SECURITY ASPECTS: TETRA AND GSM

Shivi Saxena*

Arpit Kumar**

ABSTRACT

The Terrestrial Trunked Radio (TETRA) is a digital trunked mobile radio standard developed by the European Telecommunications Standards Institute (ETSI). The purpose of the TETRA standard was to meet the needs of traditional Professional Mobile Radio (PMR). There is one more recognized Mobile communication standard called GSM which is a cellular telephony standard and all calls are full duplex one to one. TETRA is principally used as trunked PMR and offers Group calls (one to many half duplex) as well as individual calls (one to one full or half duplex) and telephony (full duplex).TETRA has a much faster call set up (less than 300 ms) and has stronger encryption. It also has the option of end to end encryption (i.e. encrypted through the fixed infrastructure as well as on the radio interface). They both use TDMA, but TETRA uses 4 timeslots per frame and GSM uses 8. This paper describes the comparison between the Tetra radio networks and GSM by the focus study on the functionality of group calls, which is one of the most important requirements for public safety and security (PSS) networks. This paper discusses the air edge specification & supported functionality further based on a typical user profile & country wide network for Germany, capacity requirements & economic factors have been described.

Keywords: *GSM, TETRA*

*Asssistant Professor, Echelon Institute of Technology, Faridabad, Haryana.

**Manager (Sales & Marketing), Inative Networks (P) Ltd., Faridabad.

I. INTRODUCTION

Tetra is Terrestrial Trunked Radio.TETRA uses Time Division Multiple Access (TDMA) with four user channels on one radio carrier and 25 kHz spacing between carriers. Both point-to-point and point-to-multipoint transfer can be used. Digital data transmission is also included in the standard though at a low data rate. GSM (Global System for Mobile communication) is a digital mobile telephone system that is widely used in Europe and other parts of the world. GSM uses a variation of Time Division Multiple Access (TDMA) and is the most widely used of the three digital wireless telephone technologies (TDMA, GSM, and CDMA). GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot. GSM operates in the 900MHz, 1800MHz, or 1900Mhz frequency bands.This paper discusses the security aspects of GSM Public safety user requirements & with TETRA which is a purpose-built ETSI standard and technology for mission critical radio operations such as PSS. This paper also discuss other aspects like capacity requirements, country wide network for Germany, specialized functionality and cost.

II. SECURITY ASPECTS

1. TETRA-

TETRA contains a wealth of security functions designed to protect users information. This information can consist of the users' speech and data traffic and also other information that relates to the identities and operations of the users themselves. When describing these TETRA security functions it is important to make a distinction between the different categories of functions and their specific application. In TETRA the following categories can be identified.

1(a) Mutual authentication over the air interface

The TETRA standard supports the mutual authentication of a Mobile Station (MS) and the network, which is in TETRA normally referred to as the Switching and Management Infrastructure (SwMI). This makes it possible for a TETRA system to control the access to it and for an MS to check if a network can be trusted.

In TETRA, as in most other secure systems, the authentication process provides aFirm basis for the overall security.This mutual authentication security mechanism is available for Voice and Data.

1(b) Encryption

The air interface is very weak to eavesdropping and so modern mobile wireless

communication systems need to have some form of air interface security.This air interface security is intended to secure the connection between MSs and the network. Air interface security is an effective means to provide security in a mobile network and some essential security functions can only be realised by air interface security. In most cases it is sufficient to rely on air interface security andtake no further security measures. However, in TETRA systems needing a very high level of security, additional security may be required to protect information transmitted from one MS to another not only over the air interface but also within the network. In this case end-to-end security provides an proficient solution.

Airborne coverage and channel

TETRA can easily support dedicated frequencies for Air-Ground-Air communications. And can do this with the same radios. Devoting GSM frequencies to this purpose so that the same frequency is not reused within say 200 km distance likely will be challenging, taking into account for example new need for cross-border coordination of the GSM frequencies. There have been proposals to organize airborne coverage by use of dedicated GSM cells but these seem to lead either to a large amount of cells or reduced capacity per channel if extended cell range is used. In both cases the availability and cost of GSM spectrum for this purpose will likely become an issue.

