Confidentiality in the UMTS Radio Access Network Simulation approach under OPNET

Said El Hajji and Ghizlane Orhanou
Laboratoire Mathématiques, Informatiques et Applications,
Université Mohammed V Agdal, Faculté des Sciences
BP 1014, Rabat, Maroc
elhajji@frs.ac.ma and ghizlane.orhanou@gmail.com

Abstract

The Universal Mobile Telecommunications System (UMTS) offers a panoply of 3G services. In addition to delivery of images, graphics and video communications, UMTS is used for such applications as banking and e-commerce and hence security is a critical concern.

In the present paper, we are interested in the confidentiality feature in the UMTS Network Access. Ciphering when applied is performed in the RNC and the UE either in the RLC sub-layer or in the MAC sub-layer. Our current research aims to examine exactly where the encryption/decryption occurs in the protocol stack of an UMTS network. And then introduce this security feature in the OPNET Modeler which is used to give a simulation approach of the use of the UTRAN confidentiality feature between RNC and UE.

This paper is organized as follows. First, a brief description of the UMTS confidentiality mechanism. Then, We will be interested in the UMTS stack layers where the ciphering and deciphering of data would be performed. After, we will describe our simulation approach by exposing the changes made to mobile station and RNC node models in order to implement the confidentiality feature.

Keywords: UMTS, Confidentiality, Encryption, f8, RLC Acknowledged Mode, RLC Unacknowledged Mode, RLC Transparent Mode, OPNET simulation

1. CONFIDENTIALITY FEATURE IN THE UMTS RADIO ACCESS NETWORK

1.1. Confidentiality

User data and some signalling data are considered sensitive and their confidentiality should be protected over the radio access link. To ensure this data confidentiality on the air interface, the following features are provided [5]:

- Cipher algorithm (f8) agreement: nowadays, there exist two variants of the cipher algorithm: UEA1 based on KASUMI algorithm and UEA2 based on SNOW 3G algorithm [1, 2]. The MS (*Mobile Station*) and the SN (*Serving Network*) can securely negotiate the algorithm to use in their mutual communication.
- Cipher key (CK) agreement: the agreement on a cipher key to use subsequently is done between the MS and SN during the Authentication and Key Agreement procedure ;
- Confidentiality of user and signaling data: this property insures that the user and signaling data cannot be overheard on the radio access interface;

1.2. UMTS Encryption function f8

The data confidentiality during its transmission over the radio interface is fulfilled by an UMTS confidentiality cryptographic function f8 [5] which is a symmetric synchronous stream cipher. This type of ciphering has the advantage to generate the mask of data before even receiving the data to encrypt, which help to save time. Furthermore, it is based on bitwise operations which are carried out quickly.

Figure 1 bellow illustrate the Encryption/Decryption operations using the f8 function.

FIGURE 1: Encryption/Decryption of user and signalling data

The input parameters of f8 are the following:

- **CK** : Cipher Key;
- **COUNT-C** : Time dependent input used to synchronize the sender and the receiver;
- **BEARER** : Service bearer identity;
- **DIRECTION** : Direction of the transmission;
- **LENGTH** : Number of bits to be encrypted/decrypted;

Based on these input parameters, the confidentiality algorithm generates the KEYSTREAM block which is used to encrypt / decrypt the input PLAINTEXT and then produces the CIPHERTEXT. The input parameter LENGTH is only used to control the length of the generated ciphertext and does not affect its bits.

As mentioned above, there exist nowadays two encryption algorithms UEA1 et UEA2. UEA1, which was used since the genesis of the UMTS network in 1999, is a stream cipher based on the block cipher KASUMI [7, 8].

The second one, UEA2, is also a stream cipher but based on an other stream cipher named SNOW 3G [2, 11, 12]. It was introduced as 3GPP standard on 2006.

In our simulation approach, we have implemented UEA1. The implementation of the second confidentiality algorithm and the negotiation between the user and the network about the confidentiality algorithm to use will done in future works. It is important to note that we have already tested and implemented UEA1 and UEA2 algorithms (C language) and perform some necessary rectifications in the 3GPP algorithms codes to meet the 3GPP Implementation testsets results [2].

