# PROTECTION IN WIRELESS NETWORKING – CONCERN AND CHALLENGES

*International Journal of Information Technology and Management*

*Vol. VII, Issue No. IX, August-2014, ISSN 2249-4510*

# Protection in Wireless Networking – Concern and Challenges

**Rashmi Kumari[1] Pushkar Raj[2]**

[1]Assistant Professor, S. Sinha College Aurangabad Bihar

[2]Assistant Professor, N.S.I.T Bihta Patna Bihar

***Abstract – Computer system security has become a major concern over the past few years. Attack, threat or intrusions, against computer system and network have become commonplace events, many system device and other tools are available to help counter the threat of these attack. Wireless and mobile networks are quickly becoming the networks of choice, not only because of large bandwidth, but due to the flexibility and freedom they offer. Option way out to the trouble of accessing information in remote areas where wired network are inaccessible is offered by Wireless Networking Technology. In this paper we have tried to discuss two latest wireless technologies: Wi-Fi. The objective in this paper is to describe the technologies as well as the benefits and risks involved in their security implementation.***

***Keywords: Wi-Fi, Wireless Security, Protection, Network Wireless Profit, Connectivity***

---------------------------♦-----------------------------

## INTRODUCTION

### Wireless Networks

This hallucination of embeddable wireless connectivity has been in development for several years at AT&T Laboratories Cambridge in the context of the Piconet [6] project and is also being pursued, although with emphasis on different aspects, by several other groups including HomeRF [2,4], IrDA [1] (which uses infrared instead of radio) and Bluetooth [5,3]. Everyone including potential users knows that wireless networking is more prone to passive eavesdropping attacks. But it would be highly misleading to take this as the only, or even the main, security concern. In this paper we investigate the security issues of an environment characterized by the presence of many principals acting as network peers in intermittent contact with each other. To base the discussion on a concrete example we shall consider a wireless temperature sensor. Nearby nodes may be authorized to request the current temperature, or to register a \watch" that will cause the thermometer to send out a reading when the temperature enters a septic range Issues in accessing several different wireless networks.

| Issue | Possible Solutions |
|---|---|
| Ways to access several different networks | 1. Use of multifunction devices |
| | 2. Use of an overlay network |
| | 3. Use of common access protocol |
| Type of handoff | 1.Allow user to access one network at a time (Hard handoff) |
| | 2.Allow user to access more than one network at a time (Soft handoff) |
| Handoff detection (how to decide when | 1. Continuous monitoring of Signal-to-Noise ratio |
| one wireless network is not available and | 2. Monitoring of delay |
| start using other one) | |
| Location coordination among networks | 1. Use of a centralized location database and local database for every |
| | network |
| | 2. Location updating by broadcasting/paging when necessary |
| Adding new users (no longer depends on | Network interaction problem (difficult to find out how much traffic will |
| one network as adding new users will | be increased on other networks by adding a user to one network) |
| affect several networks) | |
| Adding new services (multicasting and | 1. Development of minimum capability set |
| other emerging services and features) | 2. Hardware/software/implementation compatibility |
| | 3. New econometric models to divide revenue among multiple networks |
| Access and bandwidth allocation | 1. Dynamic bandwidth division among single and multiple-network users |
| | 2. Dynamic bandwidth division among native and guest users |
| | 3. Resource allocation to high priority users |
| Addressing | 1. Network specific |
| | 2. Uniform |
| | 3. Logical (using mapping) |
| | 4. One number |
| Effect on upper layer protocols | Adaptation required during handoff or delayed access to a new network |
| Security | 1.Verification with a home location register |
| | 2. Single name, password to access different networks |
| Failure and backup | 1. Internal controller in a device constantly monitoring for continued availability to networks |
| | 2. Intelligent interworking device to notify user in case of |
| | network failure |
| Network independence (so a user may be | 1. Common interface by using mobile middleware |
| unaware of the underlying physical network) | 2.Adaptive application to adjust to change in network characteristics |
| Regulation | 1. New regulation may be required on how and what information may be |
| | exchanged between different wireless networks |
| | 2.Wireless carriers may be required to provide FCC with data on failure |
| | and loss of access |
| Pricing issues | 1. New models for dividing revenues among different wireless networks |
| | (using total time a user was connected, number of packets/bytes |
| | transmitted, and total overhead caused) |
| | 2. Single bill (flat pricing, usage-sensitive pricing, pricing based on QOS |
| | delivered, pricing using guest and native networks) |

An overlay network consisting of several Universal Access Points (UAPs). These access points choose a wireless network for the user based on availability, QOS-specified, and user-specified choices. A UAP performs protocol and frequency translation, and content adaptation. By using an overlay network, the handoffs are not performed by the user or the device but by the overlay network as the user moves from one UAP to the other. UAP stores user, network, and device information/capabilities and preferences. This architecture will support single billing and single subscription for users as UAPs can keep track of various resources that have been used by a user.

Accessing several wireless networks using the Common Access Protocol. This architecture can be used if wireless networks can support one or two standard access protocols, and requires interworking between different networks. One possible way to support this architecture is to use wireless ATM, meaning every wireless network must allow the transmission of ATM cells with additional headers (or WATM cells) requiring changes in the wireless networks.

## EMERGING MOBILE AND WIRELESS NETWORKS

Mobile and wireless networks are also experiencing significant progress in the form of wireless local area networks (WLANs) [7], satellite-based networks [8], Wireless Local Loops (WLL) [9], mobile Inter- net Protocol (IP) [10], and wireless Asynchronous Transfer Mode (ATM) networks [11, 12]. A compar- ison is shown in Table 2. One emerging wireless technology is Bluetooth (www.bluetooth.net), which provides low-cost and short-range radio links for wireless connectivity among computers, printers, and scanners. Since the range is small, it can use the unlicensed ISM band in 2.4GHz.