End-to-end encryption

The TETRA end-to-end service can be realized in any number of ways. This means that a user may easily tailor an end-to-end encryption system to their particular requirements. This flexibility is essential for a standard like TETRA that will be implemented in many forms for different user groups. Public Safety organizations will have specific (high) national security requirements for their implementation of end-to-end encryption, which will be different from the requirements of Military user groups, which have even greater security requirements. All such organizations need to be able to specify an end-to-end encryption system according to their own requirements. It can also be expected that commercial user groups will have a need for secure end-to-end encryption systems.[3]

1(c) Security management features- In TETRA key management, functionality and flexibility are keywords. A large number of features have been integrated to support the key management.

(i) Authentication Key

The authentication key K is used for mutual authentication between an MS and the SwMI. The TETRA standard describes three possible methods for generating this key, which can be

a function of a fixed User Authentication Key, an Authentication Code entered by the user, or a combination of the two. Most systems require the MS to store the UAK or K itself rather than making use of user input due to the management issues associated with remembering long codes.

(ii) Keys for air interface encryption

There are several sorts of encryption keys. Some keys may be derived or transferred as part of the authentication procedure, some keys can be sent to MSs using Over The Air Re-keying (OTAR) or some may be preloaded in the MSs. There are keys with long term and short term key lifetimes. Special mechanisms are included to protect the keys with a long lifetime.

-The **Derived Cipher Key (DCK)** is derived during the authentication procedure. It can be used to encrypt the link between the network and the MS on an individual basis. Thus it can also provide an extended implicit authentication during the call, and can be used for encryption of uplink communications (i.e. the communication from the MS to the network) as well as downlink communications from network toan individual MS.[3]

-The **Common Cipher Key (CCK)** is generated by the SwMI and distributed,encrypted with the DCK, to each MS. It is efficient to use this key for encryption of messages that are directed to groups of MSs spread across one or more Location Areas (LAs). When the CCK is distributed to an MS over the air interface using OTAR it is encrypted with the DCK of this MS.

-The **Group Cipher Key (GCK)** is linked to a specific closed user group. It is generated by the SwMI and distributed to the MSs of a group (e.g. by pre-provisioning of the MS, on a Smart card, or by using OTAR (see below)). Within a Location Area the GCK is always used in a modified form. It is combined with the

CCK in a specific algorithm to obtain the Modified Group Cipher Key (MGCK). The MGCK is used to encrypt the closed user group messages for groups of MSs. When the GCK is distributed to an MS over the air interface using OTAR it is encrypted with a session encryption key derived from the Authentication Key for this MS, or with a Group Session Key.

-The **Static Cipher Key (SCK),** finally, is a predetermined key, which can be used without prior authentication. It is “static” in the sense that it is a fixed key that is not changed by another security function (e.g. by an authentication exchange) until it is replaced. TETRA supports the use of up to thirty-two (32) SCKs in an MS, per network. They can be distributed similarly to the GCKs.Their use is largely implementation dependent but they can be used for encryption in Direct Mode Operation (where they may also provide explicit

authentication) and in certain TETRA systems also for encryption for group and individual communications. The SCK may also be used in a system that normally uses DCKs and CCKs as an alternative to those keys in fallback conditions. When an SCK is distributed to an MS over the air interface using OTAR it is encrypted with a session encryption key derived from the Authentication Key for this MS.

2. GSM

GSM (Global System for Mobile communications) is an open standard for digital cellular telecommunication systems. Its target market is point-to-point communication for private or business users. Security in GSM consists of the following aspects: subscriber identity authentication, subscriber identity confidentiality, signaling data confidentiality, and user data confidentiality. The subscriber is uniquely identified by the International Mobile Subscriber Identity (IMSI).The security mechanisms of GSM are implemented in three different system elements; the Subscriber Identity Module (SIM), the GSM handset or MS, and the GSM network. The SIM contains the IMSI, the individual subscriber authentication key (Ki), the ciphering key generating algorithm (A8), the authentication algorithm (A3), as well as a Personal Identification Number (PIN). The GSM handset contains the ciphering algorithm (A5). The encryption algorithms (A3, A5, A8) are present in the GSM network as well. Figure 1 demonstrates the distribution of security information among the three system elements, the SIM, the MS, and the GSM network. Within the GSM network, the security information is further distributed among the authentication center (AUC), the home location register (HLR) and the visitor location register (VLR). The AUC is responsible for generating the sets of RAND, SRES, and Kc which are stored in the HLR and VLR for subsequent use in the authentication and encryption processes.[7]

