Habitant One-Time Furtive Mechanisms for Quick Common Validation in Mobile Interactions

Anand Yaramala[#1], Dr. S. Sai Satyanarayana Reddy Seelam[#2], Sudheer Babu Kuntumalla[#3]
#1 Student, Lakireddy Bali Reddy College of Engineering, Mylavaram, Krishna(dt),
#2 Professor, Lakireddy Bali Reddy College of Engineering, Mylavaram, Krishna(dt).
#3 Asst. Professor, Lakireddy Bali Reddy College of Engineering, Mylavaram, Krishna(dt).

Abstract : Many security mechanisms for mobile Interactions have been introduced in the literature. Among these mechanisms, Validation plays a quite important role in the entire mobile network system and acts as the first defense against attackers since it ensures the correctness of the identities of distributed communication entities before they engage in any other communication activity. Therefore, in order to guarantee the quality of this advanced service, an efficient (especially user-efficient) and secure Validation scheme is urgently desired.

In this paper, we come up with a novel Validation mechanism, called the Habitant one-time Furtive mechanism, tailored for mobile communication environments. Through maintaining inner and outer synchronously changeable common Furtives, respectively, every mobile user can be rapidly authenticated by visited location register (VLR) and home location register (HLR), respectively, in the proposed scheme. Not only does the proposed solution achieve Common Validation, but it also greatly reduces the computation and communication cost of the mobile users as compared to the existing Validation schemes. Finally, the security of the proposed scheme will be demonstrated by formal proofs.

Index Terms : Information security, Common Validation, one-time Furtives, secure mobile communication

I. I NTRODUCTION

DUE to the Quick progress of communication technologies, many popular services have been developed to take advantage of the advanced technologies. One of these popular services is wireless communication. Ubiquitous wireless networks make it possible for distributed entities to remotely and efficiently communicate with each other anytime and anywhere, even in mobile status. Furthermore, tiny and exquisite handsets greatly raise the portability of mobile devices. Owing to the features of Quick mobility and high portability, wireless communication has played an extremely important role in personal communication activities.

Most of the current mobile communication services are based on the Global System for Mobile Interactions (GSM) architecture, and some novel applications based on the third generation (3G) of mobile communication systems have also been deployed. Common Validation and other related security issues have been considered in the GSM-based Validation protocols proposed in the literature [3]–[19], but their performance should be improved as much as possible to further meet the low-computation requirement for mobile users and guarantee the quality of the communication services.

II. REVIEW OF HWANG ANDCHANG 'S SCHEME

In 2003, Hwang and Chang proposed a Common Validation scheme for mobile Interactions [10], which is briefly described below. First, the notation used in the scheme is de fined in Table I. The scheme consists of two protocols. The first one is described below.

Step (1): U_i First, randomly generates a number r0, and then sends{U_i, E_{Kuh} ($K_{uh}||r_0$)} to V .
Step (2): V generates a number r1at random and sends E_{Kuh} ($K_{uh}||r_0$) and E_{Kuh} ($K_{uh}||r_1||t$)to H for authentication. Here, t denotes the current date and time, i.e., the timestamp.
Step (3): H checks t and K_{uh} to verify the legality of U_i and V. Then, H sends E_{Kuh} (r_1) and E_{Kuh} ($r_0||$ r_1)back to U_i.
Step (4): U_i checks r_0 to judge whether V is legal or not, and then takes r_1 as K_{auth}. V sends E_{Kuh} ($r_0||r_1$) to U_i.
Step (5): U_i checks to examine whether V and H are both legal or not, and then takes r_1 as K_{auth}. Afterward, U_i sends E_{Kauth} (r_1) to V.
Step (6): If r_1=E_{Kauth} , U_i then is authenticated by V successfully.

When U_i does not leave the service area of V, it is only required for her/him to perform the second protocol with for authentication by using their common session key K_{auth}, where H does not need to participate in the protocol. The details of the second authentication protocol for U_i and V are described in the following.
Step (1): randomly generates a string and computes . Then, sends to .
Step (2): After receiving decrypts and checks whether is a prefix of the result or not. If it is true, randomly generates a string and computes . Then, sends to .
Step (3): decrypts and verifies if is equal to the one in Step (1). If it is true, computes and sends it to .
Step (4): decrypts and checks if is equal to the one it chose before. If true, and authenticate each other successfully.

