

# Information Assurance in Wireless Networks<sup>1</sup>

Joseph Kabara, Prashant Krishnamurthy, David Tipper

Department of Information Science and Telecommunications  
University of Pittsburgh  
135 N Bellefield Ave, Pittsburgh, PA 15260, USA

*Overview: Emerging wireless networks will contain a hybrid infrastructure based on fixed, mobile and ad-hoc topologies and technologies. In such a dynamic architecture, we define information assurance as the provisions for both information security and information availability. The implications of this definition are that the wireless network architecture must (a) provide sufficient security measures, (b) be survivable under node or link attack or failure and (c) be designed such that sufficient capacity remains for all critical services (and preferably most other services) in the event of attack or component failure. We have begun a research project to investigate the provision of information assurance for wireless networks viz. survivability, security and availability and here discuss the issues and challenges therein.*

## I. Introduction

The increasing reliance on wireless networks for information exchange makes it critical to maintain reliable and secure communications even in the wake of a component failure or security breach. Wireless access networks contain unique aspects that make survivability and security different than wired networks and particularly challenging. As an example, the broadcast nature of wireless communication links makes them unique in their vulnerability to security attacks and their susceptibility to unintentional damage. Additionally, in wireless networks, mobile nodes continuously enter and leave the network and change locations with the resulting mobility impacting the degree of survivability, security and communications reliability. Such unique features of wireless access networks result in limited applicability of standard survivability and security techniques developed for wired networks. Additionally, no single wireless technology is capable of supporting all the various application requirements such as coverage, bit rates, error rates, mobility, etc. and therefore the evolutionary trend is towards a mixture of various technologies that must interoperate to provide the required services [Pah00]. As an example, a wireless LAN may be employed for local coverage, low mobility and high data rates while an overlaying cellular network is used for wide area coverage, high mobility, but low data rates.

A general architecture for future wireless access networks is a hybrid of technologies that together create an infrastructure based topology with interconnecting fixed base stations (or access points) and a cellular architecture as shown in Figure 1. A wired infrastructure consisting of switches, routers and mobility management units exists to *support* the operation of the wireless network. A future wireless communications network will have many of the following elements: terrestrial cellular/PCS, high capacity links (wired or fixed point-point radio), programmable multi-band multimode radios, and high-speed WLANs connected either through an infrastructure or operating in an ad hoc fashion (communicating between peer entities). The devices consuming or supplying information range from high power servers, to desktops, laptops, handheld computers, PDAs, cellular phones and smart sensor devices. As locations of mobile nodes (MNs) change the MNs will enter and leave macro and microcells, accessing the network at various points of attachment (base stations BSs and access points APs). The technology used to access the network and the patterns of connectivity and disconnections will vary widely and yet must happen seamlessly. Horizontal handoffs must occur both between points of attachment of the same technology and vertical handoffs between different types of points of attachment [Pah00]. Protocols required to manage this seamless mobility of MNs will be susceptible to failures and security attacks if they are not designed properly. This paper discusses current implementations and drawbacks of the survivability and security in hybrid wireless access networks.

---

<sup>1</sup> The work is supported in part by the University of Pittsburgh CRDF program and DARPA F30602-97-1-0257

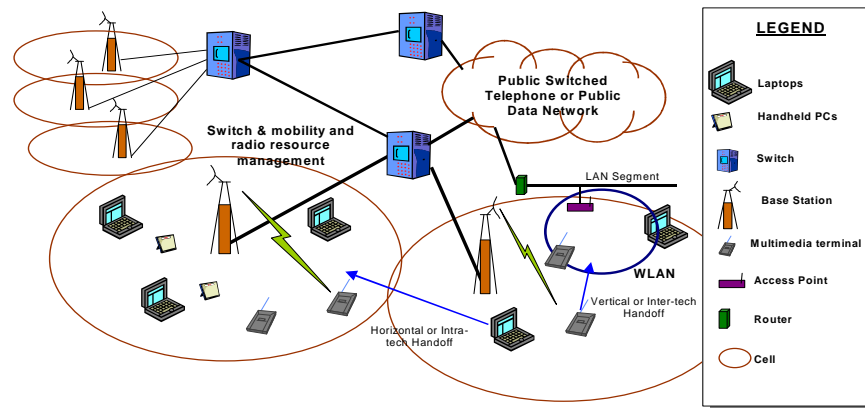


Figure 1: A hybrid wireless access network architecture

## II. Information Assurance and Wireless Specific Issues

*Information assurance* comprises the provisions for information availability via network survivability and information security. Information availability mechanisms compensate for failures in the network that result from either intentional attacks or accidental breakdown. Typically, additional capacity is allocated in critical network sections and protocols are established to automatically maintain communication and information flow. The network topology and capacity must be designed so that in the event of component failure or attack, sufficient capacity remains for automatic network reconfiguration to continue providing critical services at the minimum and other services, to the extent possible.

