Security Issues of Roaming in Wireless Networks

Jaroslav Kadlec[1], Radek Kuchta[1], Radimir Vrba[1]

[1] Dept. of Microelectronics, Faculty of Electrical Engineering and Communication
Brno University of Technology, Udolni 53
CZ-62100 Brno, Czech Republic
{kadlecja, kuchtar, vrbar}@feec.vutbr.cz

Abstract. This paper is focused on the secure roaming problematic in wireless automation applications. Description of a roaming procedure and security issues is presented along with the newest techniques for fast roaming according to prepared network roaming standard IEEE802.11r and security trends defined in IEEE802.11i. Methods for minimizing handoff delay for wireless automation applications and requirements on the sufficient security level are also presented in this paper.

Keywords: Wireless networks, roaming, handoff, security

1 Introduction

Wireless digital communication starts to increase its prominence for the industrial automation domain. Wireless LANs based on IEEE 802.11 and other wireless concepts based on 802.15 (Bluetooth and ZigBee) have been introduced and still more and more producers of automation systems try to offer complete wireless solution for some specific automation applications but the harsh noise environment, and the multiple propagation behavior limit the use of many technologies and require further research and development. To design remote mechanisms (tele-supervisory, tele-operation, tele-service) using wireless communication, an increasing number of communication technologies are available. Using of these technologies is limited by strict quality of service requirements.

We can divide typical automation applications into several scenarios. The first one is permanent wireless connection of automation device. The second is temporary connected wireless automation device, which moves in the range of one wireless network, and the third one is temporary connected wireless automation device which moves across a several wireless networks. For both of temporary connected scenarios it is necessary to guarantee uninterrupted communications with fixed QoS and this strongly limits the current use of these systems within the automation domain. Basic principles and possible solutions for roaming between wireless networks describes IEEE802.11X standard.

2 IEEE 802.11 roaming scenario

The IEEE 802.11 [4] MAC specification defines two basic modes of operation. The first mode is ad-hoc which allows peer-to-peer communications between two or more wireless devices. The second mode of operation is infrastructure mode which defines connections between access point (AP) and wireless mobile stations. In this mode AP provides wireless network connectivity to connected wireless mobile stations. Network connectivity services in one AP create Basic Service Set (BSS). A number of access points could be used in one wireless network. Collection of BSS from access points is extended with services (ESS – Extended Service Set) for solving moving problems, access points communications to authorization server and other network devices (routers etc). Definition of services for moving issues within one wireless network is described as a handoff. Mobile wireless station can also move not only in one wireless network, but across several wireless networks.

Handoff mechanism is composed from sequence of message between AP and wireless mobile station. Important part of handoff mechanism is definition of wireless mobile station identifying exchange across access points in one wireless network. Detailed explanation of handoff process is shown in Fig. 1.

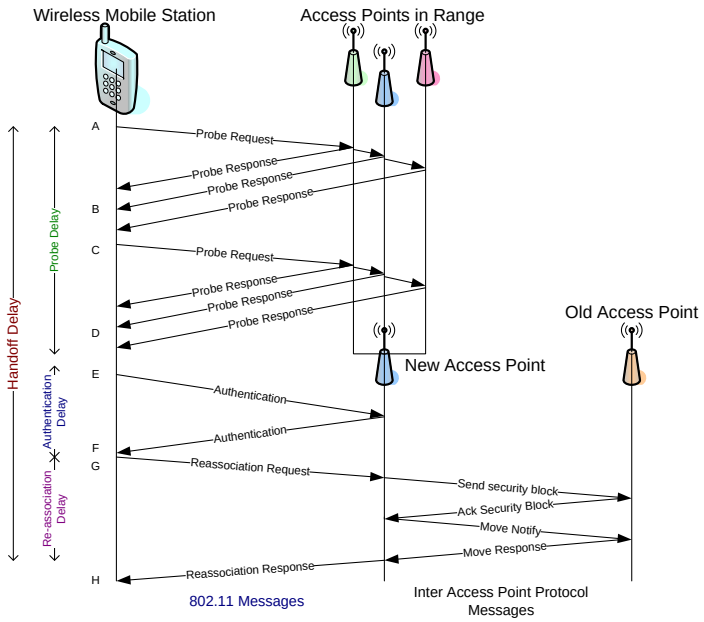

Fig. 1. Handoff process according to 802.11 standard

Preconditions of handoff process in Fig. 1 are valid connections of access points to authorizing server and no association of mobile station to access point. In the first step of handoff process, the mobile station scans for available access points by active

