Signal Processing and Renewable Energy
September 2018, (pp. 41-48)
ISSN: 2588-7327
e-ISSN: 2588-7335

Intelligent Management of User Initial Accessibility to PLMN through Fictitious Channel Sending in UMTS

Ehsan Abedi[1], Mansour Nejati Jahromi[1,2*]

[1] Department of Electrical Engineering, South Tehran Branch, Islamic Azad University, Tehran, Iran.
[2] Department of Electrical Engineering, Shahid Sattary Aeronautical University of Science and Technology, Tehran, Iran

Abstract
A management protocol level connection line with universal mobile telecommunications system (UMTS) terrestrial radio access network is required in order to enable user's connection in UMTS networks which is performed by transferring data streams among some pre-shared channels. In this paper international mobile subscriber identity (IMSI) is obtained by an intelligence supervise interception so that if the user identity is not allowed, the connection would be terminated by supervisor. The advantage of this method in comparison with traditional approaches is in attacking connection while it is not in safe layer. In other words, rejection of connection will be performed before any network capacity loss. Our investigation proved that the proposed method results in reduction of computational complexity and energy usage of networks. Furthermore, the probability of network intrusion is also improved.

Keywords: International Mobile Subscriber Identity, Radio Resource Control Protocol, Supervise interception, Universal Mobile Telecommunications System.

1. INTRODUCTION

Universal mobile telecommunications system (UMTS) is one of the proposed standards of third-generation telecommunication networks which provided by the International Telecommunication Standards Association. In this system, different encryption algorithms are used to provide security, which is hard to break. Before encrypting the connection of a user and the network, it is necessary to initiate a series of signaling processes between them in order to create a connection line at the level of radio resource control (RRC) management protocol. After establishing the above mentioned connection, the authentication and its key agreement (AKA) processes are performed, and then a secure connection is established.

In network connection and the AKA of UMTS network processes, some security holes exist that includes most of the threats and attacks. Cellular telecommunication engineers and researchers have done a lot of researches in this area to reject UMTS attacks. Most attacks on cellular networks are based on the layers and security protocols of the network. That is to say, hackers attack the intended system by obtaining some of the main parameters of these protocols.

The proposed idea is, in fact, an intelligent jamming attacks a specific user. Each attack follows a particular target according to the location. The purpose of this idea is preventing the initial

*Corresponding Author's Email: nejati@aut.ac.ir

connection of an unauthorized user from network to radio section in terms of the network's protection component by creating an RRC connection line.

The paper outline is given in following. In Section 2, the UMTS architecture and the UMTS channel type are explained. Section 3 review the signal exchange processes of the first network connection, and Section 4 is about signaling messages for the reception of RRC links. In Section 5, we have threats on the UMTS network and Section 6, explains a method for intelligent management of the user's initial connection to the network. Finally, Section 7 gives the paper conclusion.

2. UMTS NETWORK ARCHITECTURE

The components of the UMTS network as shown in Fig. 1, in terms of type of task, fall into three general categories:

I. The radio section of the network that contains the components of the network, whose function is to establish and control the radio communication with a user.
II. The core network (CN) which includes switching components and route paths for calls, and exchanging information between users and networks.
III. The user terminal (UT) is the user's utility for communicating with the network.

2.1. Layer Structure in the UTRAN User Radio Protocol

The task of the radio connection protocol is to communicate between the user and the radio network, ordering, resetting and release of radio carriers. It consists of three layers as follows:

• Physical layer (layer 1) whose task is the physical transfer of information in the radio connection.

• Connection layer (layer 2) whose task is preparing and formatting the layer information 3 and transferring it to layer 1.

• The network layer (layer 3) which has only one protocol called radio resource control (RRC)

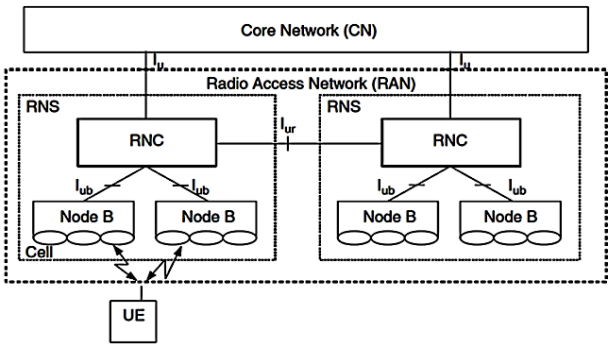

Fig.1. An overview of the UMTS network architecture [2].

