International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 12 (2015) pp. 30613-30619

http://www.ripublication.com

Authentication For Handoff In Wireless Mesh Networks By Granting Tickets

D Naga Venkata Parvaty[1] and M Bhargavi[2]
M. Tech, Department of CSE, Assistant Professor, Department of CSE
Sree Vidyanikethan Engineering College, Tirupati
[1]kalaparva@gmail.comand [2]bhargavisvec@gmail.com

Abstract

Secure and flawless handoff is important to support mobility in wireless mesh networks (WMNs).Wireless mesh networks is a technique to support large-scale wireless coverage both in industrial and academic fields. Many existing methods can be used to reduce the handoff delay, but all these methods require modifications to the original authentication protocols. In the present work, an attempt has been made to pre-distributing the handoff tickets to mesh client and the target mesh router can authenticate each other and reducing the contribution of a third party. It is expected to efficient in terms of security, computation and communication overheads and to protect user privacy-preserving seamless handoff authentication in wireless mesh networks by using pseudonyms.

Keywords: Handoff Authentication; Privacy-Preserving; Pseudonyms; Third Party; Wireless Mesh Networks.

Introduction

In wireless networks computers are connected and communicate with each other not by a visible medium, but by emissions of electromagnetic energy in that air.A mesh network is a multiple path and multiple hop area wide network that are ideal for outdoor deployment. The mesh network consists of wireless networking devices connecting within the range of the network. Hence, it will forms a decentralized networking as each nodes will only need extend its own wireless range up to next node only. Each node are consistently communicating with each other in the local mesh network and are responsible to be acting as gateway for the packets to travel inside the mesh network.A wireless mesh network has 3 characteristic of autonomic system which are self-forming, self-healing, and self-optimization.

Self-forming
New nodes joining the mesh network are transparently supported because meshing functions such as neighbor's discovery and topology learning are implemented.

Self-healing
A node may leave a mesh network due to unexpected circumstances such as failure in the networking devices, natural disaster/manmade disaster and such. Therefore, the mesh network is inherently designed to be more robust and resilient.

Self Optimization
The mesh network has the self optimization to enlarge the mesh coverage as large as possible, to minimize the interferences and also to maximize the bandwidth capacity of the mesh network.

Role of Handoff in WMN
Handoff is about to a process of transferring a data session from one channel connected to the main network to another. Due to user's mobility inWMNs, MCsneed to change their current accessMRto a new one. When anMCmoves to the serving boundary of its current connectingMR, the signal-to-noise ratio will fall due to signal attenuation. When it drops to a predetermined value, theMCwill have to find a newMRfor a better wireless service, which triggers handoff.So secure and unified handoff are more important to support mobility in WMNs and removing the participation of a third party.

Background

Due to the rapid growth of wireless LANs, many internet applications are using wireless networks. Mobile station makes a handoff whenever it travels out of the range of one access point andattempts to connect to a different one. This takes a few hundred milliseconds, producingbreaks in VoIP sessions. S. Shin, A.G. Forte, et. al., [1] developed a new handoff procedure which reduces the MAC layer handoff latency. This handoff procedure decreases the findingpoint using a selective scanning algorithm and a caching mechanism.I.Ramani, S. Savage [2]describe Syncscan, it is a technique used to constantlytrack nearby base stations by synchronizing small listening periods at the clientwith periodic broadcasts from every base station.Now days many of the live streaming applications havebeen limited in wireless LANs, partially due to the high handoff latencies experienced by mobile users. The motive of this is to eliminate handoff latency by exploiting the potential of multiple radios in WLAN devices.Multiscanis implemented completely on the client-side, and, V. Brik, A. Mishra, S. Banerjee [3]Multi Scan nodes depends on using the second wireless interface to opportunistically scan and pre-associate with alternate access points and ultimatefaultlesslyhandoff ongoing connections. Two-radio interface solution is both practical and feasible, and it is the mechanism that can remove handoff latencies in WLANs.Wireless network consists of many access points, a long delay during traveling from one access point to another access point may cause a disturbance for

streaming traffic. Y. Kim, W. Ren, et.al.,[4] proposed a method called *S*ecure *F*ast *R*oaming using ID-based *C*ryptography. It employs ID-based cryptography to condense the authentication procedure and itachieves mutual authentication for the mobile client and access point with a 3-way handshake, then produces a pairwise transient keystraightly without pre-distributing pairwise master key. This method is composed of two stages. In the first stageevery mobile client gets a temporary private key from the private key generator. In the second stage, mutual authentication and key distribution are achieved.

