, as well as interception of the user's data content.
- **Radio Frequency Jamming and Denial of Service Attacks** – can be used to disrupt service or force traffic onto an unauthorized network access element.
- **Physical Network Attacks** – power, back-haul, or the network elements themselves are compromised or destroyed by a malicious party.

Additional Security Issues in Ad Hoc Networks

In addition to the typical issues raised above, there are additional issues that must be dealt with in ad hoc network architectures.

- **Monitoring of Data Content by an Intermediate Terminal** – the multi-hopping nature of an ad hoc network necessitates that a subscriber's data transmissions are able to be routed/repeated by another subscriber's transceiver. However, this data must remain secure and private while hopping through intermediate terminals.
- **Peer-to-Peer Attacks** – subscriber devices (computers, PDAs, etc.) can be attacked by other peer devices directly (with no network infrastructure involved in the communications path). Data could be lost or stolen if the targeted device is running TCP/IP services such as Web Server, file sharing, etc.

To address these issues, MeshNetworks has implemented a multi-layered approach to minimize the risks posed by these challenges.

Security Management And Capabilities

MeshNetworks has implemented numerous security management practices and capabilities in the operations and architecture of its network. Figure 1 shows an overview of MeshNetworks' Mesh-Enabled Architecture (MEA™). Referencing this diagram, the following sections briefly discuss the security features currently implemented and envisioned in a MEA network.

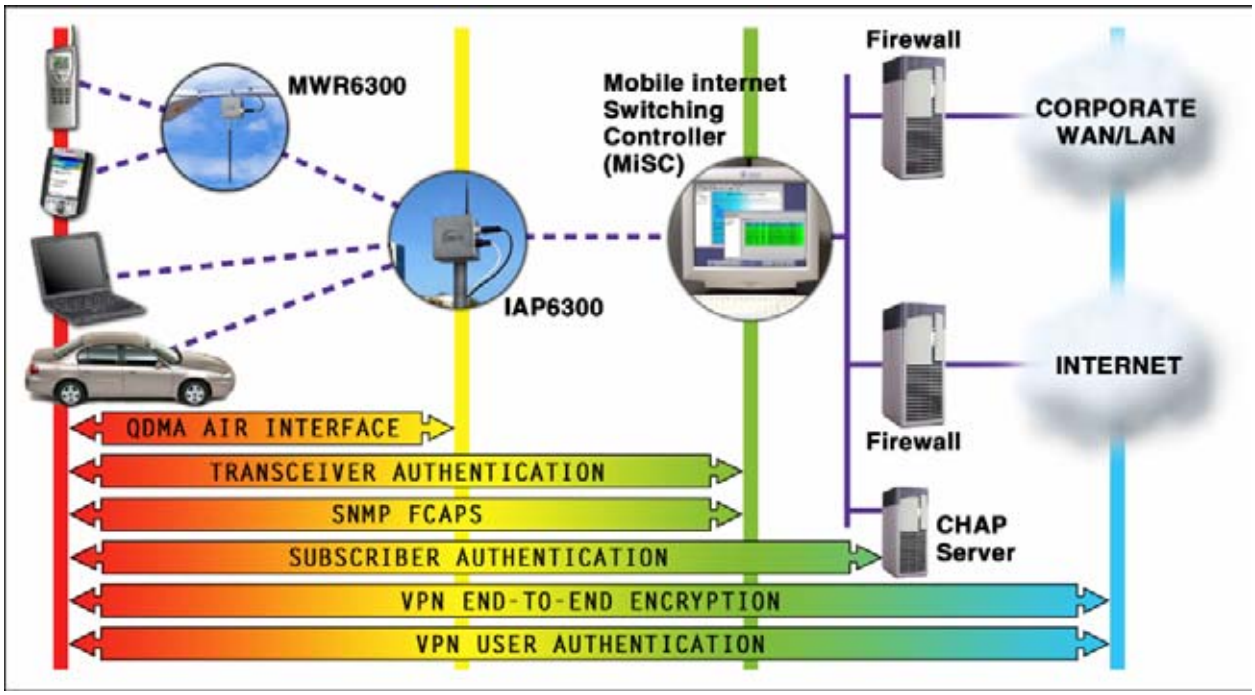


Figure 1. Overview of MeshNetworks Security Architecture

Quadarature Division Multiple Access (QDMA) Air Interface Based on State of the Art Military Technology

