Anonymous Network Information Acquirement Protocol for Mobile Users in Heterogeneous Wireless Networks

Guangsong Li[1], Qi Jiang[2], Yanan Shi[1], and Fushan Wei[1]
(Corresponding author: Guangsong Li)

State Key Laboratory of Mathematical Engineering and Advanced Computing[1]
No. 62 of Science Road, Zhengzhou 450002, P. R. China
School of Computer Science and Technology, Xidian University[2]
No. 2 of Taibai Road, Xi'an 710071, P. R. China
(Email: lgsok@163.com)
(Received Dec. 10, 2013; revised and accepted Nov. 15 & Dec. 28, 2014)

Abstract

Media independent information service is one of the important parts of the IEEE 802.21 standard to optimize vertical handover in wireless heterogeneous networks. In this paper, an anonymous network information acquirement protocol is proposed for a mobile user, which can be used to establish a secure channel between the mobile user and the information server. Security and performance analysis shows that the proposed protocol is very suitable for mobile environments.

Keywords: Anonymity, heterogeneous network, media independent information service

1 Introduction

Communication in next generation wireless networks will use multiple access technologies, creating a heterogeneous network environment. Practically, a single network cannot cater for all different user needs or provide all services. Nowadays the availability of multimode mobile devices capable of connecting to different wireless technologies provides users with the possibility to switch their network interfaces to different types of networks. Vertical handovers among heterogeneous networks should be supported to guarantee the service continuity. To achieve a seamless handover, a mobile user needs to obtain information of existing networks nearby, in order that he can choose a suitable target network and do some preparations for possible handover. However, the neighbor information discovery is the most time-consuming phase in the handover process [15].

The IEEE 802.21 working group defines the Media Independent Handover (MIH) services [4] to facilitate handover between heterogeneous networks. Media Independent Information Service (MIIS) is a very important part of MIH services, which specifies information about nearby networks and the query/response mechanism that allows mobile nodes to get that information from information servers. MIH messages will be exchanged over various wireless media between mobile nodes and access networks in future heterogeneous networks. Thus the MIH services may be a new target to attackers, which will be the main concerns for equipment vendors and service providers. Some typical threats about MIIS are listed in [9], which includes identity spoofing, tampering, replay attack, denial of service and information disclosure. Note that an attacker may be able to trace a user's movements or predict future movements by inspecting MIIS messages. Thus, it is desirable to hide the roaming user's identity and movements from eavesdroppers. However, security mechanisms are not within the scope of the IEEE 802.21 standard.

IEEE 802.21a task group was set up to address security issues of MIH services. As to MIH security, two frameworks about MIH service access control were proposed [5, 8]: (i) 3-party case, the access control is applied through EAP process (for instance, EAP-TLS [13]) with an EAP server, where the information server plays a part of authenticator; (ii) 2-party case, the access control is based on a pre-shared key or public key certification, where the user and the information server execute a mutual authentication and key establishment procedure like TLS [2]. Saadat et al. [11] describe the main technical requirements to establish a secure channel between the user and the information server. They also propose that the user should be authenticated by an authentication server and a shared key between the user and the information server should be generated by the authentication server. However, the specific authentication method is not referred. Saha et al. [12] propose a PLA-MIH scheme

to transport 802.21 messages over a secure network layer protocol in a hop-by-hop manner. It has the advantage that ensures very strong security of the signaling framework. However, it adds much overhead to all entities involved, for it needs every packet in MIH signaling to be signed. Won et al. propose another secure MIH message transport solution called MIHSec [14], which computes the MIH keys by utilizing the keys generated from the data link layer authentication procedure. Though MIHsec has a good performance for MIH message transportation, it introduces other issues. First, it is closely integrated with date link layer authentication, thus it is not media independent. Second, the access router may know the key for MIH messages encryption, which degrades the level of security.

We note that user anonymity is not addressed in all above schemes. It is very important for a roaming user to keep his identity secret and movements untraceable. In [7], we propose an access authentication scheme with user anonymity. The scheme provides an anonymous access authentication of MIIS considering that the access control for information is applied through an access authentication controller. The protocol can be used to establish a secure channel between the mobile node and the information server. The solution has the advantages of lightweight computation and easy implementation, However, it has the following weak points: first, it needs the mobile user to require a service ticket from his home server every time before accessing MIIS, which may take a long time if the user is far away from his home network; second, the home server has to be always online and available, so it is easy for the home server to become the bottleneck.