Hwang and Chang's scheme is quite efficient for mobile users without impractical assumptions.

In the following, we will present a novel practical mobile Validation scheme that is much more efficient than Hwang and Chang's scheme [10] in both computation and communication under the same assumption of.

III. OUR IDEA

In this section, we will introduce our basic idea that is the underlying foundation for the construction of the proposed Validation scheme in mobile environments.

A. An Efficient Hybrid Mechanism for Common Validation

With a preshared Furtive key K, there are two basic approaches to achieve Common Validation between two entities, say Alice and Bob. One is the timestamp-based approach, and the other is the nonce-based approach.

The assumptions of a timestamp-based Validation scheme:

1) The clocks of Alice and Bob must be synchronous.

2) The transmission time for the Validation message transmitted from Alice to Bob (or from Bob to Alice) must be stable.

The advantages of a timestamp-based Validation scheme:

1) The protocol only requires two rounds of transmission to reach the goal of Common Validation.

2) It is efficient in computation and communication.

Although timestamp-based Validation schemes are simple and efficient, the above two constraints make them impractical in the Internet and mobile environments since most of the users' clocks are not synchronous with the server's or system's clocks and the transmission time is usually not stable.

The advantages of a nonce-based Validation scheme:

1) It is not necessary to synchronize the clocks of Alice and Bob.

2) The transmission time for the Validation message transmitted from Alice to Bob (or from Bob to Alice) can be unstable.

The drawbacks of a nonce-based Validation scheme:

1) The protocol requires three rounds of transmission to reach the goal of Common Validation.

2) The scheme is less efficient than a timestamp-based Validation scheme in computation and communication.

A nonce-based Validation scheme is free from the two constraints required in a timestamp-based Validation scheme, but the performance may be a problem in the nonce-based scheme as compared to the timestamp-based one.

The assumption of an Validation scheme based on onetime Furtives:

1) Alice and Bob cannot perform the first time of Common Validation via the protocol since there is no one-time Furtive shared by them before the first Validation.

The advantages of an Validation scheme based on one time Furtives:

1) The protocol only requires two rounds of transmission to reach the goal of Common Validation.

2) It is more efficient than a nonce-based Validation scheme in computation and communication. (However, it is less efficient than a timestamp-based scheme since an additional string must be computed in the scheme based on a one-time Furtive.)

The drawback of an Validation scheme based on one time Furtives:

1) Alice and Bob must store an extra string, i.e., the one-time Furtive, in their devices or computers.

The comparisons of the three Validation mechanisms (i.e., timestamps, one-time Furtives, and nonces) are summarized in Table II.

B. Habitant One-Time Furtive Mechanisms

Consider a sequence of Common Validation processes based on our proposed hybrid mechanism between mobile user and the system (a VLR and the HLR). In the initial Validation, the user and the system authenticate each other by performing a nonce-based Validation protocol, and then they negotiate an initial value of a one-time Furtive. Thus, they make use of the one-time Furtive, called the outer one-time Furtive, to complete the following Validation processes.

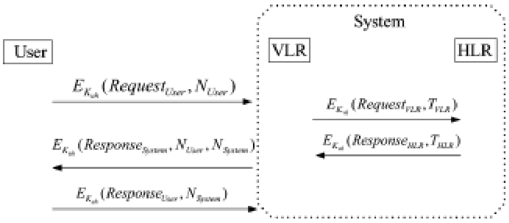

System
User
VLR
HLR
$E_{K_{uh}}(Request_{User}, N_{User})$
$E_{K_{vh}}(Request_{VLR}, T_{VLR})$
$E_{K_{uh}}(Response_{System}, N_{User}, N_{System})$
$E_{K_{vh}}(Response_{HLR}, T_{HLR})$
$E_{K_{uh}}(Response_{User}, N_{System})$

Fig. 1. Our idea for the initial authentication between a mobile user and thesystem (VLR and HLR).

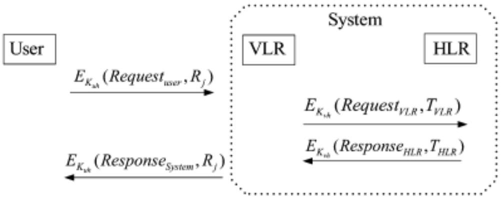

System
User
VLR
HLR
$E_{K_{uh}}(Request_{user}, R_j)$
$E_{K_{vh}}(Request_{VLR}, T_{VLR})$
$E_{K_{vh}}(Response_{HLR}, T_{HLR})$
$E_{K_{uh}}(Response_{System}, R_j)$

Fig. 2. Our idea for the th authentication between a mobile user and the system(VLR and HLR) after the initial one, where J>=1.