QDMA was designed and developed for military applications. As a result, there are numerous security/stealth features built in to its physical layer design. The QDMA system combines direct sequence spread spectrum (with high spreading rates), multiple switched data channels, proprietary spreading codes, and burst mode data transmission to create a very secure air interface. Each packet in a data stream may take a different route to a destination. Each packet may be on a different frequency data channel. MeshNetworks' complete implementation of the QDMA air interface makes capturing a data stream for any given session infeasible.

All Transceivers are Hardware Authenticated and Registered with the Network to Minimize Insertion of Unauthorized Devices

Transceivers are hardware authenticated via their unique address. Authentication is required of all subscriber transceivers, Wireless Routers and Intelligent Access Points. This is accomplished through a proprietary software application - Mesh Hardware Authentication Server (MHAS), which is similar in functionality to an Equipment Identity Register (EIR). The address of each transceiver is registered and compared against those contained in a provisionable database that identifies the devices as being on the White list (authorized), Black list (denied) or Gray list (authorized but monitored).

All Transceivers are Software Authenticated by a AAA Server to Minimize Use of Cloned or Stolen Devices

Transceivers on the White or Gray list proceed through an authentication, authorization, and accounting (AAA) server that provides similar service to Authentication Dial-In User Service (RADIUS). Only after the transceiver has been successfully authenticated is the attached subscriber device allowed to request an IP address from the network. MeshNetworks is IP transparent so second level authentication methods like Challenge Handshake Authentication Protocol (CHAP) can be applied to further authenticate network users. Devices denied service are refused access to the network.

MeshNetworks' Architecture Minimizes the Impact of RF Jamming, Denial-Of-Service, and Physical Attacks to the Network

These sorts of attacks will be relatively ineffective, since subscriber devices can self-route around (via hopping) the affected area. These attacks will be treated in the same way as network congestion or network transceiver failures. The self-healing nature of the MeshNetworks system isolates the attack and affected subscribers will be instantly routed around the problem area. A massive, coordinated attack designed to affect a large number of network access points will impact the service level of the network, however much less so than in a cell-based network. The reason for this is fundamental; in a meshed architecture, the physical network topology tends to imitate the logical network. That is, many of the communications links take the form of peer-to-peer inter-connection at the subscriber level – thus there are no large centralized nodes to attack. The military uses a meshed network architecture for this reason.

End-To-End IP-Based Infrastructure Supports VPN and Other Standards-Based Encryption Schemes

MeshNetworks implements standards-based IP transport that supports existing enterprise, personal and secure Internet VPN/encryption. Standard VPN user-authorization found in wired IP infrastructures is supported and is totally transparent in a MEA network. This makes over-the-air, as well as wired data transmissions, secure. Utilizing MeshNetworks IP architecture and VPNs allows networks to be created that meet rigorous federal and local government security standards.

Ad hoc Architecture keeps Data Secure When Hopping Through Intermediate Terminals

Each MeshNetworks transceiver is an intelligent router that keeps data destined for a third-party from leaving the transceiver and crossing the interface to the attached host.