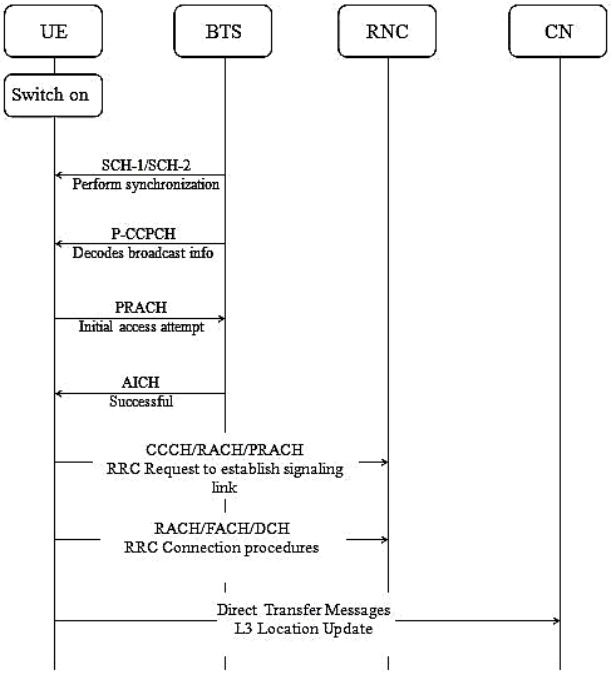

Fig. 2: Processes required establishing the first connection to the network after the UE is turned on [1].

whose task is to process and transmit the signaling information associated with the UTRAN's radio connection control.

Since the RRC protocol in layer 3 is the most important protocol in the UMTS network architecture, it is briefly explained in the following.

The RRC protocol is used to control the user's movement in the network-connected mode, AS and NAS based signaling transmission between the user and the network, and the creation, modification and release of radio carriers. Transmission processes, user information encryption, initial cell selection when the UE is turned on (see Fig. 2.), and re-selection of the cell is also within

the scope of the RRC protocol. In general, when the user wants to connect to the network, it is necessary to establish a RRC connection line with the network at first, so that it can communicate with the network.

2.2. Channel Types in UMTS

The Channels used in UMTS for radio communication with the user, are divided into three categories explained in following.

I. Logical channel: A specific type of information is transmitted by the radio burrier (RB) between the radio network controller (RNC) and a user, which broadcast control channel (BCCH) and common control channel (CCCH) are the two most important ones.

II. Transmission Channel: The method and the way of transmitting the logical channel between the physical layer 1 and layer 2 in the UE and RNC. Forward access channel (FACH) and random access channel (RACH) are the two most important ones.

III. Physical channel: The actual channel is in the propagation environment where the content of the transmission channel is moved between the user equipment (UE) and the radio network controller (RNC), where P/S-CCPCH (primary/Secondary common control physical channel) and PRACH (physical random access channel) are the two most important ones.

3. REVIEWING THE SIGNAL EXCHANGE PROCESSES OF THE FIRST NETWORK CONNECTION

In general, MS processes in idle mode are divided into three parts:

1. Select PLMN (public land-based mobile network)
2. Select and re-select the cell
3. Position registration

When a user connects to its UE device (see Fig. 2), it must have a signaling link with the core of the network to inform the core sector of its presence and position by updating the location. Before the user can connect to the kernel part for the above mentioned purpose, it must establish a RNC signaling relationship (RRC link). Before setting up the RRC link, the user first needs to set up a proper cell in his HPLMN (home public land mobile network) camp on and obtain the required system information from the BCCH logical channel (which puts on the physical channel of the P-CCPCH). In order to communicate with control cells of a cell, the "selection of the primary cell" must be initiated and synchronized with it.

