A Survey of Cryptographic Methods in Mobile Network Technologies from 1G to 4G

2 authors:

Fredrick Njoroge
Jomo Kenyatta University of Agriculture and Technology
1 PUBLICATION **1** CITATION
SEE PROFILE

Lincoln Kamau
Jomo Kenyatta University of Agriculture and Technology
3 PUBLICATIONS **5** CITATIONS
SEE PROFILE

A Survey of Cryptographic Methods in Mobile Network Technologies from 1G to 4G

Fredrick Njoroge
Email: nfmiringu@gmail.com
Telecommunication and Information Engineering Department
Jomo Kenyatta University of Agriculture and Technology

Lincoln Kamau
Email: kamaulincoln@jkuat.ac.ke
Telecommunication and Information Engineering Department
Jomo Kenyatta University of Agriculture and Technology

Abstract – **This paper presents a brief overview of the different cryptographic methods used in mobile networks. The focus here is on the mobile communication standards – 1G to 4G. The purpose of this paper is to appreciate the evolution of security measures in mobile networks from 1G to 4G, and examine the cryptosystems in each of the standards. This will be useful to offer a perspective on the development of 5G security.**

Keywords – DoS, A3, A8, A5/*x*, IMSI, SRES, RAND, AUTN, authentication triplet, authentication vector, Milenage, SNOW3G, KASUMI, eia, eea

I. INTRODUCTION

Over the years, there has been a major advancement in wireless communication. This can be pointed out from the inventions and discoveries of the likes of Heinrich Rudolf Hertz, Nikola Tesla and Guglielmo Marconi who are some of the founding fathers of wireless communication [1]. Such led to the development of the standards present today – WiFi, WiMAX, Bluetooth, ZigBee, the first to the fifth generations of mobile networks (1G – 5G) – just to name but a few.

However, this “freedom” in telecommunications came along with its insecurity issues, in that wireless communications are prone to security attacks such as eavesdropping, man-in-the-middle attack and denial of service (DoS). Part of the objectives of the evolution of these standards has been to address these security issues so as to provide more secure communication systems. This paper delves into examining each standard, exposing the weaknesses recorded over time and the solutions that have been formulated henceforth to overcome those weaknesses.

It is important to recall the features necessary for a wireless communication to be termed as secure [2]:

- User authentication – The users are who they claim to be.
- Data authentication – Data integrity (the recipient’s assurance that the data has not changed) and data origin authentication (the recipient’s assurance that the data originates from the stated sender).
- Data confidentiality – The data is encrypted so that it remains concealed while in transit.
- Non-repudiation – This pertains to a service against denial by either party of creating or acknowledging a message.
- Authorization – The ability to determine whether an authenticated entity is allowed to execute an action.
- Audit – A historical record of events used to determine whether anything has gone wrong, and if so, what it was, when it went wrong and its cause.
- Access control – This enables only authorized entities to access resources.
- Availability – Resources are accessible and are not prevented from access by malicious entities.

II. FIRST GENERATION (1G) MOBILE NETWORKS

The first ever mobile networks began around the late 1970s in Tokyo, Japan. Later, Europe (Baltic and Scandinavian countries), the USA and the UK came up with their own 1G systems, namely Nordic Mobile Telephony (NMT), Advanced Mobile Phone Service (AMPS) and Total Access Communication System (TACS) respectively [3]. These systems used

Frequency Division Multiple Access (FDMA) for analogue transmission.

AMPS and TACS lacked authentication and data encryption – this made it very easy for an attacker to intercept calls and extract the mobile identification number (MIN) together with the electronic serial number (ESN). With these two unique identifiers, a device could easily be cloned (impersonation attack). NMT employed voice scrambling at the mobile phone and the base station; this was not a strong encryption method, but it prevented attackers who intercepted calls [4].

III. SECOND GENERATION (2G) MOBILE NETWORKS

2G networks, which employ digital processing of voice, succeeded the insecure and inefficient 1G networks. With 2G came new services such as short message services (SMS). Also known as Global Systems for Mobile Communications (GSM), 2G networks use Time Division Multiple Access (TDMA). 2G networks evolved to 2.5G networks – General Packet Radio Service (GPRS) – which enabled mobile stations (MS) to connect to the Internet through the Wireless Application Protocol (WAP). Enhanced Data Rate for GSM Evolution (EDGE) wrapped up the 2G scene.

