International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

Prominent Privacy Mechanism using Tickets Granting Service for Wireless Networks

[1]K.Lavanya,[2]P.Bhuvaneshwari

PG Student, Department of Computer Science and Engineering, Hindusthan Institute of Technology, Coimbatore, India[1]

Assistant Professor, Department of Computer Science and Engineering, Hindusthan Institute of Technology, Coimbatore, India[2]

ABSTRACT- Wireless networks are indispensable for supporting such access anywhere and anytime.Due to its "open air" nature, the wireless environment imposes greater challenges on ensuring network security than in wired networks. Present mechanism for handover authentication relays on authentication module, user's privacy, access control though it hardly serves its best. This paper depicts the highly secure and dominant service called "Handauth".A drawback of session key generation can be sketched when this paper is keenly analysed. The ID simulation from the session key is most liable to hack or corrupt, privacy is lost in such an occasion. Privacy is still achieved if little advancements are done. The mechanism of session key generation is replaced by a firm mechanism called Ticket Granting Server along with inbuilt validity period, it allows us to entrust that only authorized users accesses the system, the ticket validity should go in hand with the user to assure privacy, this is achieved via synchronization. It promises privacy at high rate in real time as the ticket provided to the authorized users cannot be hacked easily, even when it is hacked it actually provides no valid information to the hacker, as it can be used only by a typical private users.

Keywords: Handover, Access points, mobile user, AAA server, security, privacy.

I INTRODUCTION

In present-days, different wireless networks like as WLANs, roadside-to-vehicle communication systems and telecommunication systems 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 connected physically. It circumscribes different types of mobile and portable applications, cellular telephones, personal digital assistants (PDAs), and wireless networking. In wireless telecommunications, the term handoff or handover 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. 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, authentication process during handover have been implemented. 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 call duration the call should be transferred to the new cell's base station. Alternatively, the call will be dropped because the link with the current base station becomes too weak as the mobile recedes.

Regardless of the technology implemented, a typical handover authentication scenario includes three parties: a mobile user, access points (APs) and an Authentication, Authorization, and Accounting (AAA) server. MU enter in to network, before that selects an AAA server for registration then subscribes services and accessing data through AP. When the MU moves from the current AP (i.e., AP1) into a new AP (i.e., AP2), handover authentication should be performed at AP2. Here, the two circles indicate the transmission ranges of AP1 and AP2, respectively. Through handover authentication, AP2 authenticates the MU to protect itself from illegitimate access. At the same time, a session key should be established between the MU and AP2 to protect the user's data against attacks.

Developing a handover authentication protocol is not a simple task. Generally, there are two major practical problems challenging the design. First, efficiency needs to be assumed. Further, such a process should be fast enough to maintain persistent connectivity for MN. 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.

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 in order 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.

II PROBLEM DEFINITION

A handover authentication protocol is very important for during MN change from one AP to another AP and it's not a easy task for designing a protocol. Generally, there are two major practical issues challenging the design. First, consider the efficiency. 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. 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. During the handover process the MN change to one access point to another access point, it should need to authenticate by AAA. So the overhead should be increased and high communication and computation costs, which will in turn result in more computation and communication delay..

III PROPOSED SCHEME

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 in order 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 security provided by the Pairhand protocol, we propose a fast handover authentication mechanism based on ticket for Wireless Local Area Network. The credential ticket CK 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. When the MN moves from the service Access Point to a target Access Point, it can sends its ticket Ck along with the message to the target AP, and this can authenticate the MN without communicating with any other third party. Therefore the proposed scheme meets the security requirements in handover authentication semantics and provides robust efficiency in terms of communication overhead and computational cost.

IV PHASE EXPLANATION

In this section, we first review the definition of FSR-GS. Definition. A FSR-GS is a tuple (G.Kg, G.Enroll, G.Revoke, G.Sign, G.Ver, and G.Open) of probabilistic polynomial-time algorithms and one interactive mechanism. The parties involved in the FSR-GS include a group manager, a group member (i.e., a signer) and a verifier.