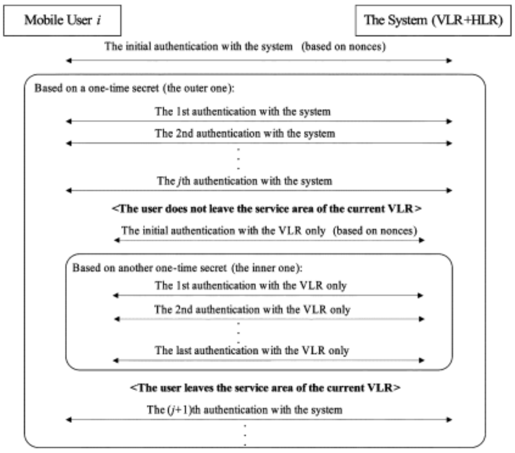
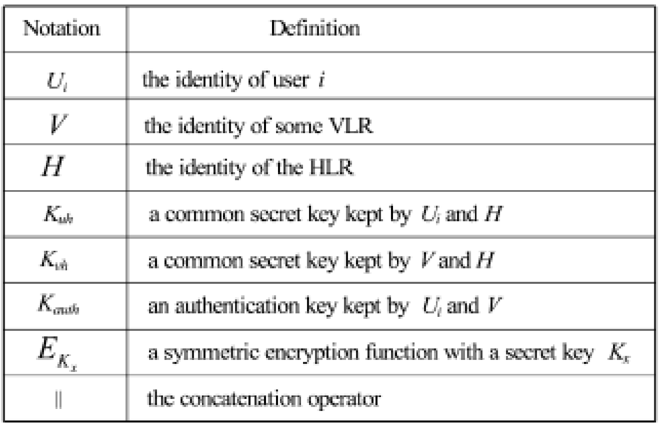

Mobile User i
The System (VLR+HLR)
The initial authentication with the system (based on nonces)
Based on a one-time secret (the outer one):
The 1st authentication with the system
The 2nd authentication with the system
The jth authentication with the system
<The user does not leave the service area of the current VLR>
The initial authentication with the VLR only (based on nonces)
Based on another one-time secret (the inner one):
The 1st authentication with the VLR only
The 2nd authentication with the VLR only
The last authentication with the VLR only
<The user leaves the service area of the current VLR>
The (j+1)th authentication with the system

Fig. 3. The proposed nested one-time secret mechanism.

TABLE I

NOTATIONUSED IN HWANG AND CHANG 'S SCHEME



Notation	Definition
U_i	the identity of user i
V	the identity of some VLR
H	the identity of the HLR
K_{uh}	a common secret key kept by U_i and H
K_{vh}	a common secret key kept by V and H
K_{auth}	an authentication key kept by U_i and V
E_{K_x}	a symmetric encryption function with a secret key K_x
$\|\|$	the concatenation operator

