Efficient Handover Authentication Scheme for Mobile Nodes in Wireless Networks

M. Vivek
II M.E, Computer Science and Engineering, Sri Shakthi Institute of Engineering and Technology, Coimbatore, India.

K. E. Kannammal
Associate Professor, Department of Computer Science and Engineering, Sri Shakthi Institute of Engineering and Technology, Coimbatore, India.

Abstract

Seamless connectivity to the mobile nodes over wireless network is highly desirable, and also achieving security such as authentication and efficiency of such process is challenging. Due to the geographical coverage limit of each access point, it is important to have an efficient handover authentication protocol. When the Mobile Node moves from the current Access Point into new Access Point, authentication should be performed at the new Access Point. Through authentication, new Access Point authenticates the Mobile Node to identify or reject any access request by an unauthorized user. Furthermore, a handover authentication process should be computationally efficient, such a process should be fast enough to maintain persistent connectivity for Mobile Node's. The major goal of this paper is to achieve a Seamless, Secure and Efficient Handover over multiple Access Point's to the Mobile Nodes by implementing a Novel Handover Mechanism.

Keywords - Handover Authentication, Seamless, Security, Privacy, Efficiency.

1. Introduction

Recently, several wireless networks such as telecommunication systems, roadside-to-vehicle communication systems and WLANs have become widely available and interconnected. Wireless access services are offered through interconnected mobile telecommunication networks. Wireless telecommunications refers to the transfer of information between two or more points that are not physically connected. Distances can be short, such as a few meters for television remote control, or as far as thousands or even millions of kilometres for deep-space radio communications. It encompasses various types of fixed, mobile, and portable applications, including two-way radios, cellular telephones, personal digital assistants (PDAs), and wireless networking. In wireless telecommunications, the term handover or handoff refers to the process of transferring an ongoing call or data session from one channel connected to the core network to another through some Access Points [1], [2], [3]. In satellite communications it is the process of transferring satellite control responsibility from one earth station to another without loss or interruption of service. To provide seamless access services for mobile users (e.g., PDA, laptop computer, smart phone and vehicle) without being limited by the geographical coverage of each access point, handover authentication modules have been deployed. It is important to have an efficient handover protocol when a mobile user travels from one area of coverage or cell to another cell within a call duration the call should be transferred to the new cell's base station. Otherwise, the call will be dropped because the link with the current base station becomes too weak as the mobile recedes.

One important module in the handover protocol is authentication. Figure 1 shows the typical handover scenario. A Handover authentication protocol enables Mobile Nodes (e.g., PDA, Laptop PC, smart phone and vehicle) to seamlessly and securely roam over multiple access points. It comprises of three main components, the Authentication Server (AS), Access Point (AP) and then the Mobile Node (MN). The AS act as a core network that maintains a database containing information about the AP's and the MN's inorder to provide the authentication. Wireless Access Points are specially configured nodes on wireless local area networks and it act as a central transmitter and receiver of radio signals. A MN is a network connected device whose location and point of attachment. A MN registers to AS, and then connects to any AP for accessing its subscribed services. When the MN moves from the current AP to target AP, handover authentication should be performed at target AP. Through handover authentication, target AP authenticates the MN to reject any access request by an unauthorized user. Also, a session key should be established between the MN and AP to protect the data exchanged over the connection subsequently.

