An Improved Privacy Preserving TETRA Authentication Protocol Seyyed Morteza pournaghi

Behnam Zahednejad
Guangzhou University
10 PUBLICATIONS **153** CITATIONS

Mahdi Azizi
Imam Hossein University
4 PUBLICATIONS **3** CITATIONS

An Improved Privacy Preserving TETRA Authentication Protocol

Behnam Zahednejad

M.A student of secure telecommunication, Shiraz University, Iran, zahednejadb@gmail.com

Mahdi Azizi

Faculty of security department, Imamhusein University, Iran, mahdiazizi@ihu.ac.ir

Seyyed Morteza pournaghi

P.H.D student of Information technology, Qom University, Iran sm.pournaghi@gmail.com

Abstract— **Terrestrial Trunked Radio (TETRA) has been developed by Telecommunications Standards Institute (ETSI) as the main European standard for the specialized and professional users. TETRA is one of the best choices to be implemented in govemental agencies, military operations, police, emergency, transportation facilities etc. The authentication and privacy-preserving of users is quite critical. In addition, the system should prevent adversary from tracking the movement of mobile radio subscribers. This paper discusses the vulnerabilities of TETRA authentication protocol namely the lack of perfect forward secrecy and unlinkability of mobile radio subscribers. Lack of user unlinkability lets the attacker track the physical movement of users which is highly undesirable specially in military operations. In the following we proposed an improved privacy preserving protocol resistant against such attacks. The security of the proposed scheme is further validated with BAN-Logic and ProVerif analysis tool.**

Keywords— ***TETRA, authentication protocol untracability, unlinkability, BAN-Logic,*** **ProVerif**

1. Introduction

Terrestrial Trunked Radio (TETRA) has been developed by Telecommunications Standards Institute (ETSI) as the main European standard for the specialized and professional users This standard has combined the features of PMR with the properties of mobile cellular phones such as fast data communication. The communication across TETRA should be secure, robust and private. The TETRA technology uses the frequency spectrum in an efficient manner [1]. The key services that distinguishes TETRA from other wireless technologies include simplex call, duplex call, group calls, pre-emptive call, voice encryption, packet data services etc. Today, different radio communication vendors support TETRA telecommunication standard. TETRA can be used in SCADA to send data between supervision center and Remote Terminal Unit (RTU) as well [2].

Most mobile radio users are not happy if one attacker can track their physical movements. In industrial environments, confidential critical missions of security organizations, military, police forces, governmental agencies etc. it is vitally critical that the anonymity and untracability of users be preserved. Untracability is quite similar to the notion of unlinkability. It refers to the property that the attacker should not be able to distinguish between the cases when different services are provided to the same user or different users.

The main focus of this paper is the authentication protocol between the mobile terminals and authentication server (SwMI). In this paper, we show vulnerabilities of TETRA authentication protocol including linkability attack against TETRA authentication protocol threatening the untracability of users in addition to lack of perfect forward secrecy.

The main authentication protocol of TETRA has been investigated in [3, 4].In addition to the authentication protocol, other features of TETRA including key management and location privacy has been discussed in [5]and [6] respectively. Similar mobile authentication protocol such as UMTS suffer linkability attack as discussed [7]. In the following we briefly describe each of them:

In [3] TETRA authentication protocol has been verified by Scyther analysis tool. It is shown that the integrity of the exchanged messages can be manipulated to violate the key agreement of the protocol. They have shown two key agreement and availability attacks suffering the protocol. They proposed to use message authentication code on the exchanged messages to avoid such attacks. However these vulnerabilities do not really threaten the TETRA network since entities check the equality of their keys before the real beginning of communications.

TETRA authentication protocol has been analyzed in other respects as well: Yong-Seok Park and colleague [4] have analyzed the threat of impersonation of infrastructure or authorized users if the secret key has been revealed to adversary. The have used REF for the establishment of session keys which cannot be revealed to adversary to provide forward security for the protocol.

In [5] a new group key agreement scheme has been proposed for lightweight Mobile users. Lightweight mobile users only need on-line XOR operation. It also allows the Mobile station and Infrastructure agree on a group key with 1-round complexity. In [6] it is shown that the location privacy and dependability of TETRA can be weakened. In particular, it can be localized by means of antenna arrays and direction finding techniques on the physical layer.

In [8] TETRA authentication protocol has been analyzed using ProVerif and Scyther analysis tools in various aspects such as authentication, anonymity, forward secrecy etc.The results show that the protocol is vulnerable to lack of perfect forward secrecy. However they believe that this vulnerability cannot be fixed unless we use public key encryption which is hard to deploy.

