Volume 6, Issue 12, December 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Multi Column Authentication (MCA) with Common Entity Amalgamation (CEA) for GSM Network

Staffy Jain
CGC, Department of Information and Technology
Landran, Mohali, Punjab, India

Amitabh Sharma
CGC, Department of Information and Technology
Landran, Mohali, Punjab, India

Abstract— The cellular networks are increasing there volume every year and adding up millions of new customer to there customer pool, which means the infrastructural requirement of the network such as bandwidth, maximum throughput, security concern and other similar resources are rising. The data and the user privacy remains the primary matter of discussion in the security expert circles of the GSM based cellular networks. The requirement of security related practices always remains on the rise in order to meet the today's requirement, in this, model security mechanism has been proposed for the privacy protection of the GSM networks. The major GSM networks are considered in the second generation and the third generation of the cellular era. The proposed model is designed using the certificate less cryptography which utilizes the public key based cryptography for the implementation of the extra layer of security among the network nodes. The proposed will be analyzed by using the performance measures associated with the network performance and security measures. The proposed model is expected to solve the problems associated with the existing models. Fourth generation of the GSM network is emerging rapidly and capable of handling the higher number of users at one point. The results of proposed model justify the performance in comparison with the existing models.

Keywords— GSM, Certificate- less public key cryptography , Security, 2G, 3G, 4G.

I. INTRODUCTION

Mobile communications are developing day by day in past years, the main reason behind his cause is immense up gradation in technology attracts more user and each have their own needs to fulfill. So, to satisfy the requirements of mobile subscriber, various telecommunication companies start working on new technologies which provide some better features to meet the defined goals of user. In early generation the face of communication is only fixed landline phones without it there is no possibility to connect to other person but in today's world cellular technology breakaway this tradition. Mobility is a key aspect to today's generation; hence wireless mobile services provide us this feature. Mobile wireless communication helps the user in communication any person anywhere and anytime. The services offered by mobile wireless communication has filled this gap and it not only focuses on voice communication but also tries to give the user access to a new global communication reality [1].

Initially by introducing 1st generation cellular technologies plot various milestones such as 2nd Generation, 3rd generation, and now 4th generation system, as by introducing each new generation it brings a new technology with some enhanced features and some additional services from the previous one. The first communicational technology that was developed is 1st generation; it is introduced in early 1980s. 1G is introduced for analog system. Therefore this communicational technology provides only analog voice services and not even any data service; even then the bandwidth provided by 1G is up to 2.4kbps. The next generation that was introduced is 2nd Generation (2G) mobile telephone networks which are the new milestone for wireless systems after 1G. 2G introduce the wireless communication that is completely digital. [2] Then the 3rd generation is ready to be launched in the market with features like higher data transmission rates up to 2Mbps and offer increased capacity. In 3G the traditional voice calls also come up with the feature of global roaming. The higher speed and greater bandwidth provide 3G mobile phones a wide range of data services, such as mobile Internet access and multimedia applications [3].

3G mobile phones are new revolution in the market due to its attributes like TV streaming, multimedia, videoconferencing, Web browsing, e-mail, paging and navigational maps. 4G wireless mobile services are developed after 3G, 2G and 1G. So, the data rate supports by 4G is much more than these services which is 100 Mbps in dynamic situation and 1Gbps in static situation. Today's cell phones are very small and delicate and the space provided for each element is very less, so diminution of internal elements is required in design of mobile phones. The miniaturized structure of mobile devices required simple con-figuration of internal elements for easy integration. Design of mobile phones is simple and small so it needs the design of an internal antenna. The cell phones are supported by 1G, 2G, 3G as well as 4G, So, the antenna should have multiband and/or wideband characteristics. The 3rd generation wireless mobile services required long-term evolution (LTE), Wi-Fi, global positioning system (GPS), and Bluetooth. So, it needs wideband characteristics of antenna. The antennas with wideband characteristics are easy available but antennas with multiband characteristics are less. So, many researchers have investigated various types of antennas to incorporate the multiband characteristic with small size [5-8]. Accordingly, the addition of so many elements makes the structure more complex

which causes a problem for integration. Even though security issues are also arises and to recover these issues many researchers are working on increasing the security feature [12-14].

