http://dx.doi.org/10.5392/JKCA.2011.11.9.017

무선망 보안 접속을 위한 효율적인 인증 기법

An Efficient Authentication Method for Secure Access to Wireless Mesh Networks

허 웅, 하우산, 유강수*, 최재호
전북대학교 전자공학부 영상정보신기술연구센터, 전주대학교 교양학부*

Ung Heo(heoprinc@jbnu.ac.kr), Yushan He(colinmengyu@hotmail.com),
Kangsoo You(gsyou@jj.ac.kr)*, Jaeho Choi(wave@jbnu.ac.kr)

요약

무선망의 적용분야가 활성화되기 시작하면서 보안 분야의 연구 또한 활발해지고 있다. 본 논문에서는 이동 메쉬 노드가 언제 어디서든지 안전한 네트워크 접속을 확보할 수 있는 인증 기법을 소개한다. 특히, 로밍 상황에서 메쉬 노드가 안전한 접속을 확보하려면 홈과 외부 도메인 사이의 인증 교류 문제와 외부 도메인들 사이의 인증 교류 문제를 효과적으로 고려해야 한다. 제안한 인증 방법의 새로운 특징으로는 홈과 외부 도메인 사이의 직접적인 연결이나 교류 없이도 안전한 로밍 접속 인증을 제공할 수 있다는 점이다. 홈과 외부 도메인의 연결에 관계없이, 메쉬 노드의 인증을 수행하는 외부 도메인 라우터는 인접하는 또 다른 외부 도메인을 선택하여 접촉하는 방식을 사용한다. 물론, 접촉대상인 외부 도메인 라우터 그룹에는 메쉬 노드의 방문 기록을 보유한 라우터들만이 포함된다. 본 인증 방식의 성능을 평가하기 위하여 분석적인 기법을 사용하였고 기존 방식들과 비교하였다. 평가 결과, 제안한 방식이 인증 응답 시간 및 인증 서비스 제공 능력 측면에서 비교 대상 기법에 비하여 우수한 성능을 보유함을 확인하였다.

■ 중심어 : | 무선망 | 접속 보안 | 인증 | 로밍 |

Abstract

The wireless mesh networks are recently getting much attention for commercial applications. In such networks, the service should be uninterrupted when roaming from one domain to another while the authentication for a secure access should be maintained. The challenge is to consider the authentic coordination between the home domain and foreign domains and the maintenance of local authenticity between foreign domains. In this paper, a novel authentication method is presented so that a mobile mesh node can be effectively authenticated and obtain an secure connection in foreign domains. In the proposed method, the authentication process does not rely on an end-to-end connection between the foreign domain and the home domain. Even without a connectivity to the home domain, the foreign domain can provide an effective authentication of a mesh node by consulting one of the neighboring foreign domains that has been visited by the mobile mesh node. In order to verify the performance of our proposed method, a qualitative analysis has been performed and compared to those of conventional methods. The results show that our method is superior to the conventional ones in terms of authentication response time and authentication service robustness.

■ keyword : | Wireless Mesh Network | Access Security | Authentication | Roaming |

접수번호 : #110527-001
접수일자 : 2011년 05월 27일
심사완료일 : 2011년 08월 26일
교신저자 : 최재호, e-mail : wave@jbnu.ac.kr

I. INTRODUCTION

Recently, the wireless mesh networks (WMN) are attracting much attention because of their self-configurability and scalability. Their network properties are similar to those of the mobile ad-hoc networks[1]. Moreover, WMN can provide advantages such as low up-front cost, easy network maintenance, robustness, and reliable service coverage[2].

A WMN usually consists of mesh clients and mesh routers, as shown in [Fig. 1] In WMNs, the routers mostly are static and can act as internet gateways or mesh routers. Normally, the internet gateways are used to connect the mesh network with the internet, while the mesh routers act as the backbone of the mesh network connecting internet gateways and mesh clients. The mesh clients are usually connected directly to the mesh router and can also be mobile nodes. They can be one of several types of devices such as laptops, PDA, and mobile phones. The mesh clients can also act as routers depending on their hardware and software configurations[3].

