International Journal of Cyber Society and Education
Pages 27-38, Vol. 2, No. 2, December 2009

Mobile RFID of Wireless Mesh Network for Intelligent Safety Care System

Chwen-Fu Horng
National Kaohsiung Normal University, Taiwan
E-mail: horngfu@ms16.hinet.net

Gwo-Jiun Horng
National Kaohsiung University of Applied Sciences, Taiwan
E-mail: grojium.hg@msa.hinet.net

Chung-Shan Sun
National Kaohsiung Normal University, Taiwan
E-mail: horngfu@ms16.hinet.net

ABSTRACT

This paper presents the Wi-Fi phone with RFID (Radio frequency identification) of student entered the school, via Wireless Access Points (APs) of school will transmit MAC address with RFID of Wi-Fi phone to Internet Data Center (IDC) for server and then the message exchanged by using GSM (or 3G) has been transmitted message (or mail) to the mobile user of parents (or client user). The wireless access points support broadcasting multiple SSIDs, each of which can have a different set of security and network setting. The RADIUS server is used to authenticate the Wireless Access Point (AP) and mobile nodes. In safety case system, we used the several authentication and encryption options for the WLAN. We will discuss the use of Wi-Fi protected Access (WPA), RFID, IP Security (IPSec), and Secure Socket Layer (SSL), and there are high Quality of service (QoS) and performance.

Keywords: Wi-Fi, RFID, GSM, WLAN, IPSec

INTRODUCTION

Recently, we can hear very serious news about students' accidents which often occurred where parents cannot care for them. Caring the children is one common human activity and consumes a lot of time/energy to many parents. It is a fact that parents cannot always watch their child and give them prompt supervisions/helps in the school and they

are going to school (Takata, Shina, Ma, & Apduhan, 2005; Takata, Jianhua Ma, Apduhan, 2005).

The wireless mesh network has been an emerging technology in recent years. Because the transmission medium used in networking backhaul APs is radio, the wireless mesh network is not only easy and cost effective in deployment but also has good scalability in coverage area and capacity. The IEEE 802.11 MAC protocol has been adopted as the de-facto medium access control (Tsai & Chen, 2005).

RFID technology uses wireless frequency to read tags data remotely. The tag data may vary from simple identifiers to surrounding environment data collected using a sensor.

In this integrated system, wireless networking has been receiving much attention during the last few years. From GSM taking off, the mobile communication and service have been popularized in people's daily life. The 3G service has been expected for a period of time, but there seem to be many obstructions in front of it. The growth of wireless LAN (WLAN) related equipment in the market came as a surprise during the last two years (Behmann, 2005).

SYSTEM INTEGRATION

The Media Access Control (MAC) address of Wi-Fi phone with RFID code has been appointed built-in the Internet Protocol (IP) that the represented user name and then the RADIUS server must be able to support user authentication based on a native database.

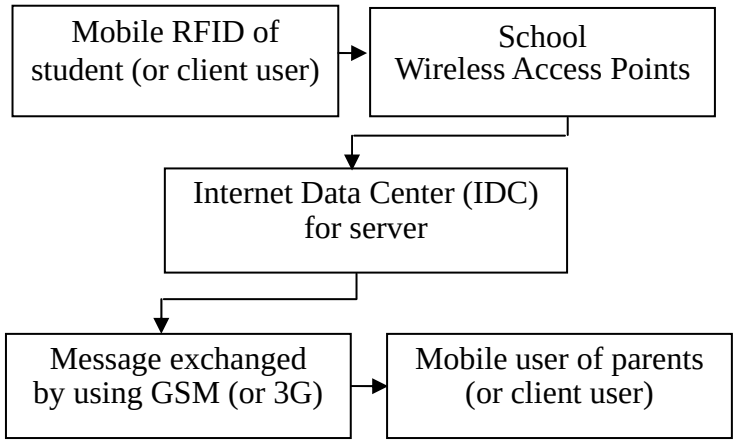

Figure1: The block diagram of the wireless network integrated mobile RFID system

Each of the users' MAC and RFID, the student number with corresponding IP and the GSM (or 3G) telephone number of parents setting in the database. When Wi-Fi phone with RFID of student entered the school, the MAC and RFID of Wi-Fi phone has been connected AP of School and Wi-Fi phone was transmitted the MAC address and RFID code for RADIUS server is used to authenticate. The DHCP server can transmit IP for Wi-Fi phone of student that the student entered to the school.