scanning through sending probe message or by passive listening of broadcasted beacon messages from access points. Steps A to D in the figure show active mode scanning of access points in communication range. Mobile station selects the new AP with the best signal strength and data rates after finished scanning. Probe Delay is the time which needs mobile station to select the new AP. After the probe delay, the STA and new AP start Authentication process according to 802.11. Authentication delay is time which is necessary for successful authentication of mobile station to AP. After authentication, the STA sends re-association request to the AP (message G) and receives re-association response from the AP (message H) which completes the handoff process. Re-association process is done by the Inter Access Point Protocol (IAPP).

2.1 Inter Access Point Protocol

The IEEE 802.11f standard specifies two types of information exchange [3]. The first set of interaction is between access points during a handoff process. The second type is between AP and authorization server. IAPP provides secure communication link during a handoff for mobile station information exchange for reducing time cost in re-association delay. When a station first associates to an AP, the AP broadcasts an Add-Notify message notifying all other access points in the network association of the new mobile station. After access points receive an Add-Notify message all old associations for the new mobile station are cleared. For securing of the mobile station information, International Association of Privacy Professionals (IAPP) recommends the use of a RADIUS server (shared keys encryption) to secure the communication between access points [1].This IAPP re-association mechanism ensures a unique association for the mobile station in the network structure.

3 IEEE 802.11r fast roaming scenarios

The IEEE802.11r standard [5] should provide solution for fast roaming applications with high level of security. Unfortunately, securing of wireless communication goes against the fast roaming process. The IEEE 802.11i standard includes several new mechanisms for speed up authentication process as pair wise master key caching and pre-authentication, but application of the newest definition of security standards from 802.1i with temporally key integrity protocol (TKIP) to wireless network can results into handoff delay in hundreds of millisecond.

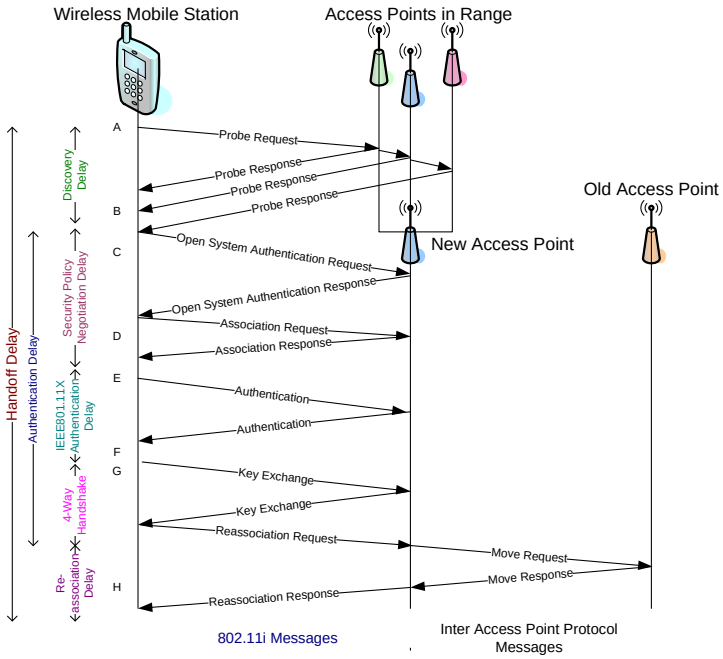

Fig. 2. Handoff process according to 802.11i standard

Fast roaming solution based on the 802.11r standard predicts handoff delay only about 50 ms. Necessity of fast roaming process with sufficient level of security results in a compromise solution based on the nature of application.