II. LITERATURE REVIEW

Alezabi, Kamal Ali, et. al. have proposed an Efficient EPS-AKA protocol (EEPS-AKA). The proposed protocol is based on the Simple Password Exponential Key Exchange (SPEKE) protocol. They compared their methods and found their method is fast than other, because of using secret key method that performs faster than certificate-based methods. N. Suganthi have purposed the algorithm that support three types of keys for each sensor node, first one is single key shared with the base station, second is pair wise key shared with neighbour sensor node, and third is group key that is shared by all the nodes in the network. Zongwei Zhou et. al. proposed Key it Simple and Secure (KISS) algorithm. In their paper new key management architecture is given, called KISS, to enable comprehensive, trustworthy, user-verifiable, and cost-effective key management. Ivan Damgård et. al. proposed the key management method for cloud environments. The authors have proposed a higher security light-weighted protocol, and report on their practical performance.

III. EXPERIMENTAL SETUP

The design of the proposed solution has been prepared to mitigate the threats from the cellular networks. The security of the pre-setup and post-setup phases has been covered under this system design by using the amalgamation of the cryptography methods along with the random generator key table production. The multi-column key pairing is utilized to scramble the key data up to the highly secure manner. The multi-round elliptic key cryptography has been utilized for the purpose of cryptography of the key data during transfers. The major aim of this thesis is to protect the cellular networks against the passive attacks which include replication, replay and session hijacking attacks, which are launched to snoop the information from the active data channel. For authentication purpose, we are using a table with 6 columns and multiple rows in which the first 2 columns (i.e. a, b) are used for query key generation and the other 2 columns (i.e. c, d) are used for reply key building and last two columns(i.e e,f) are taken as common columns. In this algorithm to generate the query key first two columns and last two columns are used and for reply key middle 2 columns and last two columns are used to generate the table is shown below:

Column No.	1	2	3	4	5	6
Column Title	A	B	C	D	E	F

The construction of the query and reply keys becomes the tedious task for the implementation of the security paradigm over the GSM network for the establishment of the secure channels. The query and reply key are generated from the amalgamation of the multiple columns together for the construction of the keys. The query is establishes the ground over the four columns, which are A, B, E and F, for the construction of the complex and robust key, whereas the reply utilizes the C, D, E and F columns for the key construction. Hence, its known that both of the keys utilizes 4-columns for the construction of the authentication keys. The following equation is following by the query key construction:

$$K1 = (sin(A)) \quad (1)$$

The first phase of key requires the computation of the sine function over the value in the A (1) column of the randomly selected row, whereas the common columns E (3) and F (4) undergoes the tangent computation with the coefficient B in order to construct the keys. The column B undergoes the cosine function (2) in order to process the second phase of the key.

$$K2 = (cos(B)) \quad (2)$$

$$K3 = (tan(E, B)) \quad (3)$$

$$K4 = (tan(F, B)) \quad (4)$$

Afterwards, all of the coefficients are combined in order to obtain the composite key from the given set of the coefficients or columns in the equation (5) along with the Logarithmic value definition for the addition of the higher order of complexity for the mitigation of the decoding chances.

$$KeyTemp = log_{10}(K1 * K2 * K3 * K4) \quad (5)$$

$$QueryKey = round\ (KeyTemp) * Constant \quad (6)$$

Then the final key is obtained by rounding the values (6) obtained from the keyTemp variable in the equation (5) for the finalization of the security key.

$$KR1 = (sin(C)) \quad (7)$$

$$KR2 = (cos(D)) \quad (8)$$

$$KR3 = \left(tan(E, F) * \frac{180}{\pi}\right) \quad (9)$$

$$KR4 = (tan(F, D)) \quad (10)$$

The first phase of reply key requires the computation of the sine function over the value in the C (7) column of the randomly selected row, whereas the common columns E & F (9) and F & D (10) undergoes the tangent computation in order to construct the reply keys. The column D undergoes the cosine function (8) in order to process the second phase of the key.

Afterwards, all of the coefficients are combined in order to obtain the composite key from the given set of the coefficients or columns in the equation (11) along with the Logarithmic value definition for the addition of the higher order of complexity for the mitigation of the decoding chances. Then the final key is obtained by rounding the values (12) obtained from the keyTemp variable in the equation (11) for the finalization of the security key.

A. Main Key Generation Policy:

Algorithm 1: Key Scheme Algorithm Sequence for Function Calling

CASE 1: Request from mobile phone to base station for calling:

1. Turn on first step for call by send demand to base station.
2. Authenticate the mobile node by base station.

CASE 2: When Base station allows the mobile node to send data:

1. A setup call is received by base station from mobile node.
2. Base station checks the mobile node for standing by state.
3. Then authentication process is started by Base station after receiving of standing by state.