2. UMTS LAYER OF CIPHERING

As mentioned above, the confidentiality function f_8 is located in the UE (User Equipment) and the RNC. Encryption is applied either in the Radio Link Control (RLC) sub-layer [9] or in the Medium Access Control (MAC) sub-layer [10] of the data link layer (Layer 2), according to the following rules [5]:

- if a radio bearer is using a non-transparent RLC mode (Acknowledged Mode or Unacknowledged Mode), ciphering is performed in the RLC sub-layer.
- if radio bearer is using the transparent RLC mode, ciphering is performed in the MAC sub-layer (MAC-d entity).

To show the place of the RLC and MAC sub-layers in the UMTS Protocol stack, Figure 2 below illustrate the user and control planes protocol stack in the UMTS Terrestrial Radio Access Network (UTRAN).

FIGURE 2: UTRAN Protocol stack [3]

The ciphering algorithm (UEA1 or UEA2) and the key CK to be used are negotiated by upper layers during the Authentication and Key Agreement procedure.

In order to be able to implement the ciphering inside an existing OPNET MS (Mobile Station) and RNC node models, we need to understand how ciphering in each RLC mode is working and in which step the ciphering and the deciphering are performed. Furthermore, the data unit to cipher depends on the transmission mode. These issues will be presented in the following sub-sections.

2.1. RLC Unacknowledged Mode (UM)

2.1.1. Unacknowledged Mode RLC entity

Figure 3 shows the model of two unacknowledged mode peer RLC entities (in the UE and in the RNC).

We notice that the ciphering is applied as the last step before submitting the packet to the lower layer. On the receiving side, the packet is first decrypted before being sent to the reception buffer.

When the transmitting UM-RLC entity receives RLC SDU from upper layers, it segments it into UMD PDUs of appropriate size. The UMD PDU may contain segmented and/or concatenated RLC SDUs. It may also contain Padding to ensure that it is of a valid size.

FIGURE 3: Ciphering in two unacknowledged mode peer entities [9]

If ciphering is configured and started, an UMD PDU is ciphered (except for the UMD PDU header, see below for more details) before it is submitted to the lower layer. On the receiving side, the receiving UM RLC entity deciphers the received UMD PDUs (except for the UMD PDU header). It removes RLC headers from received UMD PDUs and reassembles RLC SDUs [9].

2.1.2. Unacknowledged Mode ciphering unit

For RLC UM mode, the ciphering unit is the UMD PDU excluding the first octet (the UMD PDU header) which represents the RLC Sequence Number [9]. This is illustrated in Figure 4 below.

FIGURE 4: Ciphering unit for UMD PDU [9]

2.2. RLC Acknowledged Mode (AM)

2.2.1. Acknowledged Mode RLC entity

Figure 5 shows the model of an acknowledged mode RLC entity. The ciphering and deciphering steps are presented.

FIGURE 5: Ciphering in a model of an AM mode entity [9]

When the transmitting AM-RLC entity receives RLC SDUs from upper layers, it segments them into UMD PDUs of appropriate size, fixed or flexible depending on the AM-RLC entity configuration. The AMD PDU may contain segmented and/or concatenated RLC SDUs. It may also contain Padding to ensure that it is of a valid size.

The ciphering is applied to AMD PDUs. The AMD PDU header is not ciphered, as for the UM mode. Piggybacked STATUS PDU and Padding in AMD PDU (when present) are ciphered. Control PDUs (i.e. STATUS PDU, RESET PDU, and RESET ACK PDU) are not ciphered. In the receiving side, AMD PDUs are routed to the Deciphering Unit, where AMD PDUs (without header) are ciphered, and then delivered to the reception buffer [9].

2.2.2. Acknowledged Mode ciphering unit

For RLC AM mode, the ciphering unit is the AMD PDU excluding the first two octets (the AMD PDU header) as shows Figure 6 bellow.

