Role of IPv6 to Secure Wireless Sensor

Kevin Cheng
IPv6 Summit in Taiwan 2004
Outline

• Benefits from IPv6
• IPv6 IPSec Routers
• Wireless Sensors
• Security for Sensor Networks
• IPv6 Security
• Wireless Sensors with IPv6
• Secure Sensors with IPv6
Benefits from IPv6

• Bigger address space – plenty.
• Support for mobile devices – friendly roaming, Mobile IP.
• Built-in security – IPSec, Neighbor Discovery, autoconfiguration.
• Emerging new applications – services, monitoring, P2P, etc.
IPv6 IPSec Routers

- 6WIND
- FreeBSD/KAME (www.kame.net)
  Fujitsu, Hitachi, NEC, Yahama, Toshiba, etc.
- IOS – Cisco IPv6 Router
- JUNOS – Juniper Networks
- OpenBSD/ISAKMPD - Our AWG-60 that supports Wireless
- ...
Wireless IPv6 IPSec Router (AWG60)

The **AWG60** facilitates IPSec-based VPN-over-broadband with next generation Internet Protocol version 6 (IPv6) infrastructure solutions. It is capable of fulfilling future demands on *address space, encryption, authentication, and mobility*. This allows full, unconstrained IP connectivity for today's IP-based machines as well as upcoming mobile devices like PDAs and wireless phones – all will benefit from full IP access through GPRS and UMTS.

**Key features include:**
- AES, DES, 3DES encryption
- Both IPv4 and IPv6 IPSec tunnels, IKE/ISAKMP protocols. Configurable site-to-site or site-to-clients VPN.
- VLAN Technology
- Dynamic routing performance
- Security policies can be set on a per-host or per-network basis, not per application/service.
- BGP4
- RIP, RIP2, RIPng
- OSPF (v4/v6)
- Single Sign-On with external authentication servers (Kerberos, LDAP, and RADIUS)
- OS fingerprinting with packet frame captured to small footprint database
- Comprehensive firewall for wired and wireless subnets
- QoS (packet shaping functions)
- SSH remote configuration, console mode.
Wireless IPv6 IPSec Router (AWG60)
### Wireless Sensors - Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Application Focus</th>
<th>Success Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZigBee 802.15.4</td>
<td>Remote control, battery-operated products, sensors</td>
<td>Reliable, secure networking Protocol simplicity Low power consumption, low cost</td>
</tr>
<tr>
<td>Bluetooth 802.15.1</td>
<td>Interoperability, cable replacement, wireless, USB, handset, headset</td>
<td>Low incremental cost Ease of use / convenience Moderate data rate</td>
</tr>
<tr>
<td>Wi-Fi 802.11</td>
<td>Web, email, P2P, PC networking, file transfers, and video</td>
<td>High data throughput Flexibility (work and home) Hot Spot connectivity</td>
</tr>
<tr>
<td>GPRS / GSM 1XRTT/C DMA</td>
<td>Wireless voice and data</td>
<td>Broad geographic coverage Datacentric pricing plans Network build-out</td>
</tr>
<tr>
<td>System resource</td>
<td>Battery life (days)</td>
<td>Nodes per network</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>ZigBee</td>
<td>4-32 KB</td>
<td>100-1,000+</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>250 KB+</td>
<td>1-7</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>1 MB ±</td>
<td>0.1-5</td>
</tr>
<tr>
<td>GPRS/GSM</td>
<td>16 MB+</td>
<td>1-7</td>
</tr>
</tbody>
</table>
Microcontroller for Sensors

- Applications: AV equipment, sensor, Home appliances.
- Memory: 512KB ROM with 20-64KB RAM.
- CPU: RISC/32bits (< 20Mhz) with 8-16 MPU optimizations is necessary to squeeze IPv6 into such small ROM
- Functions and Security become optional features
Sensors Networking

- Query for required data in sensor network involves lot of communication, which is power consuming for sensor motes. Also sensor motes are subject to failure for different reasons. How can we ensure availability of required data to application with minimum power consumption?
  - Create an abstraction between sensor network and application
  - Provide energy efficient access method to required data using contacts/look-ahead
  - Hide possible failures and vulnerability of sensor motes from application
  - Develop distributed resource management to ensure fault tolerance
Case Study: Generic Prognostic Module Components

- Sensor Features (Raw Data, Diagnostic Features, etc.)
- Knowledge-base Features (Mission Plans, Failure Rates, etc.)
- History Data (Past Predictions, Operations Profiles, etc.)

