Ad hoc Network and Bluetooth Security

Ad Hoc Networks

- Ad hoc -- a Latin phrase which means "for this [purpose]".
- An autonomous system of mobile hosts connected by wireless links, often called Mobile Ad hoc NETworks (MANETs)

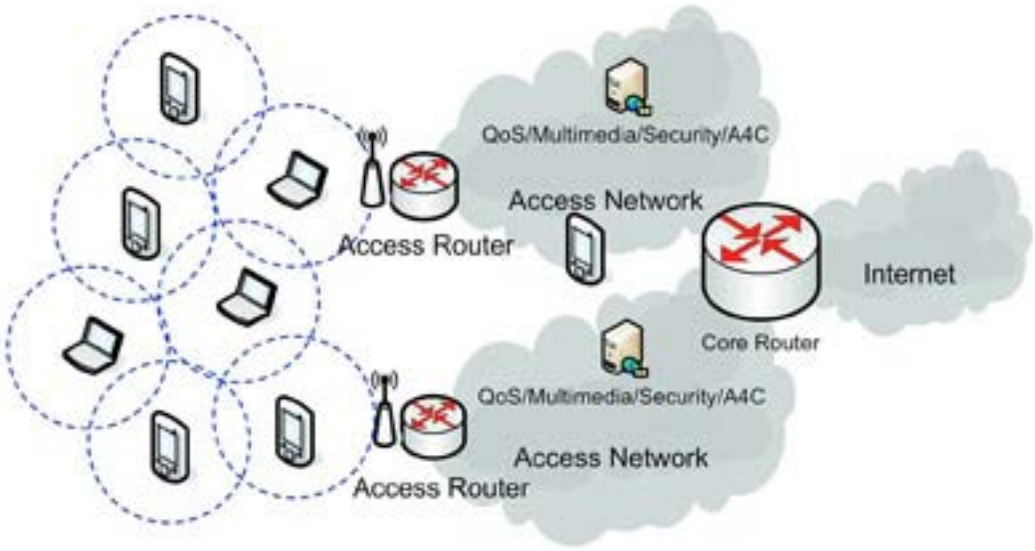
Characteristics

- No fixed infrastructure
- Dynamic changing topology
  - Mobile devices join/leave the network unexpectedly; they can also move freely
- Energy-constrained
- Limited bandwidth
- Each node also serves as router
  - Help to relay packets received from neighbors
- Interoperation with the Internet

Comparison

- MANETs vs. Wired networks
  - In MANETs, each node also works as router for forwarding packets
  - In wired networks, routers perform routing task
- MANETs vs. Managed wireless networks
  - No infrastructure in MANETs
  - Special node known as access point (AP) in managed wireless networks