Security Requirements

Secure and efficient handoff authentication protocol in WMNs should satisfy the following requirements:

1. **Mutual authentication**: Both of the roaming MC and the target MR are convinced of the validity of each other, i.e., they are all authorized by the AS. To reduce the latency, this process does not have the involvement of AS.
2. **Access grant**: The AS authorizes the MC to connect to the network based on the above authentication.
3. **Key agreement**: The MC, the target MR and the AS all share a common secret.
4. **Data integrity**: Data transmitted in the network cannot be tampered with, replayed and delayed maliciously. Eavesdropping is infeasible to get the communication content.
5. **Forward and backward secrecy**: Using a compromised session key, an adversary cannot acquire previous keys that have ever been used or calculate any future ones. The protected sessions are invisible to the adversary.
6. **Attack resistance**: Under various types of attacks (e.g., eavesdropping, replay, spoofing, etc.), the security of the users and the network will not be compromised.
7. **Compatibility**: The proposed scheme can work together with the original authentication protocol, and no additional security vulnerabilities are introduced.

Existing Scheme

In this section, existing method is to support fast handoff and previously mentioned security requirements in WMNs. It consists of two phase. In general, in the in the ticket issuing phase, the AS generates for the roaming MC based on the shared secret MKs between the AS and neighbor MRs.In the re-authentication, according to the identity of the target MR, the roaming MC chooses a ticket and sends corresponding parameters to the MR.This is completed by a three-way-handshake.It is a localized handoff by now, because MC can communicate with a target MR, and the target MR relay messages between the old MR and the roaming MC. Therefore cut down the handoff latency.Butthe problem is the all routers can able to find out client in existing method to avoid that pseudonym generation and revocation method is using.

Proposed Scheme

In this section we describe our scheme to support fast handoff and previously mentioned security requirements and also protecting privacy-preserving seamless handoff authentication in wireless mesh networks by using pseudonym generation and revocation. Privacyoffers protection for users to enjoy network services without being outlined. So to protect privacy-preserving seamless handoff authentication in WMNs by using pseudonym generation and revocation. The pseudonym is used to replace the real ID in the authentication which is necessary for both anonymous network access and location privacy. In the intra-domain authentication in our system, the client generates his own pseudonym by selecting a secret number $\varpi \epsilon_R Z_p^*$ and computing the pseudonym $PS_{CL} = \varpi H_1(ID_{CL})$. The corresponding private key can be derived as $\Gamma_{CL} = \varpi\Gamma_{CL} = \varpi\pi H_1 (ID_{CL}) = \pi$

Ticket Issuing Phase

The purpose of this phase is to prepare for the future handoff. Assume that the AS has previously established a secure channel with every single MR. Fig.1and the following steps describe the details of this phase.

1. After the first full successful authentication, the MC and the AS generate a master key MK_{MC}, and the MC, the HMR and the AS share a pairwise master key PMK_{HMR} derived from MK_{MC}. With the keys derived from $PMK_{HMR,}$ the MC and the HMR establish a secure channel. The MC and the AS establish a secure channel protected by the keys derived from the MK_{MC}.
2. The HMR sends the identities of its one-hop neighbors (candidate FMRs) $\{ID_{FMR1}, ID_{FMR2,\ldots}\}$, and the identity of the MC, ID_{MC}, to the AS.