In order to achieve an efficient network information discovery process with more security properties, this paper proposes a new Anonymous Network Information Acquirement (ANIA) protocol using an Schnorr like ID-based signature scheme [3]. The anonymous authentication process does not involve the home server, which resulting a very short authentication latency. We also give a rigorous formal analysis of its security using a modular approach.

Our contribution mainly includes:

- Quick mutual authentication with user anonymity between the user and the information server;
- A shared session key established for MIIS information secure transmitting;
- Lightweight computation and low communication cost in the proposed protocol.

The rest of this paper is organized as follows. Section 2 gives a quick review of eCK model. In Section 3 we present our new approach in detail. Section 4 gives a formal security proof of our protocol under the ECK model. Section 5 includes performance analysis. Finally, conclusions are drawn in Section 6.

2 Related Work

The extended Canetti-Krawczyk (eCK) model [6] is described as an experiment between an adversary Δ and a challenger Σ. Initially, Δ selects the identities of n honest parties, for whom Σ generates static private key/public key pairs.

Execution of an Authenticated Key Exchange (AKE) protocol by one of these parties is called an AKE session. A session identifier *sid* is defined as

$sid = (role, \Phi, \Psi, comm)$,

where $role = \{I, R\}$ is the role (initiator/responder) of the owner of the session, Φ is the identity of the owner, Ψ is the identity of the other party in the session, and *comm* is the concatenation of communication messages between the two parties. Two sessions $sid = (role, \Phi, \Psi, comm1)$ and $sid^* = (role, \Phi, \Psi, comm2)$ are matching sessions if role is the complement of $role^*$ and $comm1 = comm2$. A protocol execution between Φ and Ψ without the intervention of an adversary produces two matching sessions.

In the experiment, Δ controls all communications between the parties, and can reveal the static private key of a party, the ephemeral private key in a session, and the session key of a session. Δ can make any sequence of the following queries, which Σ needs to answer accordingly:

- Send(Φ, Ψ, *comm*). Δ sends a message *comm* to Φ on behalf of Ψ. Σ returns Φ's response.
- StaticKeyReveal(Φ). Σ returns the static private key of Φ.
- EphemeralKeyReveal(*sid*). Σ returns the ephemeral private key of the session *sid*.
- SessionKeyReveal(*sid*). Σ returns the session key of the session sid.
- Establish(Φ). Using this query, the adversary registers an arbitrary public key on behalf of an adversary controlled party Φ. Σ only checks the validity of the public key, but does not need to check the possession of the corresponding private key.

A session *sid* (*role*, Φ, Ψ, *comm*) is fresh if the following conditions hold:

- Both Φ and Ψ are honest parties.
- Δ did not query the session key of sid or its matching session sid^* (if the matching session exists).
- Δ did not query both the static private key of Φ and the ephemeral private key of Φ in this session.
- If sid^* exists, then Δ did not query both the static private key of Ψ and the ephemeral private key of Ψ in this session.
- If sid^* does not exist, then Δ did not query the static private key of Ψ.

Security of an AKE is defined as follows. In an eCK experiment, Δ issues Send, StaticKeyReveal, EphemeralKeyReveal, SessionKeyReveal, and Establish queries polynomial times (in a security parameter) in any sequence. Then Δ selects a completed session *sid*, and makes a query Test(*sid*). To answer Test(*sid*), Σ chooses a bit $b\in \{0,1\}$uniformly at random. If $b = 1$, then Σ sets the session key of *sid* as **K**. Otherwise, Σ selects **K** from the key space uniformly at random. Σ then returns **K** as the answer of Test(*sid*). Δ continues to query Send, StaticKeyReveal, EphemeralKeyReveal, SessionKeyReveal, and Establish polynomial times. At last, Δ outputs a bit b^*, and terminates the game. If the selected test session is fresh and $b^* = b$,then Δ wins the game.

The advantage of the adversary Δ in the eCK experiment with AKE protocol Π is defined as $\mathrm{ADV}_{\Pi}(\Omega) = \Pr\{\Delta \text{ wins}\}-1/2$.

eCK Security

An AKE protocol is secure (in the eCK model) if no efficient adversary Δ has more than a negligible advantage in winning the above experiment, i.e., $\mathrm{ADV}_{\Pi}(\Delta) < 1/Q(\mu)$ for any polynomial $Q(\cdot)$ when μ sufficiently large.

3 Network Information Acquirement Protocol with User Anonymity

This section focuses on a new proposal for anonymous network information acquirement using an efficient Schnorr like ID-based signature scheme [3].

