

# Security Services in WPAN

Venkata Koonaparaju  
Ramaseshan Iyengar

## **Introduction**

A new network paradigm concerning *a short-range wireless connectivity* attracts researchers and industrial attention in the last few years. Wireless personal area networks (WPANs) presents the person centered network concept, which allows a person to move, surrounded by its personal space (PS) and devices, and to communicate with them and through them with the outside world. The coverage area of WPAN is in the range of 10m radiuses. Bluetooth radio system has emerged as the first technology addressing WPAN applications with its salient features of low power consumption, small package size and low cost. Bluetooth adopts master-slave architecture to form an ad hoc wireless network named piconet. A master in a piconet may communicate with up to seven active slaves. Several connected piconets can further form a scatternet

The proposed work for this project is to make an extensive literature survey in security architecture shown below for WPANs.

- **Component Initialization**

- Protocols for manual authentication: MANA – I, II, III.
  - Imprinting for Symmetric System.
  - Imprinting for Public Key System.

- **WPAN Communication Security**

- Analysis of Existing Solutions
    - Link Layer Solution
    - Limitations of Layer 2 Security
    - Network Layer Solution.

- Ideal Link Layer Solution

- Authentication And Initial Key Generation.
    - Identity Privacy.
    - Key Management.
    - Key Derivation.
    - Confidentiality.
    - Integrity.

- Identification and Location Privacy

- **Policies and Access Control**

WPAN Security Domain Specification

- PSD controller
- Resource Sharing Using a PSD.
- Advantages of PSD.

Access Control Using Public Key And Symmetric Key Methods

- Public Key Based Systems
- Secret Key Based System

Methods For Access Control

- Objects Under Access Control
- Secret Key Based Methods
- Public Key Based Methods

- **Recommendations for Security Services and some examples of the security architecture.**

### **Schedule**

October 15 <sup>th</sup>	First Progress Report - Understanding “Bluetooth” in WPANs
October 29 <sup>th</sup>	Second Progress Report – Comprehensive study of Security Mechanisms in WPANs
November 12 <sup>th</sup>	Third Progress Report – Complete evaluation of Security Protocols And Recommendations
December 3 <sup>rd</sup>	Final Draft Report
December 6 <sup>th</sup>	Final project report submission.
December 12 <sup>th</sup>	Final Project Presentation (Oral Presentation).

### **Proposed Changes in future**

WPAN applications span a wide variety of authentication needs and devices associated with WPAN applications may have very limited user interfaces and no connection to external certification resources. There is no way to completely address all possible scenarios here, but the primary goal is that the user of the WPAN be able to control piconet access. Depending on the availability of time and resources, we might extend the scope of this project to cover as many security scenarios as possible.

## References:

- 1 **Bluetooth - One of the Best WPAN Solutions for Bridging PAN and Wider Networks?**  
[http://www.hurray.isep.ipp.pt/rtlia2002/full\\_papers/16\\_rtlia.pdf](http://www.hurray.isep.ipp.pt/rtlia2002/full_papers/16_rtlia.pdf)
- 2 **Wireless Personal Area Networking Systems: A Comparison of Bluetooth, IrDA Data and HomeRF.**  
<http://www.bluetoothforum.org.cn/college/wireless%20PAN%20systems%20comparison%20of%20bluetooth%20IrDA%20data%20and%20HomeRF.pdf>
- 3 **Case Study of Wireless Personal Area Network Security: Bluetooth security**  
<http://www.people.virginia.edu/~yy6m/project.pdf>
- 4 **Research Challenges for Wireless Personal Area Networks**  
<http://www.eng.ukm.my/~micc2001/html/prasad.pdf>
- 5 **Design, Implementation, And Evaluation Of Bluetooth Security**  
<http://www.mediateam oulu.fi/publications/pdf/87.pdf>
- 6 **Bluetooth - Technology, Security and Weaknesses**  
[http://www.datensicherheit.nrw.de/Daten/co020716/abstracts/abstract\\_bernhard\\_loehlein.pdf](http://www.datensicherheit.nrw.de/Daten/co020716/abstracts/abstract_bernhard_loehlein.pdf)
- 7 **Introduction to the IEEE 802.15.3 Security Architecture** by Ari Singer, Principal engineer, NTRU.
- 8 **Guide To Wireless Personal Area Networks White paper**  
<http://www.intermec.com/>.
- 9 **Path Toward Next Generation Wireless Internet – Cellular Mobile 4G, WLAN/WPAN and IPV6 Backbone** by Ying Li, Shihbua Zhu, Pinyi Ren and Gang Hu.
- 10 **Mobile Security Overview White Paper**  
<http://www.hp.com/mobile>  
<http://www.hp.com/security>.
- 11 **Detailed technical specification of distributed mobile terminal system security** by ATEA, Ericsson, Nokia, Siemens AG, T-Nova and Vodafone at Information Society Technologies.  
<http://www.isrc.rhul.ac.uk/shaman/docs/d10v1.pdf>