International Journal of scientific research and management (IJSRM)
||Volume|| 1 ||Issue|| 6 ||Pages|| 311-315 ||2013||
Website: www.ijsrm.in ISSN (e): 2321-3418

A Novel Model for Efficient Communication in 2g/2.5g Or 3g Through Reduced Signalling Overhead

Selim Mahmud[1], Mohammad Mahbubur Rahman Khan Mamun[2] and Saikat Biswas[3]

E-mail: s.mahmud067@gmail.com

Abstract: With its great features like providing access to users at anytime and anywhere in the world, mobile communication has been very attractive among the users as well as operators and service providers. However, despite of several advantages, mobile communication has also been facing many safety problems. In 2G/2.5G (GSM, GPRS) and 3G (UMTS) technologies, the architectures comprise of mainly three nodes; the mobile station (MS), Visitor Location Register/Serving GPRS support Node (VLR/SGSN), and Home Location Register (HLR). These nodes are involved to encode/decode the data and validate the user (MS) in 2G and 3G. To add more and more protected features, we propose a new generalized approach in this paper which is based on reduced signaling overhead.

I. Induction

Wireless and mobile communication systems are very famous among the customers as well the operators and service providers. Unlike wired networks, the wireless networks provide anywhere and anytime access to users. The Global System for Mobile Communications (GSM) occupy almost 70% of the wireless market and is used by millions of subscribers in the world [1]. In the wireless services, protected and stealthy communication is desirable. It is the interest of both, the customers and the service providers. These parties would never want their resources and services to be used by unapproved users.

The services like online banking, e-payment, and e/m-commerce are already using the Internet. The financial institutions like banks and other organizations would like their customers to use online services through mobile devices keeping the wireless transaction as protected as possible from the safety threats. Smart cards (e.g. SIM card) have been proposed for applications like protected access to services in GSM to validate users and protected payment in Visa and MasterCard [2]. Wireless transactions are facing several safety challenges. Wireless data passing through air interface face almost the same retreat threats as the wired data. However, the limited wireless bandwidth, battery, computational power and memory of wireless devices add further limitations to the safety mechanisms implementation [3].

The use of mobile communication in e/m-commerce has increased the importance of sanctuary. An efficient wireless communication infrastructure is required in every organization for safe voice/data communication and users verification. Among the main objectives of an efficient infrastructure is to reduce the signaling overhead and reduce the number of updating Home Location Register (HLR) while the Mobile Station (MS) changes its location frequently [3]. In this paper, we propose an approach based on reduced signaling overhead and meet other safety requirements like non-repudiations, protection from denial-of-service attacks and integrity of confirmation signaling messages.

II. GSM Overview/Evolution

GSM, the Group Special Mobile, was a group formed by European Conference of Post and Telecommunication Administrations (CEPT) in 1982 to develop cellular systems for the replacement of already incompatible cellular systems in Europe. Later in 1991, when the GSM started services, its meaning was changed to Global System for Mobile Communications (GSM) [1]. The entire architecture of the GSM is divided into three subsystems: Mobile Station (MS), Base Station Subsystem (BSS) and Network Subsystem (NSS) as shown in Fig-1. The MS consists of Mobile Equipment (ME) (e.g. mobile phone) and Subscriber Identity Module (SIM) which stores undisclosed information like International Mobile Subscriber Identity Module (IMSI), furtive key (Ki) for verification and other user related information (e.g. certificates). The BSS, the radio network, controls the radio link and provides a radio interface for the rest of the network. It consists of two types of nodes: Base Station Controller (BSC) and Base Station (BS). The BS covers a specific geographical area (hexagon) which is called a cell. Each cell comprises of many mobile stations. A BSC controls several base stations by managing their radio resources. The BSC is connected to Mobile services Switching Center (MSC) in the third part of the network NSS also called the Core Network (CN). In addition to MSC, the NSS consists of several other databases like Visitor Location Register

(VLR), HLR and Gateway MSC (GMSC) which connects the GSM network to Public Switched Telephone Network (PSTN). The MSC, in cooperation with HLR and VLR, provides lots of functions including registration, verification, location updating, handovers and call routing. The HLR holds administrative information of subscribers registered in the GSM network with its current location. Similarly, the VLR contains only the needed administrative information of subscribers currently located/moved to its area. The Equipment Identity Register (EIR) contains list of valid mobile equipment's and subscribers' verification information respectively [1, 5].