In the GSM network architecture, two security procedures are undertaken – authentication and encryption – in different nodes of the architecture. Authentication occurs in the Authentication Centre (AuC) located in the Home Location Register (HLR). The AuC contains an individual 128-bit key per subscriber (K_i), which is a copy of the K_i on the subscriber identification module (SIM) card. This key is stored secretly in the AuC (it never leaves the AuC), and it is by this key that the subscriber is identified [5]. The authentication process is as follows: A subscriber initiates a signaling connection with the network before the call establishment request is sent. The Mobile Switching Centre (MSC) sends the International Mobile Subscriber Identity (IMSI) to and requests an authentication triplet from the AuC, which then retrieves K_i of the subscriber and the A3 authentication algorithm based on the subscriber IMSI. The K_i together with a 128-bit random number (RAND) are fed into the A3 algorithm to give a 32-bit signed response (SRES). K_i and RAND are also fed into the A8 key generator to produce a 64-bit cipher key (K_c) for encryption. The authentication triplet consists of RAND, SRES and K_c. The triplet is sent to the MSC as requested, and it is here that the subscriber is authenticated. To speed up subsequent connection establishments, the AuC returns several triplets per request which are buffered by the MSC to be used in those subsequent establishments. After this, the MSC sends the RAND to the MS, which forwards it to the SIM. The SIM uses K_i and the A3 algorithm to generate a parallel signed response (SRES*) which is sent back to the MSC for comparison. If *SRES=SRES**, the subscriber is authenticated. With this, it is not easy to calculate the SRES since K_i is not transmitted. Since A3 and A8 algorithms rely on the same inputs, they are executed at the same time – an algorithm called COMP128 [6]. COMP128 takes in a 256-bit sequence and gives out a 96-bit output consisting of the SRES and K_c.

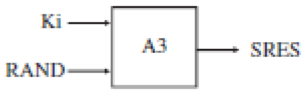

Fig. 1: Generation of a signed response (SRES)

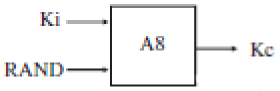

Fig. 2: Generation of a cipher key (K_c)

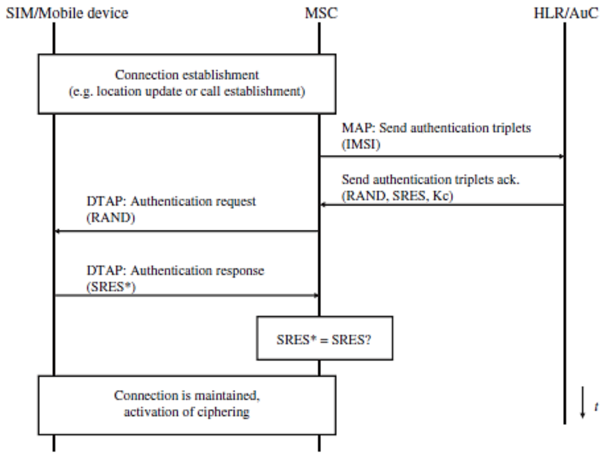
SIM/Mobile device
MSC
HLR/AuC
Connection establishment
(e.g. location update or call establishment)
MAP: Send authentication triplets
(IMSI)
Send authentication triplets ack.
(RAND, SRES, Kc)
DTAP: Authentication request
(RAND)
DTAP: Authentication response
(SRES*)
SRES* = SRES?
Connection is maintained,
activation of ciphering
t

Fig. 3: Message flow during the authentication process

At the base transceiver station (BTS), encryption is done using a stream cipher. This encryption only occurs between the MS and the BTS (over-the-air). Data past the BTS is transmitted in plaintext form, hence it becomes easy for an attacker who can access the signaling network [7]. To achieve encryption, K_c and a unique frame number (22-bit) act as input parameters to an A5/x algorithm, where 'x' denotes a number 1, 2, 3, and so on. The choice of the algorithm depends on the mobile device capabilities (in which the mobile device will let the network know about the algorithm it supports) and laws governing the sale of ciphering algorithms in some countries. The output of the algorithm is a 114-bit sequence that is XOR-combined with a 114-bit sequence of the original data stream. The ciphertext is then sent to the modulator. The frame number changes for every frame transmitted on the air interface.