B. Complete Procedure

1. The base station generate query key by using the multi-column keys.
2. Then by using the ECC algorithm Query key is encrypted.
3. After encryption this encrypted key is send to mobile station.
4. This key is verified by mobile station from column data and make reply key from rows.
5. The reply key is prepared by using columns.
6. Then by using ECC algorithm reply key is encrypted.
7. Then this key is transmitted back to base station...
    a. Which is verified and makes the decision?
        i. If verification is flourishing
            1. The call is initiated and forward to other mobile station and counter is started.
        ii. Else
            1. The call is not forward and tells the mobile station for failure of authentication.
8. If during communication timer expires these steps are repeated.

IV. RESULT COMPARISON

The results of the proposed model are obtained in the form of the scrambling or encryption times as well as the retrieval or decryption times from the proposed security models. The proposed model has been designed based upon the encryption based tunnelling mechanism for the GSM networks in the certificate less manner, where the encryption certificate is not shared among the two nodes, rather the encryption key sharing program is established under this model.

Table 4.1: Table of comparison on the basis of elapsed time for key scrambling and Retrieval

Key Scrambling Scheme	Scrambling/Encryption Time	Retrieval/Decryption Time
AES-128	0.0054	0.0067
AES-192	0.0056	0.0070
AES-256	0.0057	0.0071
AES-512	0.0062	0.0076
Proposed Scheme	0.0011	0.0009

The proposed certificate less scheme has been assessed against the most robust schemes, which are utilizing the advance encryption standard (AES) in the 128-bit, 192-bit, 256-bit and 512-bit options. The proposed model has been recorded quite lower than the existing models for the encryption of the keys in the certificate less program. The proposed model has been recorded quite lower than the existing models at 0.0011 seconds against the minimum of 0.0054 seconds taken by the AES-128 bit for encryption, which shows nearly 4 times improvement in the encryption times. The proposed model has been recorded quite lower at 0.0009 seconds than the lowest among existing models (0.0067 seconds) taken by the AES-128 bit for decryption, which shows nearly 6-7 times better performance than the existing model.

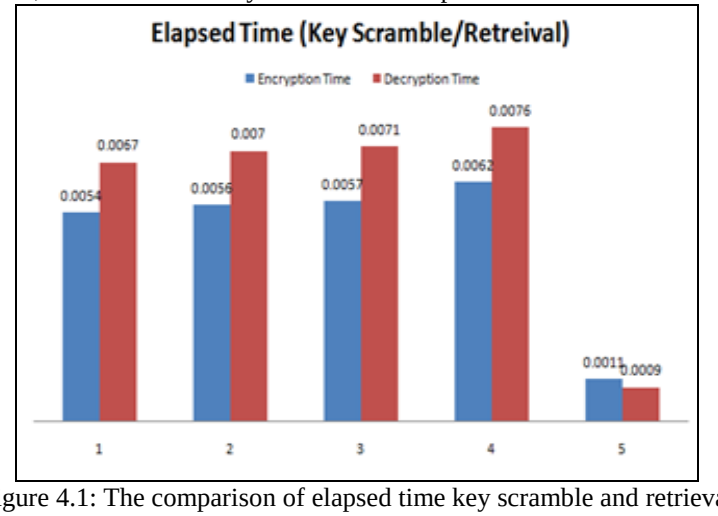

Figure 4.1: The comparison of elapsed time key scramble and retrieval

The figure 4.1 elaborates the graphical results obtained from the table 4.1 and clearly defines the differences of the encryption and decryption models over the certificate less key exchange programs. The proposed model has been recorded way lower as per shown in the figure 4.1.

V. CONCLUSION

The proposed model has been improved by utilizing the simpler but complexly scrambled using the elliptic curve cryptography rather than the traditional advanced encryption standard (AES) for the existing models. The existing models are utilizing the AES-128, AES-192, AES-256 and AES-512 bits for the encryption of the authentication keys, whereas the proposed model works in the 16-layered model for the encryption of the keys, which established the more secure model than the existing model. The proposed model has been found nearly 4-6 times improved practices of encryption and decryption in comparison with the existing models.

REFERENCES

[1] Mishra, Ajay K. "Fundamentals of Cellular Network Planning and Optimization, 2G/2.5G/3G...Evolution of 4G", John Wiley and Sons, 2004.

[2] Amit Kumar1; Dr.Yunfei Liu2; Dr.Jyotsna Sengupta3; Divya4, "Evolution of Mobile Wireless Communication Networks: 1G to 4G", Vol. 1, Issue 1. IJECTDecember 2010.pp 68-72.