3.1 Network Initialization

We consider a network model as depicted in Figure 1. A mobile user (MU) roams into a visited network (V) and he wants to get network information nearby for possible handover. We assume the MU registers with a home authentication server (HAS) in his home network (H) and has a long term shared key k_{MH} with the HAS. The MIIS is provided by an information server (IS) in the Internet. Suppose there is an agreement between the IS and the HAS for MUs using MIIS to optimize handover. We also assume there is a time synchronization mechanism in the system.

In this phase, the HAS runs a setup algorithm and generates the system parameters, including a master secret key (s), and the corresponding master public key (PK_{HAS}), by using a security parameter k. The HAS performs the following steps:

1) Specifies q, p, E/F_p, P and G where q is a large prime number and p is the field size, E/F_p is an elliptic curve E over a finite field F_p, P is a base point of order q on the curve E and G is a cyclic group of order q under the point addition "+" generated by P.

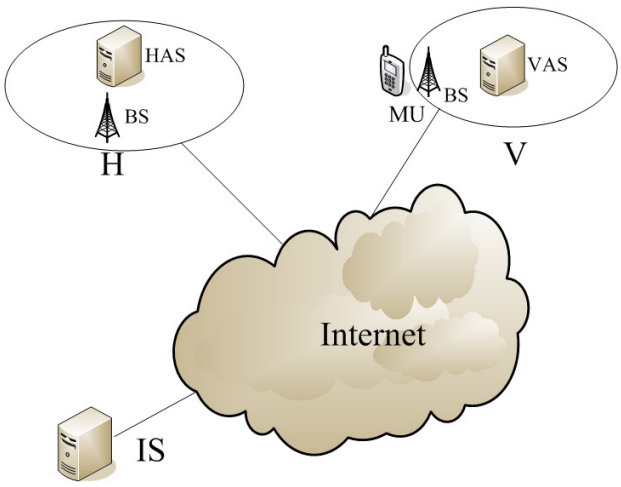

Figure 1: Network model

2) For the randomly chosen master secret key $s\in Z_q^*$, computes PK_{HAS} as sP.

3) Chooses two hash function H_1: $\{0,1\}^* \longrightarrow Z_q^*$, H_2: $\{0,1\}^*\times G\times\{0,1\}^* \longrightarrow Z_q^*$.

4) Chooses one key derivation function f: $G\longrightarrow\{0,1\}^k$.

5) Outputs system parameters $\{q, p, E/F_p, P, G, PK_{HAS}, H, f\}$, and keeps s secret.

Later, the HAS computes the private keys of all users and the IS. This algorithm takes the master secret key s and an identifier (ID) as input and generates a private key corresponding to that ID. In order to achieve MIIS access anonymity, the HAS selects a pseudo-ID (PID) for each MU and based on the PID a private key is generated. The HAS works as follows for each MU with identifier PID_{MU}. It chooses at random $r_{MU} \in_R Z_q^*$,compute $R_{MU} = r_{MU}P$ and $h_{MU} = H_1(PID_{MU}, R_{MU})$. Then it computes $s_{MU} = r_{MU}+h_{MU}s$. The MU's private key is the tuple (s_{MU}, R_{MU}) and is transmitted to the MU via a secure channel, namely encrypted by the key shared between the HAS and the MU. The MU's public key is defined as $PK_{MU} = s_{MU}P$, which can also be computed with R_{MU}, PID_{MU}, and PK_{HAS} from the equation: $PK_{MU}=R_{MU}+H_1(PID_{MU}, R_{MU})PK_{HAS}$. The HAS also generates a private key for the IS as above procedure using ID_{IS}. The private key and public key of the IS are denoted as (s_{IS}, R_{IS}) and $PK_{IS}=s_{IS}P$, respectively.

3.2 Anonymous Secure Channel Establishment

When a MU moves to a new place, it should contact the IS to get information about neighbor networks. Suppose that the MU is now in coverage area of network V and he

is already connected with the network. Then an anonymous authentication and key establishment process will be conducted between the MU and the IS. The flow chart of our scheme is depicted in Figure 2.

1) MIIS Authentication Request (MU⟶IS):

   PID_{MU}, A, t_{MU}, σ.

