Issues on Handoff and Security in IP-based Broadband Wireless Networks

Yoshihiro Ohba*, Tadahiko Maeda**, Shinichi Baba* and Tao Zhang***
(*)Toshiba America Research, Inc.
P.O. Box. 136, Convent Station, NJ 07961-0136, U.S.A.
Email: yohba@tari.toshiba.com; sbaba@tari.toshiba.com
(**)Faculty of Science and Engineering, Ritsumeikan University
1-1-1, Noji-Higashi, Kusatsu-shi, Shiga 525-8577, Japan
Email: tmaeda@cs.ritsumei.ac.jp
(***)Telcordia Technologies, 445 South St., Morristown NJ 07960, U.S.A.
Email: tao@research.telcordia.com

1. Introduction

Wireless communication networks such as second-generation (2G) cellular networks are already important infrastructures in human life. Trends towards wireless communication are continuing, with the rapid growth of wireless LANs (Local Area Networks) and the emerging 3G and 4G cellular networks. Such new wireless networks tend to use IP (Internet Protocols) for both signaling and data transfer on top of radio access technologies in order to provide required services at lower cost and with maximum interoperability. In this paper, the wireless network means the network that provides wireless access links to wireless client devices that may be mobile stations.

Since IP is designed to operate over any layer-2 technologies, it could enable mobile stations to roam seamlessly among different layer-2 technologies, which is one of the most important capabilities needed by today's and future wireless networks.

This paper focuses on handoff and security aspects in designing and implementing IP-based wireless networks. With regard to handoff, we propose two schemes that are closely related with each other. One is an IP-based soft handoff scheme. The other is a scheme to configure base stations in an autonomous and automated manner in order to reduce installation and management costs. With regard to security, we review the existing security protocols and mechanisms for wireless networks as well as standardization process of security protocols.

2. IP-based Soft Handoff

Soft handoff is a form of handoff in which a mobile station starts communicating with the target base stations without interrupting the communication with the serving base station. During soft handoff, a mobile station receives the same data from two or more base stations at the same time. Soft handoff is used in CDMA to increase system capability, reliability, and coverage range.

In conventional CDMA networks, soft handoff is based on a centralized scheme in which a SDU (Selection and Distribution Unit) is responsible for distributing traffic, over layer-2 circuits, via different base stations to the mobile station and ensuring that the matching link-layer (and physical-layer) frames sent to different base stations contain copies of the same data. This applies to the forward direction (from the SDU to the mobile station). In the reserve direction, the mobile station ensures that the matching link-layer frames sent to different base stations contain copies of the same data. In CDMA2000 networks, BSC/MSC acts as a SDU [CDMA2000]

However, the conventional scheme is not suitable for future broadband wireless networks for the following reasons:

- Future wireless networks will seamlessly work over different layer-2 technologies

and a soft handoff mechanism that is independent of any layer-2 technologies is needed.

- The centralized approach assumes that data packets always pass through the SDU, but the assumption does not generally hold if the wireless networks are IP-based in the future, since routing of IP datagrams is performed in a distributed and autonomous manner.

To overcome these problems, we propose a new soft handoff scheme in which soft handoff is performed at the IP layer without using a centralized server for sending (receiving) duplicated packets to (from) mobile stations. The proposed scheme is described in detail in the following.

Each base station is an IP node. Soft handoff along the forward direction is performed in the following way. When a base station (i.e., a serving base station) receives an IP packet destined for a mobile station that is in the middle of handoff, it creates one or more copies of the packet and forwards them to the other base stations (target base stations) that are involved in the handoff procedure. The serving and the target base stations will then transfer the copies of the packet over their radio links to the mobile (Figure 1). The mobile station will receive multiple copies of the packet from multiple base stations and it composes a single packet from the copies. When the serving base station forwards packets to the target base stations, it encapsulates the IP packet with an IP header as illustrated in Figure 2. The outer IP header of each copy to be forwarded to a target base station contains an IP address of the target base station. Soft handoff also requires data synchronization among the copies of data received at the mobile station. To achieve this, an additional option header that contains a timestamp is attached together with the outer IP header. The timestamp is used by the base stations to determine when to inject the copies of a packet over the radio links so that the mobile station can receive them within a required time period. Soft handoff for reverse direction is performed in the reverse manner of what is defined for forward direction.

