Efficient End-to-End Authentication Protocols for Mobile Networks

Cheng-Hsin Chang[*] Kwei Tu[†] and Kwang-Cheng Chen[‡]

Abstract

For conventional authentication protocols, distribution of session keys and maintenance of large databases are serious problems especially for large-scale wireless networks. ID-based authentication protocol eliminates the problem while it contributes the heavy computation load. We propose a hybrid end-to-end authentication and key agreement (AKA) protocol which provides authentication and key exchange between both end entities. It not only eliminates the drawbacks of conventional protocols but also reduces the computation load. Services of message confidentiality, caller ID confidentiality, service request intractability, and fraud control are provided. Roaming and handover, are also taken into consideration here.

1 Introduction

With dramatic development of mobile networks, more and more information is transmitted via radio communications. While wireless communication is inherently less private than wire-line communication since wireless (radio) communication

For conventional approaches to achieve privacy and authentication, it is necessary for the communication entities to share a session key which is known to no one else. This is done by sending the key in advance in secure way. However, a private conversation among entities with no prior contact is a common occurrence. Thus, the key distribution problem is a major obstacle to large-scale networks.

In modern large-scale telecommunication networks, it is required that each entity is able to communicate with arbitrary entities through the network. However, key management is a serious problem in private-key cryptosystem (e.g., DES or triple DES) and public-key cryptosystems (e.g., RSA), if the system contains a vast amount of entities.

In 1984, Shamir proposed the concept of an ID-based system [2], i.e., an ID-based cryptosystem and an ID-based signature scheme, as a countermeasure for key management in large-scale networks. No public directory is required in the system. Tsujii and Itoh [5] proposed an ID-based cryptosystem based on the discrete logarithm problem. Most recently, Harn and Yang [6] also proposed three identity-based cryptographic schemes based on the discrete logarithm problem in GF(p), where p is a large prime. Their scheme is based on the Agnew *et al.* digital signature scheme [4], which was due to ElGamel's signature scheme [3], and can provide user identification, digital signature, and key distribution.

Now, wireless networks are being driven by the massive need for providing network access to mobile computing devices. Therefore, the radio link between the *portables* and an array of *ports* is susceptible to eavesdropping. In earlier papers [8], [9] and [10], several protocols employed conventional or public-key cryptographic technology to accomplish *key agreement* and *authentication.* Several concerns or requirements are also addressed in [11], and [12]. However, authentication and privacy are generally linked together since the derivation of a "session key" for an encryption algorithm is often an integral part of the authentication process [11]. The access control and derivation of a session key form a single activity called *Authentication and Key Agreement* (AKA) from the designer's perspective. This is our major concern. Thus, the subsequent use of the session key to encrypt the traffic of users can be treated as a separate topic.

2 A Hybrid End-to-End AKA Protocols

In order to eliminate the requirements of a large database to hold all the session keys which are used to establish connections for conventional approaches, and the heavy load contributed by the exponential computations of ID-based authentication protocol. We propose a hybrid protocol and use cache to maintain the session keys set up by the modified ID-based authentication protocol.

Furthermore, the end-to-end authentication is also our concern. With link authentication, two entities must be directly linked. If two entities are far apart, they have to authenticate with any neighboring entity (e.g., switch), and have to set up the session key with it. Thus, the message is vulnerable at each intermediate entity and it

[*] The author is with Powerchip Semiconductor Corp., 12, Li-Hsin RD. 1, Hsinchu, Taiwan, R.O.C. E-mail:keynes@ccmail.psc.com.tw

[†] The author is with LinCom Corporation, 1020 Bay Area Blvd., #200, Houston, U.S.A.

[‡] The author is with the Department of Electrical Engineering, National Tsing Hua University, Hsinchu, Taiwan 30043, R.O.C. E-mail:chenkc@euler.ee.nthu.edu.tw

0-7803-3692-5/96 © 1996 IEEE

is inefficient since each intermediate entity on the routing path has to decrypt and encrypt the message once. Here, we construct our hybrid protocol with the modified ID-based protocol part [6] and a canonical protocol part [7].

