Computers and Mathematics with Applications 60 (2010) 245–255

Contents lists available at ScienceDirect

Computers and Mathematics with Applications

journal homepage: www.elsevier.com/locate/camwa

Kerberos based authentication for inter-domain roaming in wireless heterogeneous network

Anish Prasad Shrestha, Dong-You Choi, Goo Rak Kwon, Seung-Jo Han *

Department of Information and Communication Engineering, Chosun University, Gwangju, Republic of Korea[1]

ARTICLE INFO

Keywords:
Authentication
Kerberos
Inter-domain roaming
Trusted third party
Session key

ABSTRACT

An increased demand in ubiquitous high speed wireless access has led integration of different wireless technologies provided by different administrative domains creating truly a heterogeneous network. Security is one of the major hurdles in such network environment. As a mobile station moves in and out of the coverage area of one wireless network to another, it needs to be authenticated. The existing protocols for authentication of a mobile station are typically centralized, where the home network participates in each authentication process. It requires home network to maintain roaming agreement with all other visiting networks. Moreover, the round trip time to home network results high latency. This paper is focused on developing authentication protocol for wireless network irrespective of the technologies or the administrative domain. We propose a secure protocol which adopts strong features of Kerberos based on tickets for rigorous mutual authentication and session key establishment along with issuance of token so that the mobile station can have access to not only the roaming partner of home network but also to the roaming partner of previous visited networks. The performance evaluation and comparative analysis of the proposed protocol is carried out with the already implemented standard protocols and most remarkable research works till date to confirm the solidity of the results presented.

1. Introduction

Existing wireless network technologies ranges from Wide Area Networks (WAN) such as cellular technology like UMTS and CDMA2000 to Wireless Personal Area Networks (WPAN) such as Bluetooth and Infrared [1]. However, each technology has its own limitations in terms of coverage and bandwidth. With the increased demand in ubiquitous high speed wireless access, the current trend is to integrate different but complementary wireless access technologies and make inter-operation among different administrative domains possible. As such, we have heterogeneous wireless network with almost a global coverage. This has led to the Always Best Connected (ABC) concept. For a mobile user, it is desirable to have higher speed with lower price supporting seamless connectivity allowing inter-operation of the different technologies and providers. For example, we can consider integration of 3G network and WLAN. A mobile user with dual radio interface supporting both technologies can enjoy high bandwidth in WLAN network and switch to cellular network in the absence of WLAN for universal roaming.

Maintaining strong security becomes inevitable requirement while integrating different wireless networks. The first and foremost step to maintain security is to verify both the Mobile Station (MS) and the network by performing authentication

* Corresponding author. Tel.: +82 62 230 7069; fax: +82 62 230 6569.
E-mail addresses: anishpshrestha@gmail.com (A.P. Shrestha), dychoi@chosun.ac.kr (D.-Y. Choi), grkwon@chosun.ac.kr (G.R. Kwon), sjbhan@chosun.ac.kr (S.-J. Han).
[1] 375 Seosuk-dong, Dong-gu, Gwangju, 501-759, Republic of Korea.

0898-1221/$ – see front matter © 2010 Published by Elsevier Ltd
doi:10.1016/j.camwa.2010.01.019

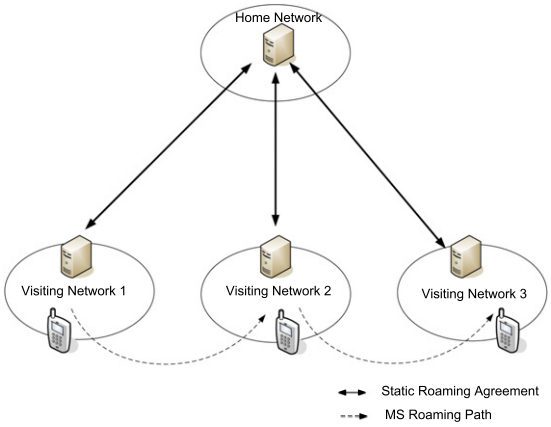

Fig. 1. Centralized scheme.

process prior to any service delivery in each administrative domain. The critical problem in performing authentication in such a distributed heterogeneous network lies in the following two facts.

Firstly, the roaming agreement should exist between two administrative domains for an inter-domain authentication. For N numbers of administrative domain, we need to establish $\frac{N(N-1)}{2}$ roaming agreements. In a true heterogeneous network, there exist several administrative domains of different sizes each providing access to different wireless technologies. The total number of inter-domain roaming agreements to be established in such a case would grow tremendously with increase in number of administrative domains. Therefore, it is almost infeasible to maintain roaming agreement with all the administrative domains in a practical scenario. To avoid such a situation, we need to establish spontaneous roaming agreement between pair of domains.

Secondly, the authentication delay should be as minimal as possible to provide the experience of seamless transition. It can be normally subjected to computation delay and propagation delay. We do not refer scanning delay here. To minimize the authentication delay we need to focus on simple computations and limit the message flow between nodes. The round trip time (RTT) between the home network (HN) and visiting network (VN) presents an overwhelming impact on propagation delay. Hence, the communication between HN and VN should be avoided, if possible. Most of the existing protocols are based on centralized scheme. Each time an MS hand-offs to another VN, HN is required to participate in authentication as shown in Fig. 1.

This paper describes a novel authentication protocol based on Kerberos suitable for heterogeneous network. Kerberos is a network authentication protocol designed to provide strong authentication for client/server applications by deploying Kerberos Server as Trusted Third Party (TTP). It was developed at the Massachusetts Institute of Technology as part of Project Athena in the mid-1980s and uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection [2]. Since Kerberos is a lightweight protocol based on inexpensive symmetric key cryptography, it is more adaptable for small devices with low computational power.