1. **G:Kg.** The group manager runs this algorithm to generate a master public key mpk, a master secret key msk (for enrolling group members), a trace key tk (for opening a signature), and an initial membership information Ω.
2. **G:Enroll**. This is an interactive procedure running between the group manager and a new user. Through this procedure, the new member U_i obtains a user signing key usk_i, a (public) user membership key upk_i, a user revocation key rvk_i and ticket C_K.
3. **G:Revoke.** On input mpk, rvk_i (of member U_i) and the current membership information Ω, the group manager outputs an updated Ω.
4. **G:Sign.** It takes mpk, upk_i, usk_i, rvk_i, Ω , ticket C_k and a message m, and outputs a group signature σ.
5. **G:Ver.** On input mpk, Ω, m, C_k and σ, it outputs 1 or 0 indicating acceptance or rejection on the validity of the signature σon message m.
6. **G:Open.** On input mpk, tk, Ω, C_k and a valid message signature pair (m, σ) , the group manager outputs the user membership key upk_i of the actual signer.

Next, we review a concrete FSR-GS in which will be employed in Handauth. Note that any other efficient forward secure revocable group signature schemes can just as easily be applied in Handauth.

4.1 New User Joining Phase

User before accessing the network MN should be register to AAA server and an MU has to authenticate itself to the AAA server by in-person contact. For subscriber U_i, the AAA server runs G:Enroll to generate a user signing key usk_i, a (public) user membership key upki, ticket C_k and a user revocation key rvk_i. The AAA server distributes all these keys, C_k and pk to U_i using a secure transmission protocol. Note that the AAA server maintains a user list, which is composed of every user's related keys (e.g., user membership key, user revocation key) and expiration time. It is clear that different user may have different expiration time. Obviously, the above method is invoked whenever a user wants to register with the AAA server.

4.2 Handover Authentication Phase

The handover authentication protocol which is carried out between a mobile user U_i and the visited access point AP2 is as follows. U_i first sends a login request to AP2 for mutual authentication. Then, AP2 checks the validity of U_i, establishes a session key and then gives a response to U_i. Subsequently, U_i validates AP2, establishes the session key and then responds to AP2. We illustrate this procedure in Fig. 1

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 Pair hand protocol; we propose a fast handover authentication mechanism based on ticket for Wireless 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 Pair hand protocol as shown in Figure 2.

Ui AP2

σ_i= G. Sign (mpk, upk_i, usk_i, rvk_i, Ω, alias|| g^{R_v}|| ts, C_k)

$C_i = (alias, g^{R_v}, ts, \sigma_i)_{p^k_{AP2}}$ C_i

$\xrightarrow{\text{Check}}$ C_k,ts, σ_i

λ_{AP2} = ECDSA. Sig(sk_{AP2}, alias||g^{R_v}|| g^{R_v}||

SK = $((g^{R_v})^{R_v})$

g^{R_v}, λ_{AP2} ←

ECDSA.Ver $(pk_{AP2}, alias||g^{R_v}||g^{R_v}, \lambda_{AP2})$

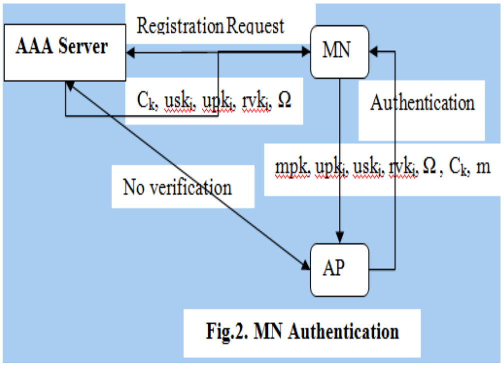

Fig. 1 Authentication procedure of Handauth

VSIMULATION ENVIRONMENT

Our protocol is implemented in Java. Using this tool we create the 100 nodes. In that network create flat topology, one node act as AAA server; some of the nodes are act as access point and mobile node (MN). The MN communicating the network, first the MN registers in AAA server and authenticate from access point then MN accesses the network.

VI EXPERIMENTAL EVALUATION

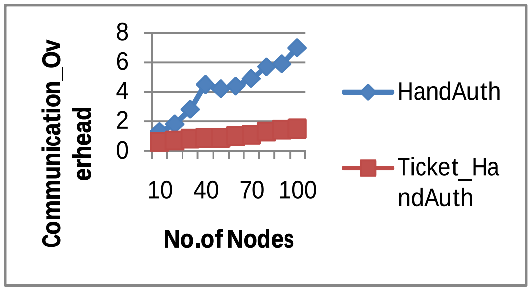

Fig 3. Communication Overhead Graph

Communication Overhead is the proportion of time user spends communicating with network. In Fig 3 shows the communication overhead of HandAuth and Ticket based Authentication protocol. The graph of communication Overhead is shown in following Fig.3 in which number of nodes ranging from 10 to 100 nodes is taken along x–axis and communication overhead ranging from 0.5 to 7 is taken along y–axis. If the number of nodes increases our proposed protocol have efficient results compare to existing protocol.