In a wireless network, several operational aspects exist that do not occur in a wired network, specifically, *location management*, *mobility management* and *radio resource management*. All three management procedures play an important role in providing seamless mobility. The primary objectives of resource management have been to maximize the available capacity at a radio-level and to allocate this capacity in a way to meet QoS guarantees. While resource management is addressed in terms of standards, benchmarks, network architectures and protocols little work exists that addresses wireless access network performance in the wake of failures, or considers survivability and information assurance in the network design/architecture. Failure or breach of these management protocols and databases can be disastrous to network operation in that the effects may not be limited to single users or single cells, but may cause resource misallocation through large parts or even the entire network.

### II.I. Wireless Network Survivability

Network survivability focuses on three basic issues: (1) understanding system functionality in the wake of failures, (2) minimizing the impact of failures on the user and (3) providing the means for the network to automatically overcome failures. The goal is to design the restoration protocols and network so that service can be maintained, at reasonable cost, during and after a failure.

Recently attention to the problem of the survivability of wireless access networks has focused primarily on database survivability for the cellular network databases (i.e., HLR, VLR, etc.) [Nev97], [Chang98]. This work developed checkpoint algorithms and authentication techniques for the fault recovery of database content. In [AL98] the design of a survivable landline topology was discussed using a mixture of a linear integer-programming model of a single link failure survivable mesh-topology and capacity allocation design. This paper is one of the first to mention the topic of survivable wireless access network design, however the approach and assumptions were identical to techniques used for wired backbone network design. The model incorporates none of the unique aspects of wireless networks.

Survivability approaches for wired networks, are not entirely applicable to the mobile domain. In wired networks, the number of physical cables and their interconnection configuration influences system capacity. Diversity techniques often add spare capacity by adding of physical

cables and are therefore primarily subject to cost constraints. In contrast, in the mobile domain the radio channel capacity is not static and is influenced by changing network conditions due to environmental factors, and co-channel interference. In wireless access networks diversity techniques are constrained by both cost and a *regulated* frequency spectrum. Unlike wired networks duplicating the medium is impossible. Spectrum is a non-expandable resource and allocating spare capacity is much more difficult than in wired networks. Existing approaches for network survivability do not account for the mobility and radio resource management. In wireless access networks, *user mobility worsens transient conditions* as disconnected users move among geographical areas in an attempt to reconnect to the network [Shin]. Hybrid wireless networks offer alternatives to restoration schemes by enabling the use of overlays or underlays under failure of components of one particular technology. However, such schemes have also not been studied and their benefits are not well understood.

Survivable wireless access network design must also consider transient conditions in the capacity allocation. Work in wired circuit switched [LOG] and packet switched [Tip94] networks show that incorporating transient congestion control can result in a 50% increase in network capacity requirements over a survivable design that ignores transient effects and therefore does not actually meet QoS requirements. Similarly, restoration techniques must consider spatial, as well as temporal properties and must address both the transient and steady state periods. Another limitation of the current literature is that the lack of investigation into the impact that a failure in the wireless access networks has on the signaling network. In fact, our preliminary studies show that radio-level failure (e.g., loss of BS) causes a large increase in transient congestion in the signaling network [Shin].

## II.II. Security in Wireless Access Networks

In wireless networks the threat to security of information flow is the most common and includes masquerade, information modification, information interception, and compromise of access control by security breaches and denial of service attacks. Unlike wired networks that have some degree of physical security, physical security of the wireless networks channel is impossible and therefore security attacks on information flow are the most widespread. Additionally, information security protocols must counter these attacks under the assumption that hardware and software compromises may occur. However, most security protocols and architectures are designed for wired networks and may not be effective in wireless networks.

Currently most wireless networks rely on the inherent technical complexity as a principle means of security, with some adding mild variations of wired security mechanisms. In particular, only confidentiality and identification (authentication) are given importance in current wireless networks. It is generally suggested that the shared secret (whether a password or a PIN) should be at least 80 to 128 bits and the hash algorithm employed should have an output of at least 160 bits because of a square-root attack called the "birthday attack" [STA98]. The key sizes used in current wireless systems are not sufficiently large enough for good security. In IEEE 802.11 WLANs and CDPD mobile data service, a 40-bit key is used in the encryption algorithm. IS-136 uses a 64-bit key that is more secure, but still considered weak. In most cases (like IEEE 802.11 WLANs and Bluetooth) the size of the identification parameter (PIN number or master key) and the algorithms employing it provide loopholes and vulnerability in the protocol [WET01]. Security issues outside of confidentiality and identification are not often addressed in current wireless networks. Almost all wireless networks do not address security issues related to the infrastructure support.

