Information security in digital trunking systems

Claudiu Dan BARCA
The Romanian-American University, Bucharest

In Europe, most countries have implemented its digital trunking systems to meet the communication needs of various public safety organizations.The development of these systems will be closely correlated with the evolution of operational requirements and communications services needed by users. For all these digital trunking systems, information security has proven to be an essential aspect. In this paper we present some aspects of the security functions of the Tetra system because this system was imposed as an open standard ETSI and is used as a Schengen cooperation system.
Keywords:*digital trunking systems, Tetra , algorithm, encryption,interoperability*

1 Introduction

Digital systems are trunking radio communications networks used for public safety services necessary for organizations such as police, fire, emergency medical services and critical infrastructure services (nuclear, energy, gas, etc.). Most security and civil protection organizations use dedicated systems based on telecommunication standards developed especially for public safety communications such as the ARCP-25 (P25) Tetrapol and Tetra Project, which use narrowband technology [1] .In Europe the frequency spectrum used for these services is 380-400 MHz.

The Tetra system has been developed since the beginning by ETSI (The European Institute for Telecommunication Standards).This has led to rapid adoption by manufacturers, operators, government users.The second generation of the system, TEDS (Tetra Enhanced Data Service), is currently being implemented.TEDS is also known as Tetra Release 2 or Tetra Broadband.This generation uses frequency bands of 25, 50, 100 and 150 kHz, and several modulation schemes: π / 4-DQPSK, π / 8-D8PSK, 4-QAM, 16-QAM and 64-QAM. Depending on the frequency band and the modulation scheme used, net transfer speeds can reach 500 kbit / s [2].

The system has various operating modes and allows radio communication on large areas with a single frequency.Tetra is the radio communication system with high spectral efficiency due to the use of TDMA (Time Division Multiple Access)

To meet the needs of the users were offered numerous voice and data services. Of these, the most important are considered to be: voice services, group call, emergency call, priority calls, Dynamic Group Assignment (DGNA), ambient listening, dispatcher authorized call, selection of the area, data services, data packets.

From the point of view of technology, ETSI develops the standard through modern reception techniques, dynamic power emission control techniques, optimization of protocols, and the development of encryption algorithms certified by authorized bodies.

2.Tetra digital trunking system architecture

The digital trunking system is based on standardized technical architectures consisting of functional structures (Figure 1) [3], namely:

- Tetra radio terminal - Trt - represents a fixed or mobile radio terminal in Tetra technology: each radio terminal is identified in the network by two parameters: SIM (Subscriber

Identity) and TEI (Tetra Equipment Identity)

- Tetra Network Management TNM - includes a set of Tetra network base stations, Tetra network interfaces with other networks (ISDN - Integrated Sevice Digital Network, PSTN), terminal databases
- Network management control unit - UTNM - represents the structure that performs the programming of the network functions
- External networks - fixed, mobile, analogue, digital communications networks
- Operators dispatchers - are the dispatchers / operators that coordinate the different sub-networks made on the system infrastructure - the police network, the fire network, the public utility operator network.

Depending on the complexity of networks Tetra digital trunking, manufacturers can provide standardized interfacesThe main standardized Tetra system interfaces are: [4]

- AI - air interface - via this interface is established the connection between a radio terminal and the base station or directly between two radio terminals (DMO - Direct Mode Operation establishes the direct connection between the two terminals without interacting with the base station
- ENGI -External Network Gateway Interface- standardized interface that connects to other communication networks
- UTNMI - Interface that links TNM to UTNM
- PEI - makes the connection between the radio terminal and an external device
- ISI -the interface that makes possible the connection between Tetra networks of different infrastructures
- RCI-interface between TNM and dispatchers / operators