A MANET Example

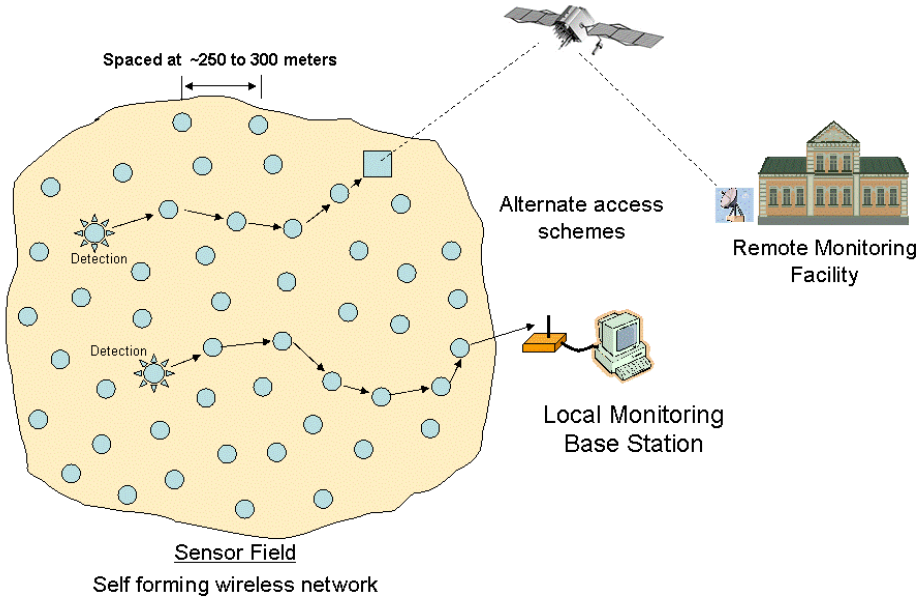


Mobile Devices

- Laptop computers
- Pagers, cellular phones, PDAs
- In-car navigators -Dash Express
  - Dash units talk to each other and form
  - a network that connects to the Internet
  - Traffic speed data is sent back to the company,
  - then broadcast back to all local dash units
- Sensors

Wireless Sensor Network (WSN)

- An emerging application area for MANETs
- A collection of cheap to manufacture, stationary, tiny sensors
- Network lifetime -- power as a major driving issue
- Battlefield surveillance, environment monitoring, health care, etc.



Other MANETs applications

- Collaborative work
- Crisis-management applications
- Personal Area Networking (PAN)

Security Requirements in MANETs

- Availability
- Authorization and Key Management
- Data Confidentiality
- Data Integrity
- Non-repudiation

Security Solution Constraints

- Lightweight
- Decentralized
- Reactive
- Fault-tolerant

Challenges

- No infrastructure
- Peer-to-peer architecture with multi-hop routing
- Mobile device physical vulnerability
- Stringent resource constraints
- Wireless medium
- Node mobility

Threats

- Attacks
  - External attacks
  - Internal attacks
  - Passive attacks
  - Active attacks
- Misbehavior

MANETs Security

- Routing security
- Data forwarding security
- Link layer security
- Key management
- Intrusion detection systems (IDSs)

Routing in MANETs

- Nodes' mobility -topology changes rapidly
- Large network size -significant amount of network control traffic

MANET Routing Protocols

- Topology-based approaches
  - Proactive routing (table driven)
  - Reactive routing (on demand)
  - Hybrid routing
- Position-based approaches

Comparison

- Reactive routing
  - Only discover routes to destinations on-demand
  - Consume much less bandwidth but experience substantial delay
  - E.g. DSR, ADOV, TORA, etc.
- Dynamic source routing (DSR)
  - Source broadcasts RREQ through the network
  - Intermediate nodes add its addr to RREQ and continue broadcasting until RREP received
  - Full path chosen by source and put into each packet sent
- Ad hoc on-demand distance vector (AOVD)
  - Hop-by-hop routing
  - Source sends RREQ to neighbors
  - Each neighbor does so until reach the destination
  - Destination node sends RREP follow the reverse path
  - Source doesn't put whole path but only next hop addr in outgoing packets

Routing Protocol Attacks

- Attacks using modification
  - Redirection by modifying route sequence number
  - Redirection by modifying hop count
  - Source route modification
  - Tunneling
- Attacks using fabrication
  - Falsifying route errors
  - Broadcast falsified routes
- Spoofing attacks
- Rushing attacks

Data Forwarding Security

- Threats
  - Eavesdropping (passive attacks)
    - cryptography can help to prevent but how to detect eavesdropping is still an open research topic
  - Dropping data packets (similar to selfishness)
  - Selfish behavior on data forwarding
    - Drops other nodes' packets to preserve its resources, e.g. battery power

Detection Solution against Selfishness

- End-to-end feedbacks
- Monitoring in promiscuous mode (watchdog)
- Activity-based overhearing
- Mutually according admission in neighborhood
- Reputation based solution
- Probing

Preventive Solution against Selfishness

- Nuglets
  - Nodes who use the service must pay for it to nodes that provide the service
- Data dispersal
  - Adding redundancy to the messages to send; thus partial reception can lead to successful reconstruction of messages

Link Layer Security

- IEEE 802.11 MAC
  - Vulnerable to DoS attacks
  - Attacks can exploit its binary exponential backoff scheme to launch DoS
  - A security extension to 802.11 was proposed
    - Backoff time at the sender is provided by the receiver
- IEEE 802.11 WEP -discussed in wireless security

Key Management

- Most of the solutions for secure routing and data forwarding rely on cryptography
- Key management is problematic because of the lack of any central infrastructure
  - Private key infrastructure
  - Public key infrastructure

