ENHANCED RESEARCH PUBLICATIONS

INTERNATIONAL JOURNAL OF ENHANCED RESEARCH IN SCIENCE TECHNOLOGY AND ENGINEERING (IJERSTE)

Security in LTE using Artificial Neural Network

By: Vivek Chamoli, Karanpreet Singh, Renu Punera

2015

VOL. 4, ISSUE 2, FEBRUARY-2015, ISSN: 2319-7463, IMPACT FACTOR: 1.252

Security in LTE using Artificial Neural Network

Vivek Chamoli[1] Karanpreet Singh[2] Renu Punera[3]
M.tech (Communication System),Graphic Era University
Dehradun (India)

***Abstract*—Securing the transfer of data in wireless network is still a challenging issue. This paper propose a method for providing message security in LTE,we approach combines cryptography with artificial neural network to deal with the issues underlying message confidentially,integrity,and access control. With LTE being commercially deployed all around the world and the daily increase of its users and subscribers, specific issue and difficulties have emerged. Security does not affect the QoS and user experience. As one of the main goals of LTE is the decrease in latency, security mechanisms are not allowed to cause noticeable impact on the establishment of a communication and the transmission during the communication, as well as on the quality of LTEs services.**

Keywords: LTE (Long Term Evolution), Security in LTE, Artificial Neural Network (ANN)

I. Introduction

While developing and designing the LTE system, special attention was given to security measures and their most efficient implementation means. All functions and network elements were involved with equal priority. This approach resulted in special security applications for every aspect of the system, as each of them has its own requirements and processing capabilities. Moreover, already existing security measures such as ciphering algorithms and the authentication methods were taken over from previous mobile generation networks, applied with minimal changes to be supported by the new Evolved Packet System structure

Security measures are of utmost importance in every mobile communication system, which also includes LTE. Since the LTE system represents an all-IP structured network, traditional security measures from previous mobile communication systems are combined with additional security procedures covering the IP-architecture and techniques. Their main aim is to offer optimum security without reducing the QoS or negatively impacting the user.

II. SECURITY CONCEPT IN LTE [4]

With the development of LTE mobile networks, new communication standards were set and combined with existing IP-related standards, thus creating a broad spectrum of required security measures. The concept of security within the system is therefore based on the following requirements:

- High security level. The lowest security level allowed is the utilization of security techniques and measures from previous mobile communication networks such as 2G and 3G. Additional measures apply to the use of the IP structure within the Evolved Packet System.
- Security does not affect the QoS and user experience. As one of the main goals of LTE is the decrease in latency, security mechanisms are not allowed to cause noticeable impacts on the establishment of a communication and the transmission during the communication, as well as on the quality of LTEs services.
- Identification and authentication of every data transmission. Every transmission from the UE to the network and vice versa needs to be authenticated prior to establishment. This secures the identities of the UE, network and ultimately all user information
- Protection against internet based threats and attacks. A double layer security structure is set up in combination with reliable IP-security protocols to avoid threats and attacks from outside the network.
- User privacy, integrity and confidentiality. This prevents eavesdroppers from identifying the communicating parties and their information. To ensure that the signaling messages are genuine and not modified due to external access, a verification procedure is initiated.

III. CRYPTOGRAPHY [1]

There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of cryptography. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet. Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication.

Cryptography has two core styles of encrypting data; symmetrical and asymmetrical. Symmetric encryptions use the same key for encryption and decryption process, and also can be defined as a secret-key, shared-key, and private-key. Asymmetric cryptography uses different encryption keys for encryption and decryption process. In this case an end user on a network, public or private, has a pair of keys; one for encryption and one for decryption [1]. These keys can be identified as a public and a private key, which can be shown in Fig.1.