We exploit the Kerberos protocol for mutual authentication between the MS and the VN that shares roaming agreement with the MS' HN. HN acts as a TTP based on the trust relation it shares with VN and the MS. It grants a ticket to MS and mutual authentication is performed between MS and VN. After successful authentication, MS receives a token from the visited network with which it can roam to another foreign network that shares roaming agreement with previous visited network, but not with its home network. As such, HN is not required in the successive authentication process. As the proposed protocol adapts Kerberos protocol and offers inter-domain authentication, we refer it herein as Kerberos based Authentication for Inter-domain Roaming (KAIR). Unlike centralized scheme, KAIR is a distributed scheme as shown in Fig. 2.

The main contributions of our work are:

(i) to extend the mobility range of MS beyond the roaming partners of HN by using previous visited domain as TTP, and
(ii) to reduce the authentication latency by avoiding RTT to HN in succeeding authentication process once it is successfully authenticated in the presence of HN.

The rest of the paper is organized as follows. In Section 2, we present the related works followed by Section 3 in which we discuss the proposed protocol in detail. The security analysis is carried out in Section 4. In Section 5, we carry out comparative analysis with other different protocols. In Section 6, the performance evaluation is measured in terms of average authentication delay. Finally, the conclusion is drawn in Section 7.

2. Related work

The authentication protocols developed for wireless network are technology specific or meant for a set of technologies (like integrated cellular network and 802.11). Due to emerging heterogeneous network, technology independent protocols

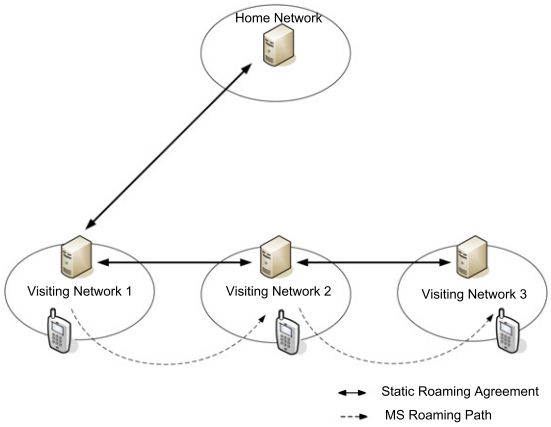

Fig. 2. Distributed scheme.

are required to be addressed. In this section, we look at some of the already implemented standard protocols for technology specific wireless networks and the recently designed protocols for heterogeneous network.

2.1. Implemented standards

The Extensible Authentication Protocol (EAP) that runs directly over data link layer, originally developed to use with PPP, has also been applied subsequently to IEEE 802 wired networks, wireless networks such as IEEE 802.11i, IEEE 802.16e, and IKEv2. EAP is used as an encapsulation protocol for upper layer authentication information and allows for various authentication mechanisms so called, EAP methods. Out of more than 40 EAP methods, Transport Layer Security (TLS) [3] is considered to be promising as it has undergone an extensive review and is considered to be cryptographically strong. It is based on Public Key Interface (PKI) and uses client and server-side certificates for authentication in 802.11. The Wi-Fi Alliance has added EAP–TLS to Wi-Fi certified products. Therefore, the implementation of EAP–TLS is pervasive in WLAN world. To exploit the popularity and strong features of TLS, the variants of TLS protocol such as USIM based EAP–TLS [4], advanced SSL/TLS based authentication [5] and many other protocols have been proposed to support interworking of different wireless technologies. Since all of these protocols authenticate by means of digital certificates, it automatically inherits all certificate-related problems. For small devices, storing long digital certificates require higher memory. Similarly, the certificate should be issued by same Certificate Authority (CA) or maintain a chain to the trusted root CA. Moreover, it lacks potential scalability in distributed heterogeneous environment and appears to be expensive particularly for micro-transactions.

EAP-AKA is another EAP-method popular for interworking 3G-WLAN developed in the 3GPP by Ericsson and Nokia [6]. It provides an opportunity to any application or protocol which can perform EAP authentication to perform UMTS authentication (i.e. UMTS AKA) mechanism as well. It is based upon symmetric keys and runs typically on a UMTS Subscriber Identity Module (USIM). It comprises of two phases: (i) distribution of authentication vectors from the HN to VN and (ii) authentication and key agreement procedure between the MS and the Serving Network. AKA lacks rigorous mutual authentication. As such, it is vulnerable to re-directive attack as cited in [7].

2.2. Proactive solutions

The proactive methods are normally used for intra-domain authentication. However, recently this approach is suggested for inter-domain authentication also. In proactive methods, the MS is authenticated to neighbouring networks before handover takes place.

In [8], a shadow registration method is proposed. The concept is to establish the security association between MS and the Authentication Server (AS) in neighbouring networks so that after hand off, the registration process is processed locally within that particular domain without contacting home network. As this method operates like the shadow as one walks, it is referred as shadow registration. However, for the pre-establishment of security association, HN needs to be contacted by local network to inform about neighbouring network.

