Technical Journal, University of Engineering and Technology (UET) Taxila, Pakistan Vol. 24 No. 4-2019
ISSN:1813-1786 (Print) 2313-7770 (Online)

Analysis and Evaluation of Secure Solutions for Terrestrial Networks

A.Mahmood[1], S.M.M.Gilani[2], M.J.Iqbal[3], Z.Haider[4], S.Daud[5]

[1, 2 ,4,5] *University Institute of Information Technology, PMAS-ARID Agriculture University, Rawalpindi, Pakistan*
[3] *Department of Computer Science, UET Taxila University, Pakistan*

[4] scholarxeeshan@gmail.com

Abstract- Terrestrial European Trunk Radio Access (TETRA) technology is a European Telecommunication Standard Institute (ETSI) approved standard, designed for public safety applications. TETRA technology has been in service in many developed and developing countries for Fire Fighting, Police Surveillance, and Flood Recovery, etc. Due to its critical use in public safety applications, the requirements for safe, timely and reliable communication are having utmost importance. The present encryption algorithm (Data Encryption Standard and Triple DES) computation time is high for fast voice or data communication. In this paper, we are highlighting the state of art TETRA research challenges for secure and reliable communication. Secondly, a secure and robust solution using AES is also analyzed for TETRA based device communication. In the proposed model of evaluation, an Advanced Encryption Standard (AES) 128-bit key length and 128-bit data block using byte substitution and byte-level block processed TETRA communication designed for fast computation to ensure optimal radio resource utilization. The evaluated parameters are SNR, Encryption/Decryption time and varying packet size determine the appropriateness of the AES in comparison to the other encryption techniques. The proposed work is simulated in MATLAB SIMULINK and our evaluation has proved that 128-bit AES end to end encryption is better and more fast, accurate and better than conventional (DES, 3DES) encryption algorithm. .

Keywords- TETRA, Advance Encryption Standard (AES), Data encryption Standard (DES), Triples DES (3DES), Terrestrial Radio Network.

I. INTRODUCTION

A technological transition about three decades ago, TETRA (Terrestrial Trunked Radio) and Global System for mobile communication (GSM) both were started for public voice and data communication under the umbrella of European Telecommunication Standard Institute (ETSI) [i]. However, GSM was globally adopted for voice and data communication in most of the world as a standard for mobile communication. But the TETRA group did not make prominent existence in commercial voice/data application. To get public exposure, the TETRA group shifted his gear towards public safety applications, and they were very much successful in this area of market acceptance [ii][iii]. TETRA is still in use of many developed and developing countries for their public safely related departments and disaster recovery systems. Due to large and complex infrastructure provided by the TETRA network communication, it is very difficult to manage and control TETRA communication in terms of fast, reliable and secure communication [iv]. TETRA is an open standard and it is not secure and robust for end-to-end communication in a specified disaster and critical environment where an exchange of data information from one end to another end must be user priority. To secure end to end communication current solutions are complex, resource-intensive and more time-consuming processes must fulfill the criteria of the Security Fraud Prevention Group (SFPG).

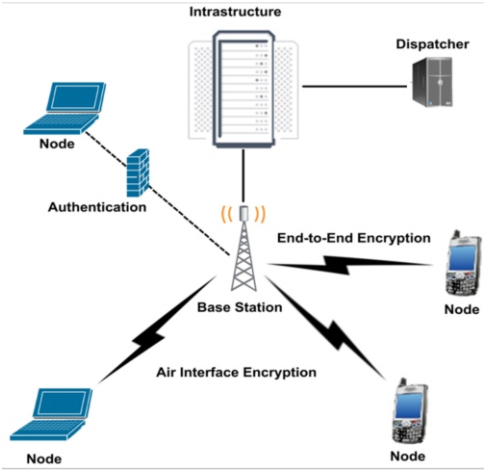

Fig. 1. Security Architecture of TETRA

We proposed the end-to-end encryption mechanism for secure and strong TETRA network using the modules of physical layer of TETRA. We proposed the end-to-end encryption from sender side to receiver side which also includes air media or air interface. A typical, TETRA based communication architecture for secure communication being shown in Fig. 1.

Tetra devices work in two modes of operation (i) Trunked mode of operation, (ii) Direct mode of operation [v].

In trunk mode of operation, the Tetra base station (TBS) manages all call and data operation, the range is maximized to many kilometers in a city. In a direct mode of operation, there is no need for any centralized control. Similarly, two types of encryption are necessary for secure communication which is also depicted in Fig. 1. The first is the air interface encryption which deals with the device to base station encryption and the base station handles all-controlling and authentication. The second is the end to end encryption where two devices authenticate each other and work in ad hoc mode of operation. TETRA supports various kinds of encryption techniques like Advanced Encryption Standard (AES) and the International Data Encryption Algorithm (IDEA) algorithms in different modes of operation[vi].

