

Communicate. Locate. Interoperate.

Examining security issues in ad hoc networks and delivering appropriate solutions

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 minimised.

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 unauthorised terminals or network devices - including cloned or stolen user devices and fraudulent network access elements.

Interception and 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 unauthorised network access element.

Physical network attacks - power, back-haul or the network elements themselves are compromised or destroyed by a malicious third 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, Motorola has implemented a multi-layered approach to minimise the risks.

Security management and capabilities

Motorola has implemented numerous security management practices and capabilities in the operations and architecture of its network.

Figure 1 shows an overview of Motorola's MESH Enabled Architecture (MEA®).

Referencing this diagram, the following sections briefly discuss the security features currently implemented and envisioned in a MEA network.

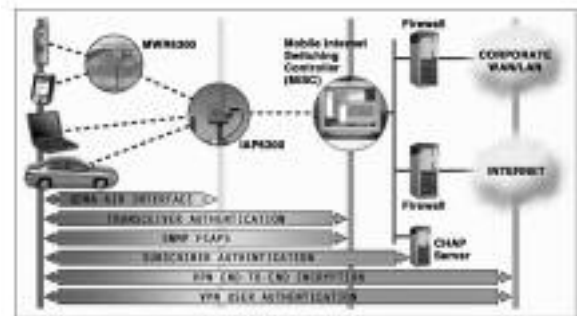


Figure 1. Overview of MEA's Security Architecture

Quadrature 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. Motorola's complete implementation of the QDMA air interface makes capturing a data stream for any given session infeasible.

Transceivers are hardware authenticated and registered with the network to minimise insertion of unauthorised 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 database that identifies the devices as being on the 'white list' (authorised), 'black list' (denied) or 'grey list' (authorised but monitored).

Transceivers are software authenticated by an AAA Server to minimise use of cloned or stolen devices

Transceivers on the white or grey list proceed through an Authentication, Authorisation 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. Motorola 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.

Motorola's architecture minimises 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 Motorola 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 centralised nodes to attack. The military use meshed network architectures for this reason.

End-to-end IP-based infrastructure supports VPN and other industry standards-based encryption schemes

Motorola implements standards-based IP transport that supports existing enterprise, personal and secure Internet VPN/encryption. Standard VPN user-authorisation 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. Utilising Motorola's IP architecture and VPN's 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 Motorola 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. 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.



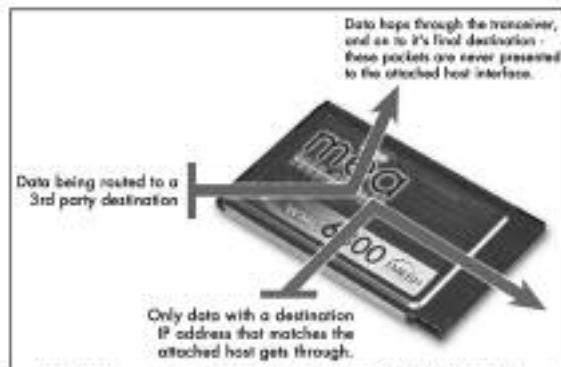


Figure 2. Hopping Through an Intermediate Transceiver

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 illegally monitor 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, 'always-connected' broadband communications such as cable modems and DSL, has caused even casual home-computer users to implement security measures. Motorola's transparent IP implementation allows personal firewalls and other security filters such as buddy lists (which show lists of friends, fellow workers etc.) to be implemented to fend off peer-to-peer attacks.

Summary

Motorola's MESH networks meet federal and local government standards for data privacy

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

Motorola's architecture is resilient to interference, attacks and failures

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

Motorola's MESH network 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 Motorola system. Authentication, authorisation, and management of every element – including the subscriber transceiver, minimise the impact of an attack on the network from a rogue device. Support for standards-based software encryption (and VPN security) ensures that data is protected from prying eyes while it is transmitted over the air, hopping through other transceivers, or travelling 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 Motorola system is more secure than a typical fixed wire network.

Security issues are constantly evolving and changing. Accordingly, Motorola 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, Motorola will evaluate these for inclusion in its overall security strategy as well.

To learn more about Motorola's MEA products and other MESH enabled solutions, please visit our MESH website at www.motorola.com/emea/mesh



MOTOROLA

Motorola Limited

Jays Close
Viabes Industrial Estate
BASINGSTOKE
Hampshire
RG22 4PD
UK

email: mesh@motorola.com

MESH Enabled Architecture, MEA, MESH Scalable Routing, MSR, MESHManager, Mobile Internet Switching Controller, MiSC, QDMA, and Multi-Hopping are trademarks or registered trademarks of Motorola, Inc. MOTOROLA and the Stylised M Logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners. © Motorola Inc, 2005.

MESH.MAHN.WP-RE (0605)