The authentication of Wi-Fi phone has succeeded, the database server has been dialed the GSM (or 3G) telephone number of parents and transmitted message or speech message. Let mobile user of parents was known student entered the school in Figure 1.

MOBILE RFID

RFID stands for radio frequency identification. It is an automatic identification technology whereby digital data encoded in a RFID tag or smart label is captured by a reader using radio waves. Mobile RFID loads a compact RFID reader in a cellular phone, providing diverse services through mobile telecommunication networks when reading RFID tags through a cellular phone. It uses a mobile phone as RFID reader with wireless technology and provides new valuable services to users by integrating RFID and wireless mesh network infrastructure with mobile communication and wireless internet (Lee & Kim, 2006).

RFID stands for radio frequency identification. It is an automatic identification technology whereby digital data encoded in a RFID tag or smart label is captured by a reader using radio waves. Mobile RFID loads a compact RFID reader in a cellular phone, providing diverse services through mobile telecommunication networks when reading RFID tags through a cellular phone. It uses a mobile phone as RFID reader with wireless technology and provides new valuable services to users by integrating RFID and wireless mesh network infrastructure with mobile communication and wireless internet (Takata, Jianhua Ma, & Apduhan, 2006).

RFID systems using a contact-less IC card or IC tag are being used as automatic ticket checkers used in the railway stations, security systems checking people going entering or exiting from buildings, and electronic-money systems. New fabrication techniques and algorithms providing better security have been developed so mobile systems using RFID communication systems are now possible. 13.56MHz-RFID systems have realized near-field communication by adopting electromagnetic induction. An electromagnetic field radiated from a loop antenna provided in the reader/writer is

coupled by electromagnetic induction to a loop antenna in the IC card. However, if the loop antenna is installed on a metallic housing such as that of a PDA (personal digital assistant) or a mobile phone, the loop antenna for the reader/writer cannot efficiently radiate an electromagnetic field to the IC card: due to eddy current loss, the communication range between the IC card and reader/writer is narrow. Current non-portable products apply magnetic sheets to minimize the influence of metallic housing, however a small, thin magnetic sheet for mobile systems is not effective in allowing communication with a reader/writer at some distance (Ryoson et al., 2005).

SECURITY OF MOBILE RFID

Encrypting a tag identifier seems to be a good solution to address the problems of privacy, but it does not solve all problems because encrypted identifier is itself just another identifier. In addition to this problem, there is the problem of key management in encryption scheme. But the most important problem above all, is the problem of cost. There are an increasing number of researches related to encryption, but it would be difficult to apply them to low-cost tags because of the cost problem (Lee et al., 2006).

There are a wide variety of security concerns with RFID tags. One concern of interest is the ability to track the location of a person or asset by an unintended actor. While the RFID specifications generally deal with short ranges (a few inches to a few feet) between the readers and the tags, specialized equipment can pick up a signal from an RFID tag much farther away.

This is a similar problem to that with wireless LAN’s. Normally a WLAN is only effective for a user within 100m or so. But an attacker with powerful antennas can be more than 10km away and still access the network. RFID tags fall prey to the same problem; an attacker can be two orders of magnitude farther away than intended and still read data. For instance, if an RFID tag is designed to be read at 1 foot, an attacker may be able to be 100 ft away and still interact with it. RFID tags typically only contain a unique number that is useless on its own. The idea is that the reader interfaces with some backend system and database for all transactions. The database stores the information that ties the unique ID to something of interest. For instance, the database knows that ID 1234 is attached to a bar of soap. An attacker reading RFID’s would not know, without access to the database, what ID 1234 is.

Unfortunately, we cannot always assume that an attacker will not have access to the backend database. As the last decades of network security have demonstrated, backend systems are often all too easy a target for an attacker. And once the database tying the unique ID's to physical items has been compromised, it would be nearly impossible to retag all items in response.