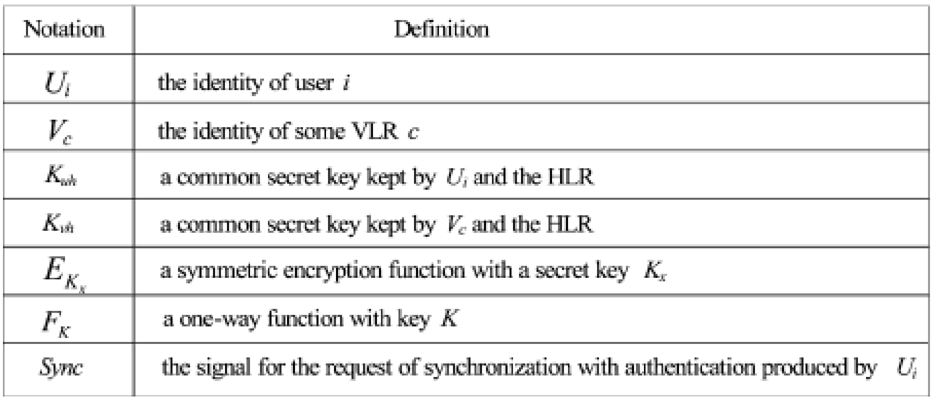
TABLE II

COMPARISONS OF THETHREE AUTHENTICATION MECHANISMS

	Timestamps	One-Time Secrets	Nonces
Assumptions:	1. ClockSynchronization 2. Stable transmisson time	The perevious authentication be successfully finished	None
Performance:	The most efficient solution	Slightly less efficient	Much less efficient
Suitable for:	The authentication between VLR and HLR	The authentication between a user and the system for the authentication processes after the initial one	The initial authentication between a user and the system

TABLE III

D EFINITION OF NOTATION IN THE PROPOSED SCHEME



Notation	Definition
U_i	the identity of user i
V_c	the identity of some VLR c
K_{uh}	a common secret key kept by U_i and the HLR
K_{vh}	a common secret key kept by V_c and the HLR
E_{K_x}	a symmetric encryption function with a secret key K_x
F_K	a one-way function with key K
$Sync$	the signal for the request of synchronization with authentication produced by U_i

In the proposed idea, mobile user shares the outer one-time Furtive with the HLR and shares the inner one-time Furtive with the current VLR. This is referred to as the Habitant one-time Furtive mechanism, which is illustrated in Fig. 3.

IV. T HEPROPOSED SCHEME

Based on the ideas introduced in Section III, we propose a Quick Common Validation and key exchange scheme for mobile Interactions. Our scheme consists of two parts and each of the two parts contains two protocols. The first part of the scheme is designed for Common Validation between a mobile user and the system (a VLR and the HLR) where it includes two protocols: The second part of the scheme is tailored for Common Validation between a mobile user and a VLR when the user does not leave the service area of the VLR. Similarly, the second part contains two protocols:

1) an initial Validation protocol for Common Validation and the initialization or reinitialization of the inner one-time Furtive (described in Section IV-C); and

2) an Validation protocol based on the inner one-time Furtive for the Validation after the most recent performance of the initial Validation protocol in Section IV-C between the user and the VLR where is a positive integer.

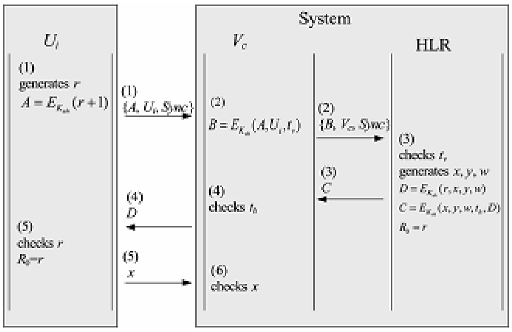


Fig. 4. The initial authentication protocol for a user and the system.

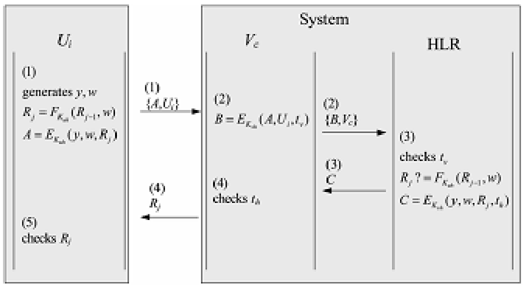


Fig. 5. The th authentication protocol for a user and the system (VLR andHLR) after the most recent initialization.

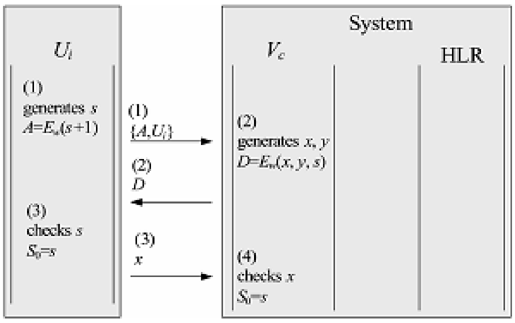


Fig. 6. The initial authentication protocol for a user and a VLR.