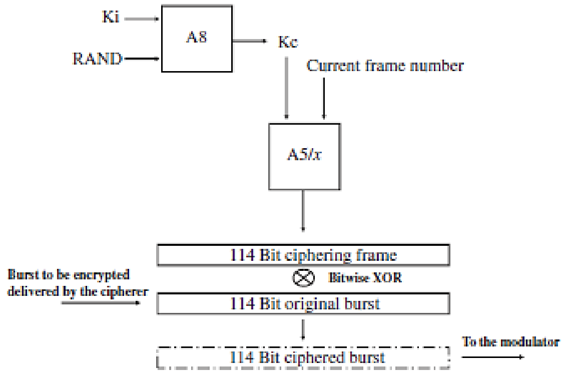

Fig. 4: BTS ciphertext generation

GSM authentication and encryption procedures have been proven to be insecure after several of its weaknesses being discovered. Barkan, Biham and Keller documented a practical ciphertext-only cryptanalysis of GSM encrypted communication. Some of the issues discussed are as follows [8]:

- The Abis interface (interface between the BTS and the base station controller (BSC)) is not encrypted. This makes it easy for attackers with the capability to intercept E1-based communication to intercept voice and signaling messages (man-in-the-middle attack).
- Some phones may lack air interface encryption, making them vulnerable to eavesdropping. However, nowadays air interface encryption is always activated today.
- A5/2 is vulnerable to passive attacks. K_c can be obtained within seconds using the ciphertext-only attack.
- By using session hijacking (a method that exploits network authentication in GSM), a false base station may be set up and its transmitting power set to be higher than the rest, making it the priority BTS for the MS to communicate to. This can lead to the attacker obtaining information from the MS such as the IMSI.
- K_c can be obtained from data encrypted with A5/1 as long as that data is intercepted for at least five minutes, and that the attacker has a precomputed decryption table around 4 TB big.
- An active attack may be launched against devices using A5/1 and A5/3 algorithms by the attacker contacting the device then instructing it to activate A5/2 ciphering without supplying new keying material. This will make the device vulnerable to the A5/2 passive attacks.

GPRS systems have improved security measures over GSM. These include the fact that data remains encrypted on all radio links. Ciphering for packet-switched traffic is terminated in the serving GPRS gateway node (SGSN), unlike in circuit-switched traffic where it is terminated in the BTS.

IV. THIRD GENERATION (3G) MOBILE NETWORKS\

As an improvement to the GSM network which had security and bandwidth issues, Universal Mobile Telecommunications Systems (UMTS) was launched – also known as 3G. One of the major differences between UMTS and GSM is the use of a new medium access scheme on the air interface, namely Code Division Multiple Access (CDMA). CDMA allows many users to communicate at the same time. The bandwidth per carrier was increased from 200 kHz to 5 MHz. CDMA uses a technique called spreading in which a bit is encoded into several chips [5].

Security-wise, engineers wanted to stay as close to the GSM system while designing the 3G security architecture for backward compatibility reasons, but still being able to overcome the weaknesses of GSM [9].

UMTS authentication is done using an extension of the GSM authentication and key agreement (AKA) protocol to support mutual entity authentication. A user equipment (UE) device tries to register to the network by initiating location and routing area update procedures. The UE transmits its IMSI (retrieved from the universal SIM (USIM)) to the nodeB (UMTS BTS). The MSC uses the IMSI to retrieve authentication information specific to that UE. The network returns a 64-bit message authentication code (MAC) that consists of K_i, a 48-bit sequence number (SQN), the 128-bit RAND and a 16-bit authentication management field (AMF) that allows to trigger session key changes or cryptographic algorithm upgrades. As a result, two keys are generated – K_c and an integrity key (IK) – both of which are different functions of K_i and RAND. To avoid attacks based on the SQN, a third key – anonymity key (AK) [which is also a function of K_i and RAND] – is XORed with the SQN to make part of the authentication token (AUTN). An authentication vector consisting of five elements – RAND, the expected response (XRES), IK, CK and the AUTN – is returned to the UE. The AUTN is used by the UE to verify that the authentication procedure was initiated by an authorized network, hence preventing attackers from using intercepted authentication vectors for fake authentications. The UE then sends a 32 to 128-bit response (RES) that consists of K_i and RAND back to the nodeB, completing the authentication process. Authentication becomes successful if *XRES=RES*. Authentication can be summarized into seven algorithms called the 'Milenage'.