   The MU selects a random number $a \in Z_q^*$, and computes $A = aP$. He sends a MIIS authentication request message to the IS. The message content is as the following, $\{PID_{MU}, A, t_{MU}, \sigma\}$, where t_{MU} is the timestamp of the MU, and σ is a signature generated by the schnorr like ID-based signature using s_{MU}. Denote $\{PID_{MU}, A, t_{MU}, \sigma\}$as m, then σ is generated as follows [3]: The MU selects a random number $x \in Z_q^*$,and computes xP, $y{=}x{+}s_{MU}H_2(PID_{MU}, xP, m)$, then he outputs the signature $\sigma{=}\{xP, y, R_{MU}\}$.

2) MIIS Authentication Response (IS⟶MU)

   ID_{IS}, R_{IS}, B, A, c, MAC.

   Upon receiving the request message from the MU, first the IS checks the time stamp t_{MU}. If it is fresh, the IS computes the MU's public key by the equation $PK_{MU}{=}\ H_1(PID_{MU},\ R_{MU})\ PK_{HAS}{+}R_{MU}$ (Note R_{MU} can be extracted from σ). Then the IS verifies the signature σ using PK_{MU} by checking the following equation: $yP{=}xP{+}\ H_2(PID_{MU}, xP, m)PK_{MU}$. Successful signature verification implies the message is actually sent by a valid user of the HAS. Hence, the IS accepts the message. Otherwise the protocol is terminated at this stage. Next the IS selects a random number $b \in Z_q^*$, and computes $B = bP$. Then it computes the shared secret k_{IM} as follows: $K_{IM}{=}(b{+}s_{IS})(PK_{MU}{+}A)$, $k_{IM}{=}f(K_{IM}, PID_{MU}, ID_{IS})$. The IS randomly chooses a temporary ID (TID_{MU}) for the MU and stores an item $\{TID_{MU}, PID_{MU}, R_{MU}\}$. The IS generates a ciphertext c by encrypting TID_{MU} using k_{IM} and a symmetric cryptographic algorithm. Later it sends a MIIS authentication response message to the MU. The message content is as the following, $\{ID_{IS}, R_{IS}, B, A, c, MAC\}$, where MAC is a value computed using a secure message authentication function λ by the equation $MAC{=}\lambda(ID_{IS}, R_{IS}, B, A, c, k_{IM})$.

On receiving the response message from the IS, the MU computes as bellow.

$PK_{IS} = H_1(ID_{IS}, R_{IS})PK_{HAS} + R_{IS}$; $K_{MI} = (a + s_{MU})(PK_{IS} + B)$. Then the shared session key k_{MI} is derived from the equation: $k_{MI}{=}f(K_{MI}, PID_{MU}, ID_{IS})$.

Next the MU checks whether the MAC equals to $\sigma(ID_{IS}, R_{IS}, B, A, c, k_{MI})$. If it does not hold, the IS fails to pass the authentication. Otherwise, the IS passes the authentication and a secure channel between the IS and the MU is established using the shared key. The MU decrypts c and stores TID_{MU}. Then neighbor network information of the MU can be acquired from the IS through the secure channel.

Notes.

The MU authentication is achieved by verifying the signature of the user. On the other side, the MU authenticates the IS by MAC generated using the shared key. It is easy to see that $K_{MI}{=}K_{IM}$.

Later, if the MU moves to another place and wants to access the IS again, the MU will uses TID_{MU} as his identity. The ANIA protocol will be performed except that the message sent in Step (1) consists of $\{TID_{MU}, A, t_{MU}, xP, y\}$. Note that R_{MU} (a part of the MU's signature σ composed of $\{xP, y, R_{MU}\}$) is not sent in the message, since the PID_{MU} and $R_{MU}$are stored in the IS. The IS identifies the MU by the TID_{MU}, and it generates a new temporary identity $TID_{MU}^*$for the MU during the authentication procedure.

4 Security Analysis

We assume that the cryptography suites employed in our protocol are all secure, such as, hash function, message authentication function and ID-based signature scheme. Then our protocol is secure under the extended Canetti-Krawczyk (eCK) model [6].

Computational Diffie-Hellman (CDH) Assumption.

Let G be a cyclic group generated by P, whose order is a prime q. View G as an additive group. The CDH assumption states that, given (P, aP, bP), for randomly chosen $a, b{\in}\{0, 1, 2, \ldots, q{-}1\}$, it is computationally intractable to compute the value abP [6].