The major drawback of current approaches is that they do not consider security issues related to location, mobility and radio resource management procedures, or issues that arise due to the nature of the radio medium. The Internet Engineering Task Force (IETF) is now investigating authentication, authorization and accounting (AAA) procedures in the context of mobile IP, roaming and portability between different ISPs and but does not account for the wireless specific issues. In WLANs the point of access (AP) is small and inexpensive, thus WLAN APs must be authenticated. Finally, wireless communication devices are expected to be mobile and should thus consume as little power as possible while performing computations for encrypting or decrypting data. Additionally, security protocols requiring excessive overhead or several handshakes may be inappropriate for MNs as the algorithm may be vulnerable due to mobility, or be so slow as to

prevent user acceptance or even usefulness due to user speed. In such cases, a policy based security mechanism that can contain the effects of potential security breaches needs to be implemented [KRI00, KRI01].

### III. Summary

Wireless networks are unique in that the channel is not physically secure and has a lower data rate and higher error rate compared to a wired connection. Additionally, mobile nodes are limited in computational and battery power, all of which combine to constrain information security and availability mechanisms. Information availability is limited by failures in the network that may be a result of intentional attacks or accidental breakdown. Designing networks with sufficient alternate capacity can maintain communication and information flow. Information security provides means to counter security attacks by employing effective and efficient security protocols based on a variety of encryption schemes. To protect user information and the network itself requires development and evaluation in a hybrid wireless network architecture comprising of an infrastructure with several technologies and mobile nodes with a dynamically changing environment.

### References and Selected publications

- [AL98] D. Alevras, M. Grotchel, P. Jonas, U. Paul, and R. Wessaly, "Survivable Mobile Phone Network Architectures: Models and Solution Methods," *IEEE Comm. Mag.*, pp.88-93, March, 1998.
  - [Chang98] M.-F. Chang, Y.-B. Lin, and S.-C. Su, "Improving the Fault Tolerance of GSM Networks," *IEEE Network*, pp. 58-63, Jan./Feb., 1998.
  - [KRI00] P. Krishnamurthy and J. Kabara, "Security architecture for wireless residential networks", *Proc. VTC'2000*, Boston, MA, September 2000.
  - [KRI01] P. Krishnamurthy, J. Kabara, and T. Anusas-amornkul, "Security in wireless residential networks", *Submitted to the IEEE Personal Communications Magazine*.
  - [LOG] D. Logothetis and K. Trivedi, "The Effect of Detection and Restoration Times on Error Recovery in Communications Networks," *Journal of Network and Systems Management*, Vol. 5, No. 2, June, 1997.
  - [Nev97] N. Neves, and W. K. Fuchs, "Adaptive Recovery for Mobile Environments," *Comm. of the ACM*, Vol. 40, No. 1, pp.68-74, Jan 1997.
  - [Pah00] K. Pahlavan, P. Krishnamurthy, et al., "Handoff in hybrid mobile data networks", *IEEE Personal Communications*, April 2000.
  - [Shin] H. Shin, et.al., "The Effects of Failures in PCS Networks," *Proc, 3rd International Workshop on Design of Reliable Communication Networks*, Oct. 2001, Budapest, Hungary
  - [Sta98] W. Stallings, "*Cryptography & Network Security: Principles & Practice, 2<sup>nd</sup> Ed.*", Prentice Hall, Inc., Upper Saddle River, NJ, July 15, 1998.
  - [Tip94] D. Tipper, J. Hammond, S. Sharma, A. Khetan, K. Balakrishnan, and S. Menon, "An Analysis of the Congestion Effects of Link Failures in Wide Area Networks," *IEEE Journal on Sel. Areas in Comm.*, Vol. 12, pp.179-192, 1994.
  - [Wet01] M. Jakobsson and S. Wetzel, "Security Weaknesses in Bluetooth", *RSA Conference'01*, April 8-12, 2001.
- [1] D. Medhi and D. Tipper, Multi-Layered Network Survivability -- Models, Analysis, Architecture, Framework and Implementation: An Overview", (to appear) Proc. of the DARPA Information Survivability Conference and Exposition (DISCEX'2000), Hilton Head Island, South Carolina, January 25-27, 2000, available at [http://www.cstp.umkc.edu/public/papers/dmedhi/mt\\_disce00.pdf](http://www.cstp.umkc.edu/public/papers/dmedhi/mt_disce00.pdf)
  - [2] Anotai Srikitja, David Tipper, Deep Medhi, Virtual private network design for the next generation Internet, In the 5th INFORMS Telecommunications Conferences, BOCA 2000, Boca Raton, FL, March 2000.
  - [3] Yu Liu, David Tipper, Peerapon Siripongwutikorn, Approximating Optimal Spare Capacity Allocation by Successive Survivable Routing, submitted to INFOCOM'01, available at <http://www2.sis.pitt.edu/~yliu/pub.html>
  - [4] Yu Liu, D Tipper, etc., Spare sharing matrix method and its application in the survivable Internet, paper under preparation for ICC'01, available at <http://www2.sis.pitt.edu/~yliu/pub.html>