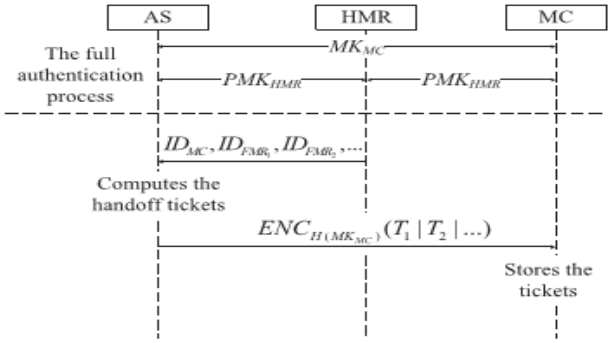

Figure 1: Ticket Issuing

3. The AS chooses an expiration time t, picks a nonce nonce n,uses the identities and the MKs corresponding to the FMRs, to generate handoff tickets for the MC. The AS computes the ith tickets T_i for the authentication between the MC and the ith FMR as in Eqs. (1) and (2). It then sends the tickets as in Eq. (3) to the MC (using the secret key between AS and MC) so that the tickets are only known to the MC.

$$TAK_i = H_{MKFMRi}(ID_{HMR} |ID_{FMRi} |ID_{MC} |n|t) \quad (1)$$

$$T_i = \{TAK_i, ID_{HMR}, ID_{MC}, n, t\} \quad (2)$$

$$C_T = ENC_{H(MKMC)} (T_1|T2\ldots.) \quad (3)$$

4. The MC decrypts the tickets as in Eq. (4) and stores them for later use. This ends the ticket issuing phase.

$$T_1|T_{2\ldots.} = DEC_{H(MKMC)} (c_T). \quad (4)$$

Re-Authentication Phase

The MC performs a three-way-handshake with the chosen FMR to authenticate with each other and establish security keys. We describe the details as the following steps in the fig. 2.

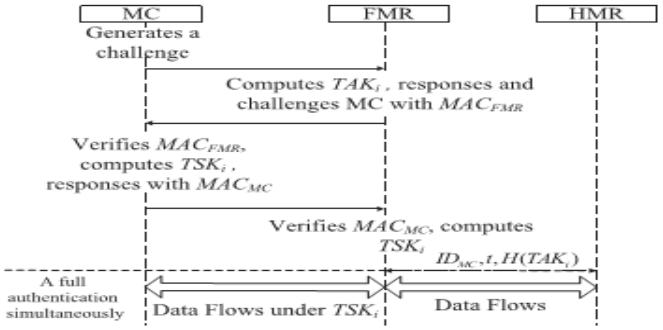

Figure 2: Re-Authentication

The MC chooses the ith FMR as the target FMR to start the authentication (according to signal quality). It picks a random number $r_{MC} \epsilon_R Z_p^*$ computes g^{rMC}(where g is a generator for Z_p^*), finds the ticket T_i corresponding to the FMR, and then sends$\{g^{rMC}, ID_{HMR}, ID_{FMRi}, ID_{MC}, n, t\}$ to the FMR.

1. Upon receiving the message, the FMR picks $r_{FMRi} \epsilon_R Z_p^*$ randomly, and computes g^{rFMRi}. It then uses Formula (1) to generate TAK_i. The FMR generates a message as in Formula (5), computes a message authentication code (MAC) using TAK_i as in Formula (6) and sends $\{m_{FMR}, MAC_{TAKi} (m_{FMR})\}$ to the MC.

$$M_{FMR} = ID_{FMRi}|g^{rMC}|g^{rMC} \quad (5)$$

$$MAC_{TAKi} (m_{FMR}) = H_{TAKi} (m_{FMR}). \quad (6)$$

2. On receipt of $\{m_{FMR}, MAC_{TAKi} (m_{FMR})\}$, the MC verifies the message using TAK_i contained in the ticket T_i as in Formulas (5) and (6). If $g^{rMC}$is the one it sent before, it computes a temporary session key TSK_i as in Formula (7). The MC computes a message and its MAC as in Formulas (8) and (9), and then sends $\{m_{MC}, MAC_{TAKi} (m_{MC})\}$ to the FMR.