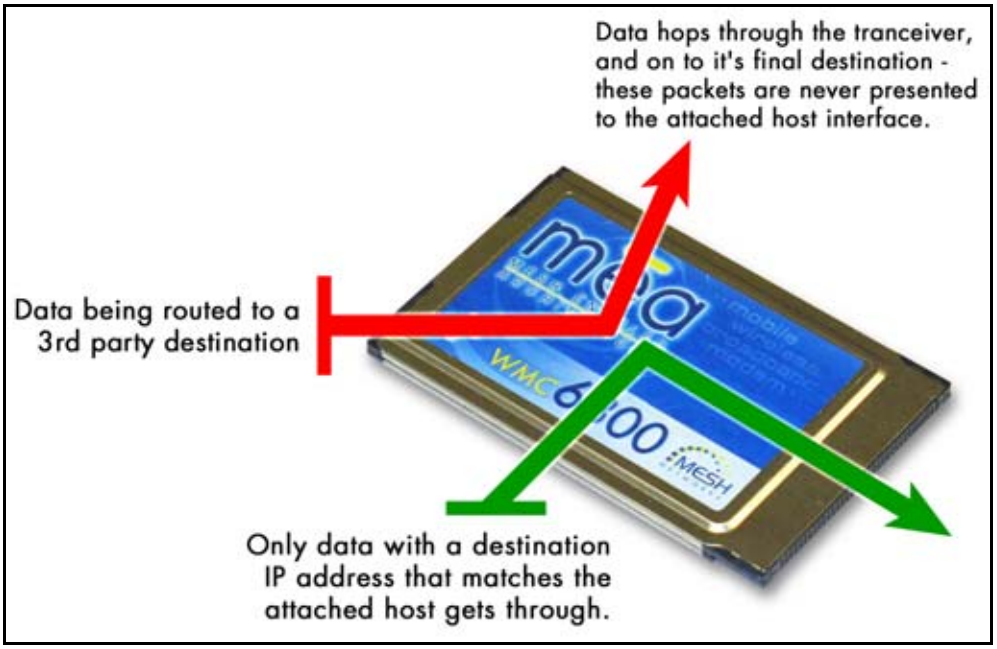


Figure 2. Hopping Through an Intermediate Transceiver

As Figure 2 indicates, only packets with IP destination addresses matching the attached host device are allowed to cross the transceiver/host interface. The host is not able to access memory on the transceiver card. As a result, data that is hopping through a transceiver is inaccessible to the attached device.

QDMA Air Link is Secure

The QDMA waveform combines TDMA, FDMA and DSSS to create a robust, secure transmission system. Unlike 802.11, monitor mode is not available on this configuration. No public shareware exists that allows a third party to snoop the air interface. This provides an effective deterrent to first level data privacy attacks.

Buddy Lists and Personal Firewalls Protect Subscriber Devices from Peer-To-Peer Attacks

The advent of shared, persistent broadband communications, such as cable modems and DSL, has caused even casual home-computer users to implement security measures. MeshNetworks transparent IP implementation allows personal firewalls and other security filters such as buddy lists to be implemented to fend off peer-to-peer attacks.

Summary

MeshNetworks meet federal and local governments standards for data privacy

MeshNetworks has addressed the security issues commonly found in wireless networks. Using the combination of secure network elements and IP layer security systems(like VPNs) , Networks can be created that meet strict federal and local government standards for voice and data security.

MeshNetworks architecture is resilient to interference, attacks, and failures

MeshNetworks has designed a radio system that is resistant to interference. The MeshNetworks architecture allows automatic rerouting of data flows around network problems, whether the cause is malicious or not. In any case, unauthorized network elements are simply denied service on the network.

MeshNetworks is Flexible for the Future

There are many security issues that must be addressed in wireless and wired networks. In order to address these issues, numerous policies, procedures and safeguards have been implemented or planned for in the MeshNetworks system. Authentication, authorization, and management of every element – including the subscriber transceiver, minimize the impact of an attack on the network from a rogue device. Support for standards-based software encryption (and VPN security) insures that data is protected from prying eyes while it is transmitted over the air, hopping through other transceivers, or traveling through another network. Federal and local government standards for voice

and data transmission can be supported. By taking a layered approach to security issues, a MeshNetworks system is more secure than a typical wireline network.

Security issues are constantly evolving and changing. Accordingly, MeshNetworks continuously evaluates these issues, and responds with enhanced security capabilities and solutions. For example, the emerging 802.1x standard is planned to be supported in a future software release. As other security standards evolve, MeshNetworks will evaluate these for inclusion in its overall security strategy as well.