$$MAC = f1(K_i\,,\text{SQN}||\text{RAND}||\text{AMF})$$

$$AUTN = SQN \oplus AK||MAC||AMF$$

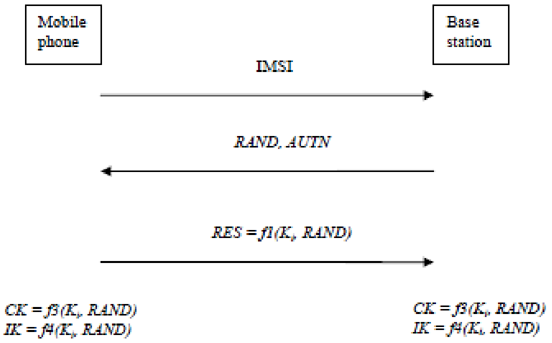

Fig. 5: UMTS AKA protocol

Several encryption methods have been employed in 3G systems – KASUMI cipher, SNOW3G cipher and the Rijndael cipher. KASUMI is a block cipher with a 64-bit input operated on by a 128-bit key to give out a 64-bit output. This algorithm features in the newer GSM systems too as A5/3 algorithm. The KASUMI cipher has its core as an eight-round Feistel network; in each round, the round function uses a round key consisting of eight 16-bit sub keys derived from the 128-bit key using a fixed key schedule [10]. SNOW3G is a two components stream cipher with an internal state of 608 bits initialized by a 128-bit key and a 128-bit initialization vector IV. It consists of two interacting modules – a linear feedback shift register (LFSR) and a finite state machine (FSM). The LFSR is constructed from 16 stages, each holding 32 bits and the feedback is defined by a primitive polynomial over a finite field. The FSM is based on three 32-bit registers and uses two substitution box ensembles that utilize XOR and modulo- 2^{32} addition operations [10]. The newest method of the three, Rijndael cipher (a block cipher), is based on the Advanced Encryption Standard (AES). A 128-bit key is used together with a 128-bit input by the Milenage set of algorithms [6].

3G systems are still prone to security issues, as follows [4]:

- An intruder can spoof a deregistration request to the network, instructing the VLR and HLR to deregister a user. The user becomes unreachable (DoS attack).
- 3G lacks end-to-end security. An attacker can intercept calls at the Radio Network Controller (RNC).
- The fake nodeB problem still applies here as in the case of GSM. Authentication vectors can be generated by the thousands of operators around the world, and create fake nodeB stations.
- An attacker can use compromised authentication vectors intended to be used by the network to authenticate a legitimate user, hence impersonating the user.

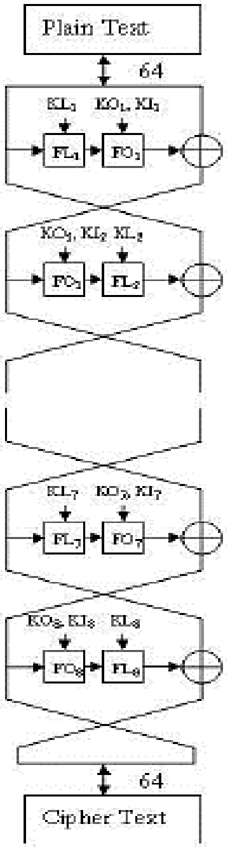

Fig. 6: KASUMI Block Cipher

V. FOURTH GENERATION (4G) MOBILE NETWORKS

4G networks are the latest networks being used globally at the moment. It is also known as Long Term Evolution (LTE). LTE uses orthogonal frequency division multiplexing (OFDM) that transmits data over many narrowband carriers of 180 kHz each over the air interface. MIMO antennas are used in LTE networks to increase the data rate.

In the LTE network architecture, there exists a node called the Mobility Management Entity (MME) which is responsible for authentication. When a subscriber first connects to an LTE network, the eNode-B (LTE BTS) communicates with the MME over the S1 interface to help exchange authentication information between the mobile device and the MME. The MME then requests authentication information from the Home Subscriber Server (HSS, similar to the HLR in GSM and UMTS) to authenticate the subscriber. The HSS generates encryption keys to encrypt communication from the mobile device on a session basis. These keys are sent to the eNode-B.