Most of the work available on TETRA security using Data Encryption Standard (DES) and triple DES lacks performance due to high computation power and hinders QoS performance [vii]. There are numerous advantages of big block size is, if AES is increased from 128, 192, and 256-bit key length [iv][vii][viii]. The mobile devices have limited battery and network resources. To optimally use the available resources, it is necessary to build a secure, require less computation and a minimum end to end delay. The drawback of conventional Feistel (DES, 3DES) ciphers are, it requires bit-level processing and confusion and diffusion performance is lower than AES 128-bit and more computation time ultimately increase encryption and decryption time [vi][ix]. To find an optimum block size, for efficient, fast and reliable communication in TETRA architecture is still an open research issue.

The performance analysis of proposed AES work carried out in MATLAB SIMULINK for an AES based encryption/decryption module using 128-bit block size. The comparison with an existing block cipher is evaluated and results approved that AES is faster and less resource-intensive. The main advantage of this AES is its process byte by byte mechanism for bigger avalanche effect on output. Secondly, the AES is it is less recourse intensive and less computation is required. This recommendation also related to providing a necessary additional environment for end-to-end encryption. The proposed model addresses the challenges and threats in secure and fast encryption/decryption processing which ultimately improves the security of the network. The contribution of this research is the proposed model for the secure communication which includes AES with TETRA modules. To the best of our knowledge, secure communications in TETRA are implemented in a terrestrial network are categorized in Fig. 2. Whereas, Taxonomy demonstrated the related work so far in the field of a cryptographic algorithm proposed in TETRA Communication.

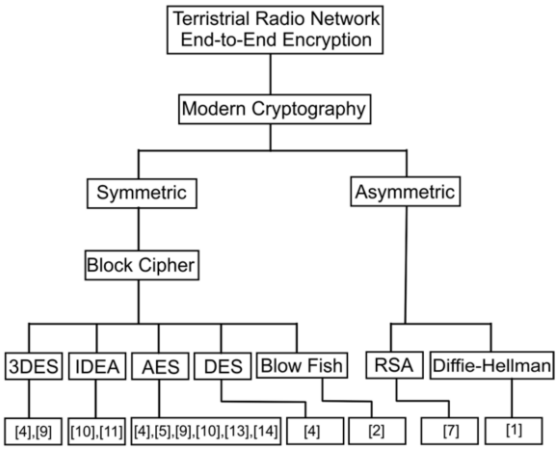

Fig. 2. Taxonomy of TETRA Cryptographic Techniques

This research is organized as follows, section II covered the literature review and section III elaborated on the security threats of the TETRA communication, section IV deals with the challenges and solution, section V was demonstrated in the proposed work methodology. Section VI and VII are the evaluation and conclusion sections, respectively.

II. Literature Review

In [iii],[iv] presented a study against various attacks on the security aspect of TETRA, TETRA Police, and future mobile networks. This study also describes the wireless sensor network security countermeasure using cryptographic techniques. Social engineering is related to the human dimension because it is a non-technical intrusion. Social engineering victim thinks he/she provides information to the hacker because social engineering is the manipulation of information[v].

The author describes the decryption of Advanced Encryption Standard (AES) [vi] on wireless radio like mobile and this study defines that decryption timing varies prominently with the actual state physical channel. With the growing needs of human safety related to communication between users over a radio channel, a security threats that a terrestrial trunked radio face is a social engineering security threat.

However, in [vii], the study presented specifies the needs of protection of data of particular types in a Radio

system for Monitoring and Acquisition of data from traffic Enforcement Cameras (RSMAD) techniques. The intention of designing this system is to reduce the traffic load on the road, to reduce the obstacle facing a vehicle and also to reduce the no. of victims to make traffic smooth and flow able. This data of traffic load is noticeable by the Global System for Mobile (GSM) module internet or police TETRA cellular network. The Data Acquisition Center plays an important role in data management that is received by the defined system. The encryption here was done based on Advanced Encryption Standard AES in support of Triple-DES and blowfish algorithms if system needs to move from the AES algorithm. This paper states that AES is the most currently used encryption algorithm for data encryption in radio and wireless communication.

These studies describe the AES algorithms working with functionality and AES based encryption for Single, Double, Triple, and TETRA Adjacent Error Detection designing respectively [viii]. This study deals with the overview of the security aspects of TETRA which include Air Interface Encryption as well as a description about End-to-End encryption [ix].