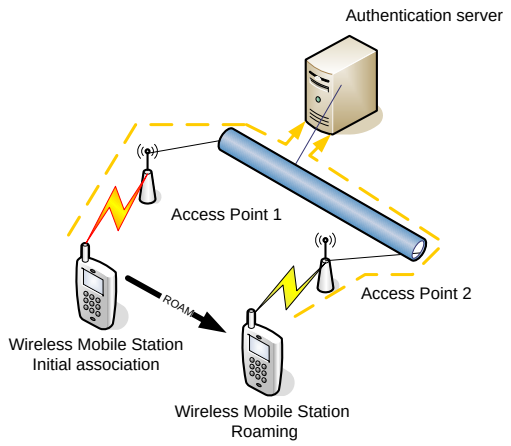

Fig. 3. Association of Wireless Mobile Station to Access Points in roaming process according to 802.11i standard

IEEE 802.11r ensures that the authentication processes and encryption keys are established before roaming request.

Main principle consists in roaming across the network with cryptographic information derived from the first authentication into the network. This pre-authentication reduces load on the authentication server and decreases handoff delay.

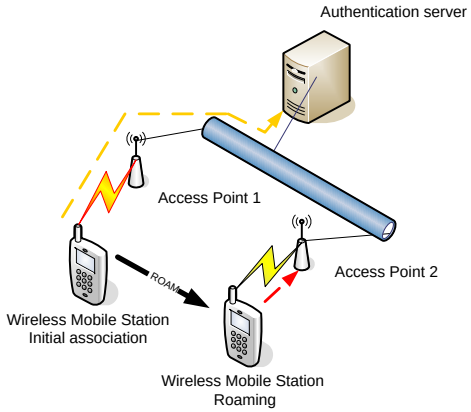

Fig. 4. Association of Wireless Mobile Station to Access Points in roaming process according to 802.11r standard

The 802.11r standard includes a new hierarchy of key-management for secure key caching and distributing. In this hierarchical key-management, the top level key holder has access to original cryptographic information and has to derive keys for holders in lowest level. Deriving of keys is based on the one-way hash algorithm for preventing of decryption original cryptographic information from lower level keys [2]. The main difference between IEEE802.11i standard (Fig. 3) authentication process and IEEE802.11r standard (Fig. 4) consists in requirements on the performing a full authentication with the authorization server for each re-association of wireless mobile station and AP in the IEEE802.11i standard case and initial association and redistributing information about new AP through whole network according to IEEE802.11r standard.

4 Conclusion

We proposed a set of problems of routing scheme for wireless automation applications in this paper. We focused on the routing and security technologies definition for wireless mobile platform and on the selection of available technologies from wireless network applications. Possibilities of integration security mechanisms to the roaming by IEEE802.11r standard were described in this paper, too. Otherwise IEEE802.11r standard hasn't been officially released we can derived main principles of roaming techniques from it. The main gap between the used security level and a

handoff delay by IEEE802.11r standard will be rapidly decreased. Based on those findings it should be possible to develop wireless automation system with well defined parameters of wireless communication link. We presented basic scenarios for typical wireless automation application and our future work will be application of roaming functionality into real wireless automation system.

Acknowledgments. The research has been supported by Czech Ministry of Education in the frame of Research Program MSM1850032 *MIKROSYN* and by the European Commission in the 6th Framework Program under the project IST-016969 *VAN - Virtual Automation Networks*.

References

1. Hill, Joshua. An Analysis of the RADIUS Authentication Protocol. *Untruth Networks* . http://www.untruth.org/~josh/security/radius/radius-auth.html. [Online] 10 24, 2001. [Cited: 5 1, 2007.]
2. Alexander Wiesmaier, Marcus Lippert, Vangelis Karatsiolis. *The Key Authority – Secure Key Management in Hierarchical Public Key Infrastructures.* Department of Computer Science. Darmstadt, Germany : Proc. of the International Conference on Security and Management (SAM 2004), 2004. p. 5
3. IEEE. *Draft 4 Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11Operation.* s.l. : IEEE, 2002. Draft 802.1f/D4
4. IEEE. *Part 11: Wireless LAN Medium Access Control(MAC) and Physical Layer (PHY) Specifications.* 1999. IEEE Standard 802.11
5. Molta, Dave. 802.11r: Wireless LAN Fast Roaming. *Network Computing.* [Online] 4 16, 2007. [Cited: 5 1, 2007.] http://www.networkcomputing.com/channels/wireless/showArticle.jhtml?articleID=198900107.