## SECURITY CHALLENGES FOR WIRELESS SENSOR NETWORKS

Wireless sensor networks processing sensitive data are facing the risks of data manipulation, data fraud and sensor destruction or replacement. This concerns applications such as the gathering of data on environmental pollution around industrial installations, or sensor systems replacing traditional video monitoring. Large-scale deployment in practice is conditioned by solving these kinds of security problem and reducing the risks due to limited physical protection of the devices and openness of the wireless communication channel.

Mobile and wireless networks represent the next wave of networking because of their value in assisting an emerging mobile labor force in a growing information-oriented society. However, mobile and wireless networks also present many challenges to application, hardware, software, and network designers and implementers. During the past five years, research has focused on methodically alleviating the limitations of wireless and mobile environment. For example, several optimizations have been introduced to improve the performance of TCP/IP to make it work in slow, failure-prone, and limited bandwidth wireless networks. in addition, proxy servers have been used to improve the performance of application-specific programs (Web browsers, file systems, database servers, and so forth) and mobile users. Over the next five years, research on enabling architectures for mobile client/proxy/servers, mobile agents, and detached users will be carried out. In addition, data-centric models such as mobile and location-sensitive queries, mobile dealings, and mobile workflows are also recognized as important emerging research areas.

In the near future, worldwide devices that can access the closest/best quality/cheapest wireless network out of several choices will be urbanized. Wireless net- works will be able to implement a uniform addressing system in which a person has a consistent identifying number or network address that is moveable across all wireless networks. Within two to three years, these networks will compete with "wired" networks for applications with low to medium bandwidth supplies. However, with greater than before frequency allocations, advances in semiconductor technology, and more efficient coding of information over wireless channels, mobile and wireless networks will become the net- works of choice for the majority users and applications.

While modern cryptography and computer security offer many ways of solving these problems, they are focused on solutions for high-performance devices, and not for computationally weak sensors with limited communication bandwidth. New 'lightweight' solutions tailored for the special needs of wireless sensor networks have to be designed

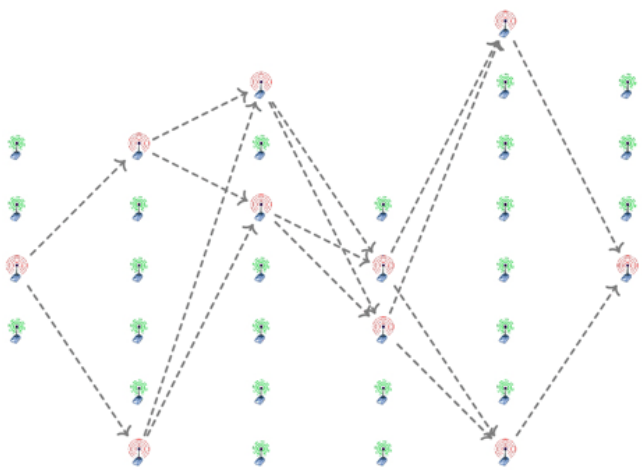

Fig - Snapshot of a single routing path.

## CONCLUSIONS

Wireless networks not only enable more efficient, scalable, and reliable wireless services but also provides wider variety of services. These opportunities come with a need for rethinking our security, privacy, architect and billing technologies have been used for previous generations. We believe, however, that future research will overcome these challenges and integrate newly developed services to new generation networks making them available to everyone, anytime and everywhere.

## REFERENCES:


1. Infrared Data Association. http://www.irda.org/.

2. Home RF Working Group. http://www.homerf.org/.

3. Jaap Haartsen, Mahmoud Naghshineh, Jon Inouye, Olaf J. Joeressen, and Warren Allen. Bluetooth: Visions, goals, and architecture. ACM Mobile Computing and Communications Review, 2(4):38{45, October 1998.

4. Kevin J. Negus, John Waters, Jean Tourrilhes, Chris Romans, Jim Lansford, and Stephen Hui. Home RF and SWAP: Wireless networking for the connected home. ACM Mobile Computing and Communications Review, 2(4):28{37, October 1998.

5. Bluetooth SIG. http://www.bluetooth.com/

6. Frazer Bennett, David Clarke, Joseph B. Evans, Andy Hopper, Alan Jones, and David Leask. Piconet: Embedded mobile networking. IEEE Personal Communications, 4(5):8{15, October 1997.

7. LaMaire, R.O., Krishna, A., and Bhagwat, P. Wireless LAN and mobile networking: Standards and future directions. IEEE Communications Magazine (Aug. 1996).

8. Miller, B. Satellites free the mobile phone. IEEE Spectrum (Mar. 1998).

9. Noerpel, A.R., and Lin, Y.-B. Wireless Local Loop: Architecture, technologies, and services. IEEE Personal Communications Magazine (June 1998).

10. Perkins, C.E. Mobile IP. IEEE Communications Magazine (May 1997).

11. Raychaudhuri, D. and Wilson, N.D. ATM-based transport architecture for multiservice wireless personal communication networks. IEEE Journal on Selected Areas in Communications (Oct. 1994).

12. Varshney, U. Supporting mobile computing using wireless ATM. IEEE Computer (Jan. 1997).

13. http://ercim-news.ercim.eu/en76/special/security-challenges-for-wireless-sensor-networks-dynamic-routing-as-a-security-paradigm