IV. CIPHERING TECHNIQUES IN LTE [4],[6]

Even through the key structure and management in LTE differs from those used in previous mobile communication systems, their encryption mechanisms are very similar. LTE

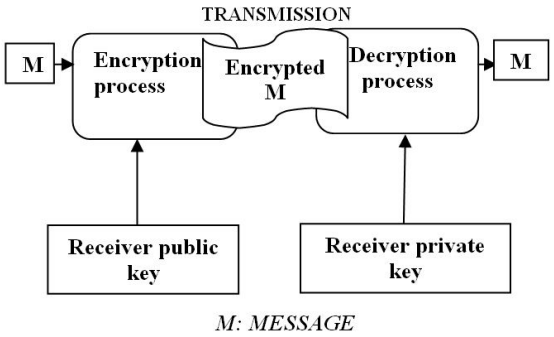

Fig. 1. CRYPTOGRAPHY PUBLIC KEY COMPONENT [1]

uses these mechanisms on both the AS and NAS level, providing an optimal secure environment for communications between a UE and the network. Depending on the sort of communication and between which elements it is established, four different ciphering techniques and algorithms are used: the null algorithm, SNOW 3G, AES and ZUC.

Null Algorithms (i.e. NAs) represent a technique used in the event of emergency calls, in which the connection must not be secured. Since an MME in LTE is obligated to let the UE know if the air interface will be secured or not, explicit messages which contain security off commands are sent instead of not sending a security on command. The procedure of starting a non-protected transmission is similar to the procedure of establishing a protected connection, except for the first step, in which a NA is selected instead of the most suitable protection algorithm. Although the NA contains algorithm in its name, it is in fact just a keystream with a simple equation function. This function depends on the type of NA realization, as there are different NA applications in LTE

The first type, known as EPS Encryption Algorithm Type 0 (EEA0), enables a non-protected transmission through the specific contents of its message, where the usual ciphertext is exchanged with plaintext. Another possible application of this type contains a keystream of all zeroes, taking advantage of the ciphertext formation which is calculated with a xor operation from the plaintext and keystream. The second type of NAs is realized through the use of simple mathematical operations, such as the appending of a 32-bit string of all zeroes to the end of the message. This way, a fake integrity protection is triggered15.A specific approach is introduced regarding AS and NAS security. To successfully provide a secure environment, two different encryption techniques are used, meeting the requirement of sufficient cryptographic diversity. This ensures that a possible attacker is hindered of compromising the identities (i.e. information) of the UE and network, as there is no realistic possibility of decrypting both parts in an acceptable time. These ciphering algorithms are called SNOW 3G and AES, and are explained below.

The SNOW 3G ciphering algorithm was taken over from 3G mobile communication networks with minimal adaptation changes to be fully supported by the EPS architecture. The LTE version is called 128-EEA1, which implies that 128-bit keys are used. A future upgrade to 256-bit keys is foreseen, thus the algorithms have been chosen accordingly. AES (i.e. Advanced Encryption System) ciphering algorithms were partially redesigned for the use in LTE, as its original functions were not designed for mobile packet data communications. The LTE version is called 128-EEA2 Counter Mode, also implying on the 128-bit nature of secure keys. Counter Mode indicates the specific bit allocation, where the message is comprised out of the ciphering algorithm input parameters (BEARER, COUNT and DIRECTION), located in the most significant part, and all zeroes, located in the least significant part.

The latest implementation in terms of ciphering algorithms is the ZUC stream cipher (i.e. cryptographic) set, building the core of two new LTE algorithms: the encryption algorithm called 128-EEA3 (i.e. ZUC) and the integrity protection algorithm known as 128-EIA3. These were designed as an alternative to AES, in order to enable cryptographic diversity of LTE systems and the use of LTE systems itself in as many countries as possible16. [5] From all above ciphering technique we see that there is no use of ANN in telecommunication field . So this paper propose a method for providing security in LTE using ANN.

V. CRYPTOGRAPHY/ CIPHERING USING ARTIFICIAL NEURAL NETWORK IN LTE

In the paper security in LTE has been achieved by using Artificial neural network in the following manner:-

- Using a Sequential machine
- Using a Chaotic neural network(CNN)

A. Cryptography/Ciphering using Sequential Machine[3]

For a sequential Machine, the output depends on the input as well as the state of the machine. Thus a sequential machine can be used in cryptography where the input data stream is the input to the sequential machine and the state determines the output input relationship. We can use the state of the sequential machine as the key and then use the data as an input to the sequential machine. The relationship between different output and states can be any random but unique sequence providing security to the encryption. As a sequential machine can be implemented by using a neural network, therefore a neural network can be used to encrypt data and another to decrypt data. In this case the starting state of the sequential machine can act as a key. For this application the state diagram is drawn and the data is used to train the neural network as it provides the way the machine moves from one state to another.