Bluetooth

- Consortium: Ericsson, Intel, IBM, Nokia, Toshiba…
- Scenarios:
  - connection of peripheral devices
    - loudspeaker, joystick, headset
  - support of ad-hoc networking
    - small devices, low-cost
  - bridging of networks
    - e.g., GSM via mobile phone - Bluetooth - laptop
- Simple, cheap, replacement of IrDA, low range, lower data rates, low-power
  - Worldwide operation: 2.4 GHz
  - Resistance to jamming and selective frequency fading:
    - FHSS over 79 channels (of 1MHz each), 1600hops/s
  - Coexistence of multiple piconets: like CDMA
  - Links: synchronous connections and asynchronous connectionless
  - Interoperability: protocol stack supporting TCP/IP, OBEX, SDP
  - Range: 10 meters, can be extended to 100 meters

Bluetooth Application Areas

- Data and voice access points
  - Real-time voice and data transmissions
- Cable replacement
  - Eliminates need for numerous cable attachments for connection
- Low cost < $5
- Ad hoc networking
  - Device with Bluetooth radio can establish connection with another when in range

Protocol Architecture

- Bluetooth is a layered protocol architecture
  - Core protocols
  - Cable replacement and telephony control protocols
  - Adopted protocols
- Core protocols
  - Radio
  - Baseband
  - Link manager protocol (LMP)
  - Logical link control and adaptation protocol (L2CAP)
  - Service discovery protocol (SDP)

Protocol Architecture cont'd

- Cable replacement protocol
  - RFCOMM
- Telephony control protocol
  - Telephony control specification – binary (TCS BIN)
- Adopted protocols
  - PPP
  - TCP/UDP/IP
  - OBEX
  - WAE/WAP

Usage Models

- File transfer
- Internet bridge
- LAN access
- Synchronization
- Three-in-one phone
- Headset

Piconets and Scatternets

- Piconet
  - Basic unit of Bluetooth networking
  - Master and one to seven slave devices
  - Master determines channel and phase
- Scatternet
  - Device in one piconet may exist as master or slave in another piconet
  - Allows many devices to share same area
  - Makes efficient use of bandwidth

Radio Specification

- Classes of transmitters
  - Class 1: Outputs 100 mW for maximum range
    - Power control mandatory
    - Provides greatest distance
  - Class 2: Outputs 2.4 mW at maximum
    - Power control optional
  - Class 3: Nominal output is 1 mW
    - Lowest power
- Frequency Hopping in Bluetooth
  - Provides resistance to interference and multipath effects
  - Provides a form of multiple access among co-located devices in different piconets

Frequency Hopping

- Total bandwidth divided into 1MHz physical channels
- FH occurs by jumping from one channel to another in pseudorandom sequence
- Hopping sequence shared with all devices on piconet
- Piconet access:
  - Bluetooth devices use time division duplex (TDD)
  - Access technique is TDMA
  - FH-TDD-TDMA

Physical Links

- Synchronous connection oriented (SCO)
  - Allocates fixed bandwidth between point-to-point connection of master and slave
  - Master maintains link using reserved slots
  - Master can support three simultaneous links
- Asynchronous connectionless (ACL)
  - Point-to-multipoint link between master and all slaves
  - Only single ACL link can exist

Channel Control

- Major states
  - Standby – default state
  - Connection – device connected
- Interim substates for adding new slaves
  - Page – device issued a page (used by master)
  - Page scan – device is listening for a page
  - Master response – master receives a page response from slave
  - Slave response – slave responds to a page from master
  - Inquiry – device has issued an inquiry for identity of devices within range
  - Inquiry scan – device is listening for an inquiry
  - Inquiry response – device receives an inquiry response

Inquiry Procedure

- Potential master identifies devices in range that wish to participate
  - Transmits ID packet with inquiry access code (IAC)
  - Occurs in Inquiry state
- Device receives inquiry
  - Enter Inquiry Response state
  - Returns FHS (Frequency Hop Synchrnonization) packet with address and timing information
  - Moves to page scan state