The rapid deployment and network scalability make WMNs possible for commercial networks. Since the mobile clients usually roam from one router to another, seamless and safe roaming connections between mesh clients and mesh routers are necessary. In other words, an authentication protocol for enabling a secure access to a foreign mesh router is essential to guarantee the proper use of WMNs.

WMNs normally relies on wireless connections, and they are easily prone to interference and can impart a lack of security. As any other wireless systems, WMNs are vulnerable to malicious intruders. The typical types of intrusions and attacks to WMNs can be found in Ref.[4], and they include replay attacks and man-in-the-middle attacks.

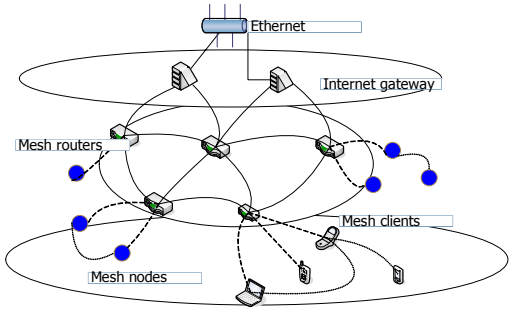


Fig. 1. Wireless mesh network

As the variety of applications using WMNs gets more feasible, the provision for access security become critical. In this paper we investigate an authentication method for the WMN so that a mesh client can obtain a secure access to a mesh router, particular in roaming in a foreign domain.

The remainder of the paper is organized as follows. We discuss related works in Section Ⅱ. The proposed authentication protocol between a mesh node and the foreign domain is presented in Section Ⅲ, and the analytical performance evaluation is presented in Section Ⅳ. Finally, the conclusion is made in Section Ⅴ.

II. RELATED WORKS

In this section, literatures related to authentication approaches presented for the wireless mesh networks are reviewed and studied. Most of papers studied are focused on mobile mesh node roaming situations, particularly.

Consider that a mobile mesh node first visit several domains and then roam to a new domain, which is called the foreign domain. Normally, both the inter-domain handoff and the intra-domain handoff need to ensure the authenticities of the entities involved, and also need to minimize handoff time. Authentication approaches for wireless networks

have been researched for several years. The earliest method for authentication was very simple, consisting of group keys that can support a fast handover scheme. The method by Lee in [5] is based on Bresson's group key agreement protocol [6] and it presents a fast re-authentication protocol. However, it lacks scalability that, as more nodes join the network, the computational cost increases. Since the mobile mesh nodes are usually limited by their batteries, it calls for a more energy efficient authentication protocol.

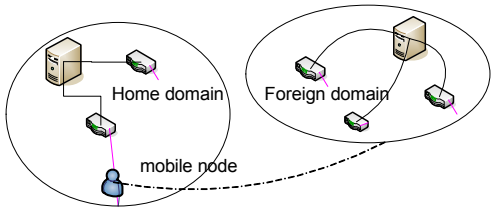


Fig. 2. Simple roaming architecture

Furthermore, as to deal with the delay time involved in authentication, the home-foreign domain approaches have been introduce. When a mesh node roams to a foreign domain, a challenge response mechanism will be carried out between these entities. The AAA service provider will directly contact this mesh node and the foreign domain when the mesh node asks for the authentication contract and billing information[7]. The typical application of the home-foreign domain re-authentication scheme is found in services such as Global System for Mobile Communications (GSM) [8], Personal Communication Systems (PCS) [9] and Mobile IP networks[10]. The main characteristic of this scheme is that each pair of service providers should trust each other so that each user can be authenticated when it roams into a foreign domain. Moreover, the node should be authenticated by the home domain and this relationship should help it to be demonstrated immediately in the foreign domain. However, there is a disadvantage that one cannot ignore. It is quite possible that the home AAA service provider can be much distance away from the foreign AAA server, while the mobile mesh node and the foreign domain node are geographically close. If there is any problem or transmission failure along the path between the foreign domain and the home domain, the authentication can be unsuccessful.

Another approach is the certificate-based authentication to ensure the security between two entities or even between two wireless domains[11]. In the roaming situation, each domain has roaming agreements with other domains known to be secure. These certificates issued by trustworthy domains are called the "roaming-certificate." As illustrated in [Fig. 2], when the new node moves from the home domain to the foreign domain, must it be identified by the certification service (CA) of the foreign domain. When the mesh node roams to the foreign domain, a mutual authentication between the visited network and the roaming user in which those two entities authenticate each other without contacting the user's home domain for further authentication. As the scale of WMN gets larger, however, a problem may arise. If there is no secure, direct relationship between the home domain and the foreign domain, the authentication takes long time or may not be successful.