2.1 The Modified ID-Based Protocol Part

First of all, we briefly introduce the initiation phase, user registration phase, and application phase of the ID-based cryptosystem.

In the initiation phase, the KAC selects a large prime p, and primitive element α of GF(p) publicly. An odd random $x \in [1, p-1]$ is also selected as its private key and the public key, $Y = \alpha^x \bmod p$. In the user registration phase, the KAC computes an extended identity EID_i for user i as

$$EID_i = h(ID_i),$$

and the signature (r_i, s_i) of EID_i as

$$s_i = (EID_i - k_i r_i)x^{-1} \bmod (p-1)$$

where $r_i = \alpha^{k_i} \bmod p$ and $k_i \in [1, p-1]$ is random. Finally, challenge-response procedure is applied in user identification phase. The challenge and response are as follows respectively:

$$W = Y^\gamma \bmod p$$

$$Z = W^{s_i} \bmod p$$

And, the identification procedure is to verify if

$$\alpha^{EID_i} = r_i^{r_i} Z^{\gamma^{-1}} \bmod p$$

Mutual authentication in large-scale networks can be achieved by adding another ID-based user identification scheme in the opposite direction. Anyway, the negotiation of setting up a session key is also necessary due to the connection of two entities. In such case, we embed Diffie–Hellman key exchange protocol [1] at the end of mutual authentication. Table 1 shows such simple mutual authentication of user i and server k where $h()$ represents the hash function chosen by the KAC. Steps are executed from top to bottom.

However, this simple protocol cannot resist some attacks from the intermediate node if user i and server k are directly linked. Assume the caller which invokes the connection knows the identity of the called entity. The intermediate node can still replace the identity of the caller, and the corresponding challenge and response. Thus, the session key set up is the same for caller and the intermediate node. And, the sensitive information is disclosed if the caller sends it out immediately after authentication. Table 2 provides a more secure protocol to resist such an attack in an intuitive way. Here, $E(K, M)$ and $D(K, M)$ denotes the encryption and decryption algorithm with the key, K, and the message, M.

user i		**server** k
ID_i,r_i	$\xrightarrow{ID_i,r_i}$	generates γ
$Z = W^{s_i} \bmod p$ generates γ'	$\xleftarrow{W,ID_k,r_k}$	$W = Y^\gamma \bmod p$
$W' = Y^{\gamma'} \bmod p$	$\xrightarrow{Z,W'}$	$EID_i = h(ID_i)$ verifies if $\alpha^{-EID_i} r_i^{r_i} Z^{\gamma^{-1}}$ mod $p = 1$ (aborts if not)
$EID_k = h(ID_k)$ verifies if . $\alpha^{-EID_k} r_k^{r_k} Z'^{\gamma'^{-1}}$	$\xleftarrow{Z'}$	$Z' = W'^{s_k}$
mod $p = 1$ (aborts if not) $K_{i,k} = W^{\gamma'}$		$K_{i,k} = W'^{\gamma}$

Table 1: A simple mutual authentication protocol with key exchange

entity i		**entity** j
ID_i,r_i	$\xrightarrow{ID_i,r_i}$	generates γ
$Z = W^{s_i} \bmod p$ generates γ'	$\xleftarrow{W,(ID_j),r_j}$	$W = Y^\gamma \bmod p$ $EID_i = h(ID_i)$
$W' = Y^{\gamma'} \bmod p$	$\xrightarrow{Z,W'}$	verifies if $\alpha^{-EID_i} r_i^{r_i} Z^{\gamma^{-1}}$ mod $p = 1$
$K_{i,j} = W^{\gamma'}$ $EID_j = h(ID_j)$		(aborts if not) $K_{j,i} = W'^{\gamma}$
$Z' = D(K_{i,j}, Z'_e)$ verifies if $\alpha^{-EID_j} r_j^{r_j} Z'^{\gamma'^{-1}}$ mod $p = 1$ (aborts if not)	$\xleftarrow{Z'_e}$	$Z'_e = E(K_{j,i}, W'^{s_j})$