Page Procedure

- Master uses devices address to calculate a page frequency-hopping sequence
- Master pages with ID packet and device access code (DAC) of specific slave
- Slave responds with DAC ID packet
- Master responds with its FHS packet
- Slave confirms receipt with DAC ID
- Slaves moves to Connection state

Slave Connection State Modes

- Active – participates in piconet
  - Listens, transmits and receives packets
- Sniff – only listens on specified slots
- Hold – does not support ACL packets
  - Reduced power status
  - May still participate in SCO exchanges
- Park – does not participate on piconet
  - Still retained as part of piconet

Bluetooth Audio

- Voice encoding schemes:
  - Pulse code modulation (PCM)
  - Continuously variable slope delta (CVSD) modulation
- Choice of scheme made by link manager
  - Negotiates most appropriate scheme for application

Bluetooth Link Security

- Elements:
  - Authentication – verify claimed identity
  - Encryption – privacy
  - Key management and usage
- Security algorithm parameters:
  - Unit address
  - Secret authentication key (128 bits key)
  - Secret privacy key (4-128 bits secret key)
  - Random number

Link Management

- Manages master-slave radio link
- Security Service: authentication, encryption, and key distribution
- Clock synchronization
- Exchange station capability information
- Mode management:
  - switch master/slave role
  - change hold, sniff, park modes
  - QoS

Security Modes

- Bluetooth has three different security modes build in it
- **Security Mode 1:** A device will not initiate any security. A non-secure mode.
- **Security Mode 2:** A device does not initiate security procedures before channel establishment on logical link control and adaptation protocol (L2CAP) level. This mode allows different and flexible access policies for applications, especially running applications with different security requirements in parallel. A service level enforced security mode.
- **Security Mode 3:** A device initiates security procedures before the link set-up on low power mode (LPM) level is completed. A link level enforced security mode.

Initialization

- Needed before two secure devices can communicate. 5 parts:
  - Generation of initialization key
  - Authentication
  - Generation of link key
  - Link key exchange
  - Generation of encryption key in both devices.
- Conclusion: link is either built or aborted

Generation of initialization key

- Initialization key generation only occurs when two devices have not yet communicated before.
- Highest security demands PIN be entered by both users. Two devices with fixed pins cannot talk securely (mode 3).
- This key used to secure the process of generating a shared link key between the devices.

Authentication

- Does not always need to be mutual, specified by app
- If it is mutual, then both act as verifiers, one after the other
- Device A: verifier
- Device B: claimant
- Basically determines if both have same shared key (ACO generated at this time as well for encryption)

Generation of Link Key

- Unit key does not change, it was made when device was installed.
- Application decides which device will provide its unit key as a link key (favors the device with less memory).
- Shared initialization key is used to protect the transaction: it is XORed with the new link key.

Link Key Exchange

- After the unit key is stored on the other device, the initialization key is discarded.
- Higher security: combination key is used rather than the unit key, and this is formed by F(unit key, RAND, BD_ADDR) on both A and B.
- Master-slave communications use Master link key. A slave gets a master link key when first connected to Master and then changes it when prompted by Master

Encryption

- Encryption requires an authenticated link with an established link key
- Devices must agree on an encryption key to communicate.
- Packet payloads are encrypted (not the packet headers or access codes).
- Devices negotiate on what size Encryption key they need, typically around 64 bits. Range is 1-16 bytes.

Encryption Modes

- Encryption Mode depends on the shared key:
- If unit or combination key, then point-to-multipoint traffic is not encrypted. Individual traffic may or may not be encrypted (app specific)
- If a master key is used, there are three possible modes:
- Mode 1, nothing is encrypted.
- Mode 2, broadcast traffic is not encrypted, but the individually addressed traffic is encrypted with the master key.
- Mode 3, all traffic is encrypted with the master key.

General Problems

- Device versus User authentication. Bluetooth authenticates devices, not users. This is not always appropriate. Depends on app-specific fixes.
- Device versus Service specific security. You must implement the same security policy (mode) on all services on the device.
- Dependence on addresses, shared keys. Fixed PINs also pose a problem.
- Legacy applications do not use the Service Manager (need adapter kits).
- Cannot enforce unidirectional traffic
- Once connection established, assumed permanently secure. (unless called by Master to renegotiate, which rarely occurs in most implementations.)