Theorem 1. *Under the CDH assumption in the cyclic group G of prime order q, using a signature scheme sig and a message authentication function λ that are both existentially unforgeable under adaptively chosen-message attacks, the ANIA protocol is a secure authenticated key-exchange protocol with respect to the eCK model, when hash functions H_1, H_2 and key derivation function f are modeled as random oracles.*

Proof. Let Δ be any adversary against the ANIA protocol. We start by observing that since the session key sk is computed as $sk{=}f(\theta)$ for some 3-tuple θ, the adversary Δ has only two ways to distinguish sk from a random string:

1) Forging attack. At some point Δ queries f on the same 3-tuple θ.

2) Key-replication attack. Δ succeeds in forcing the establishment of another session that has the same session key as the test session.

If random oracles produce no collisions, the key-replication attack is impossible as equality of session keys implies equality of the corresponding 3-tuples (which are

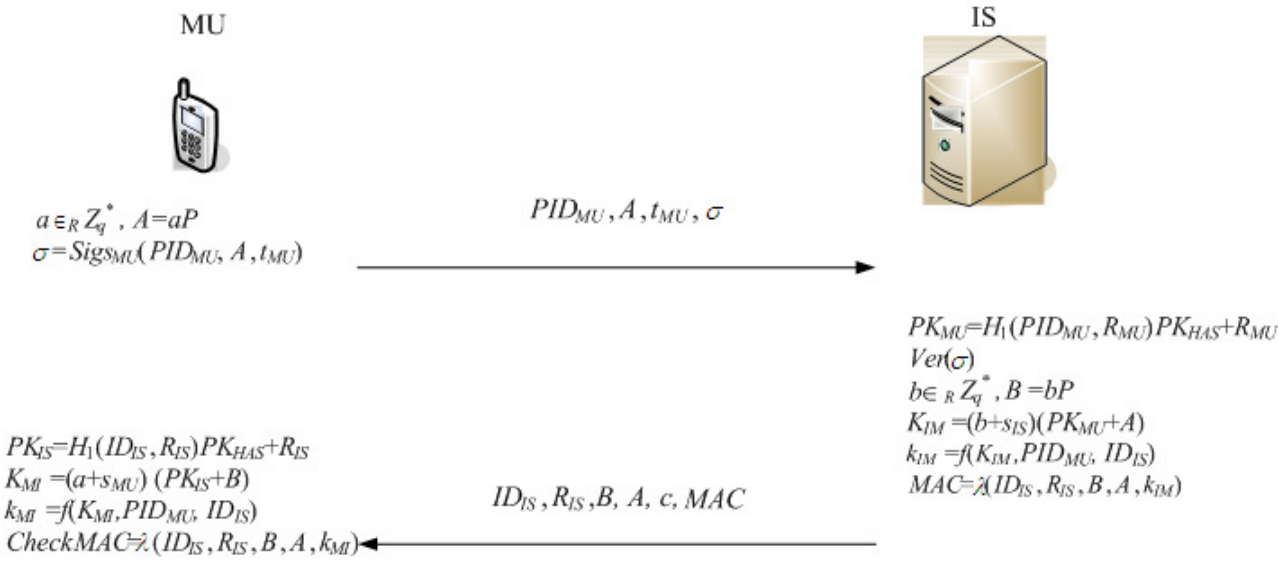

Figure 2: Anonymous authentication and key establishment with IS for MU

used to produce session keys). In turn, distinct key exchange sessions must have distinct 3-tuples. Therefore, if random oracles produce no collisions, Δ must perform a forging attack.

Case 1: Active attack. The adversary could break the security of the protocol via insertion of a message of its choice. In this case we will construct an adversary Ξ against the signature scheme *sig* or the message authentication function λ.

We only take the adversary against *sig* for example. The construction of attacker against λ is very similar. The input to Ξ consists of the parameters of the signature scheme, which includes access to a signature oracle. Ξ selects at random one party as MU. For session executed by MU, instead of using the MU's private key to compute the signatures, Ξ will make use of the signature oracle that it has access to in the signature security game that Ξ is simultaneously playing. Therefore, if the active attack occurs, Ξ succeeds in breaking the unforgeability of *sig*. By assumption forging a valid signature can only occur with negligible probability, the protocol is resilient against active attacks.

Case 2: Passive attack. In this case, the Test session has a matching session owned by another honest party. We show that if the adversary performs a successful forging attack, the CDH problem could be solved by a solver Ξ. The input to the Ξ is a CDH problem instance ($U = uP$, $V = vP$), where u, $v \in Z_q^*$ and U, $V \in G$. The goal of Ξ is to compute $\mathrm{CDH}(U, V) = uvP$. For simplicity, we use γ, ω and Γ, Ω denote the static secret keys s_{MU}, s_{IS} and public keys PK_{MU}, PK_{IS} respectively.

