Securing Mobile Access in Ubiquitous Networking via Non-roaming Agreement Protocol

Talal Alharbi, Abdullah Almuhaideb, and Phu Dung Le

Faculty of Information Technology, Monash University, Melbourne, Australia
Tralh1@student.monash.edu,
{Abdullah.Almuhaideb,Phu.Dung.Le}@infotech.monash.edu.au

Abstract. Rapid developments in wireless technologies in terms of speed, quality and coverage are great motivations that lead to an increase in the use of mobile devices such as laptops and smart phones. These developments facilitate exchanging information anywhere any time. However, some concerns have been raised especially when the mobile users want to access services that provided by foreign networks. These issues can be classified as security and performance matters. This paper proposes a fast and secure authentication protocol. The new feature about this protocol is that the foreign network (FN) can authenticate the mobile user (MU) without checking with the home network (HN). This feature can effectively enhance the network performance as just two messages are required to authenticate the MU. Moreover, we will demonstrate the strengths of this protocol against the common security attacks and we will compare the protocol performance with the previous protocols to ensure efficiency.

Keywords: Authentication, wireless networks, security, mobile user, telecommunication security.

1 Introduction

The advanced capabilities of mobile devices and wireless technologies facilitate accessing a variety of services over the Internet: e-mail, mobile commerce and mobile banking. It is becoming more and more desirable to mobile users (MUs) to access these services wirelessly while they are on the move without being restricted to specific locations. In 2007, over 750 million people accessed the Internet contents via mobile phones [1]. However, for MUs to have the best connection, they need to connect to different types of technologies and service providers based on their locations and the target speed. The existing approaches to such problem are either to have a prior roaming agreement between the home network (HN) and the foreign network (FN) for verification process or to authenticate the MUs with their HNs once they request services. Authenticating MUs with HNs sometimes results in overhead in the network as it takes a long round trip through the network to reach the authentication servers located in HNs of the MUs. Moreover, sometimes the communications with the HNs are unavailable. Fig1. is an illustration of the problem. Therefore, it is necessary to determine the

M. Soriano, S. Qing, and J. López (Eds.): ICICS 2010, LNCS 6476, pp. 126–139, 2010.

possibility to securely authenticate unknown MUs by the FNs themselves independently without any prior roaming agreements or communications with the HNs.

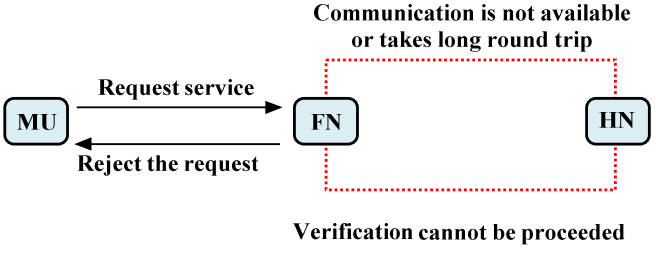

Fig. 1. Illustration of the Problem

To the best of our knowledge, no non-roaming agreement based protocol has been proposed to eliminate the verification processes with HNs. As a practical solution, we propose a fast and secure authentication protocol that assists the FNs to authenticate visiting MUs independently. Fig.2 illustrates the four steps that involved in the traditional protocols which will be reduced to two steps in the proposed protocol.

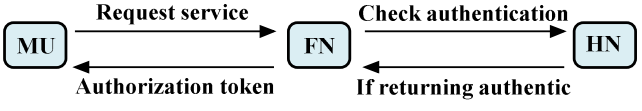

Fig. 2. An overview of the traditional authentication protocols

To address the above issue, this paper aims to:

1. Review the related works in the field of authentication in ubiquitous environment,
2. Propose a new authentication protocol, and
3. Evaluate the proposed protocol in terms of security and performance aspects.

Paper organization. The rest of this paper is organized as follows. Section 2 is a review of the existing approaches to the problem. Then the fast and secure protocol will be proposed in Section 3. We then perform the security and performance analyses (Section 4 and 5). Finally, Section 6 concludes the paper.