Table 2: Modified mutual authentication and key agreement protocol

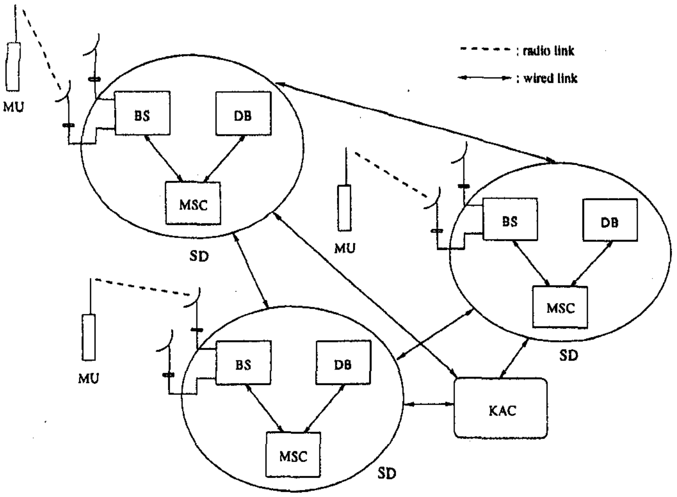

Figure 2: System architecture for the GSM and PCS like communication systems

portable unit's equipment, and makes EID as the output of an non-invertible function with UID and PID as its inputs, e.g., $EID = h(UID \,\|\, PID)$, where $h()$ is an one-way hash function and $\|$ stands for concatenation. Thus, the verification of subscriber equipment is also accompanied with the entity authentication.

Usually, party anonymity and caller confidentiality are maintained by substitution of an entity's identity by a temporary identity which is updated upon every new call. In order to overcome the problem of location registration which performed by the network for a particular mobile station. That is to effectively hide the real identity from attackers needs to protect the identity even when the subscriber just roams into a VSD and no temporary identity is present. The public key cryptographic technique, i.e., RSA scheme , is used to improve the caller ID confidentiality. Here, $g(e, m)$ is used to denote all the ciphertext of m encrypted using public key e.

The two AKA protocols are illuminated respectively as follows:

- **Link Authentication Protocol**
  Whenever a call is made after an entity roams into a VSD, the authentication process is initiated. The portable unit (entity) authenticates with the VSD and sets up a session key. An temporary identity is also assigned to the entity. We call it *the initial part* of the authentication protocol. Given the session key and the temporary identity of the entity are present, an efficient protocol is provoked and we call it *the basic part* of the protocol. For reducing the exchange of information between HSD and VSD, the generation of the signature pair (r,s) for the mobile unit can depend on his identity, account number, and the life time of the account. Thus, successful authentication denotes the correctness of his identity, equipment identity and etc.

  Table 3 and 4, which are similar to Table 2, show the initial and basic parts of the protocol respectively. Here, the variable, γ_{min} is as follows:

$$\gamma_{min} = \begin{cases} \gamma' & \text{if} \quad TID_i < SDID_j \\ \gamma & \text{if} \quad TID_i > SDID_j \end{cases}$$

entity i		VSD j
$m_i = UID_i \Vert PID_i \Vert INFO$ $c_i = g(e_j, m_i \Vert r_i)$	$\xrightarrow{c_i}$	generates a random number γ $m_i \Vert r_i = g(d_j, c_i)$ checks $INFO$ to see if expired
$Z = W^{s_i} \bmod p$ generates a random number γ'	$\xleftarrow{W,(SDID_j),r_j}$	$W = Y^{\gamma} \bmod p$ $EID_i = h(m_i)$
$W' = Y^{\gamma'} \bmod p$ $K_{i,j} = W^{\gamma'} (= Y^{\gamma\gamma'})$ $EID_j = h(SDID_j)$	$\xrightarrow{Z,W'}$	verifies if $\alpha^{-EID_i r_i^{r_i}} Z^{\gamma^{-1}} \bmod p = 1$ (aborts if not) $K_{j,i} = W'^{\gamma} (= Y^{\gamma\gamma'})$
$Z' \Vert TID_i = D(K_{i,j}, Z'_e)$ verifies if $\alpha^{-EID_j r_j^{r_j}} Z'^{\gamma'^{-1}} \bmod p = 1$ (aborts if not) records $(TID_i, K_{i,j})$ for next call	$\xleftarrow{Z'_e}$	$Z'_e = E(K_{j,i}, W'^{s_j} \Vert TID_i)$ records $(TID_i, K_{j,i}, UID_i, INFO)$ for next call