In [x], the researcher proposed a new scheme for the security of the authentication protocol in TETRA. This scheme is entirely different from Duan's Scheme. Duan's scheme illustrates that there is a different computation cost based on Symmetric Encryption T(s), Hash Function T(h) and Random Generation Function T(rgf) with 5 messages transmitted than the researcher scheme which has reduced computation cost with the reduced number of transmitted messages.

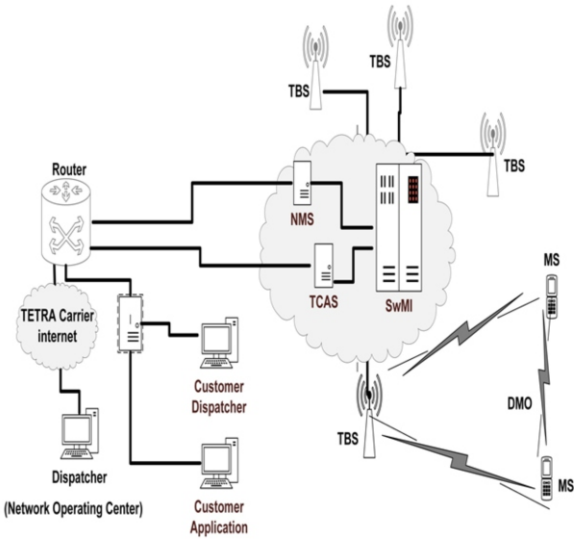

Fig. 3. The TETRA Communication Architecture

In both unilateral and mutual authentication scenario the number of messages reduced from 5 to 3 and 4 to 2 respectively. At the assumption of equal computation cost of Random Generation Key and Key Derivation Function, the number of times they invoked is also reduced in the new proposed scheme than the Duan's scheme.

Fig. 3, demonstrated the standard TETRA [xi] communication architecture where TETRA based station (TBS) are based station just like eNB nodes in 3G architecture. Mobile subscribers (MS) are the client radios which are connected through this TBS. The Switching and Management Infrastructure (SwMI) is equivalent to the MME module in 3G architecture. The direct mode (DMO) is an ad hoc mode of operation and the Tetra mode of operation is a centralized architecture for long-distance communication. The control of the networks is monitored and diagnosed through the Network Management Server (NMS). TETRA Customer Application Server (TCAS) is a specific application server that is being communicated through the Tetra infrastructure like voice, data and emergency messages recording, etc.

For this purpose, both devices must have the same algorithms and parameters. These devices use the Diffie- Hellman protocol of key agreement to seed individual session key for each call in the encryption process of a voice call. The Diffie-Hellman protocol is a public key technique that uses both public and private parameters. This protocol allows both parties to communicate with each other without the involvement of central services. These keys are then used by Advanced Encryption Standard (AES) to encrypt and decrypt voice calls. It uses 128-bit encryption keys selected from 10^{38} possible values. This scheme encapsulates the all kind of user like user end, commercial and public safety users.

In [xii], the author proposed a new encryption scheme based on physical layer called the Physical Layer Encryption (PLE). This scheme is consists of two parts: one is a conventional channel encoder and the second is modified rate less encoder. It further has three steps. This scheme is called concentrated PLE. This author proposed a Single Leader Multiple followers Stackelberg (SLMFS) game model. This model improves the physical layer security in wireless network bases on relay infrastructure to manage the basic circuit. This study lacks a comparative analysis of relays and sources. This model works on the basis of a decision of source and relay follows decision as it is. Different relays in the network offer services to source so this system enhances the protection against eavesdropping attack to the physical layer of a wireless network [xiii].

In [xiv], the author proposed an asymmetric encryption algorithm like RSA and presents new cryptography called Elliptic Curve Cryptography (ECC). ECC is a cryptographic approach to public-key cryptography based on algebraic fundamentals of Elliptic curves over finite fields. These curves are responsible for the application of the key agreement and pseudo-random generator. Key agreement techniques based on

Diffie-Hellman. The author suggested that ECC is better than RSA in comparison to key size, low CPU consumption, and memory usage. This study shows the comparison of two cryptographic techniques involved in the security of wireless sensor networks. [xv] presents a study against various attacks on security aspect of TETRA, TETRA Police, and future mobile networks.

The findings of the author [xvi][xvii] summarized for existing TETRA parameters in public safety application are summarized in table 1. The maximum data rate, channel spacing, voice encoding scheme, data rate, access methods, slot time.