2 Related Work

Various authentication protocols have been proposed to ensure the security of the communications between the MUs and the service providers. These protocols can be classified into either roaming or non-roaming agreement protocols. In the following sections, these two types will be discussed in terms of their limitations and security vulnerabilities.

2.1 Roaming Agreement Protocols

The term "roaming agreement protocol" means that the verification process between the FN and the HN is performed based on a roaming agreement. Fig. 3 shows the architecture of the way that service providers connect to each other to authenticate the visiting MUs.

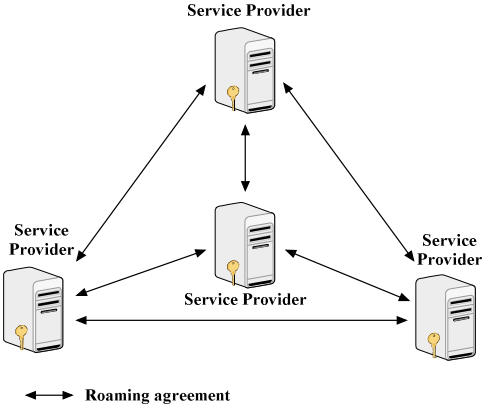

Fig. 3. The architecture of the roaming agreement authentication protocols

In [2] the authors illustrated the major drawback of this type of protocols which is the difficulty to establish and maintain roaming agreements with every possible administrative domain. Assuming that there are *N* number of administrative domains, the total number of the required roaming agreements between them can be calculated using the following formula:

$$Required\ roaming\ agreements = \frac{N(N-1)}{2}$$

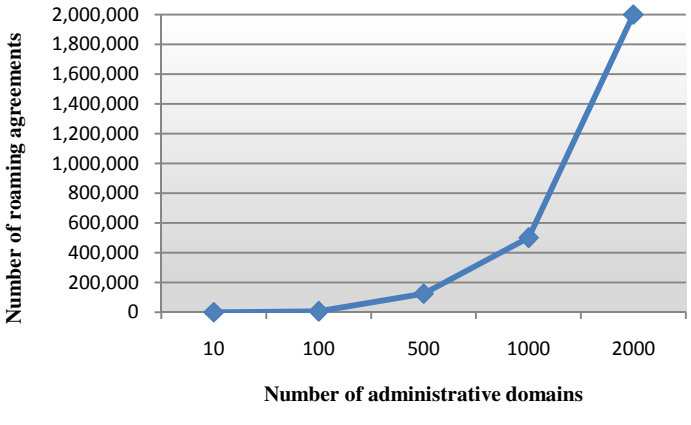

Fig. 4. The required roaming agreements increase significantly as the number of service providers increases

Fig. 4 shows that the number of roaming agreements increases dramatically compared to the number of the service providers. For example, if there are ten service providers, it requires 45 roaming agreements, while in the case of 2000 service providers; it requires around 2,000,000 roaming agreements. This is considered infeasible to be implemented and not scalable in a ubiquitous environment. Despite this significant limitation, some of these protocols will be reviewed just to provide an idea to the way that the verification processes are performed.

In [3] the authors proposed a protocol that assists the FNs to authenticate MUs through their HNs. The access is granted via anonymous tickets issued by FNs after successful verifications with their HNs. The protocol protects the user's anonymity. To secure the verification process, the HN shares a secret key with the FN. Therefore, this protocol cannot be performed if there is no agreement on a secret key between the HN and FN. Also, five messages are involved in this protocol before the FN and the MU can trust each other which can be considered a performance issue.

In [4] an authentication protocol based on the off-line roaming authentication was proposed. For each MU who wishes to roam into a FN, s/he is required to communicate to the authentication server at the HN to obtain the roaming information before requesting access to the FN. This information will assist the FN to authenticate the visiting users. In this protocol, the FN can authenticate the visiting users through exchanging only two messages rather than four as in the typical protocols. However, the user's freedom of choosing the service providers is limited. Since MU cannot request services from a FN unless prior roaming information was obtained.