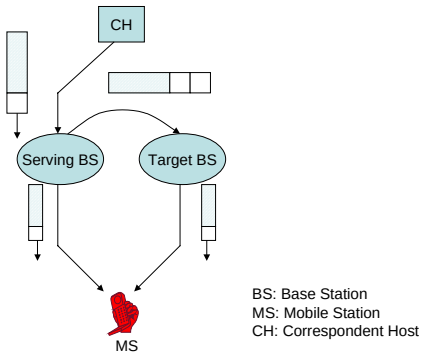

Figure 1: Proposed IP-Based Soft Handoff Scheme (Forward Path)

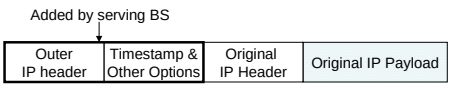

Figure 2: Format of Encapsulated Packet Used for Soft Handoff

3. Auto-Configuration of Base Stations

To support the IP-based soft handoff scheme described in the previous section, it is desired that each base station is configured in an autonomous and automated fashion, as there is no centralized server involved in the soft handoff procedure. We propose a method for a base station to auto-configure a list of candidate target base stations based on wireless communication. As illustrated in Figure 3, the proposed auto-configuration scheme contains the following main steps:

- Each base station broadcasts pilot signal over a common signaling radio channel

periodically and also measures the power of pilot signal received from the neighboring base stations. Each pilot signal contains information identifying the sending base station. (Step 1)

- If the power of the pilot signal measured at a base station exceeds a threshold value, the base station recognizes the sending base station as a candidate target base station and starts exchanging additional information with it, where the additional information is used for soft handoff and includes but not limited to; the base station's IP address assigned on the radio link and the IP prefix of the radio link. Based on the collected information, each base station constitutes a list of candidate target base stations. (Step 2)
- To improve efficiency of soft handoff, each base station may also trace movement pattern of the mobile stations and prune some of the base stations from the list of candidate target base stations if transitions to those base stations never happen in the actual movement patterns. (Step 3)

The IP address of each base station can be automatically configured by using, e.g., DHCP (Dynamic Host Configuration Protocol) [RFC2131].

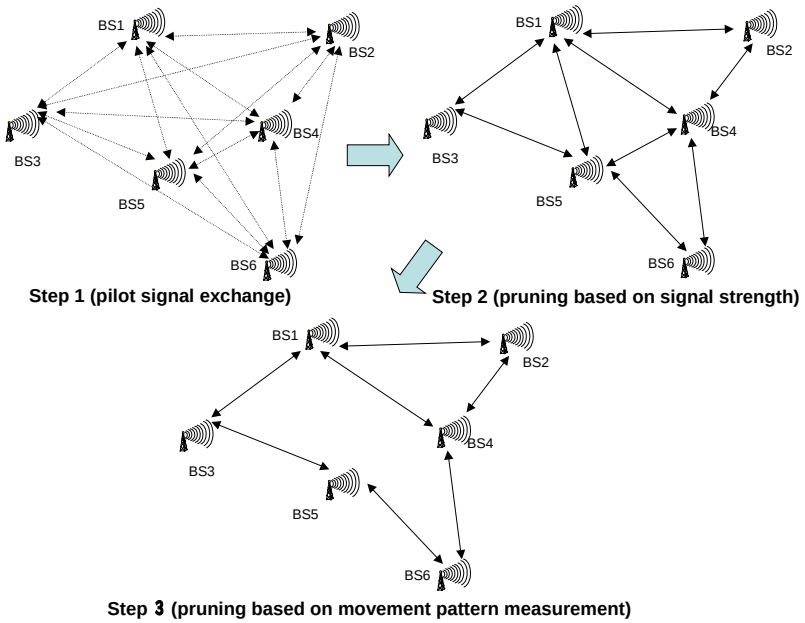

Figure 3: Auto-configuration of Base Stations

4. Security Issues

4.1. Review of Existing Security Protocols and Mechanisms

Figure 4 illustrates the relationship among different protocols and mechanisms related to security. Network security protocols and mechanisms are classified into host-related ones and infrastructure-related ones. The former class requires authentication among two or more entities involved in communication before starting to exchange data. When a host-related security protocol or mechanism requires 3rd party authentication, an infrastructure-related protocol or mechanism such as AAA (Authentication, Authorization and Accounting) or PKI (Public Key Infrastructure) may be used via a NAS (Network Access Server) that supports protocol translation between the host-related and infrastructure-related protocols. Dialup PPP access points, 802.11 access points and PANA (Protocol for Carrying Authentication for Network Access) Authentication Agents [Penno] are examples of NAS.