Table 1: Conventional Tetra Radio Parameter

Maximum Data Rate	28 kb/s
Channel Spacing	25 KHz
Modulation	π/4 – DQPSK
Voice coding	ACELP (4.6 kb/s net)
User Data Rate	7.2 kb/s per time slot
Carrier data rate	36 kb/s
Access Scheme	4 slots TDMA
Slot Time	14.7 ms
TDMA frame	4 time slots = 56.7 ms

III. Security Threats

Wireless communication networks are too sensitive and an easy target for attackers to steal or alter the information like text and data by attacking it. Wireless communication network has some limitations from a security perspective. This weak aspect of wireless communication network faces a lot of security threats from attackers. These security threats affect the performance and lower the security level. Wireless communication networks like Terrestrial Trunked Radio which is a wireless communication network for a limited range needs secure and firm steps to control the threats. Security of wired networks can be made stronger using physical access controlling of wired connection of the network. But wireless network lacks this aspect because we cannot make wireless medium ideally secure and strong from all kind of threats initiated by attackers within the range. There is always a hope of threats; a wireless communication network has gone through.

Since the wireless network doesn't have fixed decreased limits, so wireless network may go beyond outside our building area and anywhere, so anyone outside it, can fetch its signals. Now with the various use of wireless communication networks, the security of the user is a primarily genuine issue. A security system must comply and maintain the authentication, authorization, integrity, and confidentiality of the user [xviii]. It should describe techniques of key management and security protocol which surely will handle all the ingredients that make a robust wireless network and offer important services like access control, authentication of users, availability, the confidentiality of user and integrity. These are the aspects of radio communication that face security threats. As discussed earlier, these are security threats that terrestrial trunked radio networks face.

Some confidentiality attacks are given such as eavesdropping, but Wired Equivalent Privacy (WEP) key cracking, also twin access point, access point phishing, a man in middle attack exists. Integrity attacks involve changing in frame, data and authentication replay. Authentication attacks are like shared key guessing, pre-shared key, identity theft, VPN login cracking. Availability attacks are a kind of access point theft, Denial of Service (DOS) attacks [xix]. Non-repudiation attacks involve attacks using fake clients, spam messages attacks.

IV. Challenges and Solution

This means that what kind of scenario or obstacle TETRA has to endure during its communication concerning security. These challenges affect TETRA performance in all aspects. Challenges are the parameters which are to be considered as future work topics. A few challenges regarding security attacks are given below.

A. Security Attacks

There are two kind of attacks which a terrestrial radio network faces.

a) Passive Attack

In the former type of attack, the attacker attacks the network to obtain the nature of data or kind the activities between the networks. For example eavesdropping, leakage of data.

b) Active Attack

In an active attack, the attacker attempts to alter, inject new data to previous information or try to delete some chunks of data from the original message which is transmitted between networks. This is also further classified into more categories such as DOS attacks, Routing attacks.

The possible solution to these is to have encryption mechanism which can reduce and minimize the level of attacks. The more secure, strong and robust mechanism of encryption is, the lower will be the frequencies of

of attacks to networks. Replay and impersonation attacks with passive and active also evaluated and handled to some extent while handover authentication [xx]. In the following study, the author reviewed and briefly studied the possible threats and security requirements for the different proposed architecture used in a disaster management situation [xxi].

B. Time

Time is the important challenge of TETRA security. To improve and enhance the robustness of our encryption mechanism, decrease our encryption time. Encryption time of an encryption algorithm affects the encryption process performance. A decrease in encryption time means the encryption mechanism will be able to transfer data quickly to the receiver side.

C. Number of Rounds

Increment in several rounds also increase the complexity of the encryption mechanism so as it improves the security but in this scenario, the security increase but mechanism speed slows down.

D. Selection of algorithm

Encryption time plays a vital role in the efficiency of an encryption algorithm. Encryption time can be decreased by controlling the bit error rate. Bit error rate defines the number of erroneous bits includes in the receiving bits. If we handle the bit error rate by improving the channel noise using Additive White Gaussian Noise (AWGN) then encryption time can be reduced. At the moderate level, a number of byte that need to be sent to a destination, are encrypted with minimum encryption time. Many rounds and sections of algorithm come under a safe decision.

V. Materials and Methods

Wireless communication networks are very sensitive and soft targets for the attacker to steal or alter the information. Wireless communication network has some limitation This weak aspect of wireless communication network faces a lot of security threats from attackers. Wireless networks are very prone to much denial of service (DoS) attacks. One of its kind is, eavesdropping a communicating session that leads to executing a black hole or wormhole attack to fulfill their notorious needs.

Therefore, secure communication is very necessary to overcome eavesdropping. These security threats affect the performance and lower the security level. Wireless communication networks like Terrestrial Trunked Radio which is a wireless communication network for a limited range needs secure and firm steps to control the threats. This mechanism includes the AES encryption at the transmitter end and a set of TETRA modules that includes different modules. The AES has a different key and blocks size variants that differ in performance and computation power to execute the AES algorithm.