The initial connection processes are summarized as follows:

1. Turning on the phone by user.
2. Establishing a link with the core of the network in order to inform the core of the network of presence, the location, and the identification of its identity.
3. Establishing a RRC signaling relationship with the RNC to connect the user to the network core.
4. Obtaining the system information from the BCCH logical channel written on the PCCPCH physical channel by the user before the RRC establishes a link with the RNC.
5. Determining the user's scrambling group using the synchronization channels and obtaining the scramble vector by the CPICH (common pilot channel).
6. Applying descramble operations and eliminating the expansion of the received data from the P-CCPCH and obtaining dissemination data.
7. Sending to the PRACH, a random access to the network by the user, (sending its initial 4096 chip to node B, and repeatedly sending it in case of necessity).
8. Confirming the correct receipt of information from node B by sending the AICH (acquisition indicator channel) to the user.

9. Sending identity, reason for requesting an RRC link (such as network registration or location update), measurement results of the CPICH (to set the power through node B) by the RRC signaling link via the "connection request" signal RRC "to the RNC by the user at this stage (by the CCCH logical channel on the PRACH physical channel).
10. Checking the user's acceptance or denied (sending a RRC "denied connection" message to the user in case of non-acceptance).
11. Sending the identity, temporary user ID, TFS, TFCS, frequency, UR and UM code to the user by RNC with the message "setting up RRC connection".
12. Declaring the success of the RRC link to the RNC by the user, with the message "completing RRC setup" on the channel (logical) of the DCCH specific signaling, after synchronizing between the physical layer and the node B (this message contains information about encryption, and integrity of the phone).

4. SIGNALING MESSAGES FOR THE RECEPTION OF RRC LINKS

4.1. Receiving an RRC Connection Request Message by UTRAN

To receive an RRC connection request message, UTRAN must:

- Accept the request and use a predefined or conventional radio configuration.
- Provide the message "set up RRC connection" to the lower layers if the message is received for sending on the CCCH channel in the DL direction.
- Provide a "RRC deny" message if the CCCH logical channel is not received in the DL direction
- In this message, the UTRAN may direct the UE to another UTRA or another system. After sending this message, all conceptual information for the UE may be cleared at UTRAN.

4.2. Receiving a "RRC Connection Denial" Message by the UE

When the UE receives a "Dispatch RRC connection" message on CCCH in the DL direction, it should compare the "user ID" information element in the received message with the INITIAL-UE-IDENTITY variable value.

1. If the values are different; the UE must ignore the reminder of the message.
2. If the values are the same, the UE should:
   • Stop the T300 timer.
   • If the UE deactivates the selection of the cell in a UTRA carrier due to the above message, the UE must re-open the cell selection on the UTRA.
3. If the "waiting time" information element is non zero and there is "frequency information":

3.1. If V300 is smaller than or equal to N300:

- Select a suitable cell in the UTRA in accordance with the standard.

After selecting the cell and acting “camp on” a suitable cell in the UTRA carrier:

• Set the CFN to fit the SFN of the current cell according to the standard.
• Set the content of the message "RRC connection request" according to the standard.
• Send "RRC connection request" message to CCCH in UL direction.
• Reset the V300 counter.
• When the MAC layer shows the success or failure, start the T300 timer.
• Disable the re-selection of the cell in the UTRA carrier when the waiting time is completed or the RRC connection process is completed.

- If no suitable cell was found on UTRA:

• Wait at least as much as the waiting time.
• Follow the steps above.

3.2. If the V300 is bigger than the N300:

• Enter idle mode.

If the inter-RAT-info information element is present:

• If the waiting time is zero, the UE behavior is indefinite.

5. THREATS ON THE UMTS NETWORK

The protection and security of communication in the UMTS system is difficult, as various attacks on this system are implemented. Attacks such as DOS and MIM attacks, “Identity catching attack” and “Redirection attack” are the most important threats. Major threats and attacks have been based on three security factors: authentication, confidentiality and data integrity. Table 1 shows the Types of threats and their effects on the UMTS network [1].

In following, two “Identity catching attack” and “Redirection attack” are briefly explained.

5.1. Identity Catching Attack

Unfortunately, the UMTS system has little protection against attacks. Although the IMSI is replaced with TMSI after the first communication request, it sends out the first RRC connection during the request, and then assigns the VLR a temporary identity identifier (TMSI). The attacker introduces itself as an UMTS VLR. During a RRC request, a victim may use TMSI. If the TMSI is rejected by the network, it sends an identity request to the victim. In this case, MS sends its IMSI clearly and after the acquisition of IMSI, the attacker disconnects his connection. This type of attack is classified in two ways.