FIGURE 6: Ciphering unit for AMD PDU [9]

2.3. RLC Transparent Mode (TM)

2.3.1. Transparent Mode MAC entity

If a radio bearer is using the RLC Transparent Mode, the ciphering function is performed in the MAC sub-layer, precisely in the MAC-d entity [10]. In the UE, there is one MAC-d entity while in the RNC, there is one MAC-d entity for each UE that has one or more dedicated logical channel to or from the RNC.

FIGURE 7: Ciphering in two MAC-d peer entities [10]

2.3.2. Transparent Mode ciphering unit

For RLC TM, the plaintext to be encrypted consists of all the MAC SDUs containing data for one and the same radio bearer and sent in one Transmission Time Interval (TTI). Figure 8 shows the part of the MAC PDU to be encrypted [6].

FIGURE 8: Ciphered part unit for a MAC PDU [10]

3. CONFIDENTIALITY SIMULATION APPROACH

3.1. Simulation methodology

Our current work is focused on establishing the foundation for future deep study of the UMTS security features in order to improve and enhance the actual procedures and features.

We have chosen OPNET as the simulation environment because its flexibility allows us to implement the security features in its UE and RNC model nodes and test these features as in a real UMTS network with respect to the control plane, the user plane, protocols characteristics in their deep details. In our research, we are using the UMTS specialized model set.

The UMTS model is based on 3GPP Release 1999 standards. The network architecture of this release consist on the User Equipment domain (UE), the UMTS Terrestrial Radio Access Network (UTRAN) domain and the Core Network domain (CN) as shown in Figure 9 bellow.

FIGURE 9: UMTS Network representation

Since the confidentiality feature in the UMTS Radio Access Network is located in the UE (User Equipment) and the RNC (Radio Network Controller), we have modified only *umts.station* and *umts.rnc* simulator node models to implement the ciphering algorithm in their RLC entities. All other UMTS elements within the UTRAN and the Core Network remain unchanged.

3.2. Enhanced OPNET UE node model

The UMTS station node model *umts.station* shown in Figure 10 includes an application layer CLIENT related to the GMM layer. It also includes the RLC/MAC layer where the encryption has to be implemented, a radio transmitter and receiver, and one antenna.

In this node model, the RLC/MAC layer is modeled by the Process Model *umts_rlc_mac* shown in Figure 11, which define the behavior of this module. This process handles segmentation and reassembly of higher layers PDUs into and from smaller RLC PUs. It also handles transparent, unacknowledged and acknowledged RLC modes [4].

FIGURE 10: *umts_station* node model FIGURE 11: *umts_rlc_mac* Process Model in the UE

Since the ciphering is done just before sending the RLC PDU to the lower layers, and the deciphering is applied when a packet is received from lower layers, our principal work in the UE side is done essentially in the two forced states SEND_DATA and FROM_LOW of the Process Model *umts_rlc_mac*. The other states remain unchanged.

The state SEND_DATA, is responsible of sending data out from the UE. It computes the size of the MAC header depending on which logical and transport channels are used to send the packet to the physical layer. It handles also packets segmentation and transmission for the three RLC modes and packets retransmission for Acknowledged Mode.

For our case, we have focused on the RLC Unacknowledged and Acknowledged Mode (UM and AM). So, the Enhanced SEND_DATA state performs data ciphering before the transmission of the packet to the lower layer for these two modes as follows:

- In the RLC Unacknowledged Mode, PDUs from higher layers are segmented and the RLC header is added to each segment to constitute the RLC PDU. At this step, we perform the encryption of the different fields of the UMD PDU, which represent the RLC PDU excluding the sequence number. After that, the ciphered UMD PDU is re-encapsulated into the RLC PDU and the MAC header is added. The MAC PDU is then sent to the L1 layer.
- In the RLC Acknowledged Mode, things are more complicated than for RLC UM. We have to check that the PDUs received from upper layers are not a CONTROL PDUs (like STATUS PDU, RESET PDU, and RESET ACK PDU) because these PDUs have not to be ciphered. Then, as for RLC UM, PDUs from higher layers are segmented and the RLC header is added to each segment to constitute the RLC PDU. At this step, the encryption of the different fields of the AMD PDU is done. The ciphered AMD PDU is re-encapsulated into the RLC PDU. The MAC header is added and then the MAC PDU is sent to the L1 layer.