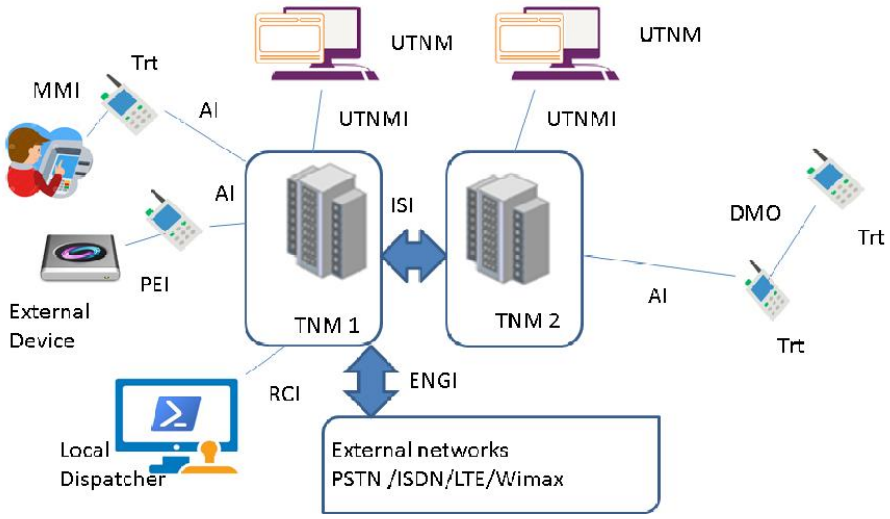

Fig. 1. Architecture of the Tetra digital trunking system

3.Security features in the Tetra digital trunk system

The digital trunk system Tetra, especially for governmental organizations, required that the information transmitted on this system be secured. This system is designed and implemented to provide high-security services[5].

The system presents three security classes [6] presented in Table 1.

Table 1. Tetra Security Classes

	Authetification	Air Interface Encryption	Enable/Disable	End to End Encryption	OTAR
Security Class 1	optional	not use	optional	optional	not used
Security Class 2	optional	mandatory	optional	optional	optional
Security Class 3	mandatory	mandatory	optional	optional	mandatory

A radio terminal may have:
- *1, 2 or 3 class*
- *classes 1 and 2*
-*classes 1 and 3*
-*classes 2 and 3*
- *classes 1,2 and 3*

A radio cell can have:
- *1, 2 or 3 class*
- *classes 1 and 2*
-*classes 1 and 3*

The Tetra standard specifies security mechanisms for the protection of various protocols, interfaces, and applications [7].
In general, these security mechanisms are implemented in the functional blocks of the communication network.
The main system security mechanisms [7] are
-authetification
-air interface encryption
- enable /disable
- end to end encryption

Authentification
Authentication means recognizing the radio terminal in the system by an authentication center to allow it to communicate with the network. (The identity of the transmitter is verified by the receiver) (Figure 2).

Fig. 2. Authentication process

The two parameters by which a radio terminal is identified are: SIM (Subscriber Identity) and TEI (Tetra Equipment Identity).
In the Tetra Authentication Procedure, two main entities appear - Authentication Center and Authentication Keys.
Generally use two classes of algorithms for key generation:

- symmetric algorithms - between the transmitter and receiver are the same keys
- asymmetric algorithms - different keys are used between the transmitter and receiver

In Tetra, authentication is based on symmetric keys, and the length of the secret keys is 128 bits regardless of how they are generated.
In all procedures, radio terminal are registered in the network for the first time with a User Authentification Key (UAK).This key will be recorded in the handheld as well as database authentication center
The authentication process between the radio terminal and the infrastructure is carried out according to the procedures:

- authentication of a radio terminal by the infrastructure (which may include the base station and the authentication center)
- infrastructure authentication by the radio terminal
- mutual authentication

Authentication provides proof identity of all radio's attempting use of the network.A session key system from a central authentication centre allows key storage (Secret key need never be exposed). Authentication process derives air interface key (TETRA standard) (Figure 3).