[3] Gunawan, A.H., "LTE network and protocol", Advanced Communication Technology (ICACT), 2013 15th International Conference.

[4] mK. Kumaravel, Comparative Study of 3G and 4G in Mobile Technology, 2nd Vol. 8, Issue 5, No 3, IJCSI International Journal of Computer Science Issues, pp. 256-263, September 2011

[5] K. C. Lin, C. H. Lin, and Y. C. Lin, "Simple printed multiband antenna with novel parasitic-element design for multistandard mobile phone applications," IEEE Transactions on Antennas and Propagation, vol. 61, no. 1, pp. 488–491, 2013.

[6] J. Guo, L. Zhou, B. Sun, and Y. Zou, "Magneto-electric monopole antenna for terminal multiband applications," Electronics Letters, vol. 48, no. 20, pp. 1249–1250, 2012.

[7] R. Valkonen, J. Ilvonen, C. Icheln, and P. Vainikainen, "Inherently non-resonant multi-band mobile terminal antenna," Electronics Letters , vol. 49, no. 1, pp. 11-13, 2013.

[8] T. Zhang, R. Li, G. Jin, G. Wei, and M. M. Tentzeris, "A novel multiband planar antenna for GSM/UMTS/LTE/ Zigbee/RFID mobile devices," IEEE Transactions on Ante-nnas and Propagation, vol. 59, no. 11, pp. 4209–4214, 2011.

[9] Y. L. Ban, J. H. Chen, J. L. W. Li, and Y. Wu, "Small-size printed coupled-fed antenna for eight-band LTE/GSM/ UMTS wireless wide area network operation in an internal mobile handset," IET Microwaves, Antennas & Propagation, vol. 7, no. 6, pp. 399–407, 2013.

[10] K. L. Wong, M. F. Tu, C. Y. Wu, and W. Y. Li, " On-board 7-band WWAN/LTE antenna with small size and compact integration with nearby ground plane in the mobile phone," Microwave and Optical Technology Letters , vol. 52, no. 12, pp. 2847–2853, 2010.

[11] K. L. Wong, W. Y. Chen, C. Y. Wu, and W. Y. Li, " S mal l size internal eight-band LTE/WWAN mobile phone antenna with internal distributed LC matching circuit," Mi-crowave and Optical Technology Letters, vol. 52, no. 10, pp. 2244–2250, 2010.

[12] X. Zhao, K. Kwon, and J. Choi, "MIMO antenna using resonance of ground planes for 4G mobile application, "Journal of Electromagnetic Engineering and Science, vol. 13, no. 1, pp. 51–53, 2013.

[13] S. Jeon, S. Oh, H. H. Kim, and H. Kim, "Mobile handset antenna with double planar inverted-E (PIE) feed structure," Electronics Letters, vol. 48, no. 11, pp. 612–614, 2012.

[14] J. Lee and Y. Sung, "Heptaband inverted-F antenna with independent resonance control for mobile handset applications," IEEE Antennas and Wireless Propagation Letters, vol. 13, pp. 1267–1270, 2014.

[15] Alezabi, Kamal Ali, Fazirulhisyam Hashim, Shaiful Jahari Hashim, and Borhanuddin M. Ali. "An efficient authentication and key agreement protocol for GSM (LTE) networks." In *Region 10 Symposium, 2014 IEEE*, pp. 502-507. IEEE, 2014.

[16] Zongwei Zhou, Jun Han, Yue-Hsun Lin, Adrian Perrig, Virgil Gligor, "KISS: Key it Simple and Secure Corporate Key Management", Trust and Trustworthy Computing Lecture Notes in Computer Science, volume 7904, pp. 1-18, Springer, 2013.

[17] N. Suganthi, V. Sumathy, "Energy Efficient Key Management Scheme for Wireless Sensor Networks", vol 9, issue 1, pp. 71-78, INT J COMPUT COMMUN, 2014.

[18] Ivan Damgård, Thomas P. Jakobsen, Jesper Buus Nielsen, and Jakob I. Pagter, "Secure Key Management in the Cloud", Cryptography and Coding Lecture Notes in Computer Science, volume 8306, pp. 270-289, Springer, 2013.

[19] Ramaswamy Chandramouli, Michaela Iorga, Santosh Chokhani, "Cryptographic Key Management Issues & Challenges in Cloud Services", Computer Security Division Information Technology Laboratory, NIST, 2013.