Implementation of squential machine in MATLAB is following whera a 3-bit encryption machine was successfully

built using an ANN based sequential machine. The sequential machine used had 2 states (0 and 1) and the input is the 3-bit data to be encrypted. Letters A to H were used to represent all the possible 3-bit inputs. If the state is 0, the input letter is shifted by one to generate the encrypted letter while if the state is 1, the letter is shifted by 2. During this operation, the state is automatically switched. Thus, if the starting state is 0 and the input is A, the output will be B and the state switches to 1. If the next input is again A, the output will be C as the current state now is 1. For H, state 0 will flip the letter to A while state 1 will flip the output to B. This method can be used to encrypt a word containing only the letters A to H. .The implementation of the above method is following.

- The word ABCDEFGH is to be encrypted using the starting state of 1. The output in this case will be CCEEGGAA.
- ABCDEFGH is to be encrypted using the starting state of 0.The output in this case will be BDDFFHHB.

B. CRYPTOGRAPHY USING A CHAOTIC NEURAL NETWORK [3]

Chaotic neural networks offer greatly increase memory capacity. Each memory is encoded by an Unstable Periodic Orbit (UPO) on the chaotic attractor. A chaotic attractor is a set of states in a system's state space with very special property that the set is an attracting set. So the system starting with its initial condition in the appropriate basin, eventually ends up in the set. The most important, once the system is on the attractor nearby states diverge from each other exponentially fast, however small amounts of noise are amplified. The chaotic neural network can be used to encrypt digital signal. A network is called a chaotic neural network if its weights and biases are determined by a chaotic sequence. The network's features are high security, no distortion.Encryption algorithm using chaotic neural network is following. Let f denote a digital signal of length M and f(n), 0 M-1 , be the one-byte value of the signal f at position n.

Step 1: enter the sequence of length M.

Step 2: Set the parameter,the initial point x(0) and μ .

Step 3: Evolve the chaotic sequence x(l), x(2), ... , x(M) by x(n+l) = (n)(l-x(n)), and create b(0), b(l), ..., b(8M-1) from x(l), x(2), ..., x(M) by the generating scheme that 0. b(8m-8)b(8m-7) .. b(8m-2)b(8m-l) is the binary representation of x(m) for m = 1, 2,. . . ., M.

Step 4: for n: 0 to (m-1) do

$$f(n) = \sum_i d_i \times 2^i \quad \textit{for i= 0 to 7} \tag{1}$$

do

$$w_{ij} = \begin{cases} 1, & if\ j = i\ and\ b(8 \times n + i) = 0 \\ -1, & if\ j = i\ and\ b(8 \times n + i) = 1 \\ 0, & if\ j \neq i \end{cases} \tag{2}$$

$j \in (0, 1, 2, 3, 4, 5, 6, 7)$

$$\theta_i = \begin{cases} -1/2, & if\ b(8 \times n + i) = 0 \\ 1/2, & if\ b(8 \times n + i) = 1 \quad \textit{for i= 0 to 7} \end{cases} \tag{3}$$

for i= 0 t0 7

do

$$d_i^{'} = f(\sum_i w_{ij} \times d_i + \theta_i) \tag{4}$$

end

$$v(n) = \sum_i d_i^{'} \times 2^i \quad \textit{for i= 0 to 7} \tag{5}$$

end

Step 5: the encrypted signal v(n) message is obtained and the algorithm is terminated.

A chaotic network is a neural network whose weights depend on a chaotic sequence. Here a sequence of M= 28 numbers .The chaotic sequence highly depends upon the initial conditions and the parameters, x(0) and μ. Implementation of algorithm in MATLAB is following:

- x(0) = 0.88 and μ= 3.9 are set. Here a sequence of 28 numbers [10 35 46 78 23 89 01 20 49 76 10 39 59 89 56 09 14 45 10 00 11 44 55 95 39 67 45 67] is used for encryption as shown in fig.2 and the initial parameters for the chaotic network are used as mentioned. The fig.3 shows the encrypted message signal [194 110 247 88 144 150 57 208 104 147 10 106 226 76 188 219 32 154 118 216 19 160 253 24 242 103 136 224].
- fig.4 shows the encrypted message signal[10 63 62 89 3 76 21 1 36 89 31 50 46 76 45 28 27 56 31 21 30 57 34 74 50 86 56 86] when x(0) = 0.55 and μ= 2.5 are set .