In 2009, [11] proposed an enhanced authentication protocol to protect the roaming user's anonymity. Their protocol uses nonces to provide a strong security against any possible attacks. The communication between the FN and the HN is encrypted using a long term secret key. However, some security, performance and storage issues have been found in this scheme. In [12], four types of attacks are introduced to break the anonymity of the MUs. Another vulnerability is that any exposure of the MU's identity can easily lead to the discovery of the session keys. As a performance issue, eight messages are required to be exchanged to verify the MU's identity. A secure and efficient database is needed to store all the session keys between the HN and their service provider partners.

2.2 Non-roaming Agreement Protocols

This type of protocols do not relay on prior agreements between the FNs and the HNs for the verification processes and the service provisions. They are also known as "Seamless Roaming Protocols". This type of protocols is more desirable and efficient in the ubiquitous wireless environment. However, security in this type of protocols is more challenging [5].

In [6] an authentication scheme for wireless communications has been proposed. They argued that the protocol provides strong authentication that can grant the user's anonymity. However, three security issues in this protocol were illustrated in [7]. Firstly, it failed to provide a mutual authentication. Secondly, a forgery attack can be achieved. Finally, if the attacker discovers a session key, s/he can easily compute the future session keys. To overcome these shortcomings, they proposed some improvements that can eliminate the weaknesses of this protocol.

In [8] the authors demonstrated that even the enhanced protocol by Lee, Hwang and Liao failed to protect the anonymity. They also pointed out the protocol does not achieve backward secrecy. As a solution, they modified the scheme to solve these issues.

In [9] the authors pointed out that all the above schemes the original and the two enhanced protocols have not succeeded in protecting the user's anonymity. For any two users who are registered with the same service provider, one can obtain the other's identity. Moreover, [10] illustrated that impersonation attack can be performed using a stolen smart card. Finally, they came to the conclusion that these schemes are not secure enough to be implemented and that similar design mistakes should be considered properly in the future protocols.

In 2010, a user authentication scheme for wireless communication with smart cards was proposed [5]. The FNs issue temporary certificates for the MUs ($TCert_{MU}$) as verifications tokens. The authors argued that their protocol enjoys a high level of security and performance. However, we found that this protocol has a security issue that the HN can compute the session key between the MU and the FN. When the HN verifies the MU is a legitimate user, it computes $w=h(h(N||ID_{MU}))||X||X_0)$ and sends it with other values to the FN. To encrypt the message to the MU, the FN computes the session key by hashing the w. Thus, the session key will be $k=h(h(h(N||ID_{MU}))||X||X_0)$. Now, the HN is able to compute this session key. A further issue is that four messages are exchanged in their protocol. This can result in huge consumption of the network bandwidth. Moreover, since the HN is involved in the verification process, the protocol cannot be implemented if the FN is unable to communicate with the HN due to network or communication problems.

2.3 Summary

As seen in the above sections, the major drawback of the roaming agreement protocols is that the difficulty for any HN to establish a roaming agreement with every possible service provider. As a result, the MU's freedom is restricted to a limited number of service providers. On the other hand, the non-roaming protocols are more convenient to the MUs in term of flexibility. However, they can be vulnerable to some security attacks or may have performance issues.

3 The Proposed Scheme

To achieve ubiquitous wireless access, MUs should be able to have a direct negotiation with any potential FNs regarding service provisions. The FNs are required to verify the MU's identity and credentials. There should be more flexible ways to establish trust without verifying the MU's credentials with the HN.

The MUs should be pre-registered with their HNs to get identification tokens. In this protocol, MUs are able to negotiate directly with potential FN providers to get the authorization tokens. Also, FN providers are able to communicate directly with visiting MUs and make trust decisions whether to provide network services or not. For MUs to establish trust with the FNs, Certificate Authority (CA) is employed to obtain the public key of the FN.