The adversary Δ is allowed to reveal a subset of (γ, a, ω, b), but it is not allowed to reveal both (γ, a) or both (ω, b). We only take the subcase for example that (γ, b) is revealed by Δ. Other subcases are similar.

Ξ selects random matching sessions executed by MU and IS, and modifies the experiment as follows. Ξ sets the ephemeral public keys of MU in the test session to be U, and sets the static public key of IS in the matching session to be V (namely, $A=U$, $\Omega = V$). If Δ wins the game, it must queries f on the same 3-tuple θ, thus it successfully forges $K=(\gamma+u)(v+b)P$. Then Ξ can solve the CDH problem as below: $\mathrm{CDH}(U, V)=K-\gamma bP-\gamma V-bU$. With the hardness of the CDH assumption, the adversary could not win the experiment and hence the protocol is secure.

□

In the following, we further discuss some security properties of our protocol.

User Anonymity. In our scheme, the pseudo ID, instead of the MU's real identity, is used in access MIIS for privacy protection.

Key Freshness. The session key k_{MI} is computed from a function using random numbers from the MU and the IS respectively, which assures the freshness of session key.

Forward Secrecy. The random numbers used in session key generation are unpredictable for any party except the MU or the IS. Even if the intruder attacks long term secret information of the MU and the IS, he can not compromise the past random numbers and the past session keys.

Resistance to Replay Attack. Replay attack involves the passive capture of data and its subsequent retransmission to produce an unauthorized effect. A replay attack can be prevented by checking the timestamp or the MAC.

5 Performance Analysis

Computation and communication overheads are considered as two important metrics of authentication protocols. We present performance comparison of 802.21a proposal [5], SAM protocol [7], and ANIA protocol according to the metrics.

The computation overhead is the time cost of all the cryptography operations. Since the MU is always resource-constraints, we primarily take the MU's computation overhead into account. We take EAP-TLS [13] and TLS [2] as 802.21a proposal instances for 3-party case and 2-party case respectively. Here, TLS handshake is based on public key certificate and Diffie-Hellman key exchange. And public key related algorithms of 802.21a and SAM are all considered based on ECC, where ECDSA and ECDH for 802.21a, and ECDH for SAM.

To evaluate computation overhead of the mobile node, we implemented all cryptographic operations required in the two schemes using the Crypto++ Library (version 5.6.2) [1]. The cryptographic experiments were executed on a laptop with PIII 1.0 GHz CPU and 128MB RAM. Here the key length of the ECC system is set as 160 bits. In the experiment, SHA-160(or its variation) is introduced to implement hash functions and key derivation function, and AES-128 is introduced as the symmetric cipher used in the protocols. The mainly results are listed in Table 1.

Table 1: Mainly cryptographic operations and computation costs

Computation operations	Notation	Time (ms)
point multiplication	T_{PM}	1.532
random number generation	T_{RG}	0.072
symmetric encryption	T_{SE}	0.106
symmetric decryption	T_{SD}	0.106
hash value computation	T_{HC}	0.031
key derivation	T_{KD}	0.031

Table 2 shows the MU's computation costs of the four schemes during the handover authentication procedure. In the ANIA protocol, the MU needs: $1T_{HC}$ and $1T_{PM}$ for computing the IS's public key; $1T_{HC}$, $1T_{RG}$, and $1T_{PM}$ for message signature; $1T_{RG}$, $2T_{PM}$, $1T_{KD}$ for key exchange; $1T_{HC}$ for MAC verification; $1T_{SD}$ for T_{ID}. From the table, we can conclude that the ANIA protocol is more efficient than 802.21a proposal, since 3 costly point multiplication operations are saved; and it is a little more complex than the SAM protocol because of one additional costly point multiplication operation.

As to communication performance, the HAS is not involved during the authentication between the MU and the IS in both 802.21a proposal 2-party case and the ANIA scheme. The SAM protocol and 802.21a proposal 3-party case both need the HAS to acts as an anchor for trust establishment. Since the MU now roams to a visited network which may be far away from his home network, communication between the MU and the HAS could take a long latency. Table 3 shows the message numbers needed between the related entities. From Table 3, we can see that ANIA performs better than other schemes.