Organization of paper. After discussing the TETRA architecture in section 2, we discuss the vulnerabilities of TETRA authentication protocol in section 3. Our improved privacy-preserving proposed scheme is then given in section 4 to be followed by its verification by ProVerif and BAN-Logic in section 6,7 respectively. Finally a conclusion is given in section 8.

2. TETRA architecture

Terrestrial Trunked Radio (TETRA) is a wireless communications standard designed to meet the needs of Professional Mobile Radio (PMR) used in over 140 countries including Western Europe, Eastern Europe, Middle East, Africa, Asia Pacific, Caribbean and Latin America. This standard has been developed by European Telecommunications Standardization Institute (ETSI) for governmental agencies and emergency services. Railway, marine and military organizations, fire, ambulance and police are among other organizations who use this standard. This technology is based on Time Division Multiple Access (TDMA). TETRA radios can operate in three different modes of operations:

- Voice plus Data (V+D)
- Direct Mode Operation (DMO)
- Packet Data Optimized (PDO)

In Voice plus Data mode, a full duplex channel allows the multiplexing of voice and data by packetizing the information into different time slots. Direct Mode Operation does not support full duplex operations but simplex mode of operation. Packet Data Optimized mode is used when high bandwidth data transmission is needed. TETRA can be used in industrial systems such as SCADA to deliver secure supplies by integrating the whole network including the generators, RTUs and master stations.

2.1. TETRA architecture

In the following we describe the architecture of the TETRA system. As shown in figure 1 the main components of the network include :

- **Mobile Station (MS):** It comprises subscribers' physical equipment, a Subscriber Identity Module (SIM) and a TETRA Equipment Identity (TEI) assigned to every equipment's by the manufacturer.
- **Switching and Management Infrastructure (SwMI):** It comprises base station and Authentication center. Base stations establish and maintain communication between mobile stations over ISDN. They allocate channels, switch calls and contain databases with subscriber's information. Authentication center is the entity that contains the long-term key k which is connected securely with the base station.

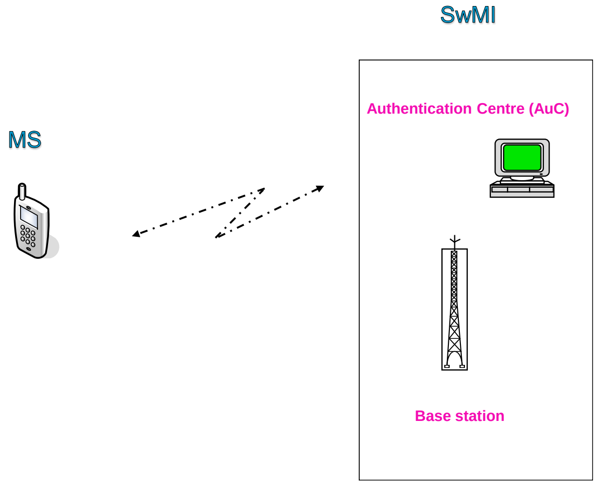

Figure 1. A schematic of TETRA architecture

2.2. TETRA security

TETRA communication aims to achieve authentication, confidentiality, availability and privacy preserving. Concerning the privacy preserving, two distinct properties should be addressed:

- **User anonymity**: the property that the Individual TETRA Subscriber Identity (ITSI) or Individual Short Subscriber Identity (ISSI) should not be disclosed to unauthorized individuals, entities or processes [3].
- **User unlinkability**: This property holds when a system that provides the services for multiple users looks the same as the one providing services for a single user.

2.3. TETRA authentication protocol

The security functions of TETRA include authentication, Air Interface Encryption (AIE), and End-To-End Encryption (E2EE) [9]. In TETRA, the authentication services include authentication of MS by SwMI, authentication of SwMI by MS and mutual authentication [1].A schematic of authentication of MS by SwMI is shown in figure 2. Challenge-response is the basis of the authentication mechanism. For the MS to be authenticated to the SwMI, the SwMI retrieves the common pre-shared key k by the received ATSI of the MS. Algorithm TA11 takes the pre-shared key k and a random seed RS as input to derive session key KS. SwMI takes RAND1 and KS as input to the algorithm TA12 to get the expected response XRES1. SwMI then generates RAND1 and sends RAND1 and RS to the MS. The MS uses the received challenges RS as input to algorithm TA11 to get KS. It further computes RES1 by algorithm TA21 with RAND1,KS as input. RES1 is then sent to the SwMI. After receiving the response of MS by SwMI, upon the equality of the expected response XRES1 with the received response RES1, the mobile station will be authenticated and the true value will be set to R. Else, the false value will be set and given to the MS. The same scenario holds for the authentication of infrastructure by mobile station with the direction of messages reversed. For more information refer to [].