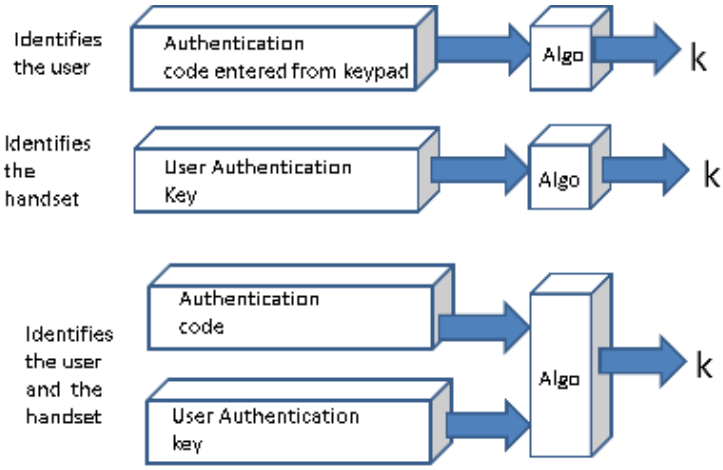

Fig. 3. Authentication key generation

Encryption

In the wireless communications system the most vulnerable interface is the air interface because it has the role of ensuring the communication between the radio terminal and the base station.Through this interface, some important security features can also be achieved.

By using the security keys required for the air interface, encryption will be performed between the radio terminal and the infrastructure (Figure 4). This encryption is valid for group or individual communications, for Direct Mode Operation, for voice and data (Figure 5).

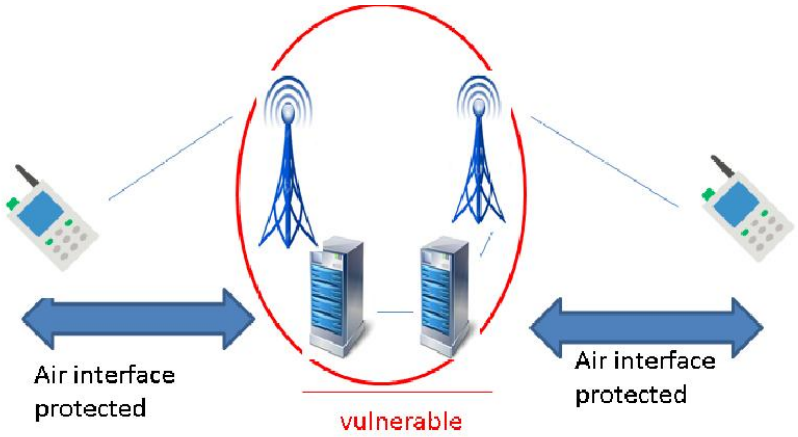

Fig. 4. Standard air interface

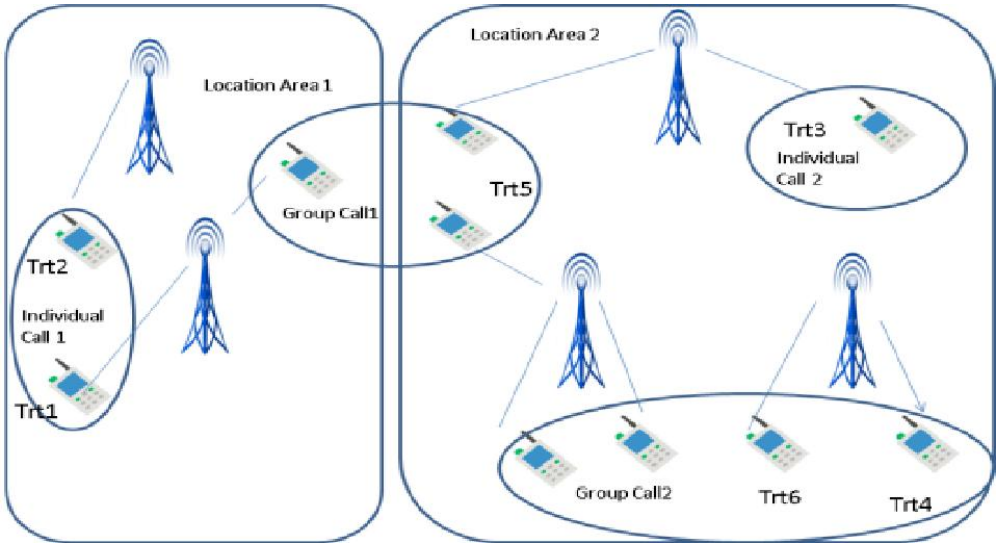

Fig. 5. Communications individual / group DMO

From the point of view of communication for Tetra system users, encryption of the air interface can be:

- dynamics (in trunking mode)
- static (in DMO mode)

In static mode air interface uses a fixed encryption key -SCK (Static ciphering key) that encrypts signaling and vocea.In this case class classification system is second class.