To solve this inter-connection problem, the token based authentication methods were also introduced [12][13]. The tokens are used to indicate that the user has been authenticated by the issuer. The user can only contact the current domain if the current domain has a secure relationship with one of domains that have been visited by the user node. The weakness of this protocol that it is vulnerable to replay attacks in

which the token copies the client-key-exchange message.

In this paper, we propose a novel, secure authentication protocol that can establish a trustworthy relation without an end-to-end direct connection to the home domain. Here, an authentication agent residing in the foreign domain performs secure roaming for a mobile mesh node in such a way that it only communicates with the currently mesh-node-visited neighboring foreign domains to achieve the equivalent authentication. The proposed method also ensures correct billing, which is very important for the commercial use.

Table 1. Definitions of symbols used

SYMBOLS	DEFINITION
P, Q	Randomly selected numbers
ID_{FA}; ID_{MN}; ID_{VR_i}	Identities of foreign agent, mesh node and visited router i
PK_{FA}	Public key of foreign agent
K_{FM}	Pairwise keys of foreign agent and mesh node
sk_{VR_i}	Secret key of visited router i
Ts	Time stamp
T	Time when the certification is valid
$\epsilon_{PK}\{\ \}$, $\epsilon_{sk}\{\ \}$	Data encrypted with the public key or secret key
$E_{PK}\{\ \}$	Data encrypted with the pairwise key
$Cert_{FA}$	Certification of mesh node from the foreign domain
Sn	Session key

III. OUR PROPOSED RE-AUTHENTICATION METHOD

In this section, our re-authentication method that provides secure connections between the roaming mobile mesh node and the foreign agent is discussed. Since the mobile nodes usually have an energy constraint, our re-authentication procedures are oriented toward achieving an efficiency in authentication processing time and delay. A list of symbols used in the authentication procedures are summarized in [Table 1] and the general phases of the proposed protocol are illustrated in [Fig. 3] The specific sequence of message exchanges is as follows:

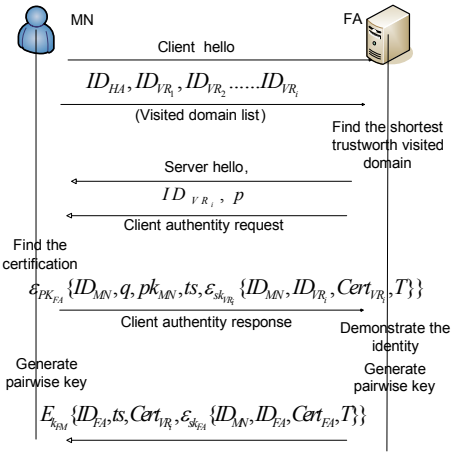


Fig. 3. Proposed re-authentication protocol

Step 1: Roaming request

$$MN \xrightarrow{ID_{HA}\ ;\ ID_{VR}} FA$$

$$\because ID_{VR} = [IDs\ of\ visited\ domains : ID_{VR_k}]$$

When a new mobile mesh node MN try to roams from the home domain to the foreign domain, it firsts send an roaming request to the foreign domain agent FA . It includes identifications of all of its recently visited domains, i.e, ID_{HA}, the ID of the home domain agent; and ID_{VR_i}, the ID of the visited foreign domain router i. Since each visited domain including the home domain has shared certificate information with the mesh node, the identities of the domains recently visited are well maintained by the mesh node.

Step 2: Verification request

$$FA \xrightarrow{ID_{VR_i};P} MN$$

Upon receiving the authentication request from a mobile mesh node trying to roam, the foreign domain will check the list of visited domains, and then it will determine one of the visited domains which has the shortest secure path to itself. Once the visited domain has been selected, the foreign domain will reply with the corresponding identity of the selected, visited domain ID_{VR_i} as well as the random number P.