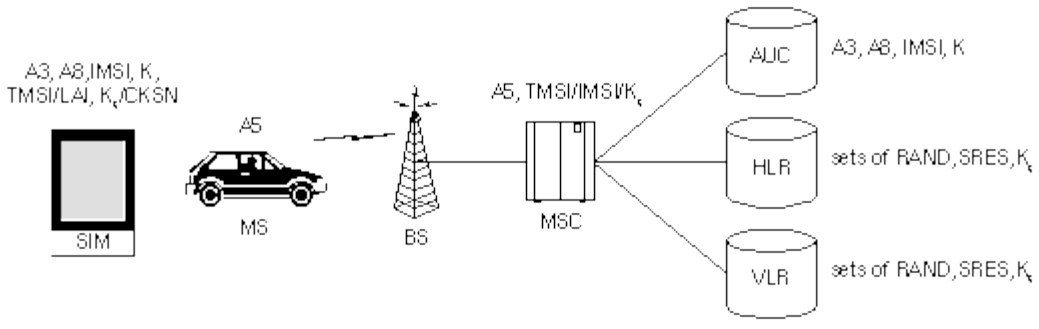

Figure 1 Distribution of Security Features in the GSM Network

2(a) Authentication

The GSM network authenticates the identity of the subscriber through the use of a challenge-response mechanism. A 128-bit random number (RAND) is sent to the MS. The MS

computes the 32-bit signed response (SRES) based on the encryption of the random number (RAND) with the authentication algorithm (A3) using the individual subscriber authentication key (Ki). Upon receiving the signed response (SRES) from the subscriber, the GSM network repeats the calculation to verify the identity of the subscriber. Note that the individual subscriber authentication key (Ki) is never transmitted over the radio channel. It is present in the subscriber's SIM, as well as the AUC, HLR, and VLR databases as previously described. If the received SRES agrees with the calculated value, the MS has been successfully authenticated and may continue. If the values do not match, the connection is terminated and an authentication failure indicated to the MS. Figure 2 shown below illustrates the authentication mechanism.[4]

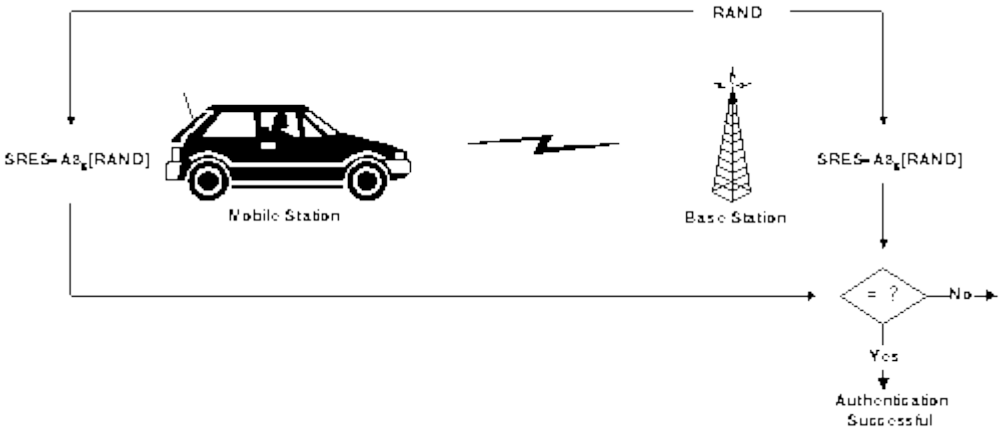

Figure 2 GSM Authentication Mechanism

The calculation of the signed response is processed within the SIM. This provides enhanced security, because the confidential subscriber information such as the IMSI or the individual subscriber authentication key (Ki) is never released from the SIM during the authentication process.