The method by which to transfer the secret keys from the infrastructure to the radio terminal is called OTAR (Over The Air Re Keying), the standardized procedure[8]

The DCK -Derived Ciphering Key is used in dynamic mode. These are generated during authentication (Figure 6).Each part of the authentication process produces a part of the DCK, DCK1 and DCK2.These are combined by algorithm TB4.DCK is used wherever possible as it is the most secure. It only has a life equivalent to the authentication period and is unique to the terminal.

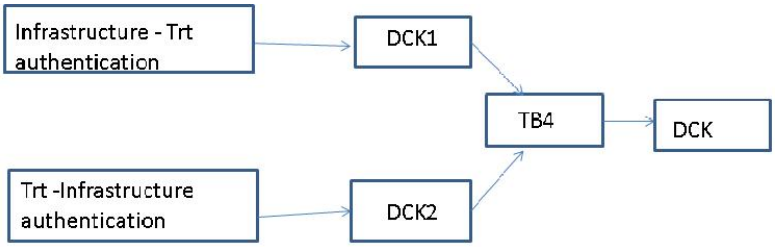

Fig. 6. Deriving DCK from mutual authentication

The keys are still in use:

-CCK - Common Cipher Key - are generated by the infrastructure server and distributed to all radio terminals

-GCK - Group Cipher Key - are generated by the infrastructure server and distributed only to radio terminals belonging to a closed group

The use of the encryption keys is shown in Figure 7.

Tetra digital trunked radio system supports both standard encryption algorithms as well as owners, which are used depending on the applications you made system.

The air interface secret algorithms allow a secure connection between the infrastructure and In order to interoperability of equipment from different manufacturers have implemented standard algorithms (TEA1, TEA2, TEA3, TEA4), which are subject to

regulations ETSI and SAGE Security Algorithm Group of Experts Group- so:

- TEA1, TEA3, TEA4 - regulatory authority is ETSI
- TEA2 - the regulator is the Public Safety Organization in Schengen

These algorithms are written in strict licensing rules (Restricted Export Algorithms)

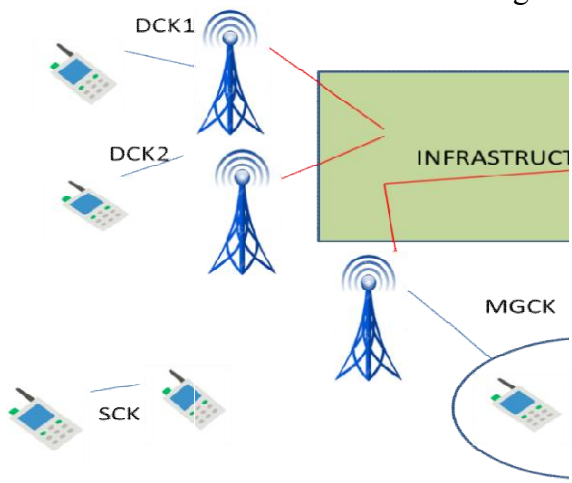

Fig. 7. Air Interface Encryption – the Keys

Secret key management and air interface authentication

Generally, a single authentication key standard attached to a key management is specified. This algorithm is TAA1 and is controlled by ETSI.

Enable/Disable

Through this mechanism, the access or prohibition of the radio terminal to the Tetra communications network functions is achieved.This is defined in the ETSI EN 392-7 document and has two levels: temporary or permanent.Each radio equipment has its own code called TEI which makes it possible to enable / disable the radio terminal in the network.