Table 3: The initial part of link authentication protocol

entity i		VSD j
generates a random number γ'	$\xrightarrow{\gamma',TID_i}$	extracts $K_{j,i}$,$INFO$ according to TID_i checks $INFO$ to see if expired
extracts $K_{i,j}$		generates a random number γ assigns a temporary ID, TID'_i $t_j = E(K_{j,i}, \gamma \otimes \gamma')$
$t_i = E(K_{i,j}, \gamma \otimes \gamma')$ $m_i = D(K_{i,j}, c_j)$ verifies if	$\xleftarrow{\gamma,c_j}$	$c_j = E(K_{j,i}, (\gamma_{min} \otimes SDID_j \otimes t_j) \Vert TID'_i)$
$m_i = (\gamma_{min} \otimes SDID_j \otimes t_i) \Vert TID'_i$ (abort if not) extracts TID'_i from m_i records $(TID'_i, K_{i,j})$ for next call	$\xrightarrow{t_i}$	verifies if $t_i = t_j$ (abort if not) records $(TID'_i, K_{j,i}, UID_i, INFO)$ for next call

Table 4: The basic part of link authentication protocol

- **End-to-End Authentication Protocol**
  In order to achieve end-to-end security and protect all the signaling information, an extra link encryption is necessary. Thus, our end-to-end authentication protocol consists of end-to-end section and link section. The former is used to authenticate the called entity and the latter is used to authenticate the VSD by the caller. Whenever a call is made after an entity roams into a VSD, the authentication process is initiated. First, the portable unit (entity) authenticates with the VSD and sets up a session key which is used to encrypt the signaling information. After successfully authenticated, VSD forwards the challenge of caller to called entity if both entities do not have a shared key, or VSD challenges caller and forwards its response to called entity given that a session key is shared by both

2.2 The Canonical Protocol Part

The modified ID-based mutual authentication protocol requires more than three modular exponentiations. Even though one exponentiation, i.e., the challenge, doesn't need to be done in real time, the computational load is still heavy especially for a portable unit. Thus, we adopt *the canonical protocol* which can resist *chosen ciphertext attacks, oracle session attack,* and *parallel session attack* as an alternative part of our hybrid protocol. Figure 1 shows the general form of the canonical protocol. The function, $E(\ )$, denotes a symmetric one-key encryption algorithm. N_i and N_j are nounces which are the challenges of entity i and j, respectively. D stands for the parameter indicating or tied to the direction of the flow. Here, we assume function $E(\ )$ is one-way with cryptographic strength, and the intuitive but unproven notion that $f()$ and $g()$ are cryptographically separate. # can be any bit-operation function.This protocol can also resist the attack mentioned above by intermediate node. The session key used to encrypt and decrypt does not appear the figure, and is generated by the modified ID-based authentication protocol. The requirements for $f()$ and $g()$ is not addressed here.