$$TSK_i = (g^{rFMRi})^{rMC} \quad (7)$$

$$m_{MC} = ID_{MC}|g^{rMC}|g^{rFMRi} \quad (8)$$

$$MAC_{TAKi} (m_{MC}) = H_{TAKi} (m_{MC}) \quad (9)$$

3. On receiving { m_{MC}, MAC_{TAKi} (m_{MC}) }, the FMR checks its validity as in Formulas (8) and (9). If the verification is successful, FMR computes TSK_i as in Formula (10) and takes it as their session key. FMR sends {ID_{MC}, t, $H(TAK_i)$} to the HMR.

$$TSK_i = (g^{rMC})^{rFMRi}. \quad (10)$$

Simulation Results

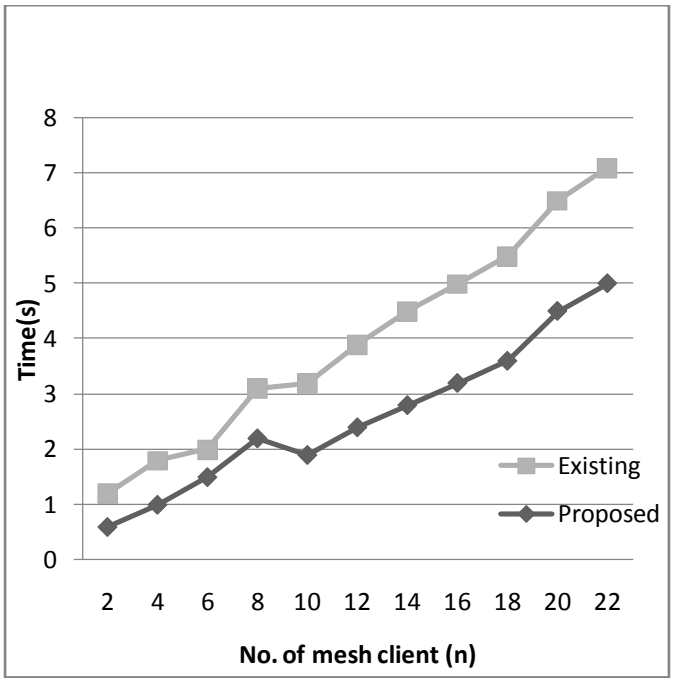

Figure 3: Reducing Handoff Latency

In the simulation results, when a mesh client moves from one mesh router to another mesh router we can reduce handoff delay and also preserving privacy handoff authentication in wireless mesh networks. In this mesh router node and number of mesh clients' nodes as specified by n parameter is shown in fig.3. As number of mesh clients increases the time that will be taken for handoff process by all the mesh clients decreased.

Conclusion

Secure and flawless handoff is important to support mobility in wireless mesh networks (WMNs) In the existing work, the privacy of the mesh client is not concerned. Based on the analysis it is found that the privacy of mesh client will be achieved by the proposed technique is to hide the real Ids of mesh clients issued by Authentication server and revocation of the same issued tickets by using pseudonym

generation and revocation. Therefore, in the present work, it also observed that the pre-distributing the handoff tickets to client and the target router can authenticate each other. Hence, it is efficient in terms of security, computation and communication overheads and also to protect user privacy-preserving seamless handoff authentication in wireless mesh networks by using pseudonyms.

References

[1] S. Shin, A.G. Forte, A.S. Rawat, H. Schulzrinne,*" Reducing MAC layer handoff latency in IEEE 802.11 wireless LANs, "* in: A. Boukerche, K.M. Sivalingam, S.E. Nikoletseas (Eds.), Mobility Management & Wireless Access Protocols, ACM, 2004, pp. 19–26.

[2] I. Ramani, S. Savage,*"SyncScan: practical fast handoff for 802.11 infrastructure networks,"* in: INFOCOM, IEEE, 2005, pp. 675–684.

[3] V. Brik, A. Mishra, S. Banerjee,*"Eliminating handoff latencies in 802.11 WLANs using multiple radios: applications, experience, and evaluation,"* in: Internet Measurement Conference, USENIX Association, 2005, pp. 299–304.

[4] Y. Kim, W. Ren, J.-Y. Jo, Y. Jiang, J. Zheng,*"SFRIC: a secure fast roaming scheme in wireless LAN using ID-based cryptography*," in: ICC, IEEE, 2007, pp. 1570–1575.