A Media-independent Pre-Authentication (MPA) is proposed in [9]. It is an MS assisted pre-configuration and pre-authentication method that is executed to a target network before the actual handoff. It is used to enhance the performance of existing mobility protocols by proactively performing layer 3 and layer 4 associations and bindings before the actual handoff takes place, thereby saving time for these operations that usually only take place after the layer 2 association. It comprises of four procedures. The first procedure is referred to as pre-authentication, the second procedure is referred to as pre-configuration, the combination of the third and fourth procedures are referred to as secure proactive handover. It requires long time to discover and select multiple candidate networks to connect, and initiate pre-authentication and

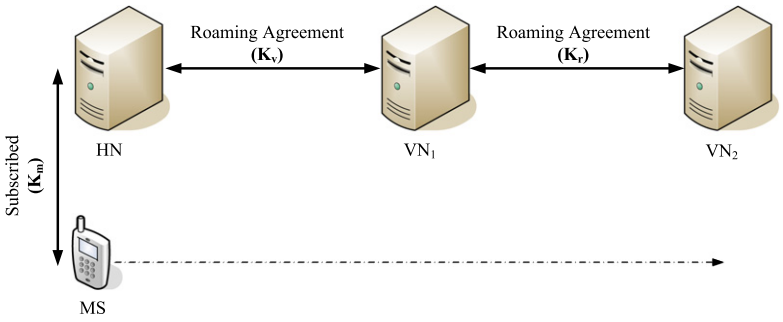

Fig. 3. Assumed roaming scenario.

pre-configuration procedures with the candidate network. Therefore, it is suitable only where an accurate prediction of movement can be made easily.

2.3. Ticket/token based solutions

The ticket/token based solution appears to be most feasible solution as it can exploit the distributed nature of roaming agreements in heterogeneous network and establish dynamic roaming agreement with other foreign networks that do not share roaming agreement with the home network.

A proof token based authentication protocol is proposed in [10] which exploit the features of EAP–TLS. The MS carries a certificate issued by its home domain's CA and proof-tokens which are similar to certificates but are issued by previous visited domain's CA after successful authentications in that particular domain. It supports establishment of spontaneous roaming agreement between pair of domains that do not already have a direct roaming agreement. It differs from EAP–TLS in the sense that instead of the MS presenting a fixed X.509 certificate issued by a root CA, it presents a proof token issued by a foreign domain it has recently visited and with which the current domain also has roaming relations. Another differing point is that the AS carries a number of roaming certificates instead of a single certificate issued by root CA. To find out which token to use, the MS sends a list of all visited domain names. The AAA server chooses a common domain between MS' visited domain list and its roaming partner domain list, and sends the corresponding roaming certificate. The rest of the message exchange is same as EAP–TLS. Although this mechanism seems promising, yet analysis needs to be carried out in terms of latency and efficiency since it involves asymmetric encryptions as in TLS.

In [11], a Fast re-Authentication Protocol (FAP) is proposed for inter-domain roaming which eliminates the need of communication between the target and home network for credentials verification and uses short living lightweight re-authentication ticket. It consists of two sub-protocols; ticket acquisition and fast re-authentication. The former is executed when the user is attached to the network and it requires inter-domain communication, and the latter is executed during handover and localizes the authentication process in the target domain. However, to generate authentication tickets, the AS should have access to results of different authentication methods, which may have been used for the last authentication. Moreover, the MS needs to update the information about future possible roaming partners frequently as the lifetime is very short.

3. Proposed protocol

3.1. Assumptions

The few assumptions considered in our protocol are illustrated in Fig. 3. The MS and its home network share a secret key K_m of 128 bits. This secret key is provided by HN at the time of subscription to MS. The MS can roam from one non-home network to another. To distinguish these visited networks, we will presume the one which MS visits at first and shares roaming agreement with the HN as the first visiting network (VN_1). VN_1 and HN share a secret key K_v of 128 bits. The secret key is established during the roaming agreement between the two networks. After successful authentication in VN_1, MS enters another visiting network close to VN_1 geographically. We call this network the second visiting network (VN_2). VN_2 shares roaming agreement with VN_1 but not with HN. VN_1 and VN_2 also share a secret key K_r established during the roaming agreement between VN_1 and VN_2 which is also 128 bits. The roaming agreement should establish strong trust relationship between the domains.

3.2. Initial authentication

During the initial authentication in VN_1, HN acts as TTP as shown in Fig. 4. It issues the ticket just like Kerberos server and assists in establishing session key between MS and VN_1. VN_1 grants a token to MS after the successful authentication for further authentication in other domains. The authentication comprises of seven steps as follows:

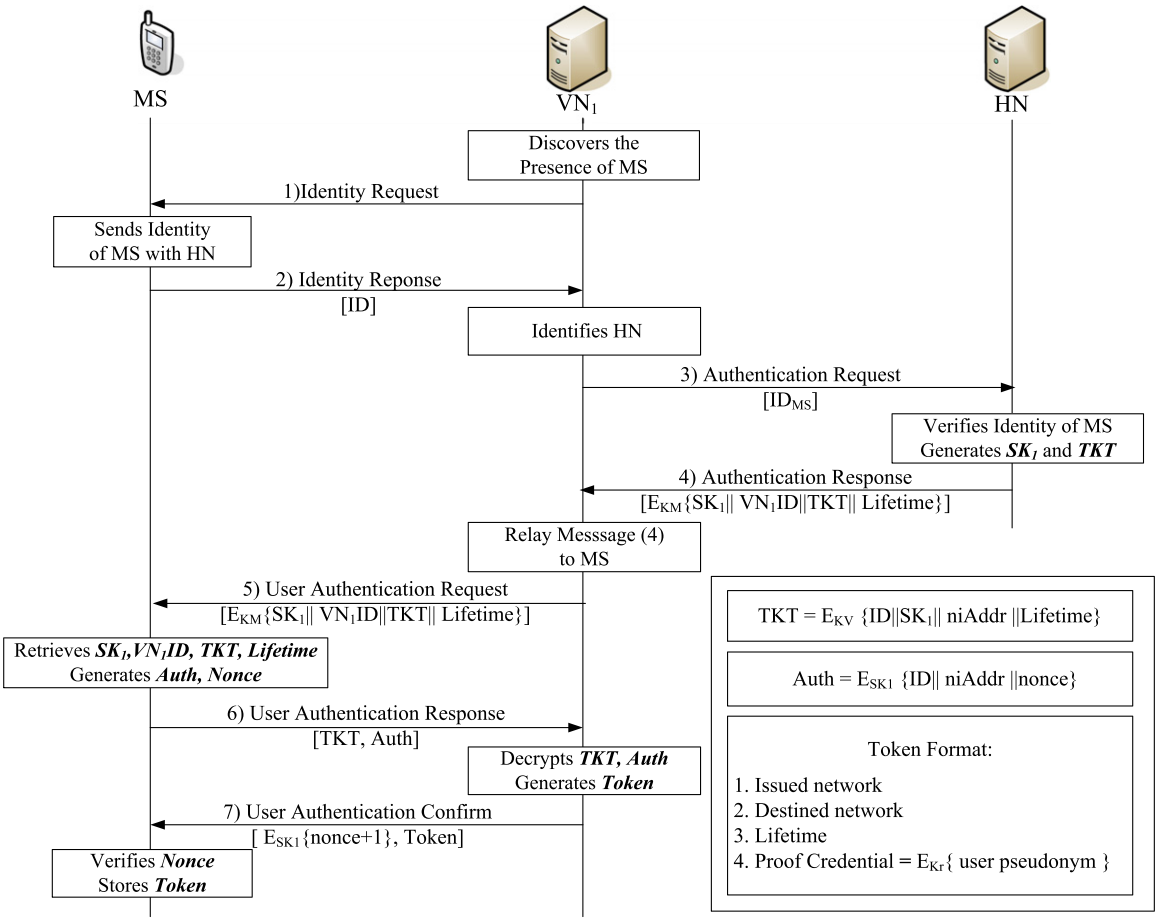

Fig. 4. Initial authentication in VN_1.

Step1: The presence of MS is perceived during scanning phase by the VN_1 within its coverage area and therefor a request is sent for identification of the MS.

Step 2: The MS responds with its identity which is in NAI (Network Access Identifier) format of 72 bytes [12] indicating its home network to which it is subscribed for routing.

Step 3: Upon receiving the address of the home network of MS, VN_1 sends the authentication request to the HN including the identity of MS.

Step 4: The HN confirms the identity of MS and if valid, responds back to MS with message (see (1)) comprising four parameters—a session key (SK_1), the identity of the visiting network (VN_1ID), a ticket (TKT), and its lifetime. The entire parameters are encrypted with secret key K_m. The ticket consists of session key between MS and VN_1, its Lifetime, MS' network interface address (niAddr), and identity of MS all encrypted by the secret key (K_v) shared between VN_1 and HN. niAddr could be IMEI (International Mobile Equipment Identity) for cellular phones or MAC address assigned to network interface cards for computers and so on depending on the devices.

$$E_{Km}\{SK_1 \parallel VN_1ID \parallel TKT \parallel \text{Lifetime}\} \tag{1}$$

$$TKT = E_{Kv}\{ID \parallel SK_1 \parallel \text{niAddr} \parallel \text{Lifetime}\}. \tag{2}$$

Step 5: As the fourth message is encrypted by the secret key K_m that is possessed by only MS and HN, VN_1 cannot decrypt it and simply relays the same message to the MS.

Step 6: The MS decrypts and retrieves the ticket TKT along with session key SK_1, VN_1ID and Lifetime. The MS checks the VN_1ID to confirm if the HN received the authentication request from the same VN as the MS has requested. The MS generates authenticator (Auth) as

$$\text{Auth} = E_{SK1}\{ID \parallel \text{niAddr} \parallel \text{nonce}\}. \tag{3}$$

It then sends TKT and Auth to VN_1.

Step 7: The VN_1 decrypts the TKT with secret key K_v and retrieves the session key SK_1. It also decrypts Auth using SK_1 and recovers identity of MS and nonce. The Auth ensures that the ticket is being presented by the same client to whom