The vast majority of RFID tags on the market require no authentication to read the information on them. This allows anyone, an attacker or even just a competitor, to read the data on an RFID chip. Further, many tags have the capability to write information to the chip without authentication. This is especially troubling for enterprises relying on RFID for things like supply chain management. An attacker could theoretically overwrite values on the RFID tags used by the enterprise, thereby wreaking havoc with their RFID system (Potter, 2005).

WI-FI AND MOBILE CELL PHONE

The emergence of VoIP will also affect the Wi-Fi and mobile markets. A Wi-Fi enabled phone might use the WLAN data infrastructure for mobile service within a building, providing an alternative to more costly cellular service (Tsai & Chen, 2005). Other examples include laptop computers/PDAs (or mobile cell phones with built-in 802.11b). With the appropriate software, these platforms can use public Wi-Fi hotspots or emerging 3G data service for VoIP-based toll bypasses. An alternative would be 3G functionality for laptops/PDAs. 3G offers enterprise workers the best of both worlds with mobility and enterprise connections (Stuart, 2005).

WIRELESS MESH NETWORK

Mesh networking is a way to route data, voice and instructions between nodes. It allows for continuous connections and reconfiguration around broken or blocked paths by hopping from node to node until the destination is reached (Horng et al., 2007). A mesh network whose nodes are all connected to each other is a fully connected network. Mobile ad-hoc networking (MANET) featured in many consumer devices, is a subsection of mesh networking in Figure 2 and Figure 3.

Mesh networks differ from other networks in that the component parts can all connect to each other via multiple hops, and they generally are not mobile.

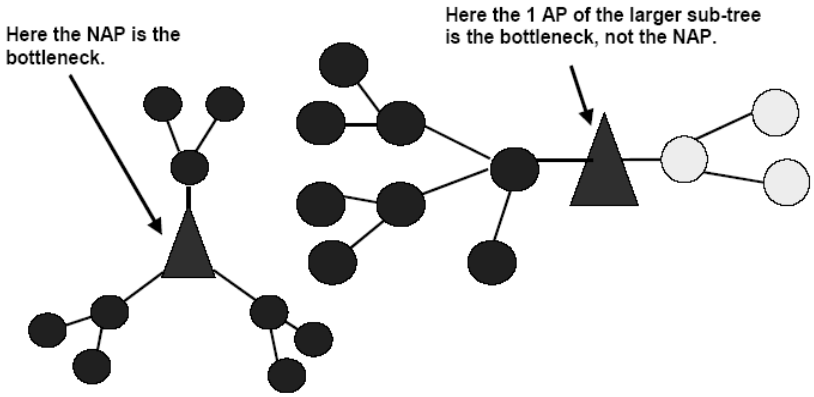

Figure 2: Wireless mesh topology

Wireless Mesh Network solution is a new, enhanced WLAN architecture that redefines the boundaries of WLAN technology, enabling wireless connectivity for enterprises and public end users. With powerful business models for government applications, enterprises, service providers, this latest addition to Network WLAN portfolio brings together Wireless and Wireline solutions for reliable wireless access in Figure 4 and Figure 5.