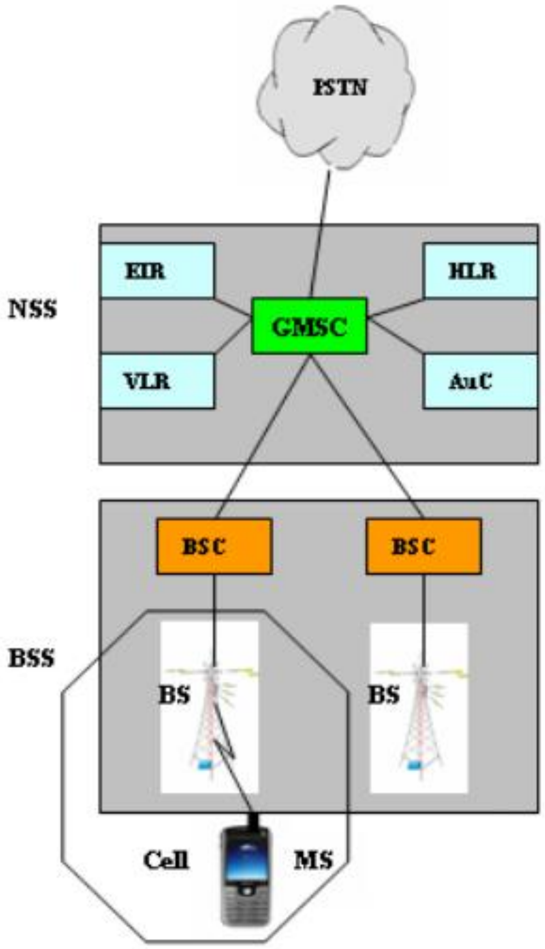

Fig-1: GSM Components

III. Ciphering in 2g or 2.5G

There are various safety threats to networks [6]. Among these threats are Masquerading or ID Spoofing where the attacker presents himself as to be an official one, unofficial use of resources, unlawful disclosure and flow of information, illegal alteration of resources and information, repudiation of actions, and denial-of-service. The GSM network incorporates certain safety services for operators as well as for their subscribers. It verifies subscribers' identity, keeps it surreptitious, keeps data and signaling messages confidential and identifies the mobile equipments through their International Mobile Equipment Identity (IMEI). In the next subsections, we explain subscribers' verification and data privacy as they are closely related to our topic [5].

3.1 Subscribers Identity Verification

As mentioned above, the SIM card holds IMSI, phone number, verification key Ki, subscriber-relevant data and safety algorithms like verification algorithm (V3). The HLR also stores a copy of Ki and IMSI etc. In GSM, the users are first identified and validated then the services are granted. The GSM verification protocol consists of a challenge-response mechanism. The validation is based on a stealthy key Ki which is shared between HLR and MS. After a visited MS gets a free channel by requesting BS, it makes a request for its location update to MSC through BSC. The MSC, in response, asks MS for its validation.

In the entire validation process, the three main actors are the MS, MSC/VLR and HLR as given in Fig-2. The mobile station sends its Temporary Mobile Subscriber Identity (TMSI) to VLR in its request for validation. The MS uses its real identity IMSI when it is switched on for the first time but the temporary identity TMSI is used later. The TMSI is used to provide anonymity to the user identity. After getting the IMSI of the mobile station from the old VLR using TMSI, the VLR sends IMSI to the corresponding HLR. The HLR uses verification algorithm (V3) and ciphering key generation algorithm (A8) to create the encryption key (Kc) and Signed RESult (SRES) respectively. The HLR sends the triplet including Kc, RAND and SRES to VLR. The VLR sends the RAND challenge to MS and ask to generate an SRES and send it back. The mobile station creates an encryption key Kc and SRES using algorithms V3 and A8 with the inputs stealthy key Ki and RAND challenge. It stores Kc to use it for encryption and sends SRES back to the VLR. The VLR compares SRES with the one sent by HLR. If they match, the verification succeeds otherwise it fails [1, 4, 5].