Step 3: Authentication request

$$MN \xrightarrow{\epsilon_{PK_{FA}}[ID_{MN};q;pk_{MN};ts;\epsilon_{sk_{VR_i}}[Cert_{VR}]]} FA$$

$$\because Cert_{VR} = [ID_{MN};ID_{VR_i};Cert_{VR_i};T]$$

Obtaining a verification reply from FA, the mesh node identifies the selected domain ID_{VR_i} by tracking the necessary information from the its store list. Then, MN integrates its identity ID_{MN}, the random number q, its public key pk_{MN}, the time stamp ts, and the certification of the VR_i, $Cert_{VR_i}$. The certification $Cert_{VR_i}$ is provided by the previously visited domain and it is encrypted by using the secret key sk_{VR_i} of VR_i. All of these items are encrypted into a single message packet by using the public key of FA, pk_{FA}. It is the authentication request packet that is sent to FA. Since FA has a secure relationship with VR_i, it can obtain the public key of VR_i, PK_{VR_i}, and decrypt the $VR_i's$ certification. All information will be encrypted using the public key of FA, and only FA is able to decrypt the certification sent by MN. The foreign domain will then determine whether the public key in the certification is the same as the public key that the mesh node sent to FA.

Step 4: Authentication acknowledgement

$$FA \xrightarrow{E_{k_{FM}}[ID_{FA};ts;Cert_{VR_i};\epsilon_{sk_{FA}}[Cert_{FA}]]} MN$$

$$\because Cert_{FA} = [ID_{MN};ID_{FA};Cert_{FA};T]$$

When the authentication request packet arrives at the foreign domain FA, FA will first decrypt the message using its secret key $\epsilon_{sk_{FA}}$ and then extract the identity of the mesh node ID_{MN}. The other items included packet are also retrieved. FA will check whether the two entities involving in the current authentication process are exact so that it prevents a malicious node from changing the message or the imitating legitimate MN. If all of the items are verified correct, FA prepares authentication acknowledgement packet and sends it to MN as a reply. The acknowledgement packet includes the identification of the foreign domain ID_{FA}, the time stamp ts, the certification of the selected VR_i, $Cert_{VR_i}$, the certification of FA encrypted by using the secret key of FA. All these items are encrypted by using a pairwise key K_{FM} shared between FA and MN.

Once the authentication between MN and FA is successfully completed, the next issue we consider is how to trace the exchange of data packets so that a proper charge can be imposed to MN. In other words, it is assumed that the service provider charges the roaming mobile node based on the number of packets exchanged.

In literatures, one can find similar billing considerations. The first example is a certificate based cryptography[14]. This method can provide real-time communication with service providers, however, it is a computationally expensive approach for mobile mesh nodes. The second example is a one-way hash chain mechanism which provides the basis for correct billing[15]. So far, most of billing

and payment protocols were developed under the home-foreign domain roaming environment.

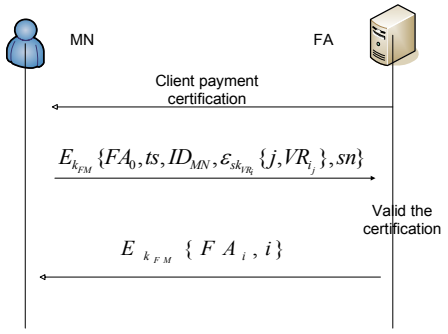


Fig. 4. Payment token and billing protocol

In our short haul re-authentication protocol, we also have adopted the one-way hash chain because it can provide an efficient and undeniable capability. Here, MN will first generate an initial value FA_0 using a hash chain and send it to FA. At each transmission time, the payment token is computed as follows:

$$FA_1 = H(FA_0), FA_n = H(FA_{n-1}) = H^n(FA_0)$$

With respect to the number of packets exchanged, the index of the payment token increases correspondingly. These tokens become the basis for a bill. In order to minimize the transmission time from the foreign domain agent FA to the home domain agent HA, the final payment token is presented to HA at the end of each roaming phase. As illustrated in [Fig. 4], our billing protocol consists of two steps as follows:

Step 1: Billing protocol initiation

$$MN \xrightarrow{E_{k_{FM}}[FA_0; ts; ID_{MN}; \epsilon_{sk_{VR_j}}[FA_k; ID_{VR_j}]; sn]} FA$$

After the mobile mesh node MN has been authenticated by the foreign agent FA, MN assembles required items into a packet, and sends it back to the FA. It should include the initial token value FA_0, the time stamp ts, the identification of MN ID_{MN}, the payment token FA_k received from the visited router VR_j, and the session key sn. All the items are encrypted by using the pairwise key for MN and FA. Other users cannot decrypt the information, as only MN and FA possess the key.