Generic Prognostics Algorithm

- Evolutionary-Based Prognostics
- Model-Based Prognostics

Probabilistic Update Process

Health Predictions (RUL, Confidence, Readiness, etc.)
Secure Wireless Sensors

• Security mechanisms: depends on network applications and environmental conditions.
• Resources of sensor nodes (CPU, memory, battery) make it impractical to use secure algorithms designed for powerful workstations.
• Standard security: availability, confidentiality, integrity, authentication, and non-repudiation
• Wireless sensors: message freshness, intrusion detection, intrusion tolerance, or containment exists.
• Security policies defined by admin of sensor nodes. Define the system architecture and the trust requirements.
• SPINS: Security protocols for sensor networks.
• 802.15.4/ZigBee with 128-bit AES encryption.
IPv6 to support Microcontroller

- **Micro IPv6**: routing and security features are optional
- **Low Cost Network Appliances (LCNA)** from TACA ([www.taca.jp](http://www.taca.jp)) for sensors.
- **Embedded IPv6**
- **NanoIP** ([www.cwc.oulu.fi](http://www.cwc.oulu.fi)): a minimal networking protocol for use with highly limited devices.
Wireless Sensors with IPv6

• Ambient intelligence for everywhere: smart sensors, transducers and measuring instruments are IPv6 enabled.
• Provide application services: powerful MCU for sensor with IPv6 that is “NATless”
• Plug-and-Play: IPv6’s address autoconfiguration and anycast address support for a large-scale sensor networks.
• Security:end-to-end IPSec over IPv6
• Mobile IP.
• Extensibility and Standardization: IPv6 is flexible to extend it’s headers and options.
• ad hoc nets: self organizing, cheap devices, mems-based sensors, energy storage limitations, benefit from IPv6.
Security Threads for Wireless Sensors

- Digital signatures for authentication are impractical for sensor networks: improved by SPINS and µTESLA (the micro version of the Timed, Efficient, Streaming, Loss-tolerant Authentication protocol)
- Assume individual sensors are untrusted, compromising the base station can render the entire sensor network to be useless.
- Insertion of malicious code – spread to all nodes
- Interception of the messages containing the physical locations of sensor nodes allows an attacker to locate the nodes and destroy them.
- An adversary can observe the application specific content of messages including message IDs, time stamps and other fields.
- Inject false messages that give incorrect information about the environment to the user.
- Inter-router authentication prior to the exchange of network control information
- Spoofed, altered, or replayed routing information
- Selective forwarding
- Sinkhole attacks
- Sybil attacks
- Wormholes
- Denial of Service (DoS), such as HELLO flood attacks
- Acknowledgement spoofing
IPv6 Security

- IPv6 Extension Headers that support IPSec, but with limitations such as weak DES algorithm, complex configuration, DoS, etc.
- It inherits similar vulnerabilities as IPv4.
- New features such as neighbor discovery, router discovery, autoconfiguration and renumbering of IPv6 nodes, MTU, DHCPv6 and DNS
Sensor Network driven by IPv6

- SensIT (DARPA): combine multiple microsensors, embedded processors, positioning ability, and wireless communication. 3 classes of information chosen for use in the system are detection data, sensor node location information, and tracking results.
- ESPv3 – for Low Cost Network Appliances (LCNA)
- Smart-dust motes (Berkeley): Autonomous sensing and communication in a cubic millimeter, apply to battlefield sensor networks, sensor mine-fields, burrs and fleas, traffic mapping, captured terrain surveillance, bunker mapping.
- Auto-ID Object Name Service (ONS): the military use tags that would carry a unique Internet Protocol address, which points to a specific location where information on that product would be stored.
- Radio Free Intel (Intel Deep Network projects): vision of adding wireless capabilities to every device by integrating the radio circuits and systems directly into every component
- m2m (machine 2 machine) communication: 50 billion machines, only 6 billion humans (Forrester, cited in International Herald Tribune oct14th)
Objectives support Sensor Networks with IPv6

- Nodes in large-scale ad hoc networks have different computing & communication capabilities, and mobility patterns.
- Provide efficient resource discovery in highly dynamic ad hoc networks (e.g., discovery of capabilities, multicast sessions and membership information – Scalability, Robustness, Self-organization, Energy consumption, Performance, Load balancing, Replication)
- Strict adherence to the IPv6 RFCs
- Be as highly portable and configurable to dual stack with IPv4
- Efficient code that has a small memory footprint
- High throughput
Mobile Agents in Sensor Networks

• **What is mobile agents?**
  - Small piece of intelligent code
  - Able to change behavior with applications need
  - Adapts to changing conditions of the sensor network
  - Smart replication enhances system robustness
  - Fits nicely with existing and new frameworks for Sensor Net
    - With Tiny OS and Maté (VM for TOS)
    - With limited memory constrains of motes

• **Some experimental works:**
  - Mobile IPv6 – using KAME kernel
  - Ad hoc routing protocol for sensor mote – beacon based
  - TCP performance analysis on multi-hop ad hoc routing protocols
  - Wireless signal strength analysis
  - TCP characteristics and performance analysis for both wired and wireless networks
  - Dynamic routing protocols – using Zebra package
  - Performance analysis of different queuing disciplines – using ALTQ kernel
  - Packages for testbed – Netperf, tcptrace, Zebra, ALTQ, TinyOS etc.
Secure Sensors with IPv6

- **Security still a work in progress.**
- Clock accuracy - less power battery v.s. time sensitive algorithms (Kerberos, SA, IKE).
- TinySec (Berkeley): a link layer encryption mechanism for tiny devices and is tightly coupled with the TinyOS radio stack.
- RFID tag to secure communication with the server, where every single object in commerce and the supply chain is allocated its own unique RFID tag and Electronic Product Code (EPC).
- Lightweight security is effective - most data is only valid for a short time.
- Security chips - Hitachi
- Workaround: put sensors behind a proxy, if lacks of any hardwares to support encryption.