Encryption End to End

Encryption is taking place between radio system terminals, the connection between them being achieved by infrastructure (Figure 8).

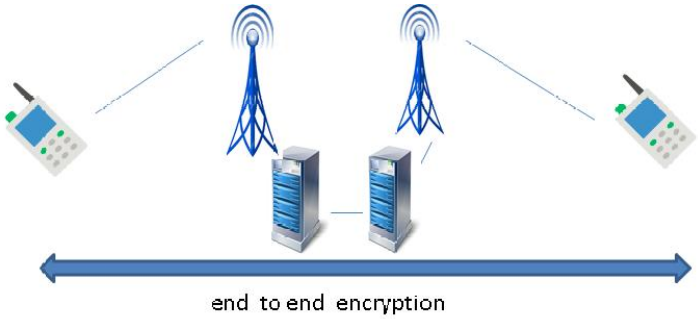

Fig. 8. End to End Encryption

For this encryption there are no 'standard' algorithms defined by SFPG, but use algorithms IDEA (International Data Encryption Algorithm) and AES (Advanced Encryption Standard)

IDEA was defined as a good candidate 64 bit block cipher algorithm for use with TETRA and test data and an example implementation was produced.

AES is a block encryption algorithm in which block and key lengths could be: 128 bits, 192 bits, or 256 bits. The AES specification restricts the block length to 128 bits. Thus, the input and output of

encryption and decryption algorithms is a 128-bit block. AES operations are defined as matrix operations, where both the key and the block are matrixed. At the beginning of the cipher roll, the block is copied to a state-of-the-art table, the first four bytes on the first column, then the next four on the second column, and so on until you complete the dashboard. The algorithm modifies this array of numbers at every step, and then supplies it as an output [9].

The Tetra standard does not have security specifications for two interfaces: the peripheral equipment interface (PEI) and interfaces with other Tetra systems (ISI).

- PEI - the interface realizes the communication between a mobile or fixed radio terminal and a peripheral terminal (mainly the transmission of data); It can virtually be considered that there is no need for encryption of the link, because in general the connection between the two equipment is made locally (distance of about 1m)
- ISI – Is the interface that allows the connection between two Tetra trunk networks.

Cross-border cooperation has to be achieved through the ISI interface specifications. In the past few years, various projects have been carried out to achieve interoperability between Tetra systems belonging to Schengen States.
A first test was conducted in Finland where there was a national Tetra network (Vivre)
Used by various public security organizations (police, border health services, fire brigades) and is perfectly interoperable. From the interoperability tests with neighbouring countries, Sweden and Norway, it has become necessary to standardize the interoperability architecture for applications (e.g. command and control) and infrastructure (e.g., interface gateways, mobile unit) [10].

Another project had been in Aachen (Germany) -Liège (Belgium) -Maastricht (The Netherlands) to demonstrate a proof of concept for ISI. Operational research was applied during the operational field trials.The functional requirements for the TETRA ISI were based on Technical TETRA ISIstandard and Interoperability profiles, operational scenarios defined for the three-countrypilot scenarios and recommendations from the users (ASTRID, BMI and C2000) [6]. This test demonstrated the migration of terminals between the three countries (Figure 9).