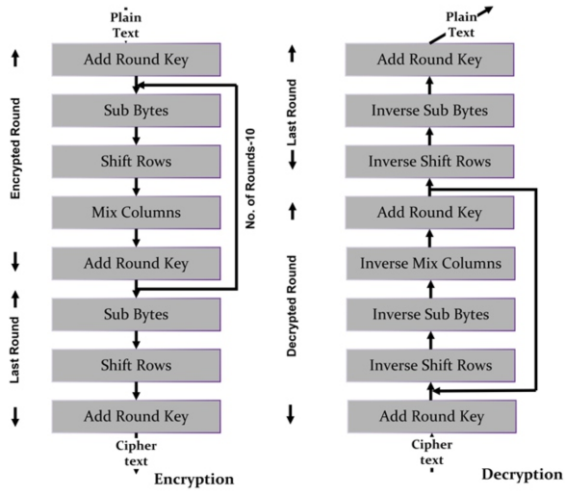

Fig. 4. AES 128-bit with 10 Rounds Processing

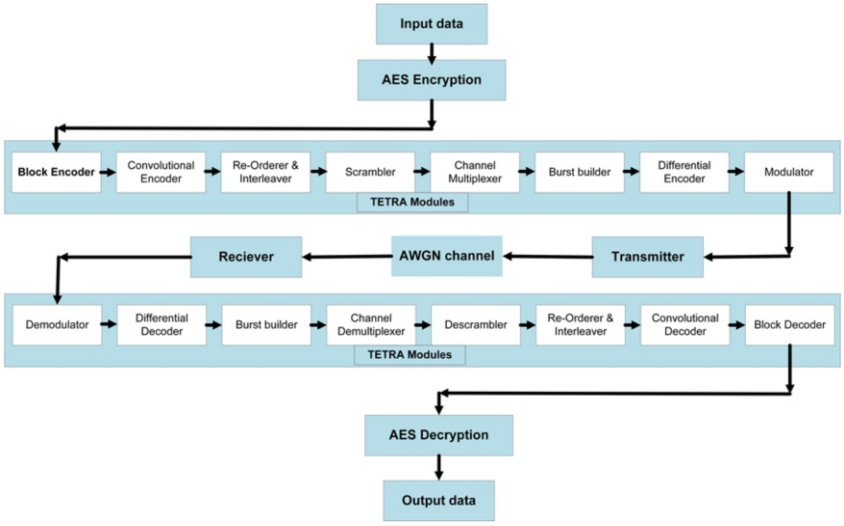

Fig. 5. Evaluation methodology for TETRA based AES Encryption/Decryption

A 128-bit AES with 128-bit key processes is shown in Fig. 4. The analyzed reference model [xxii] is shown in Fig. 5. Table 2 of parameters is listed below which are used in simulation.

Table 2: Comparison table of result of algorithms

Data size	128-bit data
Key Size	128-bit key size
Algorithm scheme	AES, DES,3DES
Simulation Time	~250-350 sec

The tetra module consists of a number of sub-modules that are briefly elaborated one by one as follows:

A. Convolutional Encoder
Convolution encoder is also an example of error-correcting codes that works using a shift register and combinational logic circuits that perform module two addition operations. It takes block encoder output data block as input and encodes this data block to yield some output data.

B. Re-ordered and Inter-Leaver
Re-ordered and inter-leaver are actually components that perform different operations on a group of data. So re-order is a component that re-orders the given data block. The Re-ordering is changing the order of the code at compile time. And interleaving is a technique or process to make forward error correction more robust with respect to burst error, so this module first put output data from the convolutional encoder in some order and then make data block more robust.

C. Scrambler
The next module is a scrambler, which is pretty much like a device that encodes a block of codes at the transmitter side to make the message impossible to understand at the receiver side. This module manipulates data in a way that it's become difficult to understand easily.

D. Multiplexer
This module multiplexes digital signals or streams of codes into one digital signal code over a common medium channel.

E. Burst builder
This technique builds the burst of data by transmitting high bandwidth data transmission over a short time span. This module is responsible to execute the burst of code so it called burst builder.

F. Differential Encoder
The Next module is a differential encoder, which is responsible to provide the unambiguous signal reception when using some types of modulation and the most common type of modulation that requires differential encoding are phase-shift keying and quadrature amplitude modulation.