When a packet is received in the RLC/MAC layer module, the Enhanced FROM_LOW state insures the deciphering and reassembling of the received segments according to the RLC mode used (UM or AM). Indeed, After removing the MAC header, the RLC mode is checked.

- In the RLC UM, the ciphertext (UMD PDU in this case), is deciphered and then sent to the reassembly buffer.
- For the RLC AM, the Enhanced FROM_LOW state checks first the received PDU type (DATA or CONTROL PDU). When it is a DATA PDU, it performs the decryption of the encrypted fields, and then send the result segment to the reassembly buffer.

3.3. Enhanced OPNET RNC node model

The RNC Node model shown in Figure 12 consists of the RNC manager and three child processes that perform the different functionalities of the RNC. The RNC manager has nine ATM or IP stacks attached to it, to be able to connect to the SGSN and the Node-Bs under its coverage [4].

FIGURE 12: RNC Process Model of the RNC Node Model [4]

One of the three child processes is the *umts_rnc_rlc_mac* process which is responsible of implementing Radio Link Control (RLC)/ Medium Access Control (MAC) functions. Figure 13 below shows its different states and transitions.

Since the deciphering is applied when a packet is received from one of the Node-Bs attached to the RNC, and the ciphering is done when a packet have to be sent to an UE over the air interface, our principal work in the RNC side is done principally in the two forced states FROM_NODEB and SEND_TO_UE of the Process Model *umts_rnc_rlc_mac*. The other states remain unchanged.

FIGURE 13: *umts_rnc_rlc_mac* Process Model in the RNC

The Enhanced FROM_NODEB state performs the decryption of packets received from one Node-B, and the Enhanced SEND_TO_UE state encrypt the packets sent to the UE. The encryption/decryption rules described for the UE side have to be respected also in the RNC side.

We are still testing our implementation, we have been able to encrypt and decrypt segments from/to the UE/RNC and we need to fix some little issues to be able to fully perform our simulation.

4. CONCLUSION

In this paper, we have tried to give a global idea of the confidentiality feature application over the radio link access. A detailed study of the different RLC modes in relation with this security feature have been carried out to be able to determine exactly where we should introduce the ciphering and the deciphering functionalities inside the Modeler node and process models. A description of the enhanced states in the concerning process models have been given in order to explain the different steps followed to implement the confidentiality feature. This OPNET simulation environment provides a platform for the continuation of work in this domain.

REFERENCES

- [1] S. El Hajji, G. Orhanou. *Sécurité du réseau UMTS - Etude des algorithmes cryptographiques du réseau d'accès radio*. 4th Conference TAMTAM'09. Kénitra. Maroc. May 2009.
- [2] S. El Hajji, G. Orhanou. *Cryptography in the UMTS Radio Access Network Security*. Next Generation Networks & Services (NGNS'09). ENSIAS. Rabat. Maroc. June 2009.

- [3] B. Walke, P. Seidenberg, M. P. Althoff. *UMTS - The Fundamentals*. WILEY. 2003.
- [4] "UMTS Model Description", OPNET Technologies. 2007.

3GPP specifications: <http://www.3gpp.org>

- [5] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture". december 2006.
- [6] 3GPP TS33.105: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; *Cryptographic Algorithm Requirements*". June 2007.
- [7] 3GPP TS35.201: 3G Security; *Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 1: f8 and f9 Specification*. June 2007
- [8] 3GPP TS35.202: 3G Security; *Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification*. June 2006.
- [9] 3GPP TS 25.322 : "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; *Radio Link Control (RLC) protocol specification*". March 2008.
- [10] 3GPP TS 25.321: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; *Medium Access Control (MAC) protocol specification*". March 2008.
- [11] ETSI/SAGE Specification: "*Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. Document 1: UEA2 and UIA2 Specification*". September 2006.
- [12] ETSI/SAGE Specification: "*Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. Document 2: SNOW 3G Specification*". September 2006.