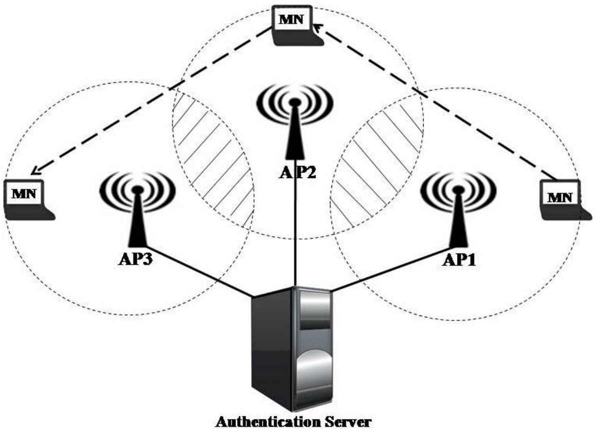

Fig.1.Handover Scenario

Designing a handover authentication protocol is not an easy task. Generally, there are two major practical issues challenging the design. First, efficiency needs to be considered. Further, such a process should be fast enough to maintain persistent connectivity for MN. Generally, MN's does not have sufficient battery power or resources in comparison with wired nodes such as, an AP's. Therefore, a handover authentication process should minimize energy consumption and authentication delay for the persistent connectivity of MN's [8], [12] – [15]. Most of the existing handover authentication protocols incur high communication and computation costs in the following aspects. (1) The conventional way of performing handover authentication is to let new AP contact AS who acts as a guarantor for vouching that a MN is its legitimate subscriber. This will incur more computation and communication delay. (2) For mutual authentication and key establishment, all protocols without communicating with AS require atleast three handshakes between the MN and new AP while other protocols require at least four handshakes among the three entities. Data transmission is a costly operation in wireless networks: sending 1-bit over a wireless medium requires over 1000 times more energy than a single 32-bit computation. (3) To provide robust security, employing a digital signature scheme is widely recognized as the most effective approach for handover authentication. Unfortunately, it is not efficient in communication, because the certificate has to be transmitted along with the digital signature as the message propagates in the network. This leads to more energy consumption on Mobile Node's. (4) To provide user anonymity, group signature-based protocols have been proposed. However, the user revocation list needs to be distributed across the entire network in a timely manner. Further, the verification delay incurred in these protocols for each access request is linearly proportional to the number of revoked users. Therefore, the performance of these protocols may deteriorate when the number of revoked users is large. (5) Generally, an AP verifies each signature individually. When the arrival rate of signatures is high, a scalability problem emerges immediately, where the AP has much less time to verify each received signature.

Second, security and privacy are serious concerns for the handover authentication service. However, all existing handover authentication protocols are subject to a few security attacks in two aspects. On the one hand, users are deeply concerned about their privacy-related information such as the identity, position, and roaming route. Unfortunately, in most of the current handover authentication schemes, it is commonly assumed that the AP's are trustworthy and would keep user's privacy-related information confidential. On the other hand, by Denial-of-Service (DoS) attacks, adversaries can exhaust the resources of AP and AS and render them less capable of serving legitimate MN's.

Above analysis conclude that, most of the available Handover schemes fail to furnish an appropriate security and efficiency guarantees. So it is important to provide an efficient handover authentication protocol for practical wireless networks. In this paper, novel handover mechanism is implemented, which uses pairing based cryptography to secure handover process and achieves a fast handover authentication based on issuing the credential Ticket to the Mobile Node inorder to reduce the communication and computation overheads by reducing the number of handshakes among the involved entities, especially it eliminates the handshake between Access Point and the Authentication Server.

The remainder of this paper is organized as follows. Section II discusses the security requirements that should be considered while designing, Section III presents the brief overview of the papers related to handover, Section IV describes the enhancement of the existing protocol and Section V concludes the paper.

2. Security Requirements

Strong handover authentication should satisfy the following security properties: (1) Mobile Node validation: An AP must authenticate MN to ensure whether it is a legitimate subscriber. (2) Authentication: MN's should be allowed to authenticate the AP they visit to avoid potential deception and other malicious attacks. (3) Data Confidentiality: It can be achieved by establishing the session key between the MN and AP to protect the data exchanged between them. (4) User anonymity: Except to AS, the registered user's information and the user activities should be anonymous and unlinkable to anyone including the visited AP. (5) Conditional privacy preservation: In some application scenarios, it is the liability for AS to reveal the related private information (e.g., identity, position) of a MN to law enforcement in case of emergency. (6) Revocation List: It should be provided inorder to terminate the MN once the subscription period ends. (7) Attack-resistance: The protocol should have the ability to resist the attacks in wireless networks such that it can be applied in the real world [6], [7].

3. Related Works

Due to the importance of seamless service of the MN's over different AP's, several authentication protocols has been proposed in the past. The schematic way of performing the authentication for the MN is, let the foreign agent to contact home agent who acts as a guarantor for confirming that the particular user is an authorized subscriber of it. Most of the available schemes adapt this approach. One of the existing protocol is Universal Authentication Protocol which follows the above approach [11]. It requires only the Mobile User (MU), the Foreign Agent (FA) to be involved during every execution and the Home Agent (HA) that can be kept off-line. This protocol works similar to the authenticated key exchange protocol which is performed between MU and HA within the home network. The protocol is Universal in the sense, same protocol and signalling flows are used regardless of where the MU is moving (e.g., HA or FA). The concept of revocation list is used, every time when the MU is entering or leaving to and from the HA it publishes the revocation list to all FA. This leads to incur high communication cost in case of wireless networks.