Step 2: Payment billing request

$$FA \xrightarrow{E_{k_{FM}}[ID_{FA}; ts; FA_n; n; sn]} MN$$

Since the initial payment token has been demonstrated, the FA will start the payment process according to $FA_n = H(FA_{n-1}) = H^n(FA_0)$. Even when one token is lost for some reason, the preciseness of the last token can be determined using the hash chain property $H^2(FA_0) = H(FA_1)$.

IV. PERFORMANCE ANALYSIS AND COMPARISON

In this section, we analytically evaluate the performance of our protocol in terms of robustness and computational cost and compare them with those of the traditional schemes.

In our re-authentication protocol, all mobile mesh nodes were authenticated safely in a new domain. There is a rationale supporting the claim for safety. First, the critical information exchanged between MN and the mesh routers are encrypted to protect against malicious nodes. Particularly, for the impersonation attack, the malicious node impersonates MN in order to appear legitimate[16].

However, in the case of the proposed authentication protocol, a malicious node cannot generate a meaningful message that matches the original and so cannot masquerade as a legal user.

Second, for the replay attack, the malicious node caches a normal authentication request and replays it at a later time. Our method uses the time stamp to prevent this type of attack. Because the time stamp is frequently refreshed, the attacker is not able to maintain the appropriate time stamp in the replayed message. It retards any replayers to execute a meaning replay attack. Third, the certifications obtained from the service providers are decrypted by using the pair-wise key to heighten the security. These three capabilities of the proposed method provides an air-proof security from the attackers.

Table 2. Performance comparisons

	Provide billing or not	Connect to HA/ AAA	Asy/ Sym for MN	Roaming situation	Computation of keys
[5] Lee	NO	YES	1Hash 3Sym	Local handoff	1Asy 3Sym
[12] Tuladar	NO	NO	2Sym	Well connected	4Sym
[7] Im	YES	YES	2Sym	Local handoff	2Asy 2Sym
[6] Bresson	YES	YES	1Asy 2Hash	Local handoff	1Asy 3Sym
Ours	YES	NO	1Sym	Well connected	1Asy 1Sym

The performance comparisons are summarized in [Table 2]. Ours is compared to four other authentication methods, which are found in [5][12][7][6]. The major factors for comparisons are 1) the capability for billing; 2) existence of a direct path to *HA*/*AAA*; 3) types and number of keys used for *MN*; 4) connectivity of WMN; and 5) complexity of key management. Particularly for the energy consumption side, our protocol beats them all. Even though we also have been using one asymmetric key in our protocol, most of the computations occur in the mesh router's side, and the energy constraint imposed to mobile mesh nodes is comparably smaller than the others.

V. CONCLUSIONS

In this paper, a re-authentication method for providing a secure roaming establishment between a mobile node and foreign domains of the wireless mesh network has been presented. In addition, a billing protocol using a hash chain is also discussed as an meaningful technical support for payment billing. The diffrentiating characteristic of our authentication protocol is that the mobile mesh node only contacts the foreign domains in order to authenticate its identity, but not necessarily the home domain. As a result, the proposed protocol is capable of effectively reducing the authentication redundancy, and hence, saves delay time and also energy consumption. At the same time, our method is much robust and potent to combat against impersonation attacks and replay attacks at the comparably lower computational cost in comparison to other conventional authentication schemes.

참 고 문 헌

[1] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," Computer Networks, Vol.47, No.4, pp.445-487, 2005.

[2] E. Hossain and Kin K.L *Wireless Mesh Networks : architectures and protocols*, Springer Verlag, 2008.

[3] P. Qiu, U. Heo, and J. Choi, "A gateway protocol architecture for Zigbee based sensor network interconnecting TCP/IP networks," Vol.10, No.3, pp.176-180, KISPS, 2009.