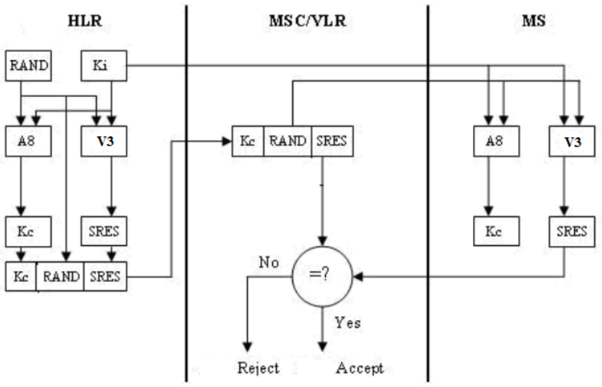

Fig-2: Verification Mechanism

3.2 User Data and Signaling Protection

The encryption key Kc is used by both of the parties (home system and mobile station) to encrypt the data and signaling information using A5 algorithm. The encryption is done by mobile equipment not the SIM because SIM does not have enough power and processing capacity [1, 4, 5].

IV. Ciphering in 3G

3G (UMTS) is the result of evolution in GSM network through 2.5G (GPRS). The GSM networks are capable of voice communication using Circuit Switched (CS) technique while GPRS adds Packet Switched (PS) technique through the use of some extra nodes like Serving GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN). The UMTS, incorporating GPRS nodes and UMTS Terrestrial Radio Access Network (UTRAN), provides both circuit switched and packet switched services with enhanced multimedia applications.

As stated in 3GPP specification [7], the circuit switched services are provided by VLR and the packet switched services are provided by SGSN. The UMTS, like GSM/GPRS, uses the concept of Verification Vector (VV) but unlike GSM/GPRS, the VV comprises of five components: the random challenge (RAND), the expected response (XRES), key for encryption (CK), integrity key (IK) and the verification token (VETN). The VLR/SGSN requests HLR for validation. The HLR computes the VV and is sent back as a response to VLR/SGSN without any encryption applied to it. After the verification is completed, the cipher key CK is used to encrypt the user data and signaling information. Similarly, to preserve the integrity of the important control signals, integrity key (IK) is used.

The GSM Consortium actually provided safety to GSM systems relying on sanctuary through anonymity where they believed that the algorithms used in GSM would be very hard to break if they were kept stealthy . Therefore, the GSM specifications and protocols were kept stealthy away from public to be studied and analyzed by scientific community. But, eventually, the GSM algorithms were accessed by scientific community and now GSM is vulnerable to many attacks [6, 7, 10]. In GSM/GPRS and UMTS, the links between MS-VLR and VLR-HLR faces many safety threats due the use of conventional encryption and mutual trust of the parties. The VLR and HLR just rely on mutual trust they have on each other.

The Public Land Mobile Network (PLMN) operators are the main candidates for this to develop PKI in their systems. The 3G networks like UMTS which offers services with very high data rates is the most favorable for the operators to incorporate PKI services to their customers. To verify the legitimacy of public keys, there should be a trusted third party to issue digital certificates to the users. These certificates are to be stored in the SIM/USIM of the mobile station. The Mobile Execution Environment (MExE) is an application execution environment which allows application programming and creating a Java Virtual Machine (JVM) in the MS. Based on the importance of safe transactions and the fact that networks operators are the big candidates for PKI implementation, it seems feasible to use public-private key pair for intra-PLMN signaling as well as for protected e/m-transaction.