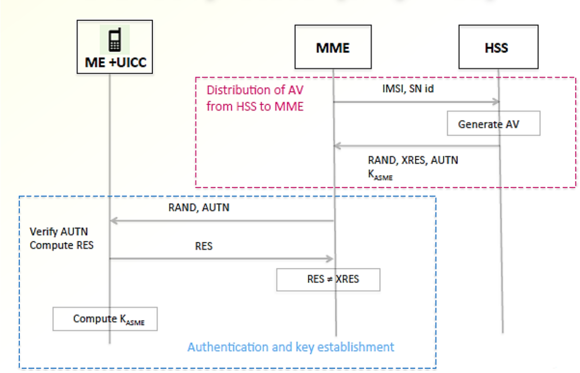

Fig. 7: LTE AKA Protocol

As is the case in UMTS networks, there exists a K_i on the SIM and another on the HSS. During authentication, the UE authenticates to the network, and the network authenticates to the UE, hence avoiding man-in-the-middle attacks. The authentication algorithms are stored and executed in the SIM card and the HSS. For encryption, ciphering and integrity protection is performed for non-access stratum (NAS) messages between the UE and the MME. NAS messages are continuous messages between the UE and the MME that can be used to monitor the change of location of the UE. The keys known by the eNode-B will help it activate integrity checking and ciphering for radio resource control (RRC) messages [the RRC protocol exists on the air interface], and ciphering for the user data bearer over the air interface. Since NAS messages are carried inside RRC messages, they are ciphered twice, and two integrity checks performed. This improves security. Algorithms for encryption are chosen after ciphering and integrity checking are activated. These include EPS Integrity Algorithm (eia1, eia2, and so on) and EPS Encryption Algorithm (eea). Eea1/eia1 correspond to SNOW3G of UMTS [5].

With efforts made to improve security in LTE networks, there still exist some security flaws [11]:

- An authentication relay attack is still possible. This allows an attacker to impersonate a legitimate user without having any legitimate credentials. The attacker can 'poison' the location of the victim's device in the core network. This can help one plant fake evidence during an investigation, or set up a false alibi.
- An attacker can hijack a device's paging channel with which it can not only stop notifications from reaching the device, but can also inject fabricated messages resulting in multiple implications such as energy depletion and activity profiling.

According to a white paper done by Juniper Networks [12], the following are some of the vulnerabilities in the LTE network:

- An attacker that can intervene in the network at a point on the S1 or X2 interface can potentially gain access to the network.
- The distributed architecture of the LTE network means that the number of network elements that can be potentially impacted by an attacker is substantially larger than in UMTS.

VI. CONCLUSION

It is evident that mobile networks are still prone to all manner of attacks, despite their evolution. A more advanced network architecture such as LTE would be expected to have less security issues than a less advanced one such as GSM. However, the more advanced networks have proven to be at greater security risk because of more connectivity and additional functionality. These vulnerabilities are brought about as long as the communication medium remains to be wireless.

Key security challenges posed in the upcoming 5G network (expected to be rolled out in 2019) include [13]:

- Encryption keys being sent over insecure channels
- Lack of security measures for operating systems, applications and configuration data on user devices (DoS on UE).
- User-security parameters not updated with roaming from one operator network to another, leading to security compromises with roaming.

It is important that these challenges be addressed, as well as those from the earlier standards, to make 5G networks secure.

REFERENCES

[1] T. K. Sarkar, R. J. Mailloux, A. A. Oliner, M. Salazar-Palma and D. L. Sengupta, History of Wireless, Hoboken: John Wiley & Sons, Inc., 2006.

[2] V. Garg, Wireless Communications and Networking, San Francisco, California: Morgan Kaufmann Publishers, 2007, p. 407.

[3] A. R. Mishra, Advanced Cellular Network Planning, Chichester, West Sussex: John Wiley & Sons, Inc., 2007, pp. 1-2.

[4] C. Hanser, S. Moritz, F. Zaloshnja and Q. Zhang, "Security in Mobile Telephony: The Security Levels in the Different Handy Generations," Uppsala Universitet, Uppsala, 2014.

[5] M. Sauter, From GSM to LTE: An Introduction to Mobile Networks and Mobile Broadband, Chichester, West Sussex: John Wiley & Sons Ltd., 2011.

[6] D. R. Lewis, "Mobile Phone Security Specializing in GSM, UMTS and LTE Networks," San Diego State University, San Diego, 2014.

[7] A. Prakash and N. Prakash, "Performance Analysis of Mobile Security Protocols: Encryption and Authentication," *International Journal of Security,* vol. 1, no. 1, p. 2.

[8] E. Barkan, E. Biham and N. Keller, "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication," Israel Institute of Technology, Haifa, 2003.

[9] K. Boman, G. Horn, P. Howard and V. Niemi, "UMTS Security," *Electronics & Communication Engineering Journal*, vol. 14, no. 5, pp. 191-204, 2002.

[10] B. P. Halagali and V. V. Desai, "Reveiw Paper on Cryptosystems Used in Cellular Networks," *International Journal of Computer Science and Mobile Computing,* vol. 6, no. 4, pp. 385-388, April 2017.

[11] Z. Zorz, "New LTE attacks open users to eavesdropping, fake messages, location spoofing," HelpNetSecurity, 05 March 2018. [Online]. Available: https://www.helpnetsecurity.com/2018/03/05/lte-attacks/. [Accessed 05 July 2018].

[12] P. Donegan, "The Security Vulnerabilities of LTE: Risk for Operators," Juniper Networks, 2013.

[13] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila and A. Gurtov, "Overview of 5G Security Challenges and Solutions," IEEE, 2018.