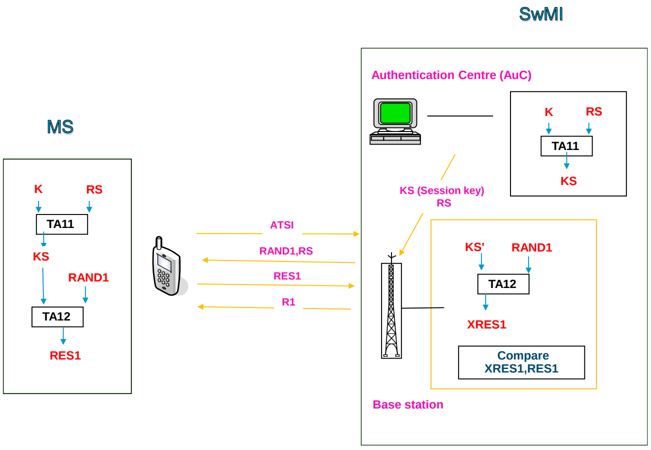

Figure 2. Authentication of MS by SwMI.

3. Vulnerabilities of TETRA authentication protocol

The main threats of TETRA authentication protocol include lack of perfect forward secrecy and user unlinkability. In the following we describe them each in detail:

3.1. Lack of perfect forward secrecy

As defined in [10], lack of perfect forward secrecy lets the attacker to discover the previous session keys given the long-term key k. As shown in figure 3, it suffices for the attacker to get the transmitted RS in a previous session. Using algorithm TA11, he/she can compute session key KS by having the long-term key k and the intercepted RS.

3.2. Lack of user unlinkability

Most mobile radio users are not happy if one attacker can track their physical movements. In confidential critical missions of security organizations, military, police forces, governmental agencies etc., it is vitally critical that the anonymity and untracability of users be preserved. Untracability is quite similar to the notion of unlinkability. Despite the use of temporary identities ATSI to avoid the linkability of TETRA subscribers, the execution of the authentication protocol paves the way for the attackers to trace TETRA subscribers.

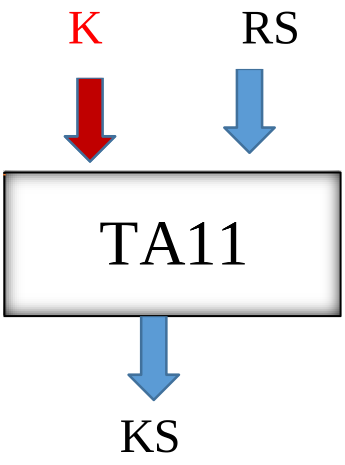

Figure 3. Lack of perfect forward secrecy in TETRA

As shown in figure 4, an active attacker is able to intercept the authentication triplet (Rs, RAND1, RES1) sent and received by the SwMI respectively to the victim mobile station MSv. The intercepted authentication challenge (RS,RAND1) is sent later by the attacker to a number of MSs to find the original MSv. Due to the fact that the output of TA12 depends on (RAND1,K,RS) the attacker is able to distinguish any mobile station from the one the authentication challenge was originally sent to (MSv*).* Upon reception of the replayed (RS,RAND1) the victim mobile station, MSv will give the same RES1 as the one given before, while other MSs give different values for RES1 due to the different pre-shared keys they have. The implementation of few false base stations would then allow an attacker to trace the movements of a victim mobile station, resulting in a breach of the subscriber untraceability. This attack is shown in figure 3. To see how the lack of this property lets the attacker to trace the movement of MS, consider the following example:

Let $\mathrm{Area}_{\mathrm{i}}$ be the area under the control of $\mathrm{SwMI}_{\mathrm{i}}$and $\mathrm{C}_{\mathrm{j}}^{\mathrm{i}}$ be the j^{th}session of MS in $\mathrm{Area}_{\mathrm{i}}$. Suppose that a MS has been present in N different areas as $(\mathrm{Area}_1 \rightarrow \mathrm{Area}_2 \rightarrow \cdots \rightarrow \mathrm{Area}_{\mathrm{N}})$. The attacker wants to recognize the one who had been present in these areas among a large number MSs. In this regard it suffices that he/she collects the triplet challenges of each session as $< \mathrm{RAND1}_{\mathrm{i}}, \mathrm{RES1}_{\mathrm{i}}\ , \mathrm{RS}_{\mathrm{i}} >$. Then he/she sends the N pairs of $<\mathrm{RAND1}_{\mathrm{i}}, \mathrm{RS}_{\mathrm{i}}>$ to suspicious MS to see which one give $\mathrm{RES1}_{\mathrm{i}}$ for j=1,2…N .