I. Passive identity catching:

In this method, the inactive attacker waits for a new registry and sends the IMSI in plaintext. In this way, the attacker is ready and stand by to receive the user's identity at perfect time.

II. Active identity catching:

In this case, the attacker acts as a changed BS and requests the user for “Camp on” his identity.

5.2. Redirect Attack

This type of attack is one of the possible attacks on multiple mobile networks. In this attack, the attacker can simultaneously place itself in place of BS and MS. In order to deceive MS, the attacker turns a legitimate BSS by publishing a fake BSS ID.

6. A METHOD FOR INTELLIGENT MANAGEMENT OF THE USER'S INITIAL CONNECTION TO THE NETWORK

The basis of the proposed method is based on several key principles in the connection process as listed in following.

• Synchronization with network

• Full implementation of signaling processes and detecting the transmitted messages.

• Obtaining a user identity (IMSI)

• Check the user's authentication by checking the identity

• Send time and correct fake channel by the attacker

• Manage the user to lead the state or mode in order to deceive

The method outlined in Fig. 3 is in fact a combination of two "passive user authentication" attacks and "redirection attacks" that, with the addition of the steps described below, can be a suitable method for intelligent and targeted attacks. Be on a specific user. In the following, the proposed idea is presented in a step-by-step manner:

1) Being lit or in the network coverage of the UE, which leads to the request of establishment the first connection with the network.

2) Before any exchange of signaling between the user and the network, the UE must be synchronized with the channel SCH by the frame rate and slot. According to the timing and timing relationships between physical channels, in order to execute this attack, the attacker should also listen to the SCH channel and synchronize the frame and slot with the network. If this step is not done, the attacker will not be able to decrypt and receive system information and also send fake valid channels to the UE.

3) Listening to the P-CCPCH broadcast channel and decoding it to obtain network system information including general network parameters, server-specific parameters, and configuration

details of PRACH channels that the UE needs to communicate with the network. In this step, the attacker must also obtain this information in order to access the PRACH channel sent by the UE and extract the user ID (IMSI) from it as well as configure the fake S-CCPCH

4) In this step, the first attempt is made to communicate with the network by the UE and, as it is verified, the UE sends a sequence of 4096 chips to node B by the PRACH. This sequence contains a string of 16 chips, 256 times repeated and informs the user about the accuracy of the receipt by sending the AICH to the UE when fully received by the network.

As explained in the previous step, the PRACH profile, to which the UE communicates with the network, is reported in the network system information, which is obtained by detecting this information by the attacker into the PRACH.

This step may be repeated several times by the UE to confirm its receipt by node B by the AICH, so the attacker should also receive this confirmation to prepare itself for the most important step of the scenario, namely to obtain the user ID.

5) At this stage, after receiving from the AICH to communicate with the core of the network, the UE must establish a higher-level communication with the network, or, in other words, an RRC connection with UTRAN. An RRC link request is always made by the UE and with the PRC request "RRC connection request" signaling. This message has information such as "user's original identity" and the "cause of establishment." After sending this message, the V300 counts the V300 equal to one and issues that start command for the T300 timer.

6) In this step, the attacker must receive this message by listening to the PRACH, which has the characteristics of the system information received from the network, and receive the above information elements according to the configuration of the channel mentioned in the standard form.

7) Now, the identity obtained from the channel in the previous step is checked by attacker with a processor or computer, so if this identifier is on the blacklist, the next step is carried out by the attacker and if that identifier is valid from the point of attacker, the attack process is stoped.

8) If the user ID is invalid for the network, this step is begun. In this step, the attacker immediately sends the message "Deny RRC connection" by a fake S-CCPCH channel. This message is configured in the attacker's memory, and only places the "user identity" information element in the “IDENTITY-UE-INITIAL” variable.

In Table 2, the information elements in this message are written. Besides, a brief explanation of them and how they are configured in the mentioned message are given.