V. Signaling Overhead Reduction in 2G/2.5G and 3G

As in GSM/GPRS, we consider the same three nodes: MS, VLR and HLR. These nodes preserve the same roles for all the three systems: GSM, GPRS and UMTS, involved in the process of verification and encryption. The nodes VLR and HLR hold the same pair of public-private keys, V_HPrK and V_HPuK, which facilitates the key distribution process because other interconnected networks would need only one public key for corresponding VLR-HLR transactions. A second option could be to use separate public-private key pairs but it will further complicate the key distribution process. The link between VLR and HLR is protected using the VLR-HLR public key (V_HPuK). The messages are encoded with this key by any of the endpoints. At the receiving end, the corresponding private key V_HPrK is used for decryption. After the channels are assigned, the users are validated through the exchange of messages among the nodes: MS, VLR and HLR as shown in Fig-3. The MS (SIM on mobile station) sends an Identity Message to VLR which includes the identity data (e.g. IMSI of the user) encrypted with MS-VLR's public key (MS_VPuK). The VLR decodes it using corresponding private key (MS_VPrK) and extracts the required information. The VLR encrypts it again with VLR-HLR link public key (V_HPuK) and forwards it to the corresponding HLR in Validation Information message. After it is decoded using VLR-HLR link private key (V_HPrK), the HLR sends the user's public key (MSPuK) back to the VLR in an Confirmation Acknowledgment message. The VLR sends a random challenge RAND to the MS encrypted with the user's public key (MSPuK) in Verification Request message. The MS decodes the random number, encrypts it with its own private key and sends it back along with SK and IK to VLR in Validation Response message. The VLR decrypts this message using the user's public key and checks if the random number is the same. If it is equal to the random number held by VLR, it will indicate the user legitimacy as it has been signed by the user with his own private key. Public key encrypting is computationally extensive. Therefore, it slows down the data rate.

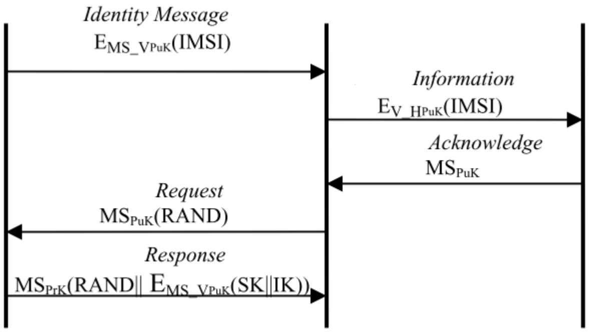

Fig-3: Verification process

Here we propose a general solution with reduced signaling overhead for all the three systems 2G, 2.5G and 3G to overcome the drawbacks discussed above. In this section, we present a solution based on reduced signaling overhead using the same concept of public-private keys but in different manner.

V_HPrK: VLR-HLR link's private key
V_HPuK: VLR-HLR link's public key

M_VPrK: MS-VLR link's private key
M_VPuK: MS-VLR link's public key

HPrK: HLR Private Key
HPuK: HLR Public Key

MPrK: Mobile station's private key
MPuK: Mobile station's public key

These three entities exchange four messages with each other as shown in Fig-4. The detail of the elements in each of these messages is –

Identity Message = EM_VPuK (IK||SK||RAND) || EHPuK (IMSI|| Ki)
Verification Information = EHPuK (IMS||Ki)
Verification Acknowledge = MPuK
Forward Verification Acknowledge = EMPuK (RAND)