It is very difficult to decrypt an encrypted data correctly by making an exhaustive search without knowing x(0) and .The output or the encrypted data is then used for decryption. .It can easily be seen that the output is in a chaotic state. Depending upon the chaotic sequence a weight matrix and a bias matrix is obtained and the net input is obtained. Then a hard limiter is applied as a transfer function in order to obtain the digital encrypted data. For decryption the same network is used and

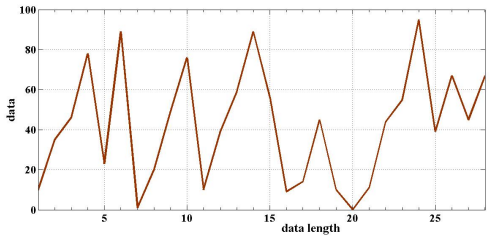

Fig. 2. Message signal

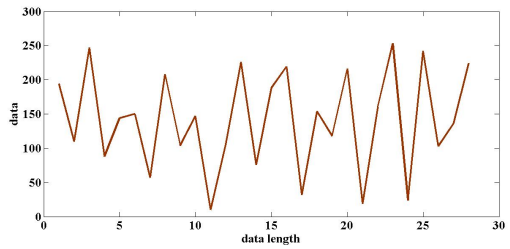

Fig. 3. Encrypted Message signal when x(0) = 0.88 and μ= 3.9 are set

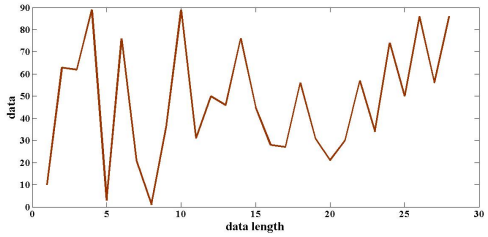

Fig. 4. Encrypted Message signal when x(0) = 0.55 and μ= 2.5 are set

the same initial value is used to generate the chaotic sequence and for decrypting the data successfully.Hence, CNN is one of guaranteed high security.

VI. Conclusion

Data security is a prime concern in data communication systems. . The use of ANN in the field of security in LTE is investigated using two methods. A sequential machine based method for encryption of data, where we see that the encrypted data will depend upon the present state of the machine. Therefore, the starting state along with the input will generate an output and then the state will change according to the state table. In case of two states, if it not known whether the state is 0 or 1, the data cannot be decrypted and hence the starting state acts as a key. Also, a chaotic neural network for digital data encryption, when the CNN is applied to a signal of length M= 28,it requires 8M bits. The number of possible encryption results is $2^8 \times$M. 8M equals 224 and all the possible results are 7168. Hence, the chaotic binary sequence is unpredictable. Better results can be achieved by improvement of code or by use of better training algorithms. Thus, Artificial Neural Network can be used as a new method of encryption and decryption of data in LTE.

References

[1] William Stallings,*Cryptography and Network Security: Principles and Practice, (5th Edition),* , Prentice Hall, 2010.

[2] Prachi Agrawal, Navita Agarwal "Use of Artificial Neural Network in the Field of security "*MIT International journal of computer science and information technology*, vol.3, n0.1, jan. 2013,pp. 42-44

[3] Adel A.El-Zoghabi,Amr H.Yassin,Hany H. Hussien I. M. Author, "Survey report on cryptography based on neural network," *International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459,ISO 9001:2008 certified journal*,, volume 3,issue 12, December 2013).

[4] Forsberg, Dan; Horn, Gnther; Moeller, Wolf-Dietrich; Niemi, Valtteri, *LTE Security,* John Wiley and Sons Ltd, Chichester, 2010.

[5] Mayur Solanki, Seyedmohammad Salehi, and Amir Esmailpour , "LTE Security: Encryption Algorithm Enhancement," *ASEE Northeast Section Conference Norwich University*, March, 2013.

[6] Ghizlane Orhanou and Said El-Hajji , "New LTE Cryptographic Algorithms EEA3 and EIA3," *Applied Mathematics and Information Sciences An International Journal* , Vol. 6,2013.