G. Modulator
Before transmission from transmitter end, the last module for the operation of the code block is modulator which changes the property of the carrier data signal with modulating signal that also contains some useful information.
For this research, we used an HP machine with 1.8 GHz processor and 4GB RAM and a tool of Mat lab version R2016a. This provides the required result. First of all, a block of 128-bit data block with 128-bit key length is given to transmitter end and it passes through different modules before transmitting and this block of message is now encrypted using AES Conversely, an encoded and encrypted message is sent to the receiver and the receiver side decrypts this data block message after passing through modules in reverse order.
Matlab Simulink is used for the implementation of the proposed work. This model contains the AES module, TETRA module which has been already explained. Next, a transmitter and Additive White Gaussian Noise (AWGN) module are added. At the receiver end, the decryption is carried out and information is retrieved at the end.

VI. Evaluation

When the communication takes place between the sender and receiver, there is a chance of error occur in the bits, so some error bits have been received on the receiver side within a specified time is termed as Bit Error Rate (BER). BER is also known as the Bit error ratio. Lower the erroneous bit in a message from the sender side, lower will be the noise in the transmission process and encryption and decryption would be done instantly. This will reduce the threats frequencies to the mechanism. BER and SNR alternatively affect the overall performance of the mechanism in terms of threats. The BER and SNR have a converse relation with each other. Our results showed that with the increase in avg. SNR, the BER value gradually reduces for AES, DES, and 3DES also. When the average SNR is 35.9 then the BER for the three schemes i.e. AES, 3DES, and DES is observed as 0.
Fig. 6, depicts the graph of BER across avg. SNR for AES, 3DES and DES.
Secondly, we evaluated the performance of three schemes namely AES, 3DES, and DES across Encryption time to file size. File size almost remains same if we rounded off it before and after encryption and decryption process but size of file affect the encryption and decryption time of the encryption mechanism that depends on the use of algorithm also. Our results showed that with the increase in file size the

encryption time gradually increases for AES, DES and 3DES also.

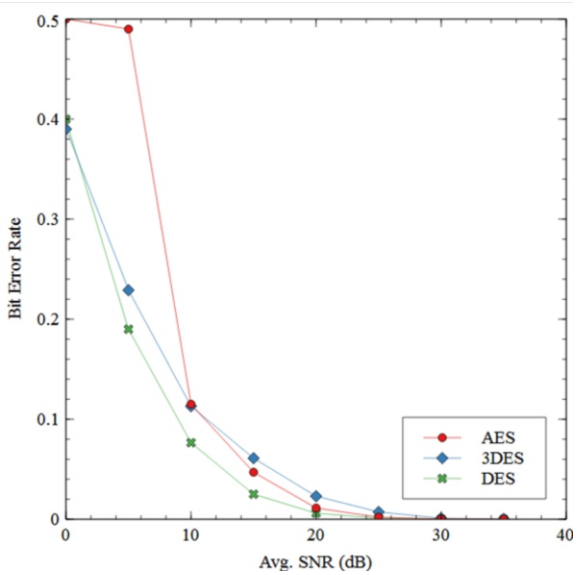

Fig. 6. BER across avg. SNR for AES, 3DES and DES

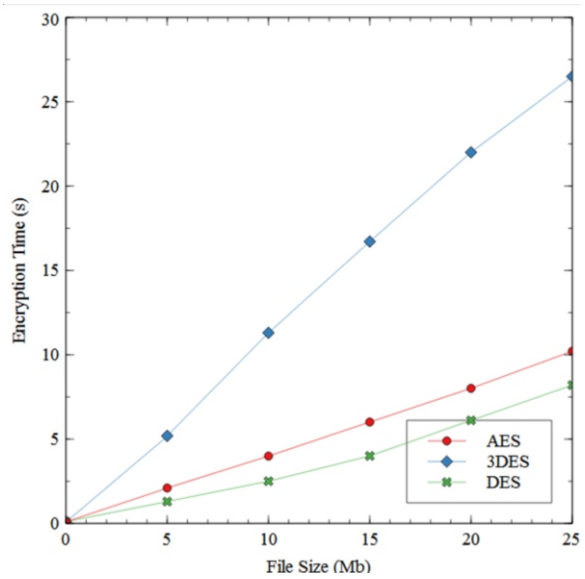

Fig. 7. AES, 3DES and DES across Encryption time with respect to file size

In the initial stage when the file size is small i.e. 5MB the encryption time for AES, 3DESand DES is 5s, 2.5 s and 1.9s respectively. When we increase the file size i.e. 25 MB then the maximum encryption time which is 26.8 s, has been observed for the case of 3DES while it is 9.9s for AES and 7s for the case of DES. Fig. 7, illustrates the graphs of encryption time with respect to file size for the AES, 3DES, and DES.