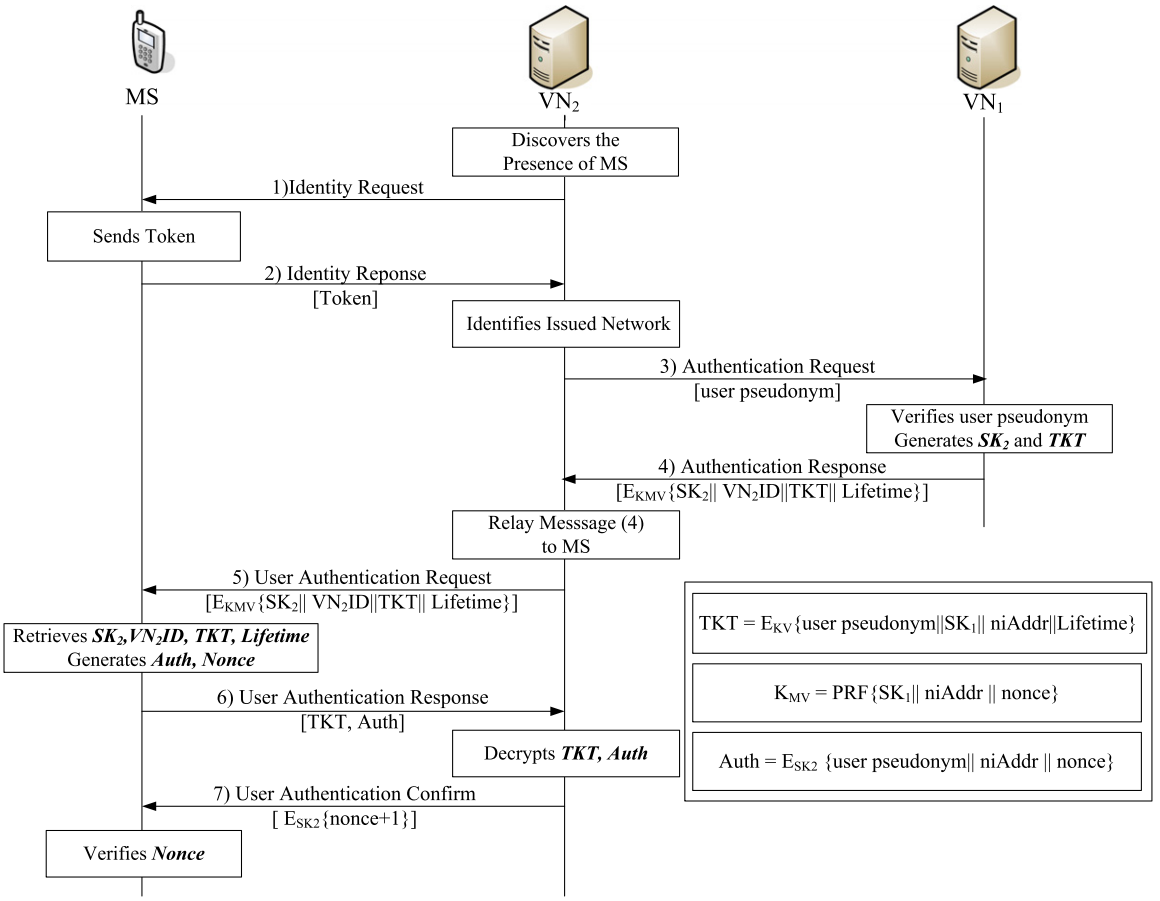

Fig. 5. Re-authentication in VN_2.

it was issued. The recovered nonce is increased by unit value which is then encrypted by the same session key. VN_1 also generates a token to verify MS has been successfully authenticated. The incremented nonce and token are sent back to the MS.

The MS decrypts the message sent by the VN_1 and after confirmation of nonce; the establishment of proper session key between them is realized.

3.3. Token format

The token issued by the first visiting network consists of:

(1) Issued network: represents the name of the network which has provided the token (i.e.VN_1).
(2) Destined network: represents the name of the roaming partner network (i.e. VN_2) of the token issuing network.
(3) Lifetime: determines the end of the token validity period. The lifetime could be set from few hours to days as per our requirement.
(4) Proof Credential: consists of anonymous identity (user pseudonym) provided by the token issuing network (VN_1) to the MS after successful authentication in its domain. The user pseudonym is encrypted by secret key K_r shared by issuing network and destined network.

$$\text{Proof Credential} = E_{Kr}\{\text{user pseudonym}\}. \tag{4}$$

3.4. Re-authentication

When the MS enters VN_2, the roaming partner of VN_1 that shares no trust relations with the HN, VN_1 acts as TTP. The MS presents the token received from VN_1 to authenticate itself in VN_2. The authentication takes place as shown in Fig. 5.

Step 1: The identity of MS is requested by VN_2.

Step 2: MS passes on the token provided to it by the VN_1 from previous authentication process.

Step 3: The VN_2 validates the token and decrypts the proof credentials by using secret key K_r. It then sends authentication request by passing on user pseudonym to the VN_1 which it had assigned to the MS.

Step 4: The VN_1 verifies the user pseudonym and if valid, generates the ticket which consists of new session key (SK_2) between MS and VN_2 encrypted by secret key K_r. VN_1 also derives another key K_{MV} which we refer as extended roaming key. It is also of 128 bits long. This key is derived by pseudorandom function (PRF) from parameters including previous session key (SK_1); nonce and the MS' network interface address (niAddr).

$$K_{MV} = PRF[SK_1 \parallel \text{nonce} \parallel \text{niAddr}]. \tag{5}$$

The MS can derive the extended roaming key before authentication start to reduce authentication latency. VN_2 sends back ticket, session key, and Lifetime along with the identity of new visiting network (VN_2) encrypted by the extended roaming key K_{MV}. The rest of the steps (5, 6, and 7) continue as described in Section 3.2, except this time Auth comprises of parameters as shown in (6)

$$\text{Auth} = E_{SK2}\{\text{proof credential} \parallel \text{niAddr} \parallel \text{nonce}\}. \tag{6}$$

4. Security analysis

4.1. Mutual authentication

Since we deploy TTP during authentication, both the MS and visiting network are certain that they are communicating with their authentic counterparts. Based on the trust shared with TTP, the authenticating entities confirm that both of them share the same session key. The visiting network retrieves session key from TKT sent by MS. The TKT is encrypted by the secret shared key between VN and TTP which assures that the MS cannot modify it. This confirms that the MS is authentic. Similarly, the MS authenticates visiting network using nonce. The nonce is sent embedded within the authenticator. The verification of the incremented nonce which is encrypted with the same session key ensures the VN also possesses the correct session key.

4.2. Key derivation and delivery

The key establishment among the authenticating entities can be divided into the key derivation and key delivery schemes. KAIR protocol involves one key derivation scheme and one key delivery scheme. The session key is always generated by TTP and it is delivered to authenticating parties using secure encryption method based on key delivery scheme. This avoids the computational overhead to client and also reduces the resources required to derive the key. On the other hand, the extended roaming key K_{MV} is based on key derivation scheme. K_{MV} is derived mutually by TTP and the client using common one-way pseudorandom functions based on the parameters like earlier session key between them, nonce and niAddr. We use the key derivation scheme because it provides the opportunity for client to contribute in generating the secret key while it is in alien network that is not trusted by HN. The key itself is not required to be transmitted in the alien network.