2(b) Signaling and Data Confidentiality

The SIM contains the ciphering key generating algorithm (A8) which is used to produce the 64-bit ciphering key (Kc). The ciphering key is computed by applying the same random number (RAND) used in the authentication process to the ciphering key generating algorithm (A8) with the individual subscriber authentication key (Ki). The ciphering key (Kc) is used to encrypt and decrypt the data between the MS and BS. An additional level of security is provided by having the means to change the ciphering key, making the system more resistant to eavesdropping. The ciphering key may be changed at regular intervals as required by network design and security considerations.Encrypted communication is initiated by a

ciphering mode request command from the GSM network. Upon receipt of this command, the mobile station begins encryption and decryption of data using the ciphering algorithm (A5) and the ciphering key (Kc).

2(c) Subscriber Identity Confidentiality

To ensure subscriber identity confidentiality, the Temporary Mobile Subscriber Identity (TMSI) is used. The TMSI is sent to the mobile station after the authentication and encryption procedures have taken place. The mobile station responds by confirming reception of the TMSI. The TMSI is valid in the location area in which it was issued. For communications outside the location area, the Location Area Identification (LAI) is necessary in addition to the TMSI. The TMSI allocation/reallocation process is shown in Figure 5 below.

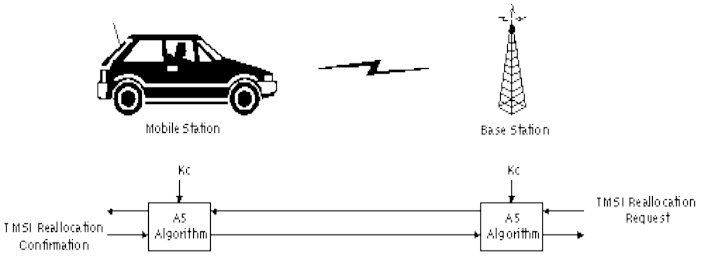

Figure 5 TMSK Reallocation

III. COMPARISON OF SPECIFIED FEATURES

TETRA has been especially developed for group calls, it fulfils most of the requirements. Some of the limitation in the table below are stated as “unlimited”. They reflect the standard; effective limitations are, however, manufacturer specific. Shifting group call area is basically possible for both technologies, TETRA and GSM . The air-interface specifications do not mention the implementation, since resource allocations are part of the core network functionalities. Several manufacturers have implemented the feature for TETRA; however, for GSM it does not exist. An implementation would require major modifications in the core network software, which is for economic reasons not feasible.

3(a) Required capacity on the radio network

Since the cell sizes are very different for TETRA and GSM it is not representative to observe the amount of used traffic channels. The required bandwidth or the amount of transceivers is more representative. The bandwidth can be either expressed in terms of radio channels or frequency. The required bandwidth depends on the carrier capacity per site, the bandwidth per channel and the frequency re-use factor R. If the amount of cells in the network is smaller

than the reuse-factor, then the amount of cells has to be used as R in the formula below. With a given carrier capacity C per site, the needed bandwidth in the network would be:

$$\text{TETRA: } B = C \cdot 25\ \text{kHz} \cdot R$$

$$\text{GSM: } B = C \cdot 200\ \text{kHz} \cdot R$$

A recent study by Simon Reison from Helinski University shown that the TETRA network is more spectrum efficient than a GSM Network.[6]. In their study Simon had considered two cases i.e A regional network with an area of 900 km^2 and 400 users representing a medium size city with rural surroundings and a Germany-wide network with an area of 357 021 km^2 and 529 000 users. In both cases, the average group call area is 400 km^2 and a group consists of 10 members The assumption is that all users are active during busy hours. This might Seem Like An Overestimation of the Traffic, however, we will see that the calculated capacity for TETRA in table is even slightly less than the recommtraendations for the Germany-wide network.[6] Analysis done by Simon indicated that the required bandwidth for TETRA is 11 times less than for GSM. Interesting is that the traffic per cell and the bandwidth requirement are the same for both GSM solutions. Therefore, a TETRA solution requires significantly less carriers than GSM. The amount of transceivers does not only determine the size of the base stations, but also the amount of required transmission lines between base stations and exchanges or base station controllers. This value has therefore a major impact on the operational costs of the network. The ratio of required bandwidths GSM:TETRA is about 7:1 for the countrywide network. The reason that this ratio is smaller than for the regional network comes from the fact that GSM has a lower frequency reuse factor than TETRA and TETRA does not need to reuse frequencies in the small network. For the GSM solutions, the size of the chosen group call area and the user density are directly proportional to the required bandwidth. In case of TETRA, however, the size of the group call area has no influence to the capacity since shifting area can be used.