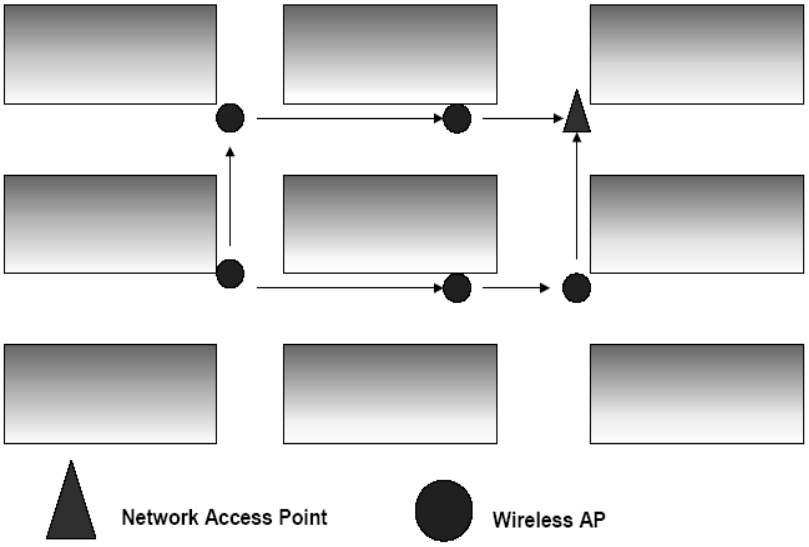

Figure 3: Wireless mesh topology in school

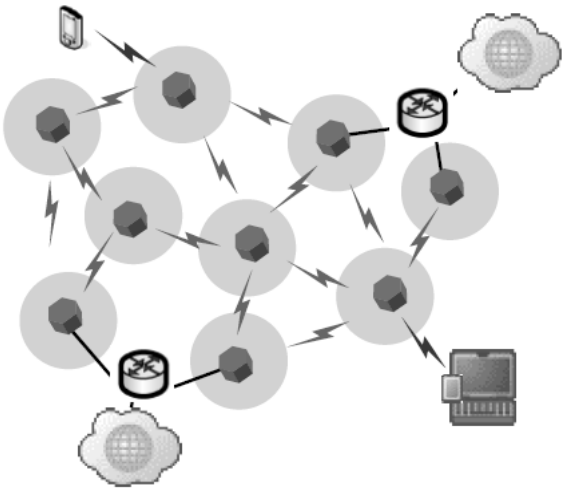

Figure 4: Wireless mesh network

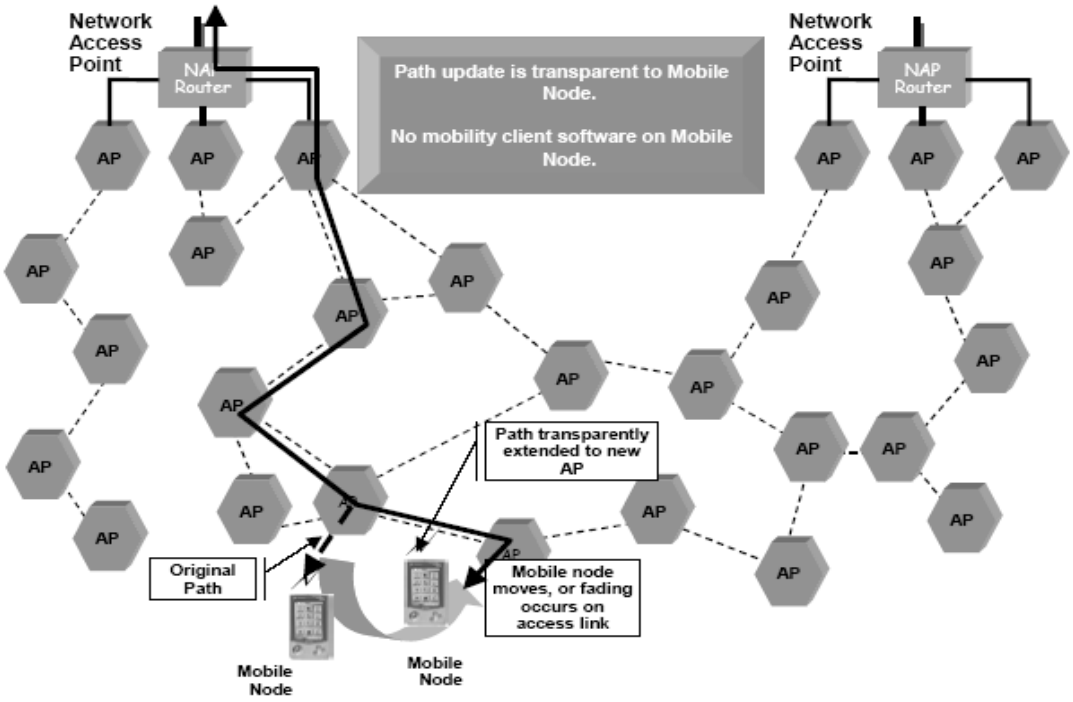

Figure 5: Wireless AP of multiple SSIDs for mesh network

The Wireless Mesh Network is intended to compliment the conventional star topology of the wireless LAN and provide cost effective coverage of large open spaces, industrial installations and clusters of hot spots. This is achieved because the connections between the Wireless AP use self-configuring Wireless broadband links with no physical communication links to build and deploy. The Wireless APs are connected to each other using a Layer 3 peer-to-peer topology.