This section proposes a fast and secure authentication protocol to address all the associated limitations with the existing approaches. Our protocol enjoys the following features:

- **It is wireless technology independent:** It is not feasible to achieve ubiquitous mobile access with a single wireless technology. Therefore, the authentication solution should enable access to the core network regardless of the types of wireless technology. The proposed authentication solution is not designed for a specific underlying wireless technology. It is aimed to be designed at the network layer of the OSI to avoid the differences in the data link and physical layer.
- **Support direct negotiation:** MUs should be able to choose and select the appropriate network based on direct negotiation of services and authentication. The proposed solution supports direct negotiation with the MU not with the HN, which will increase the satisfaction of the user.
- **It is roaming agreement independent:** Authenticating the visiting MUs should be based on non-roaming agreement scheme to establish trust with foreign network providers to access services. It is not likely to a HN to set up formal roaming agreements with every possible provider to enable their users to be always connected. Our approach does not depend on roaming agreement between the FN and the HN. Alternatively, the FN provider uses negotiation and trust decision whether to authorize or reject the MU.
- **Privacy and user anonymity:** The MU's personal details are stored confidentially with the HN. Therefore, when a MU wants to roam into a FN, s/he only needs to send his or her Passport without revealing any information related to the actual ID. This means the FN has no idea about the ID of the owner of this Passport.

3.1 The Fast and Secure Authentication Protocol

The proposed protocol consists of two tokens: Passport and Visa. The "Passport" is an authentication token that is issued by the HN to their registered MUs in order to identify and verify the MU's identity. The Passport is only to be used to request services within the HN's domain. However, when the MU becomes an authorised user to the FN, an authorisation token "Visa" will be issued for him or her. The Visa token is used to control the access to the FN's domain. In this protocol, public key cryptography is used to encrypt only the first message between the MU and the FN. Since the mobile devices are becoming more powerful and have better capabilities in memory and battery, we consider this as an acceptable encryption. This can be justified as it is performed only once and the mobile device is not required to store the FNs' public keys. The following is a set of protocols that were developed to achieve the research objectives. However, before we proceed, some notations are clarified in the following table.

3.2 Passport Acquisition Protocol

This protocol describes the MU registration process with the HN (Passport issuer). Upon completing this phase, the MU will receive a Passport (identification token). For any service request from a FN, s/he is required to have a Passport that is regisered with his or her HN.

Table 1. Notations used in the protocol

Symbol	Description
HN	Home network service provider that the mobile user is registered with
FN	Foreign network service provider that the mobile user roams into
MU	Mobile user
ID_A	Identity of an entity A
T_A	Timestamp generated by an entity A
PK_A	Encrypting a message X using the public key of A
$Sig_A(X)$	Signing a message X using the private key of A
$h(.)$	One-way has function
r_A	A random number generated by an entity A
$Passport_B^A$	A passport that issued by a home network A to the mobile user B
$Visa_B^A$	A visa that issued by a foreign network A to the mobile user B
$Pass_{No}$	The passport number
$Visa_{No}$	The visa number

The registration with the HN takes place offline and it occurs once and when completed, the HN issues a Smart Card (SC) which contains three components:

1) **A $\mathbf{Passport_{MU}^{HN}}$ for the MU:** The Passport is given in the following format:

$$Passport_{MU}^{HN} = Sig_{HN}\,(Pass_{No}, expiry, data, valid, stamp)$$

In the Passport, Sig_{HN} represents the digital signature of the Passport using the HN's private key which can be verified to ensure the integrity of the Passport. Inside the Passport, the following information can be stored: The Passport number "$Pas\,\text{帿}_{No}$", the "*expiry*" field which corresponds to the Passport expiry date and the "*data*" field which consists of other relevant information such as the type of Passport, type of the MU, issue date, the place of issuer, issuer's ID, and issuer's name. The field *"valid"* is set to TRUE unless it has been revoked. Since the proposed protocol aims to eliminate the communication and the verification between the FN and the HN, the field *"stamp"* is to be the date of the last check by the HN that the MU is an authentic user. Therefore, for a Passport to be considered as valid, it should have a recent stamp date. To do so, the MU should let the HN stamp his or her Passport before s/he leaves the HN domain.