4.3. Identity protection

The original identity of the client is hidden in the new VN that does not share any roaming agreement with the HN of MS. To achieve this, user pseudonym is deployed which has no logical relationship with the original identity of the client. The client pseudonym is assigned by the first visited network that shares roaming agreement with HN, while issuing the token. The first visited network however, needs to keep the record of client pseudonym in its database.

4.4. Man in the middle attack

An unwanted party could impersonate in the visiting network. The threat from such an attack is avoided by assuring the identity of visited network provided by TTP in step 4 and 5. TTP sends the identity of visiting network encrypted by secret key shared between MS and TTP. Thus, MS can always compare the received identity of the VN with the one which it receives from beacon signal at scanning phase before it enters to the visiting network. If the two identities do not match each other, the client can be aware of illegitimate entities in the VN. Moreover, the MS can also validate the incremented nonce send by the VN. If somehow it differs from the one sent by the MS or does not receive any nonce at all, it can be aware of false party acting as an entity of visiting network.

4.5. Compromised tickets and tokens

If somehow a ticket or token is compromised, it is still difficult to counterfeit. In order to exploit the use of compromised ticket, one should present authenticator as well. To generate authenticator, niAddr and identity of MS are required which are specific as per the device and the user of device. Similarly, for exploiting stolen token one should have knowledge of previous session key to derive secret key K_{MV}. Without deriving the secret key K_{MV} one cannot decrypt the further message. Besides that, the token has its own lifetime for validity which limits the damage.

Table 1
Comparison.

Protocol [Reference]	Hand off	Encryption key	Computational load	Mutual authentication	Inter technology roaming	Round trip to HN in successive authentication	Inter-domain trust required
TLS [3]	Reactive	Public key	Relatively High	Yes	No	Yes	Certificate based
AKA [6]	Reactive	Secret key	Low	Yes	Cellular/ WLAN	Yes	Full
FAP [11]	Reactive	Any	Variable	Yes	Yes	No	Partial
Proof token [10]	Reactive	Public key	High	Yes	Yes	No	Partial
MPA [9]	Proactive	Not defined	Not defined	Yes	Yes	Yes	Not required
Shadow registration [8]	Proactive	Not defined	Not defined	No	Yes	Yes	Full
KAIR	Reactive	Secret key	Relatively low	Yes	Yes	No	Partial

4.6. Brute-force attack

In order to prevent brute-force attack, no authentication ticket should have a lifetime longer than the expected time required to crack the encryption of the ticket. However, we use 128 bits key Advanced Encryption Standard (AES) which would require years and years to crack even with the latest computing devices, unlike Data Encryption Standard (DES) in actual Kerberos. Hence, the KAIR is safe from brute-force attack. We need to set the lifetime ticket only to avoid replay attack.

5. Comparative analysis

In this section, we analyse the proposed protocol with other protocols discussed in Section 2. We compare these protocols based on seven features as shown in Table 1. Besides MPA and Shadow registration, all the protocols are reactive i.e. authentication takes place after handoff. Although implementing proactive method in inter-domain method is simple, but for inter-domain authentication it requires accurate predictive mechanism which could be difficult to design. A pre-authentication in inter-domain requires sufficient time, so prediction should be made properly about next visiting network. Encryption key is another important parameter as it affects the computational load. The use of complex asymmetric key cryptography in TLS and Proof token methods results high computational load. AKA utilizes pre-shared key in USIM while the shadow registration and MPA do not specify whether to use public key or pre-shared secret key. The key choice is optional in FAP due to which the computational load is variable. KAIR involves symmetric encryption key and involves simple but secure encryption technique like AES.

All the protocols support mutual authentication except the shadow registration. However, although AKA provides mutual authentication, it is still vulnerable to false base station attack. Similarly, the EAP–TLS is designed to support only WLAN technology where as the AKA supports integrated WLAN and cellular network. The rest of the protocols are designed purely for heterogeneous network. During the successive authentication in other visiting networks, TLS, AKA, MPA, and shadow registration require to contact HN resulting higher latency. KAIR, Proof- Token, and FAP use token received from previous successful authentication in successive authentication.

To implement any kind of protocol, we need to have some kind of inter-domain trust. The MPA requires only the MS to have trust relation with the network to which it is trying to connect instead of the current network. In the case of FAP, Proof token and KAIR, the networks are required to have a trust relationship with neighbouring adjacent networks. Whereas in the case of AKA and shadow registration, HN should have direct trust relationship with the visiting networks. TLS is based on digital certificates. So, these certificates should be issued by same CA or should have chain to a trusted root CA. Overall, KAIR is satisfactory in terms of all the features enlisted in Table 1.

6. Performance evaluation

The authentication process introduces overhead in communication and influences QoS metrics. Hence, it is necessary to maintain the authentication latency to minimum. We compare the authentication latency of KAIR protocol with already implemented standard protocols like the EAP–TLS and AKA. Since, the rest of the protocols are still under research and exact specifications are unavailable to implement under our test bed, we limit them to comparative analysis only.

6.1. Simulation methodology and testbed

Based on the specifications of each protocol, we compute the number of messages sent and received by the MS, home network, and visiting network along with the length of each message in bytes. The computational speeds of cryptographic

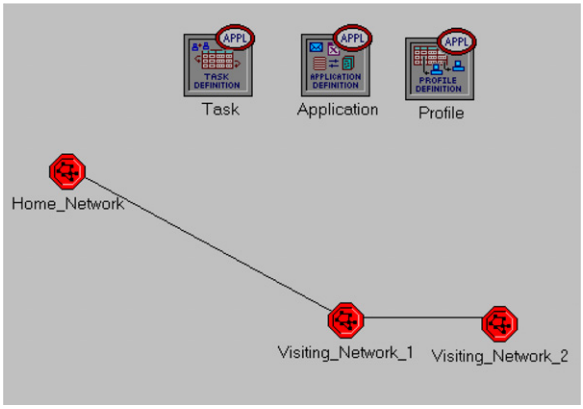

Fig. 6. Simulation setup.