[4] S. Glass, M. Portmann, and V. Muthukkumarasamy, "Securing Wireless Mesh Network," IEEE Internet Computing, Vol.12, No.4, pp.30-36, 2008.

[5] C. Lee, H. Oh, and S. Kim, "A New Authentication Protocol for IEEE 802.11 using a Group Key Supporting Fast Handover," Proc. of ICCIT 2007, pp.269-272, 2007.

[6] E. Bresson, O. Chevassut, A. Essiari, and D. Pointcheval, "Mutual authentication and group key agreement for low-power mobile devices," Computer Communications, Vol.27, No.17, pp.1730-1734, 2004.

[7] T. R. Im, Hwaseong Lee, K. T. Cho, and D. H. Lee, "Secure Mutual Authentication and Fair Billing for Roaming Service In Wireless Mobile Networks," Proc. of ICCIT 2008, Vol.2, pp.466-471, 2008.

[8] European Telecommunications Standards Institute (ETSI), *GSM 2.09: Security Aspects*, 1993.

[9] HY. Lin and L. Harn, "Authentication protocols for personal communication systems," Proc. of SIGCOMM'95, Vol.25, No.4, pp.256-261, 1995.

[10] D. Johnson, C. Perkins, and J. Arkko *Mobility support in IPv6*, RFC 3775, Jun. 2004.

[11] M. Long, C. Wu, and J. D. Irwin, "Localized Authentication for Wireless LAN Internetwork Roaming," Proc. of WCNC 2004, Vol.1, pp.264-267, 2004.

[12] S. R. Tuladhar, C. E. Caicedo, and J. B. D. Joshi, "Inter-Domain Authentication for Seamless Roaming in Heterogeneous Wireless Networks," Proc. of SUTC'08, pp.249-255, 2008(6).

[13] B. Aboba and D. Simon, *PPP EAP TLS Authentication Protocol*, IETF RFC 2716, Oct. 1999.

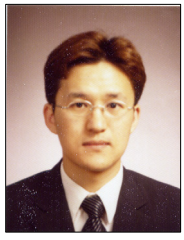
[14] Y. Zhang and Y. Fang, "A Secure Authentication and Billing Architecture for Wireless Mesh Networks," Wireless Networks, Vol.13, No.5, pp.663-678, 2007.

[15] Y. Chen, J. Jan, and C. Chen, "A Fair and Secure Mobile Billing System," Computer Networks, Vol.48, No.4, pp.517-524, 2005.

[16] D. Zhang, U. Heo, and J. Choi, "Neighborhood based security for wireless sensor networks," Proc. of KISPS, Vol.11, No.1, pp.166-169, 2010.

저 자 소 개

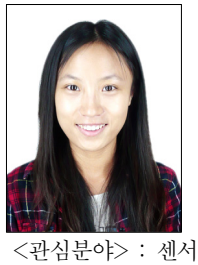
허 웅(Ung Heo) 정회원



- 2002년 2월 : 전북대학교 컴퓨터공학과(공학사)
- 2004년 2월 : 전북대학교 컴퓨터공학과(공학석사)
- 2011년 2월 : 전북대학교 컴퓨터공학과(공학박사)

<관심분야> : 무선/센서 네트워크, 게이트웨이 아키텍처, 통신 네트워크 프로토콜 성능 모델링

하 우 산(Yushan He) 준회원



- 2010년 : 중국 남중민족대학 전자공학과(공학사)
- 2010년 ~ 현재 : 전북대학교 전자공학과(석사과정)

<관심분야> : 센서 네트워크, 네트워크 보안

유 강 수(Kangsoo You) 정회원

- 1994년 2월 : 전북대학교 컴퓨터공학과(공학석사)
- 2006년 8월 : 전북대학교 영상공학과(공학박사)
- 2006년 9월 ~ 현재 : 전주대학교 교양학부 교수

<관심분야> : 영상처리, 멀티미디어 통신

최 재 호(Jaeho Choi) 정회원

- 1985년 5월 : NCSU(B.S.E.E)
- 1988년 5월 : NCSU(M.S.E.E)
- 1993년 5월 : NCSU (Ph.D in Computer Eng.)
- 1994년 3월 ~ 현재 : 전북대학교 전자공학부 교수

<관심분야> : 자가구성 네트워크, 네트워크 컨버전스