2) **A symmetric shared Key ($\mathbf{K_{MU-HN}}$):** It is used to encrypt the communication with the HN to revocate the Passport in case it has been stolen.
3) The $\mathbf{Pass_{No}}$**:** This is to be used by the MU as an element when generating the session keys. We will illustrate this in the service provision protocol.

To increase the security of the system, the SC information is encrypted with the MU's biometric information (such as finger print).

3.3 Visa Acquisition Protocol

When the MU has his/her Passport (authentication token) in hand, s/he becomes eligible to communicate with any FN to request a Visa. The process starts by obtaining the FN's certificate from Certificate Authority (CA) to encrypt the connection. The protocol can be demonstrated as follows:

Step 1: $MU \rightarrow FN$:

$$PK_{FN}\{Passport_{MU}^{HN}, Visa\ request, ID_{HN}, T_{MU}, h_{(r)}\}$$

This protocol starts once a MU sends his or her $Passport_{MU}^{HN}$, the *Visa request*, ID_{HN}, T_{MU} and $h(r)$.The ID_{HN} is the HN's ID, $h_{(r)}$is a hash random number, and T_{MU} is the MU's timestamp. All are encrypted by the FN's public key. The $h_{(r)}$is used by the FN to encrypt the message back to the MU.

Step 2: $FN \rightarrow MU$:

$$\{Visa_{MU}^{FN}, T_{FN}, IK_{MU-FN}\}_{h_{(r)}}$$

After the FN receives the message from the MU, it decrypts the message using its private key. Then it will check whether the T_{MU} within an acceptable range of time or not. If not, it will discard the message; otherwise it will check the integrity of the HN's signature using the HN's public key. If it is valid, it will check the Passport data such as the fields *"valid"* and *"stamp"* to be "TRUE" and a recent stamp date. Then the FN issues a Visa for the MU. The Visa is given as follow:

$$Visa_{MU}^{FN} = Sig_{FN}\ (Pass_N, Visa_{No}, expiry, data, valid)$$

The "Pass_{No}" is the Passport number of the MU. The Visa number *"*$Visa_{No}$*"* is the unique identity of the Visa and the *"expiry"* is the Visa expiry date. The *"*$data$*"* field includes all detailed Visa information such as Visa type, number of access, duration of access, issuer place, issuer ID, issuer's name, the issue date, service type, and service name. The field *"valid"* is set to FALSE once a Visa is revoked; otherwise it is set to TRUE. The signature of the FN Sig_{FN} in the Visa is used to stop forging Visa.

After issuing the Visa for the MU, a message will be sent to that user containing the $Visa_{MU}^{FN}$, T_{FN} and the initial key (IK_{MU-FN}) all encrypted by $h_{(r)}$.

Once the MU receives the message from the FN, s/he will decrypt the message to obtain the authorization token "Visa" and becomes an authentic user to the FN. Fig.5 illustrates the two steps to obtain the Visa.

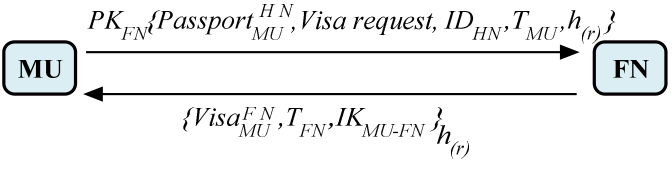

Fig. 5. An overview of the proposed protocol

3.4 Mobile Service Provision Protocol

This protocol illustrates how a MU can be granted network services from a FN in a secure manner. When the MU obtains a valid Visa, the MU will be eligible to request network services from the FN. S/he needs to generate the first session key (SK'_{MU-FN}) using the hash function of three factors: The initial key (IK_{MU-FN}) (received with the Visa), Passport and Visa numbers as follows:

$$SK'_{MU-FN} = h(IK_{MU-FN}, Visa_{No}, Pass_{No})$$

Step1: $MU \rightarrow FN$

$$SerReq, Visa_{MU}^{FN}, \{r_{MU}, Visa_{No}\}_{SK'_{MU-FN}}$$

To request an access to the FN services, the MU sends $SerReq$, the $Visa_{MU}^{FN}$ and $\{r_{MU}, Visa_N\}$ which are a random number and the Visa number all encrypted by the first session key (SK'_{MU-FN}).