MAKING THE WLAN WORK

Multiples SSIDs

Access points send out beacons. Each beacon contains information about the network. The first purpose of a beacon is to synchronize the clients that are associated with the access point. This is done through a time stamp in the beacon frame. The beacon also contains channel information and SSID information. The SSID is the service set identifier, or the name of the service set. The access point can be configured to only let clients with the same SSID associate with the access point. In addition, some access points allow advertising of the SSID in the beacon to be turned off. We will discuss this later when we talk about security on the WLAN. To facilitate roaming in an ESS, all the access points in the ESS should be configured with the same SSID. The beacon also contains a schoolyard map that lets clients know if the access point has data to send to it. The beacon also contains information about which data rates are supported by the access point (Horng et al., 2007).

Some wireless access points disable the automatic SSID broadcast feature in an improve network security. Advanced wireless access points support broadcasting multiple SSIDs, allowing the creation of Virtual Access Points-partitioning a single physical access point into several logical access points, each of which can have a different set of security and network settings.

Access Layer Technology

Wireless local area networks (WLANs) are most often used in the access layer of the network design model. After all, a WLAN is just an Ethernet network that uses the air as its medium rather than copper wires. The WLAN can extend the reach of the existing wired network by giving users network access where there are no network drops or by providing a bridge to outlying on campus.

Other applications for WLANs include last mile data delivery and mobile office/classrooms. An example of last mile data delivery would be a wireless Internet service provider that provides Internet connectivity to customers via a WLAN. Subscribers to this server may be rural customers that otherwise do not have the ability to connect to the Internet. A mobile office or classroom application would allow the entire office or classroom network to be packed up and moved to a new location very quickly. This could be used in a mobile training facility or in an office that moves often, such as a construction office (Horng et al., 2007).

Association and authentication

To begin the process of authentication, the client sends an authentication request frame to the access point. At this point, there are many options available to authenticate a WLAN client. The access point can authenticate the client, or the access point can pass on the request to a back-end server for authentication. The purpose of authentication at this level is to establish a Layer 2 data link connection between the client and the access point, not to authenticate the user. After the client's identify is verified, the access point sends an authentication response to the client.

After the client has been authentication it attempts to associate with the access point. Once the client is associated, it can begin to send data through the access point to the wired network. After the client receives the authentication response frame, it sends an association request frame to the access point. The access point returns an association response frame that either allows or disallows the association request. If association is granted, the client can then connect to the wired network.

It is possible for a client to be authenticated to more than one access point at a time, but the client can only be associated with one access point at any given time. Pre-authentication makes roaming a much smoother and seamless process to the client.

RADIUS SERVER

The RADIUS server is used to authenticate the Wireless AP and mobile nodes. It is responsible for all accounting function for the mobile nodes. The RADIUS server must be able to support user authentication based on a native database or through backend servers as well as extensible authentication protocol (EAP) support. To authenticate a mobile node, it must be matched to a profile stored on the server.

Once the mobile is authenticated, a Tunnel-ID stored in the profile is returned to the Wireless AP. The Wireless AP maps the Tunnel-ID to the Subnet Selection Option (SSO). This mapping is contained in the Wireless AP configuration file. Once the Wireless AP has completed the Tunnel-ID to SSO mapping, the DHCP Relay Agent requests a session IP address for the mobile node from the DHCP server in Figure 6.

QUALITY OF SERVICE

The IEEE 802.11e provides the multiple access links between mobile units and APs with QoS capability. However, the requirements of multimedia transport over wireless mesh networks add more challenges, especially for voice applications. It is necessary to overcome the delays and jitters though multiple hops running the IEEE 802.11e.

The wireless access points support broadcasting multiple SSIDs. The VoIP uses eighty percent of SSIDs, and other SSIDs can set the FTP and Internet.

