Introduction to the IEEE 802.15.3 Security Architecture

by Ari Singer

Principal Engineer, NTRU

March 19, 2002

Outline

- Background

- Security Context

- Security Architecture

Relevance to GSEC

- Security architecture based on a group security model
- Instantiation of protocols implementing group security
- Current IEEE standardization effort
- Architecture approved by working group last week

What is IEEE 802.15.3?

- High-speed wireless personal area network (WPAN) standard
- Ad hoc network standard similar to Bluetooth
- Specifies MAC/PHY layers only
- Focus on power management, quality of service and security

802.15.3 Characteristics

- Star network topology
- Maximum of about 250 devices per piconet
- High bandwidth (~55 Mbps)
- Short range (~10m)
- Low power consumption
- Low cost

Outline

- Background
- Security Context
- Security Architecture

Environment

- Ad hoc networking – devices may or may not have ever met before
- No connection to external networks assumed
- Assumed that devices external to the network can both eavesdrop and transmit data

Security Goals

- Only authorized devices may join a secure piconet
- Communication between identified parties only

Security Services

- Trust establishment
- Authentication of devices
- Key management
- Freshness protection
- Integrity protection on commands
- Privacy and integrity protection on data transmissions

Security Services Not Required

- Denial of service protection
- Individual source authentication on group messages
- Traffic analysis protection

Roles

- Piconet controller (PNC) controls use of piconet resources
- PNC acts as security manager (or GCKS) for piconet-wide security associations (SAs)
- Other devices are group members
- PNC role may be handed over
- Devices may establish peer-to-peer SAs

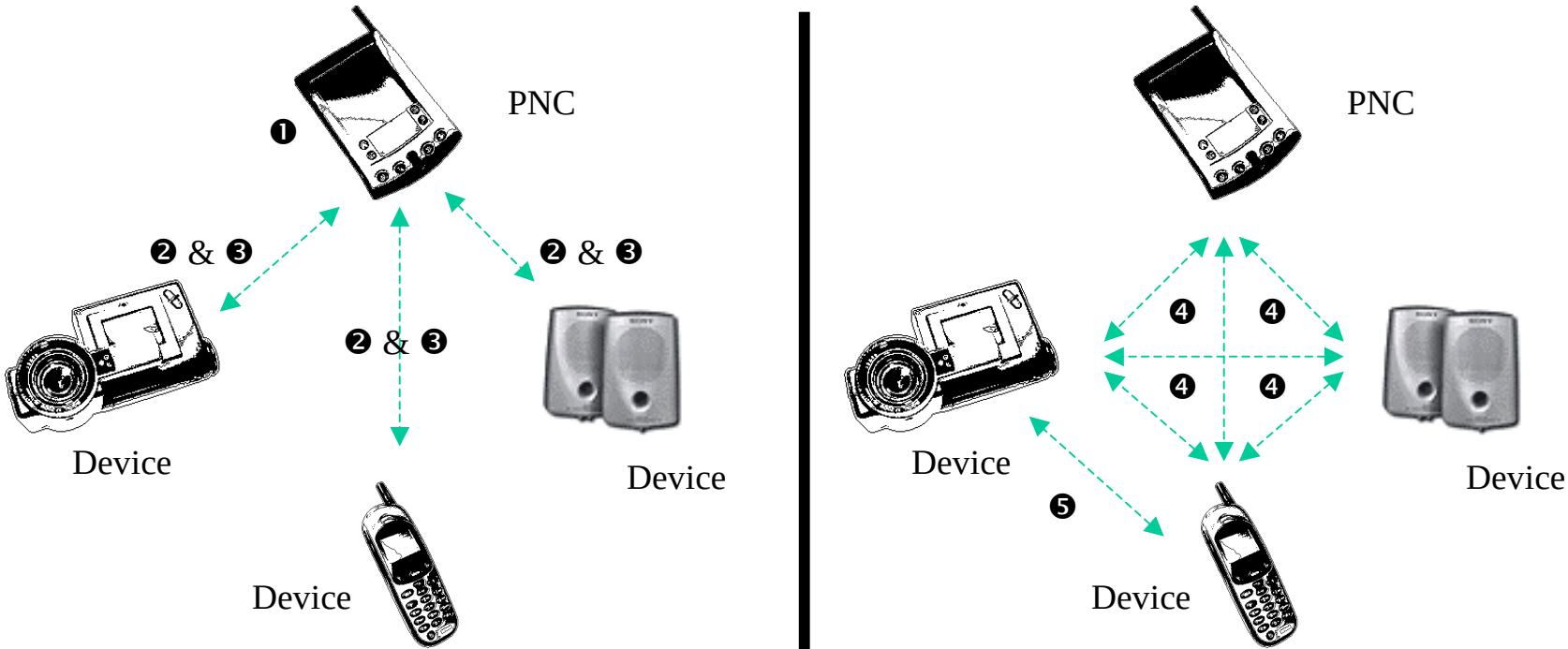
Layer Management

- Upper layers define trust relationships (e.g. of public keys) with other devices
- Upper layers set policies for participating in the piconet
- MAC/PHY implements authentication protocols and symmetric-key management
- MAC/PHY implements command and data payload protection

Outline

- Background
- Security Context
- Security Architecture

How does 802.15.3 work?



❶Devices determine which device is best suited to be piconet controller (PNC) and agree on it.

❷Each device requests to join the piconet and performs mutual authentication with the controller.

❸The controller establishes time slots for each device and distributes piconet payload protection keys.

❹Devices transmit protected data to the other devices in the piconet during their time slots.

❺Two devices may optionally establish their own secure sub-network.

Trust Establishment

- MAC/PHY layer has access to its own public/private key pair
- Higher layer provides mechanism for MAC/PHY to determine trust for other devices' public keys

Authentication of Devices

- Each device performs a public-key mutual authentication protocol with the PNC
- Authentication results in an SA between the PNC and the device
- Authentication protocol similar to TLS handshake

Key Management (1)

- Two-party SAs are established through authentication protocol
- PNC transmits group keys to each device separately encrypted and integrity protected with their shared two-party SA
- If PNC role changes, the security manager role changes and each device must authenticate with the new PNC

Key Management (2)

- Group keys are changed whenever a device joins or leaves the piconet
- If a device determines it does not have the current key, it requests the key from the PNC

Freshness Protection

- PNC transmits a “beacon” for piconet synchronization including a freshness counter
- Beacon protected with a symmetric MAC using the group integrity key
- Commands and data frames include the freshness counter and include a MAC

Beacon Header	Current SSID	Time Token	Integrity Code

Protection on Commands

- Command integrity protected by MAC
  - Group key used for general commands
  - Peer key used for commands to and from PNC
- Freshness token and source/destination included in all command
- Unique counter included for peer SAs

Command Header	Current SSID	Time Token	Counter	IV	Encrypted Command Data	Integrity Code

Protection on Data

- Data encrypted and integrity protected by group encryption and MAC keys
- Freshness token and source/destination included in all data transmissions

Data Header	Current SSID	Time Token	IV	Encrypted Data	Integrity Code

Contact Information

Ari Singer

Principal Engineer, NTRU

asinger@ntru.com

http://www.ieee802.org/15/pub/TG3.html