Table 2. ***The contents of the signaling message RRC connection reject [9].***

Information Element /Group name	**Need**	**Type and reference**	**Semantics description**	**Version**
Message Type	MP	Message Type		
UE Information Elements				
RRC transaction identifier	MP	RRC transaction identifier		
Initial UE identity	MP	Initial UE identity		
Rejection cause	MP	Rejection cause		
Wait time	MP	Wait time		
Redirection info	OP	Redirection info		
Counting completion	OP	Enumerated(TRUE)	This field may be present if the Rejection cause is set to “unspecified” otherwise it shall be ignored	REL-6

• **RRC Transaction ID**: Identifies the RRC transaction identity, which is an identifier assigned to this transaction and its existence is mandatory. The attacker has set its value in the message by default.

• **Original User ID:** It is the user's primary identity which at first communicates. The information is equal to IMSI ID of the user and its existence is mandatory. The attacker extracts its value from detecting the RRC connection request message sent by the UE.

Reason of Rejection: This element indicates the reason for regection, which has two "congestion" and "unclear" modes. An attacker can use "congestion" which means traffic congestion in the cell.

• **Waiting Time**: This element represents the amount of time (in seconds) that a UE waits to repeat the acceptance procedure. The attacker sets this value to zero, so that the procedure is not repeated by the UE.

• **Redirect Information**: This element contains information that directs the UE to a new frequency or a new RAT. The attacker put a default Inter-RAT info in the message and directs the UE to a false amount.

9) At this step, the UE receives the "rejection" message and reveals its information. Because the identity in this message is in accordance with the user ID, the UE considers it as a valid message. According to the description given in the previous Section, since the waiting time is equal to zero and the Inter-RAT info is presented, the UE behavior is indefinite. In other cases, the behavior of the UE is specified, and in this state is only unclear, which means that the UE has been interrupted with the network.

7. CONCLUSION

In this article, the UMTS network structure and architecture as the most common mobile-cellular network of the third generation were studied. Then, according to the topic of the article, initial signaling processes between user and the radio section of the network (UTRAN) and related messages were reviewed. Since the attack location of the proposed idea is in the process of establishing the RRC connection, it is continued to explain how to create and accept the signaling messages for establishing an RRC between the user and the UTRAN. Given the idea that some of the attacks on the UMTS network are exploited, there are a number of attacks and threats on the network. As stated, most attacks on cellular networks on the layer of security increase the effectiveness and some complexity of the task, but the proposed attack in order to manage the user's initial connection to the PLMN is prior to this step and, in principle, prevents the connection in layer 3 with the network. The smart word in this thesis is used due to the fact that the prevention of network connectivity is limited to one or more specific users with their own unique identity identifier (IMSI). The mentioned attack would be effective if only the attacker’s fake message was received before the main message which is sent by UTRAN to the user. In order to do this, it is necessary to use fast processors in the attacker and co-operate with the network

REFERENCES

[1] Holma, H., Toskala A., WCDMA for UMTS, Radio Access for Third Generation Mobile Communications, 4ed, 2007.

[2] Wiley, j., Ltd, S., W-CDMA: Mobile Communications System, NTT DoCoMo, Inc., Japan, 2002.

[3] ETSI TS 125 331 V7.12.0, Radio Resource Control (RRC), European Telecommunications Standards Institute (ETSI), 2014.

[4] ETSI TS 123 002 V7.11.0, Network architecture, European Telecommunications Standard Institute (ETSI), 2012.

[5] ETSI TS 123 002 V5.12.0, Network architecture, European Telecommunications Standards Institute (ETSI), 2003.

[6] ETSI TS 125 211 V7.10.0, Physical channels and mapping of transport channels onto physical channels (FDD), European Telecommunications Standards Institute (ETSI), 2010.

[7] ETSI TS 125 212 V7.12.0, Multiplexing and channel coding (FDD), European Telecommunications Standards Institute (ETSI), 2014.

[8] ETSI TS 123 122 V7.7.1, Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode, European Telecommunications Standard Institute (ETSI), 2006.

[9] Ayoubi Mobarhan. M, Ayoubi Mobarhan. M, Shahbahrami. A, "Evaluation Of Security Attacks On Umts Authentication Mechanism", International Journal of Network Security & Its Applications (IJNSA), University of Guilan, Rasht, Iran, Vol.4, No.4, July 2012.