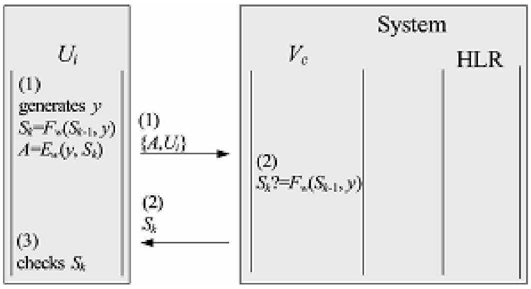


Fig. 7. The th authentication protocol for a user and the current VLR after themost recent initialization.

V. SECURITY MODELS AND PROOFS

A. Security Models and Definitions Our communication model and security notions are based on [22]. A simulator simulates an environment such that an adversary can execute the proposed protocols with .If breaks one of the proposed protocols, can use the output from to solve a hard problem.

In our model, oracle models a player attempting to authenticate a player in session of the protocol, where being the set of the

VI. PERFORMANCE COMPARISONS

Performance is a key factor for popularizing the services in mobile communication systems. Especially, almost all of the mobile users pay much attention to the performance issue due to the limited computation capabilities of their mobile devices.

Among the Validation schemes for mobile communication proposed in the literatures [7], [9], [10], [14]–[20], Hwang and Chang's scheme [10] is the most efficient one.

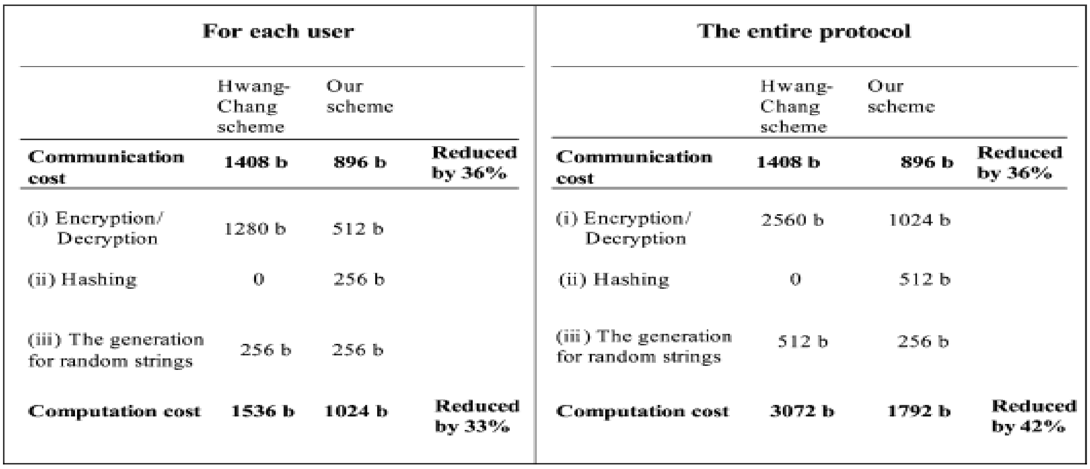
According to different situations, we properly utilize three different Validation

identities.of the players who can participate in the protocol, and being the set of positive integers. The adversary is not a player in our model. Let us define the capability of, which can be captured by the following queries:

mechanisms—i.e., timestamps, one-time Furtives, and nonces—in the proposed Validation scheme for mobile communication such that it possesses better performance than Hwang and Chang's scheme. In this section, we will demonstrate that our proposed scheme is more efficient than Hwang and Chang's scheme in both computation and communication cost.