We carried out some simulation experiments of the four schemes using OPNET 10.5 [10] to verify analysis above. For simplicity, only 2 WLANs (denoted as H and V) are used as the access network in the topology, and two ASs and one IS are deployed, where the servers are connected to the Internet as in Figure 1. The simulations run with 20˜100MUs and 10 APs uniformly distributed in each WLAN area for 5 minutes of simulation time. For the MIIS authentication request pattern, assume 20 percents of the MUs in one WLAN move into the other WLAN, and each roaming MU makes 10 requests randomly distributed over the whole simulation period. The simulation parameters are listed in Table 4. Here we mainly focus on the measurements of average authentication latency and the number of messages delivered in the network. The computation costs of MUs are considered in the simulation, while the computation costs of the servers are neglected because of their powerful processing abilities.

Figure 3 shows the average authentication latency of the four schemes as the number of MUs changes. We can see that the average authentication latency of those schemes become larger as the number of MUs increases. The reason is that the number of packets generated in the network increases as the number of MUs increases, which makes packets collision and retransmission happen more often. The ANIA protocol gets the shortest average authentication latency among those protocols in all scenarios. This suggests that the ANIA protocol is highly effective in authentication latency. Figure 4 shows the changes of the number of messages delivered in the network when the number of MUs changes. As we can see from the results, the number of messages delivered of 802.21a-3 increases sharply while that of other protocols increases smoothly as the number of MUs increases. It shows that the ANIA protocol delivers the smallest messages in the network in all scenarios. The simulation results indicate that the ANIA protocol has advantages in communication performance compared with other protocols.

6 Conclusion

In this paper, we focus specifically on security of MIIS, and propose a new anonymous access authentication protocol for MIIS. We apply an identity-based Schnorr like

Table 2: Message numbers between the related entities

Computation costs	**802.21a (2-party)**	**802.21a (3-party)**	**SAM**	**ANIA**
	$3T_{HC} + 7T_{PM}$ $+1T_{RG} + 1T_{KD}$	$3T_{HC} + 7T_{PM}$ $+1T_{RG} + 1T_{KD}$	$4T_{HC} + 3T_{PM} + 1T_{RG}$ $+1T_{KD} + 1T_{SE} + 1T_{SD}$	$3T_{HC} + 4T_{PM} + 2T_{RG}$ $+1T_{KD} + 1T_{SD}$
Total (ms)	10.917	10.917	5.101	6.502

Table 3: MUs computation costs of the four schemes

Message numbers	**802.21a (2-party)**	**802.21a (3-party)**	**SAM**	**ANIA**
Between MU and HAS	0	6	2	0
Between MU and IS	4	9	2	2

Table 4: Simulation parameters

WLAN area	300m∗300m
The number of APs in each WLAN	10
Coverage of AP	100m
The number of MUs in each WLAN	20∼ 100
The number of MIIS request for each MU	10
Simulation time	5 minutes

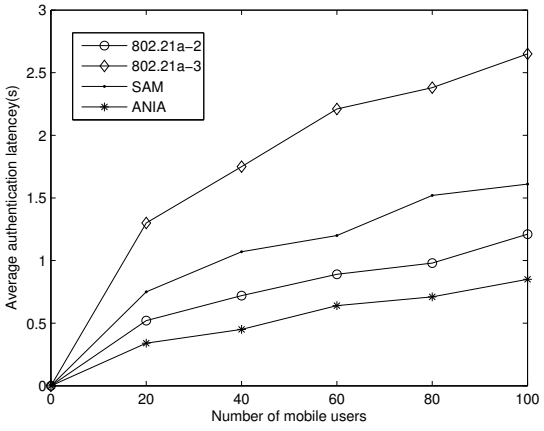

Figure 3: Comparison about average authentication latency

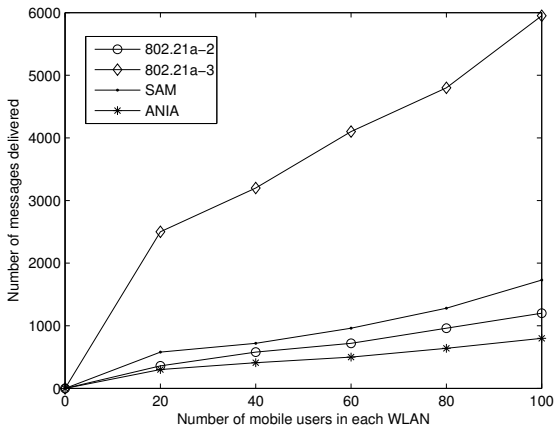

Figure 4: Comparison about number of messages delivered

signature for user authentication with a PID. The security and performance analysis shows that the proposed scheme has excellent performance. We will further analyze the performance of the proposed scheme in the future. Now we are making an effort to put up a real test-bed to evaluate performance of our protocol.