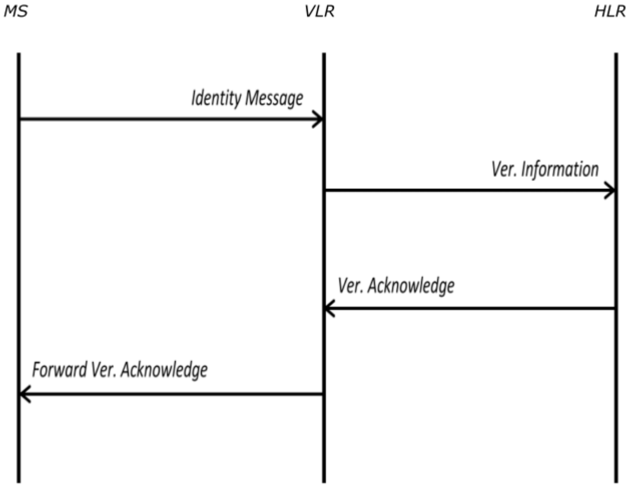

Fig-4: Proposed verification procedure

The symbol '||' represents the concatenation of two elements. The MS creates stealthy keys SK, IK and a random challenge RAND. It starts the verification exchange by sending an Identity Message to the visited VLR. This message includes concatenation of RAND, SK and IK encrypted with public key M_VPuK. The IMSI and Ki encrypted with public key HPuK is also part of the Identity Message as shown in Figure 4. Unlike the existing approach, the stealthy keys SK and IK are sent in the first message. The VLR uses the corresponding private key M_VPrK to decode the part of the message and extract the needed information RAND, SK and IK. The VLR forwards therest of message (EHPuK(IMS||Ki)) unchanged in Verification Information message to the HLR. The keys SK and IK are used later for confidentiality and integrity of both the data and signals respectively. The HLR decodes the Verification Information message with its private key HPrK and gets the IMSI and Ki sent from MS. The surreptitious key Ki is used as a random challenge for user/MS verification. The MS and the HLR have the same undisclosed key Ki. The HLR compares the received Ki with its own Ki. If they match, the user is verified. It is difficult for a third party to change this in stealthy mode without being detected by HLR. The HLR can easily detect it using IMSI of the requesting user sent in the Identity Message. Using the IMSI, the HLR finds the corresponding user's public key MPuK and is sent to VLR in the Verification Acknowledge message. This message acts as an indication to the VLR that the user has been validated by the HLR. The VLR uses the public key MPuK to encrypt the RAND challenge received from MS in the Identity Message. The MS decrypts it with its own private key. The result is compared with the RAND stored at MS. If they are equal, the VLR is validated as it ensures the MS that the VLR is the only entity having the MS-VLR link's private key M_VPrK. This approach includes all the benefits of the previous systems. This entire process requires four signaling messages and hence the signaling overhead is reduced.

VI. Conclusion

Wireless communication, having great features, is attractive among users as well service providers. With the increase in its use, safety problems of confidentiality, integrity, and verification are also increasing. The mechanism to solve these problems has been changed. In this paper, we proposed a heightened model based on the reduced signaling overhead. In this model, utilizing the real benefits of public key encryption, user as well as network certification is provided. The integrity of the signaling used during the user and network verification is ensured. The stealthy keys for data encryption and signaling integrity are distributed using public keys. These benefits are achieved with fewer signals.

VII. Reference

[1] Yong Li, Yin Chen, and Tie-Jun MA, "Security in GSM", Retrieved March 18, 2008, from http://www.gsm-security.net/gsm-security-papers.shtml.
[2] N. T. Trask and M. V. Meyerstein, "Smart Cards in Electronic Commerce", A SpringerLink journal on BT Technology, Vol. 17, No. 3, 2004, pp. 57-66.
[3] N T Trask and S A Jaweed, "Adapting Public Key Infrastructures to the Mobile Environment", A SpringerLink journal on BT Technology, Vol. 19, No. 3, 2004, pp. 76-80.
[4] Cheng-Chi Lee, Min-Shiang Hwang, and I-En Liao, "A New Verification Protocol Based on Pointer Forwarding for Mobile Communications", A Wiley InterScience journal on Wireless Communications and Mobile Computing, Published online, 2007.
[5] Vesna Hassler and Pedrick Moore, "Safety Fundamentals for E-Commerce", Artech House London Inc., 2001, pp. 356-367.
[6] Mohammad Ghulam Rahman and Hideki Imai, "Safety in Wireless Communication", A SpringerLink journal on Wireless Personal Communications, Vol. 22, No. 2, 2004, pp. 213-228.
[7] 3GPP. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Mobile Execution Environment (MExE); Service Description, StageI. Technical Specification 3G TS 22.057 version 5.2.0 (2001-10), 2001.

Authors' Biography

Selim Mahmud[1] received B. Sc. in Computer Science and Engineering (CSE) from Bangladesh University of Engineering and Technology (BUET) in 2008. At present Mr. Mahmud is working in Robi Axiata Ltd.

Mohammad Mahbubur Rahman Khan Mamun[2] accomplished B. Sc. in Electrical and Electronic Engineering (EEE) from Bangladesh University of Engineering and Technology (BUET) in 2009. Currently Mr. Khan is working in Baglalink Digital Communication Ltd.

Saikat Biswas[3] received B. Sc. in Computer Science and Engineering (CSE) from Bangladesh University of Engineering and Technology (BUET) in 2008. At present Mr. Biswas is working in Systems Solutions and Development Technologies Limited (SSD-TECH).