Step 2: $FN \rightarrow MU$

$$\{r_{FN}, Pass_{No}\}_{SK''_{MU-FN}}, \{Service\}_{SK'''_{MU-FN}}$$

After the FN receives the service request, it checks the Visa validity using its public key. If the Visa is considered as valid then, the FN gets the $Visa_{No}$ and searches in its database to see if the Visa is used for the first time. The $Visa_{No}$ is used by the FN to detect if the holder is genuine. However, the FN has to compute the SK'_{MU-FN} to verify $Visa_{No}$ and to get the MU's random number r_{MU}. The random number will be used to generate the second session key (SK''_{MU-FN}) as follows:

$$SK''_{MU-FN} = h(SK'_{MU-FN}, IK_{MU-FN}, r_{MU})$$

The third session key will be used by the FN to encrypt its random number r_{FN} and the Passport number $Pass_{No}$. Finally, the third session key (SK'''_{MU-FN}) will be generated using the FN random number r_{FN}, the first and second session keys.

$$SK'''_{MU-FN} = h(SK''_{MU-FN}, SK'_{MU-FN}\ r_{FN})$$

By having the third session key in hand, both parties know that mutual authentication has been achieved and the service can be started. However, for the next access, the MU is required to generate a new session key by performing the above protocol again and change the (IK_{MU-FN}) to be the last session key.

3.5 Passport and Visa Revocation Protocols

These protocols will be used to stop requesting services with a stolen Passport or Visa.

- **Passport Revocation**

If a Passport is considered to be stolen, the MU sends a message to the HN to revoke the Passport. The revocation message can be illustrated as:

$$MU \rightarrow HN: \{Pass_{No}, RevOke, Passport_{MU}^{HN}\}_{K_{MU-HN}}$$

The protocol starts when the MU sends the RevOke message encrypted with the shared key between the MU and the HN. The HN decrypts the message with relevant key. Then it will update the field *"valid"* to be FALSE and stop any service request from the HN with this Passport. This protocol is used when the MU is located in the HN domain.

- **Visa Revocation**

In the case of the MU is located in the FN domain and s/he believes his or her Visa has been compromised. The revocation message will be as follows:

$$MU \rightarrow FN: \{ (Pass_{No}, Visa_{No}, RevOke)_{SK'_{MU-FN}}\}_{SK_{MU-FN}}$$

When the FN receives a RevOke message from the MU, the FN decrypts the message with the last session key (SK_{MU-FN}) then verifies that by decrypting the other part of the message with the first session key (SK'_{MU-FN}) .The FN updates the status of the Visa as RevOke. For any network services requests, the FN checks whether the Visa has been revoked. If so, the request will be rejected.

4 System Security Analysis

In this section, we will analyse the security of the proposed scheme with respect to some common attacks:

Proposition 1. Passport or Visa cannot be forged.
Proof. Since the Passport and the Visa contents are signed by the issuer's private key, they cannot be generated by attackers in the name of the HN or the FN. So it is impossible to fabricate or fake a Passport or a Visa to request services as the issuer will check the integrity of the token by verifying the signature. For example, if FN cannot verify the Visa using its public key, it means this Visa was not issued by them. Therefore, the service request will be rejected.

Proposition 2. Service cannot be obtained using a revoked Passport and Visa.
Proof. The field "*stamp"* in the Passport is used to stop requesting services with a revoked Passport. Therefore, when the MU requests a Visa, the FN checks the issuer's stamp date. If the Passport has a recent stamp date, it means that the HN witnessed the MU being a registered and authentic user. Otherwise, the request is rejected.

Proposition 3. Service cannot be obtained using a stolen Passport.
Proof. As the MU's Passport is stored in the smart cart and is encrypted with his or her biometric information, the Passport cannot be retrieved by attacker. Another case might be that the MU sends his or her Passport to a malicious FN to request service.