3(b). Cost issues-

(i)Network infrastructure cost

The common perception is that a GSM network provides lower capital expenditure than TETRA. Also sharing of network infrastructure with commercial users should give cost benefit. Certainly one can assume that GSM base stations are cheaper tha TETRA base stations simply because of the volume difference. The study from Helsinki University of Technology in 2004 is suggesting that the need for network capacity and also cost would actually be clearly higher in the case of GSM requiring fast call set-up time for group calls and group area being reasonably large. It appears in the study, that if more than 30 % of

talkgroups require fastcall set-up and the group should cover more than 200 to 500 square kilometres, the GSM network cost becomes higher and increases very rapidly if the percentage figure and/or area is further increased.[8]

(ii)Mobile terminals cost

Another common perception is that GSM phones are much cheaper than TETRA radios. However, making a Public Safety radio to meet the specific needs does not seem to depend much on the selected air interface signalling technology when volumes are comparable. This means that for example a police radio with TETRA signalling or police radio with GSM signalling for a market of 500 000 units would be produced at approximately same cost.

IV. CONCLUSION

From the issues discussed in previous we can make the following conclusions concerning GSM and Tetra technology:

• The call set-up time requirements of Public Safety would require the GSM terminals to stay permanently on the group call traffic channel. This may lead to drastically bigger capacity needs and cost. Slow cell handovers may compromise officer safety.

• The group call in GSM is wasting capacity by keeping radio channels reserved at sites having no talk group members.

• GSM cannot maintain service in the event of network outage in the same way as TETRA base station fall-back operation mode provides. The ETSI standard TETRA appears to show stronger performance than a comparable GSM solution in nearly all areas. The main reason can be found in the technical maturity of the solution, but also in the capacity requirements which are based on TETRA's:

- Low bandwidth
- Large cells
- Shifting area group call
- Fast call set-up times

Shifting group calls and fast call set-up times are theoretically also achievable for GSM technology, but they would require major changes in the core network architecture. . For economic reasons it is very unlikely that these changes will be implemented in commercial GSM networks. . TETRA, however, is the only reasonable solution if the moving behavior of the users is unpredictable. It fulfils all major technical requirements at a competitive cost level.

REFERENCES

[1] Anil Kapil, Sanjeev Rana,,Identity-Based Key management in MANETs using Public Key Cryptography in International Journal of Security IJS (2009)

[2] Anderson Ross, A5 - The GSM Encryption Algorithm, 17.6.1994, [referred 30.9.1999] http://chem.leeds.ac.uk/ICAMS/people/jon/a5.html

[3] DW Parkinson (2001-07-01). "TETRA Security". *BT Technology Journal, Volume 19.* pp. 81-88. doi:10.1023/A:1011942300054

[4] David Margrave,GSM Security and Encryption, [referred 30.9.1999] http://www.net-security.sk/telekom/phreak/radiophone/gsm/gsm-secur/gsm secur.html

[5] Margrave Schneier B., Applied Cryptography, 2nd Ed., Wiley, New York, 1996, 758, [referred 29.9.1999]

[6] Simon Riesen, The usage of mainstream technologies for public safety and security network Espoo, Finland, October 9, 2003

[7] Digital Radio Communications network for Security Organizations (Tactical and Operational Requirements),Schenge working party on Telecommunication, SCH/I-Telecom (95)18, June 1995

[8] TETRA MoU Association; TETRA or UMTS – let the user decide; 2001

[9] Tetra Securty ,www.tetramou.com