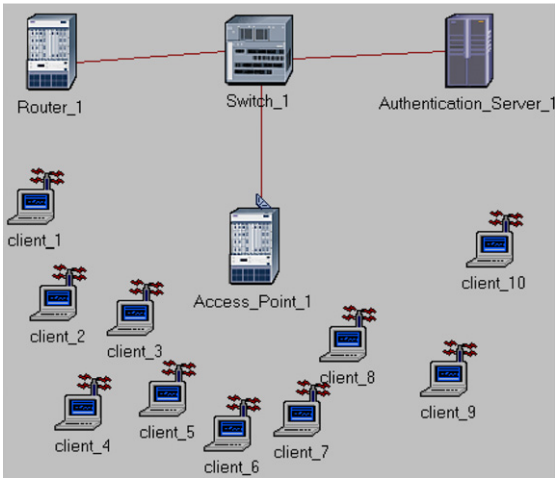

Fig. 7. Network configuration in visiting_network_1.

algorithms for encryption and decryption are obtained using a tool called Crypto++ [13]. The test is carried out running on the Intel Core 2.2.1 GHz processor under Windows XP SP1.

We implement the protocols in OPNET [14] simulator. Four scenarios are designed each one for the implementation of TLS, AKA and KAIR (initial and re-authentication) protocols. The roaming scenario for TLS is set up similar as explained in [15,16]. We set up three networks namely home_network, visiting_network_1 and visiting_network_2 as shown in Fig. 6. 802.11b environment is set up in visiting_network_1 where as UMTS network is set up in visiting_network_2 as depicted in Figs. 7 and 8 respectively. The home_network is set up geographically far from visiting_network_1 where as the roaming partner of visiting_network_1 i.e. visiting_network_2 is set up close to it. KAIR initial authentication occurs in visiting_network_1 and re-authentication in visiting_network_2. For KAIR, we chose the AES for encryption and decryption. In KAIR, the length of session key, ticket and token is 16 bytes, 102 bytes and 222 bytes respectively. The lifetime and nonce length are 6 bytes and 8 bytes respectively.

In the first experiment, we set the RTT between HN and VN around 200 ms. The RTT between visiting_network_1 and visiting_network_2 is set around 20 ms. We varied the number of MS in the VN from 1 to 35 with interval of 5. As such, each scenario is simulated 8 times. The authentication delay for each MS is recorded for all 8 simulations of each scenario. Then the average authentication is calculated. Likewise, in the second experiment, we set 20 mobile stations in the network and the RTT is varied from 100 to 500 ms with an interval of 50 ms. As in the first experiment, we run multiple simulations for each scenario and average authentication delay is recorded.

6.2. Results

Experimental results show the authentication delay of standard authentication protocols and the proposed protocol. Fig. 9 illustrates the average authentication latency for different number of MS. It can be seen that the latency provided by KAIR is least. During experiment, we found that the round trip time between visiting network and home network has an overwhelming impact on the authentication delay compared to that of the latency caused by the necessary cryptographic

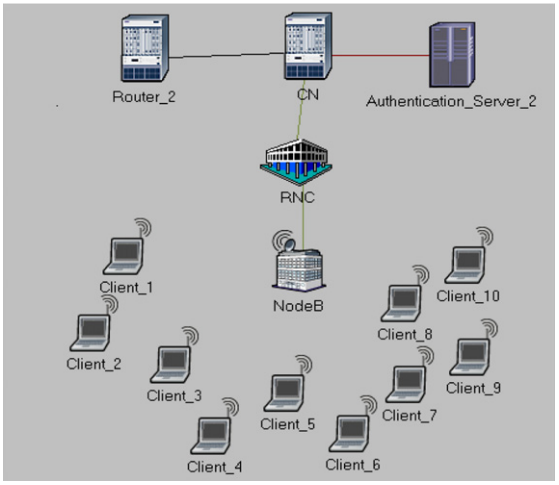

Fig. 8. Network configuration in visiting_network_2.

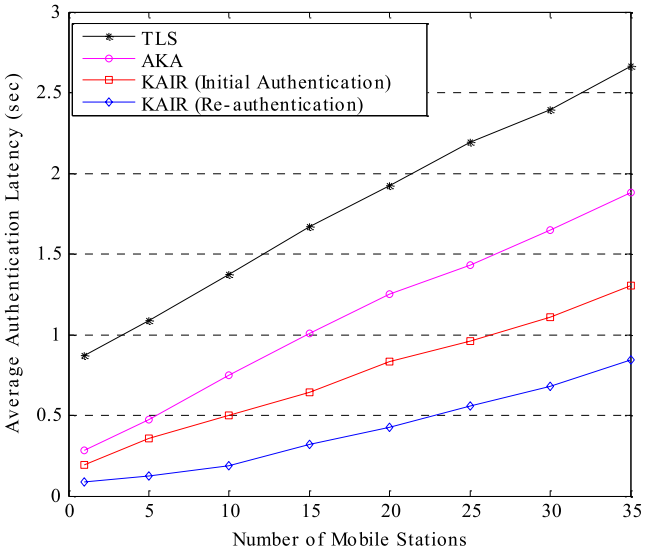

Fig. 9. Average authentication latency vs. no. of MS.

computations. Since, TLS involved multiple round trips to home network, complex cryptography, and sharing of certificates with the mandatory chain to a trusted common root CA, it presented the highest delay. In the case of AKA, the transmission of multiple sets of authentication vectors from home network to visiting network led relatively extra delay compared to the proposed protocol. As the RTT between HN and VN was very critical in determining the latency, we check the average authentication latency in terms of RTT in Fig. 10. Latency drastically increased in TLS with increasing RTT while it gradually increased in the case of AKA and KAIR. On analysing the results of two experiments, it can be seen that the average authentication delay for KAIR is least.