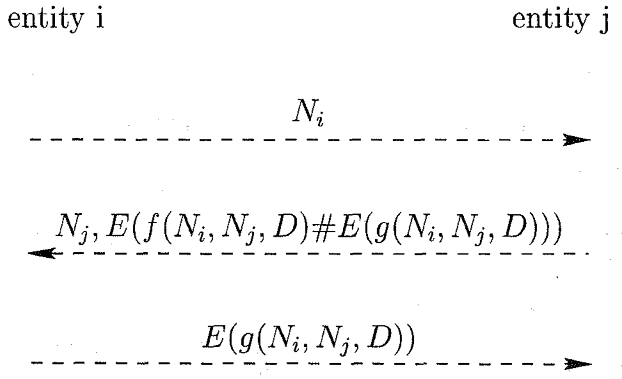

Figure 1: Canonical protocol with minimal number of encryption

2.3 The efficiency analysis

Our above analysis guarantees the hybrid protocol to resist the attacks by intermediate nodes, and thus, end-to-end authentication is achieved. However, efficiency is our major concern and depends on the *hit ratio* of the cache which is used to store the used session keys generated by the modified ID-based protocol. An auxiliary strategy, called *per-entity caching,* is proposed for storing the latest used private session keys. The object of caching is to reduce the computation and communication loads of authentication protocol in exchange of memory costs. It will be very useful when the requests to or from some specific entities are more relatively frequent than other entities.

Analytical models are established, and three different replacement policies of cache are investigated based on reasonable assumptions [13]. Without considering *expiration* of session keys, it is demonstrated that *Least Recently Used* (LRU) scheme provides the highest cache hit ratio. Asymptotic analysis and simulations are also provided to verify the analysis of hit ratio. This investigation also shows that LRU scheme provides a better capability of reusing session keys, and is the best countermeasure with smallest size of cache to achieve a fixed hit ratio.

3 AKA Protocols for Mobile Networks

Easy access to radio links makes wireless communication susceptible to the exposure of sensitive information and fraudulent use of the services. These threats may come from outsiders or insiders due to the collection of information on the radio link or the privilege to access system's secret information. Two AKA protocols are proposed to provide services such as message confidentiality, caller ID confidentiality, call intractability, and fraud control on mobile network, end-to-end authentication instead of link authentication is also the achievement we reach.

3.1 System Architecture

As shown in Figure 2, the portable unit (entity) communicates through radio with base stations (BS) which are connected to mobile switching centers (MSC). The MSC is a bridge to the existing wireline network. Another significant component, the authentication center (AC), performs the vital authentication process for each call requested. MSCs, BSs, and the AC collectively form a service domain (SD). Each service domain is owned by a service provider and may cover a metropolitan area or even a larger region. Here, we assume the SDs are not mutually trusted. Any entity which wants to have the wireless communication services needs to register itself with a SD, called *home service domain* (HSD), and becomes a visiting subscriber to another SD, called *visiting service domain* (VSD).

3.2 AKA Protocol for Mobile Networks

Here, we propose two different authentication protocols. One provides only link-to-link encryption and authentication while the other provides end-to-end encryption and authentication. The former relies heavily on the existing wireline network while the later reduces the complexity of the wireline network but adds some loads on the portable unit. The basic protocols applied are based on the hybrid protocol in the above section.

Similar to the procedure in the ID-based authentication protocol, each subscriber obtains a signature pair (r, s) of its own EID, and a unique identification, UID, with its HSD upon registration phase. The signature pair is stored in the portable unit and s is physically protected from exposure. If we assign PID as the unique identity of the entities. The protocol how VSD challenges caller entity is shown in Table 5. After called entity verifies and returns its response to caller, the authentication is complete.

entity i		VSD j
generates a random number γ'		generates a random number r_j
extracts $K_{i,k}$	$\xleftarrow{\gamma}$	$\gamma = r_j \Vert t$
$t_i = E(K_{i,k}, \gamma \otimes \gamma')$		
$c_i = E(K_{i,k}, (\gamma_{min} \otimes UID_i \otimes t_i))$	$\xrightarrow{c_i,\gamma}$	forwards c_i,γ,γ',UID_i to entity k
verifies if $t_i = t_k$	$\xleftarrow{t_k}$	receives response t_k from entity k
(aborts if not)		