We assume that the MU is fully sure that s/he is communicating with a real service provider, since the public key is obtained through the CA. Even if the Passport in the worst case has been stolen by a malicious FN, the Passport will be invalid soon as the "*stamp"* date will expire and cannot be updated.

Proposition 4. The scheme provides mutual authentication.
Proof. In the mobile service provision phase, the MU sends a message that consists of two parts: the Visa, and the encrypted new random number r_{MU}.The FN verifies the Visa with its public key and acquires the shared key. Also as the FN signed the Visa, it can check the validation of the Visa. The FN uses the previous session key with $Pass_{No}, Visa_{No}$ to generate the first session key which will be used to decrypt the second part of the message and get a new random number. The shared master key with the first session key, and r_{MU} will be used to generate the second session key. By decrypting the FN message, the MU can get the FN's random number. Now, both parties are able to generate the third session key and mutually authenticate each other.

Proposition 5. The protocol can prevent replay and man-in-the-middle attacks.
Proof. When a MU wants to communicate with a FN, s/he encrypts the message with the FN's public key. Thus, an attacker may be able to sniff the message but it is impossible to him or her to decrypt the message since s/he is required to have the private key of the FN. In addition, timestamps are used in each communication between the MU and FN to ensure the message has not been replayed by attacker.

Proposition 6. The proposed scheme is safe against impersonation attacks.
Proof. In our protocol, the stored information in SC (e.g. Passport) is encrypted with the MU's fingerprint. Thus, in the case of SC has been stolen, it is infeasible for attackers to impersonate the MU to have access to the services.

Proposition 7. The proposed scheme can withstand spoofing attack.
Proof. Since the MU obtains the FN's public key from the CA, s/he is indeed sure that s/he is communicating with a real service provider and not with a bogus entity.

Proposition 8. The proposed scheme ensures the key freshness.
Proof. In every service request, a new session key is generated and it is only valid in that session. This key is established by contributing the random numbers of both the MU and the FN. Therefore, the key freshness is guaranteed.

Proposition 9. The proposed scheme provides the user's privacy and anonymity.
Proof. The MU's personal details are kept secretly with the HN. When the MU wants to roam into a FN, s/he only needs to send his or her Passport without revealing any information related to his or her actual ID. This means that the FN would not know the ID of the owner of this Passport.

The following is the security comparisons of the related schemes and the proposed scheme.

Table 2. The security comparisons

Security requirements	[6]	[7]	[8]	[10]	[11]	[5]	Proposed scheme
Mutual authentication	No	Yes	Yes	Yes	Yes	Yes	Yes
Impersonation attack resistance	No	Yes	No	Yes	Yes	Yes	Yes
Replay attack resistance	Yes	Yes	No	Yes	Yes	Yes	Yes
Protect user's anonymity	No	No	No	No	No	No	Yes
Forgery attack resistance	No	No	No	Yes	Yes	Yes	Yes
Backward secrecy	No	No	Yes	Yes	No	Yes	Yes
The HN cannot decrypt the communication between the MU and the FN	No	No	No	No	No	No	Yes

5 Performance Analysis

In this section, we evaluate the proposed protocol in terms of communication and computation costs with the scheme in [5]. We choose to compare with this protocol because it comes as the second best protocol that meets the security requirements after the proposed scheme as shown in the previous section.

5.1 Communication Cost

We have identified three key requirements for the fast an efficient ubiquitous authentication protocol as follows:

A. **No verification with the HN:** The FNs should be able to check the authenticity of the MUs without any further communication with the HNs. This novel feature has not been implemented or even discussed in the previous non-roaming agreement protocols. In the proposed protocol, the FN does need to verify the MU's credentials with the HN due to following security features in the Passport. Firstly, the Passport is given in a digital signature format. Secondly, the field "*valid*" indicates that the Passport has not been revoked. Finally, the field "*stamp*" means that the HN witness the MU is a registered and authentic user.

B. **No re-authentication with the HN:** FNs should not be required to authenticate the MUs with their HNs for each time they try to login to their domains. The deference between this requirement and the previous one is that the MUs are needed to be authenticated again for the next logins whereas in (A) they become authorized users after the first logins.