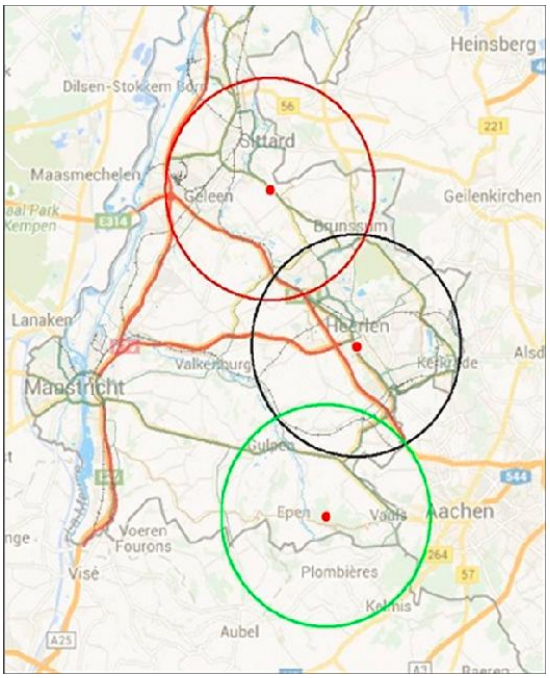

Fig. 9. Tetra pilot - Aachen (Germany) – Liège (Belgium) –Maastricht (The Netherlands)

The interoperability of the Tetra digital trunking system for cross-border cooperation was demonstrated in the DACEA (Romania-Bulgaria Danube Cross-Border Earthquake Alert) project (Figure 10).

Fig. 10. Cross-border cooperation between Romania and Bulgaria

DACEA project general objective is to develop a cross-border system for Earthquake alerts in order to prevent the natural disasters caused by those events in the cross-border area, taking into account the nuclear power plants and other high risk facilities located along the Danube on the territories of Romania and Bulgaria[11].

4.Conclusions

TETRA has historically been the digital technology with the greatest uptake in Europe

The resilience, availability and security of TETRA coupled with its efficient use of spectrum will continue to make it an attractive bearer for critical voice and dedicated data solutions.

Experience of several nations in responding to crises emphasises the crucial role ofsupport for managing communications interoperability. This includes real-time keymanagement to define the cryptographically determined communication groups thatare the fundamental feature of Tetra system, making operational choices on the 'profiles' ofsystem and security parameters, optimising gateways between systems, andmaintaining priority settings.

References

[1] Ramon Ferrús, Oriol Sallent, "Public Protection and Disaster Relief Communications," in Mobile Broadband Communications for Public Safety: The Road Ahead Through LTE Technology, Wiley, August, 2015,

[2] Milan Stojkovic Public safety networks towards mission critical mobile broadband networks Master of Telematics - Communication Networks and Networked Services Submission date: June 2016 Norwegian University of Science and Technology Department of Telematics

[3] Peter StavroulakisTErrestrial Trunked RAdio – TETRA - Springer-Verlag Berlin Heidelberg 2007

[4] Baldini, G., Karanasios, S., Allen, D., &Vergari, F. (2013). Survey of Wireless Communication Technologies for Public Safety. Communications Surveys & Tutorials, IEEE, 16(2), 619-941

[5] SALUS-Security And InteroperabiLity in Next Generation PPDR CommUnicationInfrastructurSFP7 Project Number: 313296

[6] ISITEP-Inter System Interoperability for Tetra-TetraPol Networks- FP7 Project Number: 312484

[7] Roelofsen, G. (2000) "TETRA Security", Information Security Technical Report, Elsevier Science, Vol 5, No.3

[8] SFPG Recommendation 01

[9] Benjamin Dowling, Marc Fischlin, Felix Günther, Douglas Stebila, "A Cryptographic Analysis of the TLS 1.3 Handshake Protocol Candidates," in ACM Conference onComputer and Communications Security (CCS 2015), February, 2016

[10] GianmarcoBaldini -Report of the workshop on"Interoperable communications for Safety and Security"- 28-29 June 2010 – Ispra, Italy

[11] L. Dimitrova, D. Solakov, S. Simeonova, I. Aleksandrova- System of Earthquakes Alert (SEA) in the Romania-Bulgaria cross border region- Bulgarian Chemical Communications, Volume 47, Special Issue B 2015

Claudiu Dan BÂRCĂ graduated from Faculty of Computer Science for Business Management, Romanian American University in 2007, and holds a master degree in Economic Informatics since 2008 and a PhD in the field of Engineering Sciences since 2013. He is an assistant lecturer within the Faculty of Computer Science for Business Management having nine years of teaching experience. He also has good research and publishing activity: he was a member of the research teams of international and national projects. His core competences are in software programming and connected areas.