7. Conclusion and future work

In this paper, we proposed a TTP based authentication protocol as in Kerberos suitable for inter-domain roaming in distributed heterogeneous network. The use of token helps to improve the mobility range in wide heterogeneous network in a secure manner. The ticket issuing authority is achieved by a visiting network once the client and the visiting network mutually authenticate themselves in the presence of home network's participation. The ticket issuance authority can be moved from one network to another constituting a chain formation. The main advantage of such an approach is performance because the authentication requires message deliveries no farther than the adjacent networks. If an MS has tokens of a few domains that it has visited recently, it can use the token provided by such domains to authenticate in most of the other domains it wants to visit. The simulation results and analysis demonstrate that our protocol is secure and offers lower latency.

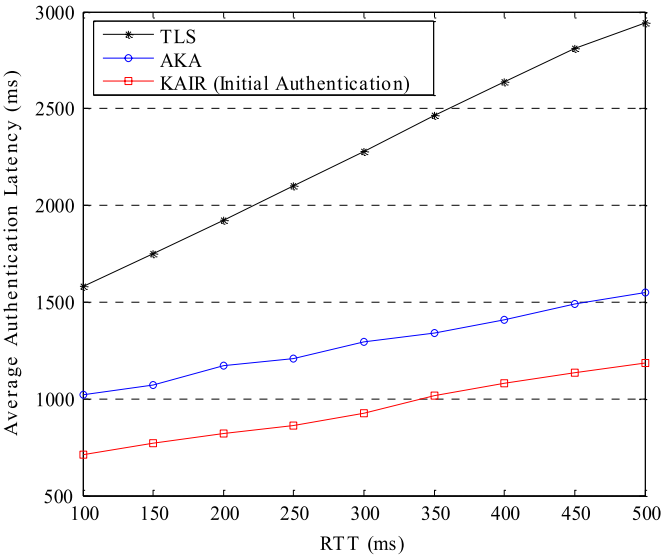

Fig. 10. Average authentication latency vs. RTT.

The proposed solution does not include the authorization and accounting issues while roaming in foreign networks that do not share any roaming agreement with home network of MS. In the future work, we will further investigate policy based authorizing and billing to overcome such problems. Managing such a policy completely lies in the hand of home network and informs about the policy to its roaming partner. As such, the previous visited network can grant token to the MS based on such policies only.

Acknowledgements

This study was supported (in part) by research funds from Chosun University 2010.

References

[1] W. Stallings, Wireless Communications & Networks, Second ed., Pearson Education International, 2005.
[2] J. Kohl, C. Neuman, The Kerberos Network Authentication Service (V5), IETF RFC 1510, Sept. 1993.
[3] D. Simon, B. Aboba, R. Hurst, EAP–TLS Authentication Protocol, RFC 5216, Mar. 2008.
[4] Y. Tseng, USIM-based EAP–TLS authentication protocol for wireless local area networks, Comput. Stand. Interfaces 31 (Jan.) (2009) 128–136.
[5] G. Kambourakis, A. Rouskas, G. Kormentzas, S. Gritzalis, Advanced SSL/TLS-based authentication for secure WLAN-3G interworking, Proc. IEE Commun. 151 (5) (2004) 501–506.
[6] J. Arkko, H. Haverinen, Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA), RFC 4187, Jan. 2006.
[7] M. Zhang, Y. Fang, Security analysis and enhancement of 3GPP authentication and key agreement protocol, IEEE Trans. Wireless Commun. 4 (2) (2005) 734–742.
[8] T.T. Kwon, M. Gerla, S. Das, Mobility management for VOIP service: Mobile IP vs. SIP, IEEE Wireless Commun. Magazine (Oct.) (2002) 66–75.
[9] A. Dutta, A framework of Media-Independent Pre-Authentication (MPA) for interdomain handover optimization, IETF draft, draft-ohbamobopts-mpa-framework-05.txt, Jul. 2007.
[10] S.R. Tuladhar, C.E. Caicedo, J.B.D. Joshi, Inter-domain authentication for seamless roaming in heterogeneous wireless networks, in: Proc. IEEE SUTC'08, Jun. 2008, pp. 249–255.
[11] M. Komarova, M. Riguidel, A. Hecker, Fast re-authentication protocol for inter-domain roaming, in: Proc. IEEE PIMRC'07, Sept. 2007, pp. 146–151.
[12] B. Aboba, M. Beadles, J. Arkko, P. Eronen, RFC 4282- The Network Access Identifier, Dec. 2005.
[13] Crypto++ Library 5.5.1, http://www.cryptopp.com.
[14] Official site of OPNET, http://www.opnet.com.
[15] B. Vaidya, Y.J. Kim, E.K. Kim, S.J. Han, Investigating authentication mechanism for wireless mobile network, in: LNCS, vol. 4159, Springer, 2006, pp. 902–911.
[16] J. Cordasco, U. Meyer, S. Wetzel, Implementation and Performance of EAP–TLS-KS, in: Proc. SecureComm'06, Aug. 2006, pp. 45–56.