Table 5: Challenge to caller from VSD which is in place of called entity

Given that there is already a session key shared by the portable unit and VSD, VSD first identifies the portable unit before allowing it to access mobile network. Table 6 shows how VSD identifies the caller entity given a session key $K_{i,j}$ is present.

entity i		VSD j
generates a random number γ'	$\xrightarrow{TID_i}$	extracts $K_{j,i}$ according to TID_i
extracts $K_{i,j}$	$\xleftarrow{\gamma}$	generates a random r, $\gamma = r \Vert t$
$t_i = E(K_{i,j}, \gamma \otimes \gamma')$	$\xrightarrow{\gamma',t_i}$	verifies if $t_i = E(K_{j,i}, \gamma \otimes \gamma')$
		(aborts if not)
	$\xleftarrow{E(K_{j,i},TID'_i)}$	assigns a temporary ID, TID'_i
extracts TID'_i		records $(TID'_i, K_{j,i}, UID_i, INFO)$
records $(TID'_i, K_{i,j})$		for next call
for next call		

Table 6: Protocol for identification of caller

4 Conclusion

The security analysis [13] is not addressed here, and the security of our protocols is based on computing discrete logarithm over GF(p), factoring a large prime product, and deriving the unknown key of the symmetric encipherment algorithm. Two protocols, link and end-to-end authentication, for mobile networks are based on the hybrid protocol and proposed here. End-to-end authentication protocol can resist the attacks from insiders, while requires an additional protocol to protect signaling information. With high cache hit ratio, the computation load is significantly reduced.

References

[1] W. Diffie and M. E. Hellman. "New directions in cryptography." *IEEE trans. Info. Theory*, vol. IT-22, pp.644-654, Nov. 1976.

[2] A. Shamir, "Identity-Based Cryptosystem and Signature Scheme", *in Advances in Cryptology: Proceedings of Crypto'84*, Berlin, West Germany: Spring-Verlag, pp.47-53, 1985.

[3] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Trans. Info. Theory*, Vol. IT-31,no.4, pp.468–472, July 1985.

[4] G. B. Agnew, R. C. Mullin, and S. A. Vanstone, "Improved Digital Signature Scheme Based on Discrete Exponentiation", *Electronics Letters*,

[5] Shigeo Thujii, and Toshiya Itoh, "An ID-Based Cryptosystem Based on the Discrete Logarithm Problem", *IEEE J. on Selected Areas in Comm.*, vol.7, no.4, May 1989.

[6] Lein Harn and Shoubao Yang, "ID-based cryptographic Schemes for User Identification, Digital Signature, and Key Distribution" *IEEE J. Select. Areas Comm.*, Vol. 11, no. 5, pp. 757–760, June 1993.

[7] Ray Bird, I. Gopal, Amir Herzberg, Philippe A. Janson, Shay Kutten, Refik Molva, and Moti Yung, "Systematic Design of a Family of Attack-Resistant Authentication protocols" *IEEE J. Select. Areas Comm.*, Vol. 11, no. 5, pp. 679–692, June 1993.

[8] H. Y. Lin and L. Harn "Authentication in Wireless Communications", *Proceedings, IEEE Globecom'93*, pp. 550–553, December, 1993.

[9] Kwei Tu, "An ID-Based Authentication Scheme in Wireless Communications"

[10] Michael J. Beller, Li-Fung Chang, and Yacov Yacobi, "Privacy and Authentication on a Portable Communications System", *IEEE J. on Sel. Areas in Comm.* vol.11, no.6, pp. 821–829, Aug. 1993.

[11] Dan Brown, "Techniques for Privacy and Authentication in Personal Communication Systems", *IEEE Personal Communications*, vol.2, no.4, pp. 6–10, August 1995.

[12] Joseph E. Wilkes "Privacy and Authentication Needs of PCS", *IEEE Personal Communications*, vol.2, no.4, pp. 11–15, August 1995.

[13] C. H. Chang, "Efficient End-to-End Authentication Protocols for Mobile Networks", Master thesis, Tsing Hua Univ., 1996.