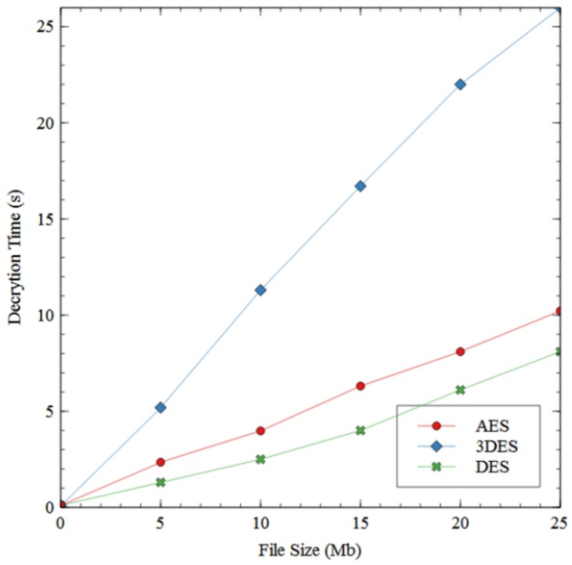

Fig. 8. AES, DES and 3DES across decryption time with respect to file size

The performance of AES, DES, 3 DES with respect to decryption time and file size is also evaluated. Fig. 8, depicts the graph of BER of three schemes AES, DES and 3DES across decryption time with respect to file size. Initially when the file size is 5MB the decryption time for AES, 3DES, and DES is 5s, 2.5s, and 2s respectively. With the increase in the file size the decryption time for all the three schemes AES,3DES, DES increases.3DES showed the maximum decryption time across 25 MB of file size whereas for the case of AES and DES it is 10s and 8s.

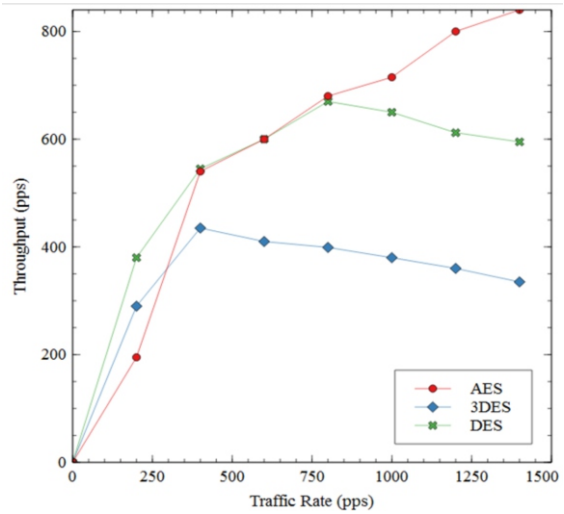

Fig. 9. Throughput evaluation with traffic rate

In the end, we evaluated the throughput with respect to the traffic rate. Initially, with the increase in traffic rate, the throughput increases for AES, 3DES, and DES. In the starting phase as the traffic rate is 250pps, the throughput for AES, DES and 3DES are 197, 398 and

296 respectively. As the traffic rate increases i.e. 1500pps then AES showed a maximum throughput which is 850 whereas for the case of DES and 3 DES the throughput is observed as 600 and 375. So the throughput decreases for the case of DES and 3DES with the increase in traffic rate. Fig. 9, depicts the throughput evaluation with the traffic rate.
Table 3 is given below created on the basis of the results for encryption/decryption time, Bit Error Rate and throughput for the different algorithms. The following table illustrates the results that affect the TETRA network system for better security and performance.

Table 3: Comparison table of result of algorithms

Algorithms	Throughput (pps)	BER	Encryption/ Decryption Time(s)
AES	850	0.012	9 sec / 10 sec
DES	600	0.001	9 sec / 8 sec
3DES	350	0.01	27sec / 26 sec

Table 3 concludes that AES is comparatively better than the other schemes. Encryption & decryption show almost no variation for AES and DES, but AES is better choice with error rate and throughput.

I. Conclusion

Terrestrial Trunked Radio is an open standard and easily targeted by the intruders or attackers to minimize its performance by affecting its security level. This review paper reveals some encryption techniques as well as threats and challenges a Terrestrial radio network faces while communicating with other devices. The novelty of this paper is the end-to-end encryption mechanism for secure and strong TETRA network using the modules of physical layer of TETRA. We just proposed the end-to-end encryption from sender side to receiver side which also include air media or air interface. The improvement in encryption time and BER performance enhance the authentication level. This encryption time reduces security threats. As low encryption time means the encryption process having a low time to encrypt and secures wireless communication. This concludes that threats can be controlled by providing some efficient security techniques to protect data and the medium of network transmission. By improving the encryption and decryption time of Network with the help of proposed techniques the security can be maximized and enhanced to control threats and attacks. But the encryption and decryption time processing requires high power if we use AES with higher rounds and key length. TETRA has different frequency ranges for different countries. So, power and frequency range are high scopes for further research. The evaluation parameters are Throughput, SNR, Encrypt/Decrypt Time, versus different packet sizes. The graphical analysis and evaluation reflected that AES bases result better, fast and more reliable than other contemporary encryption schemes.