Moreover, some of the existing techniques require the AAA server to be appears during each protocol execution [9]. Those kind of approaches leads to some security weaknesses and efficiency problems which include: (1) During each protocol execution, communication between the target AP and AAA server is needed. Suppose if the server is located across many hops then the delay in communication is even more crucial. (2) In most of these protocols, the target AP needs to forward the login request of the MN to server even if it is valid or not. So in this case there is a chance of adversaries to launch DoS attacks to the AAA server through AP.

Most recently a protocol called Pairhand has been proposed, which provides the security and efficiency requirements by adapting the privacy preserving mechanism based on the pseudonyms. Where none of the other existing cryptographic schemes, such as blind signature, ring signature, and group signature techniques, suits the purpose of providing the security and efficiency requirements as discussed above [4], [5]. The techniques such as blind signature and ring signature only provide unconditional privacy, while Pairhand demands conditional privacy, and hence, revocable anonymity. Existing group signature schemes do provide revocable anonymity, but cannot meet high efficiency. In the case of Pairhand protocol, since MNs generally have large storage capacity, rendering the preloading of a large pool of pseudonyms from AS feasible. This preloading process from AS generates large number of short-lived pseudonyms, so that the memory consumption is bounded. The preload-and-replenish mechanism has been proposed by many researchers and works efficiently.

3.1. Pairhand Protocol Functionalities

Pairhand protocol begins with the system initialization, during this phase protocol allows the MN's and AP's to register with AS before they entering in to the network. Then it subscribes the services and allows the MN to communicate with the AP for accessing the network if and only if the MN, say *i*, registers to AS with its real identity. AS chooses the random number say r as the master key and generates the corresponding public key P_{pub} and also it selects two cryptographic hash functions such as H_A and H_B inorder to compute the public key and private key for the MN's and AP's. For each AP, AS computes H_A (ID_{AP}) as the public key and $r.H_B$ (ID_{AP}) as the private key and sends back to AP. Similarly for each MN, AS checks their validity and computes the corresponding keys and then securely send back those tuples to the valid subscriber. Therefore here the AS holds the responsibility of maintaining all those privacy related informations and performs the secure transactions among the involved entities.

During the Authentication phase, the authentication is taken place between the MN and the new AP (e.g., AP2) at the time when the user is trying to move across the geographical coverage limit of the old AP (e.g., AP1). As shown in Figure 2 the authentication and verification operations comprised of the following steps.

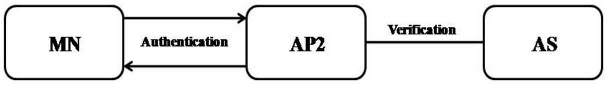

Fig.2. Authentication Scenario

i) MN (e.g., MN_i) picks an unused Pseudo-ID PID_i and its corresponding private key $r.H_A(PID_i)$ from its local memory, which was already send by the AS during registration phase. Then the MN computes the signature as $\sigma_i = H_B(M_i) * r\,H_A(PID_i)$, here $M_i = (PID_i \| ID_{AP2} \| ts)$, and ts is the timestamp added by the MN to handle the counter reply attacks. Once the above computation has been completed, then the MN propagates the request message $\{M_i, \sigma_i\}$ to new AP and computes the shared symmetric key.

ii) Once the AP receives the request message from the MN, initially it verifies the timestamp ts to ensure whether that particular MN is valid or not. If the timestamp exceeds the threshold limit then it assumes the MN is invalid and rejects the access request. On the other hand if it is a valid MN then the AP checks the validity of the received signature σ_i by checking if $\hat{e}(\sigma i, P) = \hat{e}(H_B(Mi) . H_A(PID_i), P_{pub})$. If it is a valid signature then the AP computes the authentication key and sends back to the corresponding MN.

iii) Upon receiving the authenticated key, MN verifies it with the shared symmetric key, the key which the MN was already computed before sending the request message. If both are equal, then the MN believes that the particular AP is legitimate and has established the shared key. Otherwise it rejects the connection. Finally, AP verifies the real identity of the MN with the AS by securely transmits the message $\{Mi, \sigma i\}$ to AS.

4. Enhancing Pairhand Protocol

As the energy required to transfer the data over the wireless medium is desirably high when compared to the wired network, we need to provide better mechanism to reduce the number of handshakes among the involved entities. Here in this paper in addition to the security provided by the Pairhand protocol, we propose a fast handover authentication mechanism based on ticket for Wireless Local Area Network. The credential ticket C_K of MN is issued by the AS during registration phase using a multi-BS group key, which eliminates handshake between the AP and the AS caused by the verification process in the Pairhand protocol as shown in Figure 3.