C. **Minimum number of messages:** The total required number of exchanged messages in the protocol in order to authenticate the visiting MUs should be minimized as possible.

The following table indicates that our proposed protocol can satisfy these requirements while the others cannot.

Table 3. A comparative evaluation between the existing approaches and our protocol

Approach	A	B	C
The scheme in[5]	No	Yes	4
Proposed protocol	Yes	Yes	2

5.2 Computation Cost

In this section, we compare the required operations in the entire protocol from the login phase until the MU becomes an authorized user to the FN. Our calculation time is based on [3], where they calculated that a symmetric encryption/decryption requires 0.87ms, and an asymmetric cryptography is approximately equal to 100 symmetric operations. Therefore, an asymmetric operation computation takes approximately 87ms. The computational cost of the one-way hash function (0.05ms) and XOR operations can be ignored since it is much lighter compared to asymmetric and symmetric operations. Based on the above estimated times, the total computational times for the authorization phase were 349.79ms, 700.23ms, in the proposed scheme and [5] respectively. The following table indicates that the proposed protocol is more efficient than scheme in [5].

Table 4. A computational comparison between the related protocols and the proposed protocol

Protocol	Asymmetrical Encryption / Decryption	symmetrical Encryption / Decryption	Hash function	Computation time (ms)
The scheme in [5]	6	4	15	526.23
Proposed protocol	4	2	1	349.79

6 Conclusion

In this paper, we have proposed a fast and secure authentication protocol for ubiquitous wireless access environment. Since it does not require any verification process with the HN, it will be more flexible and will enable MUs to authenticate themselves to FN providers in direct negotiation. Moreover, FNs have full control over the authorisation processes. In contrast to the existing protocols, we believe that our approach

is faster than any other protocols and minimizes the latency. The security analysis indicates that our proposed scheme is resistant to well-known attacks and efficiently ensures the security for MUs and network service providers. Also, in the performance analysis, we have demonstrated that the proposed protocol will greatly enhance the network performance.

Acknowledgments

The authors would like to thank Mr. Noriaki from Monash University for the valuable comments and suggestions that improve the presentation of this paper.

References

1. Ahonen, T.T., Moore, A.: Putting 2.7 billion in context: Mobile phone users. Communities Dominate Brands 2010 (2007)
2. Shrestha, A., Choi, D., Kwon, G., Han, S.: Kerberos based authentication for inter-domain roaming in wireless heterogeneous network. Computers & Mathematics with Applications (2010)
3. Chen, Y., Chuang, S., Yeh, L., Huang, J.: A practical authentication protocol with anonymity for wireless access networks. Wireless Communications and Mobile Computing (2010)
4. Wuu, L., Hung, C.: Anonymous Roaming Authentication Protocol with ID-Based Signatures (2006)
5. He, D., Ma, M., Zhang, Y., Chen, C., Bu, J.: A strong user authentication scheme with smart cards for wireless communications. Computer Communications (2010)
6. Zhu, J., Ma, J.: A new authentication scheme with anonymity for wireless environments. IEEE Transactions on Consumer Electronics 50, 231–235 (2004)
7. Lee, C., Hwang, M., Liao, I.: Security enhancement on a new authentication scheme with anonymity for wireless environments. IEEE Transactions on Industrial Electronics 53, 1683–1687 (2006)
8. Wu, C., Lee, W., Tsaur, W.: A secure authentication scheme with anonymity for wireless communications. IEEE Communications Letters 12 (2008)
9. Zeng, P., Cao, Z., Choo, K., Wang, S.: On the anonymity of some authentication schemes for wireless communications. IEEE Commun. Lett. 13 (2009)
10. Chang, C., Lee, C., Lee, W.: Cryptanalysis and Improvement of a Secure Authentication Scheme with Anonymity for Wireless Communications. IEEE, 902–904 (2009)
11. Chang, C., Lee, C., Chiu, Y.: Enhanced authentication scheme with anonymity for roaming service in global mobility networks. Computer Communications 32, 611–618 (2009)