Table 1: Communication Overhead

Number of Nodes	HandAuth	Ticket based Authentication protocol
10	1.5	0.5
20	1.8	0.7
40	2.9	0.9
60	4.4	1
80	5.7	1.3
100	7	1.6

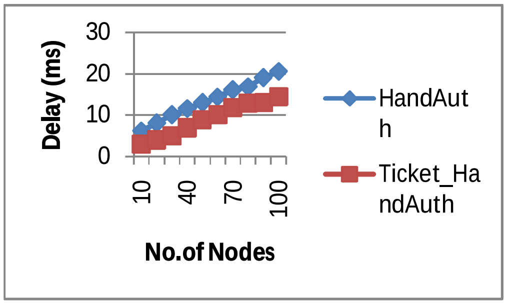

Fig 4. Time_Delay Graph

Time delay is time taken for authenticating the MN based on Handauth and Ticket based Authentication protocol. The graph of time_delay is shown in following Fig.4 in which number of nodes ranging from 10 to 100 nodes is taken along x–axis and delay ranging from 6 to 20 (ms) is taken along y–axis. Our proposed protocol is authenticating the MN in AP; there is no communication between AP to AAA. So compare existing protocol our proposed protocol is shows the better result.

Table 2: Time_Delay

Number of Nodes	HandAuth	Ticket based Authentication protocol
10	$7*10^3$	$3*10^3$
20	$8*10^3$	$5*10^3$
40	$11*10^3$	$7*10^3$
60	$15*10^3$	$11*10^3$
80	$17*10^3$	$13*10^3$
100	$21*10^3$	$15*10^3$

VII 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 AAA 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, When the MN moves from the service Access Point to a target Access Point, it can sends its ticket Ck along with the message 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 achieving secure handover process and also it reduces the communication and computation overheads by reducing the number of handshakes among the involved entities.

REFERENCES

[1] S. Pack and Y. Choi, "Fast Handoff Scheme Based on Mobility Prediction in Public Wireless LAN Systems," Proc. IEE Comm., vol. 151, no. 5, pp. 489-495, Oct. 2004.

[2] J. Choi and S. Jung, "A Handover Authentication Using Credentials Based on Chameleon Hashing," IEEE Comm. Letters, vol. 14, no. 1, pp. 54-56, Jan.2010.

[3] D. He, M. Ma, Y. Zhang, C. Chen, and J. Bu, "A Strong User Authentication Scheme with Smart Cards for Wireless Communications," Computer Comm., vol. 34, no. 3, pp. 367-374, 2011.

[4] C.-C. Chang and H.-C. Tsai, "An Anonymous and Self-Verified Mobile Authentication with Authenticated Key Agreement for Large-Scale Wireless Networks," IEEE Trans. Wireless Comm., vol. 9, no. 11, pp. 3346-3353,Nov. 2010.

[5] C. Chen, D. He, S. Chan, J. Bu, Y. Gao, and R. Fan, "Lightweight and Provably Secure User Authentication with Anonymity for the Global Mobility Network," Int'l J. Comm. Systems, vol. 24, no. 3, pp. 347-362, 2011.

[6] Daojing He, Jiajun Bu, Sammy Chan and Chun Chen," Handauth: Efficient Handover Authentication with Conditional Privacy for Wireless Networks", IEEE Transactions on Computers, VOL. 62, NO. 3, MARCH 2013.

[7] K. Zeng, K. Govindan, and P. Mohapatra, "Non-Cryptographic Authentication and Identification in Wireless Networks," IEEE Wireless Comm., vol. 17, no. 5, pp. 56-62, Oct. 2010.

[8] J. Pang, B. Greenstein, R. Gummadi, S. Seshan, and D. Wetherall, "802.11 User Fingerprinting," Proc. MobiCom '07, pp. 99-110, 2007.