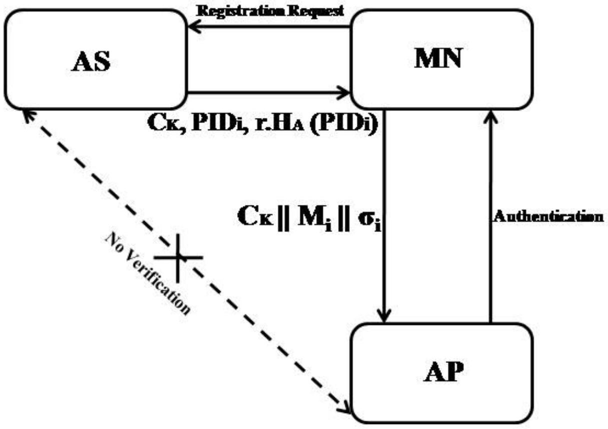

Fig.3. MN Authentication

When the MN moves from the service Access Point to a target Access Point, it can sends its ticket C_k along with the message $\{M_i, \sigma_i\}$ to the target AP, and this can authenticate the MN without communicating with any other third party (e.g., previous AP and AS). Therefore the proposed scheme meets the security requirements in handover authentication semantics and provides robust efficiency in terms of communication overhead and computational cost.

5. Conclusion

Most of the existing handover authentication protocols incur high communication and computation costs, which will in turn result in more computation and communication delay, especially when an AS is often located in a remote location. And also unfortunately, in most of the current handover authentication schemes, it is commonly assumed that the AP's are trustworthy and would keep user's privacy-related information confidential, such an assumption may not be valid. Here with the help of novel handover mechanism, we are achieving secure handover process and also it reduces the communication and computation overheads by reducing the number of handshakes among the involved entities.

6. References

[1] John C.S. Lui, "Introduction to Wireless Networking".

[2] Brandon James Carroll, "Introduction to Wireless Networking Concepts".

[3] Bulut F. Ersavas, "Introduction to Local and Wide Area Networks, Department of Electrical Engineering, Worcester Polytechnic Institute".

[4] D. He, J. Bu, S. Chan, and C. Chen, "Secure and efficient handover authentication based on bilinear pairing functions," IEEE Trans. Wireless Commun., vol. 11, no. 1, pp. 48–53, Jan. 2012.

[5] Daojing He, Chun Chen, Sammy Chan, and Jiajun Bu, "Analysis and Improvement of a Secure and Efficient Handover Authentication for Wireless Networks" IEEE Commun. Lett., Volume: 16, Issue: 8, pp: 1270 – 1273, 2012.

[6] European Telecommunications Standards Institute (ETSI), GSM 02.09: Security Aspects, 1993.

[7] 3rd Generation Partnership Project, 3GPP Specification: 3GPP TS 33.102, 3G Security, Security Architecture, Dec. 2002.

[8] D. He, M. Ma, Y. Zhang, C. Chen, and J. Bu, "A strong user authentication scheme with smart cards for wireless communications," Computer Communication, vol. 34, no. 3, pp. 367–374, 2011.

[9] Daojing he, Jiajun bu, Sammy chan, Chun chen, "Handauth: Efficient Handover Authentication with Conditional Privacy for Wireless Networks", IEEE Transactions, vol. PP , Issue: 99, 2011.

[10] J. Choi and S. Jung, "A handover authentication using credentials based on chameleon hashing," IEEE Commun. Lett., vol. 14, no. 1, pp. 54–56, 2010.

[11] G. Yang, Q. Huang, D. S. Wong, and X. Deng, "Universal authentication protocols for anonymous wireless communications," IEEE Trans. Wireless Commun., vol. 9, no. 1, pp. 168–174, 2010.

[12] D. He, J. Bu, S. Chan, C. Chen, and M. Yin, "Privacy-preserving universal authentication protocol for wireless communications," IEEE Trans. Wireless Commun., vol. 10, no. 2, pp. 431–436, 2011.

[13] K. C. Barr and K. Asanovi, "Energy aware lossless data compression," ACM Trans. Comput. Syst., vol. 24, no. 3, pp. 250–291, 2006.

[14] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in Proc. Asiacrypt 2001, vol. 2248, pp. 514–532.

[15] M. Raya and J.-P. Hubaux, "Securing vehicular adhoc networks," J.Computer Security, vol. 15, no. 1, pp. 39–68, 2007.