Reference

[1] M. Buric, "Voice end-to-end encrypted for TETRA radiocommunication system," *2010 8th Int. Conf. Commun. COMM 2010*, pp. 419–422, 2010.
[2] Y. Park, C. Kim, and J. Ryou, "The Vulnerability Analysis and Improvement of the TETRA Authentication Protocol," *2010 12th Int. Conf. Adv. Commun. Technol.*, vol. 2, pp. 1469–1473, 2010.
[3] R. Ferrús *et al.*, "Security in transnational interoperable PPDR communications: Threats and requirements," *Proc. 2015 2nd Int. Conf. Inf. Commun. Technol. Disaster Manag. ICT-DM 2015*, pp. 88–95, 2016.
[4] G. S. Y. H. A. Patel and K. Patel, "Chaos Based Encryption & Decryption System for Secure Audio/Text Communication," vol. 4, no. 02, pp. 796–799, 2016.
[5] N. P. Fouché and K. L. Thomson, "Exploring the human dimension of TETRA," *2011 Inf. Secur. South Africa - Proc. ISSA 2011 Conf.*, 2011.
[6] K. Kang, J. Ryu, S. Member, and D. K. Noh, "Accommodating the Variable Timing of Software AES Decryption on Mobile Receivers," pp. 1–11, 2013.
[7] S. Gajewski, M. Sokol, and M. Gajewska, "Data Protection and Crypto Algorithms' Performance in RSMAD," in *2011 IEEE 73rd Vehicular Technology Conference (VTC Spring)*, 2011, pp. 1–5.
[8] M. Vaidehi and B. J. Rabi, "Efficient Fault Detection Model Design ' Hamming SEC-DAED-TAED- TETRA AED ' Based AES Encryption and Decryption," vol. 11, no. 7, pp. 4945–4950, 2016.
[9] I. Europe, "Information security in digital trunking systems," vol. 8, pp. 40–48, 2017.
[10] B. Zahednejad, "A Novel and Efficient Privacy Preserving TETRA Authentication Protocol," pp. 125–132, 2017.
[11] "Key Performance Indicators for QOS Assessment in Tetra Networks," no. January, 2014.
[12] Y. Huang, W. Li, and J. Lei, "Concatenated

physical layer encryption scheme based on rateless codes," *IET Commun.*, vol. 12, no. 12, pp. 1491–1497, 2018.

[13] H. Fang, S. Member, L. Xu, and X. Wang, "Coordinated Multiple-Relays Based Physical-Layer Security Improvement : A Single-Leader Multiple- Followers Stackelberg Game Scheme," vol. 13, no. 1, pp. 197–209, 2018.

[14] I. Technology and S. Burla, "Open Access Security in Wireless Sensor Networks using Cryptographic Techniques Madhumita Panda American Journal of Engineering Research (AJER)," no. 01, pp. 50–56, 2014.

[15] D. Rupprecht, A. Dabrowski, T. Holz, E. Weippl, and P. Christina, "Future Mobile Network Generations," pp. 1–25, 2018.

[16] R. Schiphorst, "Cognitive Radio Communications and Networks Principles and Practice," no. May, 2014.

[17] F. D. Alotaibi, A. Benabdennour, and A. A. Ali, "A Real Time Intelligent Wireless Mobile Station Location Estimator with Application to TETRA Network," no. June 2014, 2009.

[18] E. Thambiraja, "A Survey on Various Most Common Encryption Techniques," vol. 2, no. 7, pp. 226–233, 2012.

[19] S. Khan, K. Loo, T. Naeem, and M. A. Khan, "Denial of Service Attacks and Challenges in Broadband Wireless Networks," vol. 8, no. 7, pp. 1–6, 2008.

[20] R. Ma, J. Cao, D. Feng, H. Li, Y. Zhang, and X. Lv, "PPSHA: Privacy preserving secure handover authentication scheme for all application scenarios in LTE-A networks," *Ad Hoc Networks*, vol. 87, pp. 49–60, 2019.

[21] A. Seba, N. Nouali-Taboudjemat, N. Badache, and H. Seba, "A review on security challenges of wireless communications in disaster emergency response and crisis management situations," *J. Netw. Comput. Appl.*, vol. 126, pp. 150–161, 2019.

[22] T. T. Radio and A. Interface, "Terrestrial Trunked Radio (TETRA); Voice plus Data (V + D); Part 2 : Air Interface (AI)," vol. 1, pp. 1–1232, 2007.