Acknowledgments

The authors would like to thank the anonymous reviewers and the editor for their comments that will help them to improve this paper. This work is supported by the National Natural Science Foundation of China (61201220, 61202389, 61309016, 61379150), and the Fundamental Research Funds for the Central Universities (Program No. JB140302).

References

[1] Cryptopp, *Crypto++ Library*, July 11, 2015. (`http://www.cryptopp.com/`)

[2] T. Dierks and E. Rescorla, *The Transport Layer Security (TLS) Protocol Ver. 1.2*, Technical Report RFC 5246, 2008.

[3] D. Galindo and F. D. Garcia, "A schnorr-like lightweight identity-based signature scheme," in *Proceedings of The Second International Conference on Cryptology in Africa (Africacrypt 2009)*, pp. 135–148, 2009.

[4] IEEE, *Media Independent Handover Services*, IEEE 802.21 Standard, 2009.

[5] IEEE, *IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services - Amendment for Security Extensions to Media Independent Handover Services and Protocol*, IEEE Standard, May 2012.

[6] B. LaMacchia, K. Lauter, and A. Mityagin, "Stronger security of authenticated key exchange," in *Proceedings of The First International Conference on Provable Security (ProvSec 2007)*, pp. 1–16, 2007.

[7] G. Li, J. Ma, and Q. Jiang, "SAM: Secure access of media independent information service with user anonymity," *EURASIP Journal on Wireless Communications and Networking*, vol. 2010, pp. 12, Apr. 2010.

[8] R. Marin-Lopez, F. Bernal-Hidalgo, S. Das, and et al., "A new standard for securing media independent handover: IEEE 802.21A," *IEEE Wireless Communications*, vol. 20, no. 6, pp. 82–90, 2013.

[9] T. Melia, G. Bajko, S. Das, N. Golmie, and J. Zuniga, *IEEE 802.21 Mobility Services Framework Design (MSFD)*, Technical Report RFC 5677, 2009.

[10] Opnet, *Opnet*, July 11, 2015. (`http://www.opnet.com/`)

[11] I. Saadat, F. Buiati, D. Rupėrez Caňas, L. Javier, and G.Villalba, "Overview of IEEE 802.21 security issues for mih networks," in *Proceedings of International Conference on Information Technology (ICIT'11)*, pp. 196–214, 2011.

[12] S. Saha and D. Lagutin, "PLA-MIH: A secure IEEE 802.21 signaling scheme," in *Proceedings of IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob'09)*, pp. 252–257, 2009.

[13] D. Simon, B. Aboba, and R. Hurst, *The EAP TLS Authentication Protocol*, Technical Report RFC 5216, 2008.

[14] J. Won, M. Vadapalli, C. Cho, and V. C. M. Leung, "Secure media independent handover message transport in heterogeneous networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, pp. 15, 2009.

[15] S. Yoo, D. Cypher, and N. Golmie, "Timely effective handover mechanism in heterogeneous wireless networks," *Wireless Personal Communications*, vol. 52, no. 3, pp. 449–475, 2010.

Guangsong Li received the B.S. degree in applied mathematics from Information Engineering University, Zhengzhou, P. R. China in 1999, and M. S. degree in applied mathematics from Information Engineering University in 2002, and the Ph. D. degree in Cryptography from Information Science and Technology Institute, Zhengzhou, P. R. China, in 2005. Now he is an associate professor of State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou. His current interests include mobile communication, wireless security, and digital rights management.

Qi Jiang received the B.S. degree in Computer Science from Shaanxi Normal University in 2005 and Ph.D. degree in Computer Science from Xidian University in 2011. He is now an associate professor of the School of Computer Science and Technology, Xidian University. His research interests include security protocols and wireless network security, etc.

Yanan Shi received his M.S. degrees in applied mathematics from the Zhengzhou Information Science and Technology Institute, China, in 2008. She is currently a lecturer of State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, China. Her research fields include cryptography and information security.

Fushan Wei received his M.S. and Ph.D. degrees in applied mathematics from the Zhengzhou Information Science and Technology Institute, China, in 2008 and 2011, respectively. He is currently a lecturer of State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, China. His research fields include cryptography and information security.