Network security mechanisms at the physical layer depend heavily on the physical characteristics. For example, smart antenna technologies that are specific to

radio links can be viewed as physical layer security mechanisms in some sense. Wired phone lines that are point-to-point physical links can be also considered as providing physical layer security. Considering the current trend towards broadband wireless networks, integration of antenna technologies and higher layer security protocols and mechanisms could become an important issue to make wireless networks more secure.

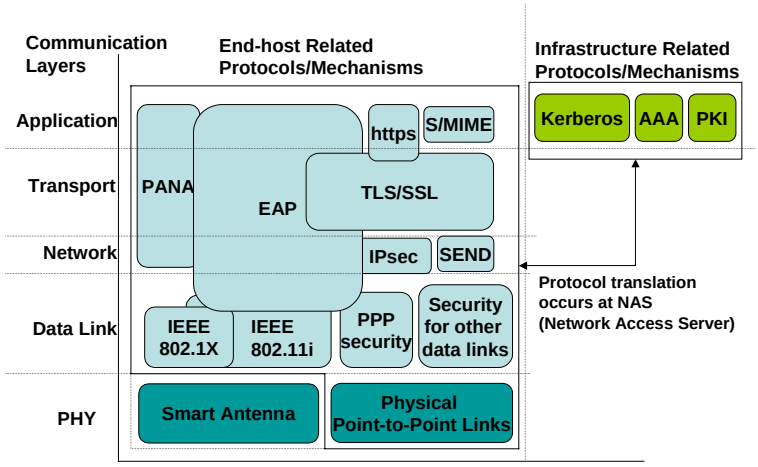

Figure 4: Relationship among security-related protocols/mechanisms

4.2. Standardization of Security Protocols

It is becoming a common practice that standardization process of security related protocols or mechanisms should be based on open discussion as much as possible so that a large number of security experts including cryptographers and security protocol specialists can contribute to the process by analyzing all possible security threats. Without participation of such security experts, it is highly possible that the resulting specification can contain security flaws due to, e.g., adopting a weak security mechanism, misusing a security mechanism and/or incorrectly combining multiple security mechanisms, where the last two problems could be induced even if strong security mechanisms are used. A typical example is the WEP (Wired-Equivalent Privacy), which is a part of IEEE 802.11 [802.11] and is well-known to be insecure regardless of the encryption key length, implying that the adopted security mechanism (i.e., RC4) is incorrectly used in the WEP mechanism [Borizov]. Now IEEE 802.11 TGi is working on defining stronger security mechanisms for 802.11 to fix the problem of WEP, with a greater number of security experts involved in the standard process.

As an example of open discussion, there is a way of standardization by the IETF (Internet Engineering Task Force), where IP-based protocol specifications are standardized in the form of Internet RFCs (Request For Comments). Discussions in the IETF are mainly based on mailing lists to which everyone can subscribe, plus three face-to-face meetings per year. There is no vote in the entire IETF decision process. Instead, a unique decision process based on running code and rough consensus is used. There are pros and cons of this type of standardization process, however, this sort of standardization process works quite effectively when defining security related protocols, since public review by security professionals can be performed at any time before a specification becomes a standard. In addition, it is becoming a best current practice in the IETF to do security threat analysis before starting a protocol design, which also helps the protocol to be robust against various kinds of security attacks. PANA (Protocol for carrying Authentication for Network Access) [PANA] and SEND (SEcure Neighbor Discovery) [SEND] are good example IETF Working Groups that follow this approach.

5. Summary

This paper presented two soft handoff mechanisms for IP-based wireless networks. They enable seamless roaming among different layer-2 technologies and provide low cost installation and management of base stations. The paper also reviewed security protocols and mechanisms as well as standardization process of security protocols. Finally, we addressed the importance of integration of antenna technologies and higher layer protocols and mechanisms to provide more secure wireless networks.

6. References

[CDMA2000] V. Garg, "IS-95 CDMA and CDMA2000 – Cellular/PCS Systems Implementation", ISBN 0130871125, Prentice Hall.

[RFC2131] R. Droms, "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[802.11] IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Network - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[Borisov] N. Borisov, I. Goldburg and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11", Proceedings of MOBICOM 2001, July 2001.

[Penno] R. Penno, A. Yegin, Y. Ohba and G. Tsirtsis, "Protocol for carrying Authentication for Network Access (PANA) Requirements and Terminology", Internet Draft, work in progress, October 2002.

[PANA] http://www.ietf.org/html.charters/pana-charter.html, http://www.toshiba.com/tari/pana/pana.htm

[SEND] http://www.ietf.org/html.charters/send-charter.html