TABLE IV

COMPARISONS OF THESECOND PROTOCOL OF AND THE PROTOCOL OF SECTION

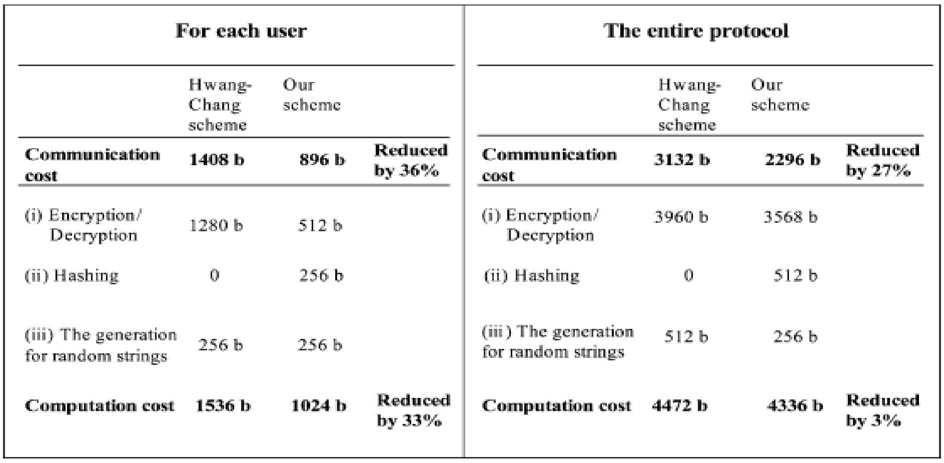


For each user				The entire protocol			
	Hwang-Chang scheme	Our scheme			Hwang-Chang scheme	Our scheme	
Communication cost	**1408 b**	**896 b**	**Reduced by 36%**	**Communication cost**	**1408 b**	**896 b**	**Reduced by 36%**
(i) Encryption/ Decryption	1280 b	512 b		(i) Encryption/ Decryption	2560 b	1024 b	
(ii) Hashing	0	256 b		(ii) Hashing	0	512 b	
(iii) The generation for random strings	256 b	256 b		(iii) The generation for random strings	512 b	256 b	
Computation cost	**1536 b**	**1024 b**	**Reduced by 33%**	**Computation cost**	**3072 b**	**1792 b**	**Reduced by 42%**

As mentioned above, our proposed scheme possesses the advantage of efficiency. Especially, the Validation protocol after the latest initialization and the Validation protocol after the latest initialization i.e., the protocol in Section IV-D) can greatly lighten the communication and computation cost.

TABLE V

COMPARISONS OF THEFIRST PROTOCOL OF AND THE PROTOCOL OFSECTION



For each user				The entire protocol			
	Hwang-Chang scheme	Our scheme			Hwang-Chang scheme	Our scheme	
Communication cost	**1408 b**	**896 b**	**Reduced by 36%**	**Communication cost**	**3132 b**	**2296 b**	**Reduced by 27%**
(i) Encryption/ Decryption	1280 b	512 b		(i) Encryption/ Decryption	3960 b	3568 b	
(ii) Hashing	0	256 b		(ii) Hashing	0	512 b	
(iii) The generation for random strings	256 b	256 b		(iii) The generation for random strings	512 b	256 b	
Computation cost	**1536 b**	**1024 b**	**Reduced by 33%**	**Computation cost**	**4472 b**	**4336 b**	**Reduced by 3%**

VII. C ONCLUSION

We have proposed a secure Common Validation and key exchange scheme for mobile Interactions based on a novel mechanism, i.e., Habitant one-time Furtives. The proposed scheme can withstand the replay attack and the impersonating attack on mobile Interactions and speed up Validation. Compared to Hwang and Chang's scheme, not only does the proposed scheme reduce the communication and computation cost, but also the security of our scheme has been formally proved.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments on this paper.

REFERENCES

[1] D. Brown, "Techniques for privacy and Validation in personal communication systems," IEEE Personal Commun. , vol. 2, no. 4, pp. 6–10, Aug. 1995.

[2] N. Jefferies, "Security in third-generation mobile systems," IEE Coll.Security Netw. , pp. 8/1–8/5, 1995.

[3] M. Rahnema, "Overview of the GSM system and protocol architecture," IEEE Commun. Mag., vol. 31, no. 4, pp. 92–100, Apr. 1993.

[4] B. Mallinder, "An overview of the GSM system," in Proc. 3rd Nordic Seminar Digital Land Mobile Radio Commun., Copenhagen, Denmark, 1998, pp. 12–15.

[5] A. Aziz and W. Diffie, "Privacy and Validation for wireless local area networks," IEEE Personal Commun. , vol. 1, no. 1, pp. 24–31, 1993.

[6] M. S. Hwang, Y. L. Tang, and C. C. Lee, "An efficient Validation protocol for GSM networks," in Proc. AFCEA/IEEE Euro-Comm, 2000, pp. 326–329.

[7] S. Suzuki and K. Nakada, "An Validation technique based on distributed security management for the global mobility network," IEEE J. Sel. Areas Commun., vol. 15, no. 8, pp. 1608–1617, Oct. 1997.

[8] C. H. Lee, M. S. Hwang, and W. P. Yang, "Enhanced privacy and Validation for the global system for mobile Interactions," Wireless Netw., vol. 5, no. 4, pp. 231–243, 1999.