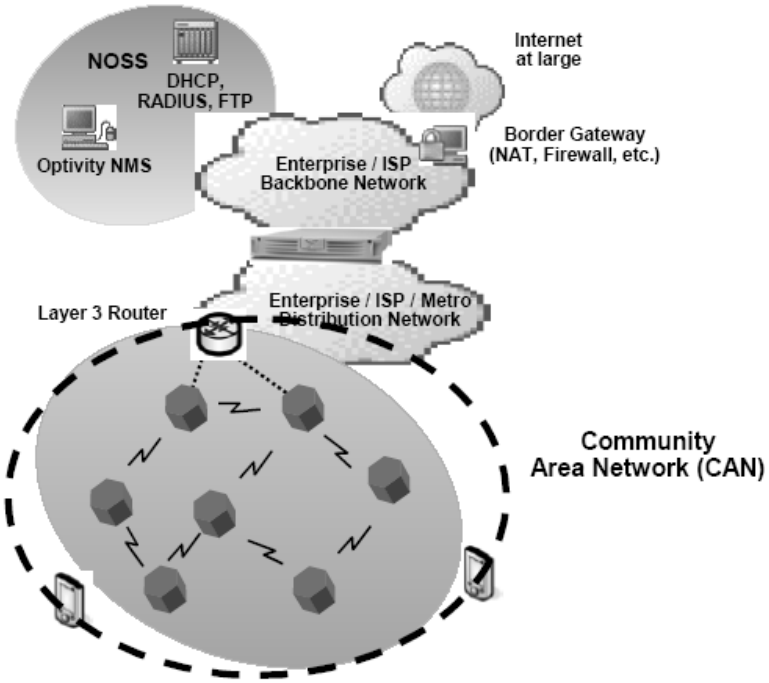

Figure 6: RADIUS server and community area network

CONCLUSIONS

The design of intelligent safety care system can develop application at local area of school (or office, home) for monitor. The Quality of service (QoS) is availability and high performance in very wide of area. The solution includes the latest security standards to protect user access, and protects both the network and the user by providing security on the wireless transit links between access points. We can easily expect that mobile RFID applications will be used for personal use, not for companies and organizations, because people have their own RFID reader. Our work seems to be the first research aimed at building a ubiquitous system to provide assistance for the intelligent safety care of school students in the real world.

REFERENCES

Behmann, F. (2005). Impact of Wireless (Wi-Fi, WiMAX) on 3G and Next Generation—An Initial Assessment. *Electro Information Technology, IEEE International Conference*, Lincoln, NE, 1-6.

Boland, H., & Mousavi, H. (2004). Security issues of the IEEE 802.11b wireless LAN. *Electrical and Computer Engineering, 1*, 333-336.

Chen, J. C., Jiang, M. C., Liu, Y. W. (2005). Wireless LAN Security and IEEE 802.11i. *IEEE Wireless Communications, 12*(1), 27-36.

Horng, G. J., Hou, M. L., Jong, G. J., & Horng, C. F. (2007). The Intelligent Safety Care System of the Wireless Mesh Network. *International MultiConference of Engineers and Computer Scientists, 2*, 1242-1245.

Lee, H., & Kim, J. (2006). Privacy threats and issues in mobile RFID. *Proceedings of the First International Conference on Availability, Reliability and Security, IEEE Computer Society*, Vienna, Austria, 5.

Potter, B. (2005). RFID: misunderstood or untrustworthy? *Network Security*, 2005(4), No.*1*, 17-18.

Ryoson, H., Goto, K., Ueno, M., Kikuchi, A., & Shimpuku, Y. (2005). A 13.56 MHz RFID device and software for mobile systems. *Consumer Communications and Networking Conference*, Second IEEE, 241- 244.

Stuart (2005). “Mobile and Wireless Services and Service Providers in US”, Gartner.

Takata, K., Jianhua Ma, & Apduhan, B.O. (2005). A context based architecture for ubiquitous kid's safety care using space-oriented model. *Parallel and Distributed Systems, 1*, 384-390.

Takata, K., Jianhua Ma, & Apduhan, B.O. (2006). A Dangerous Location Aware System for Assisting Kids Safety Care. *Advanced Information Networking and Applications, 1*, 657-662.

Takata, K., Shina, Y., Ma, J., & Apduhan, B.O. (2005). Designing a space-oriented system for ubiquitous outdoor kid's safety care. *Advanced Information Networking and Applications, 1*, 915-920.

Tsai, T.J., & Chen, J.W. (2005). IEEE 802.11 MAC protocol over wireless mesh networks: problems and perspectives. *Advanced Information Networking and Applications, 2*, 60-63.