4. Our proposed scheme

As shown in figure 5, we propose not to send challenges RAND1, RS explicitly. Instead they should be computed secretly by both parties using a Random Generating Function (RGF) seeded from the common pre-shared key k i.e. (RS, Rand1, Rand2)=RGF(k) for the first session. For

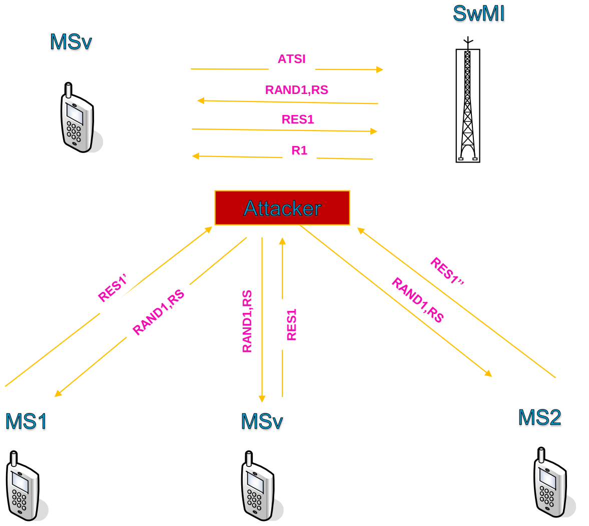

Figure 4. Violance of the user's unlinkability

the next sessions the RGF produces the new challenges (Rs', Rand1', Rand2') seeded from the previous challenges namely Rand1, Rand2 i.e. (Rs', Rand1', Rand2') = RGF (Rand1, Rand2). (RAND2 is used for the authentication of SwMI by MS). As before SwMI computes XRES1 by itself using algorithm TA21 to compare it with received RES1. Upon the equality of the two terms, the MS is authenticated and SwMI sends R1 (True) to MS. The same scenario holds for the mutual authentication of MS and SwMI. In this case, challenges such as RAND1,RAND2,RS are not transmitted in the protocol.

This improvement prevents the adversary to be able to track the movement of the user, as he no longer has access to challenges (RAND1, RS, RAND2) to re-send them to MSs. Thus the attack scenario of figure 3 never happens. In addition, despite the claim of [] we have improved the problem of perfect forward secrecy of the authentication protocol without using public key encryption. In addition the number of rounds are reduced from 4 messages to 2 messages.

In the next two sessions we prove the security of our scheme using BAN-Logic and ProVerif analysis tool.

5. VERIFYING THE PROPOSED SCHEME WITH PROVERIF

ProVerif [10] is an automatic analysis tool to analyze properties of security protocols including secrecy, authentication, anonymity, resistance against offline guessing attack etc. ProVerif‘s specification language is based on an extension of pure pi-calculus (applied pi-calculus) [11]. Our security model is a symbolic Dolev-Yao attacker model who has full control over communication channel. He can read, modify, delete and inject messages.

Modeling security protocols in ProVerif .The modelling language for the security protocols is based on the applied pi calculus introduced by abadi, fournet.

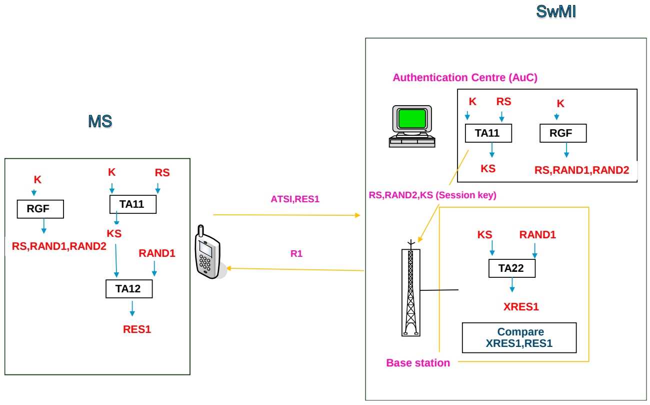

Figure 5. Our proposed authentication protocol

The language is converted to horn clause to be compiled by the machine to automatically verify our security protocols based on the queries. In this language, functions are introduced by the constructors f (M1, . . . , Ml) having arity l. Destructors such as reduc g(M1, . . . , Mt)=M0 are used to manipulate terms., and define their relation. In the following you can see the grammer used for processes.

P, Q, R ::= sub processes parallel composition !P replication new n; P name restriction if M = N then P else Q conditional let x = g(M1, . . . , Mn) in P destructor application else Q in(M, x); P message input out(M, N); P message output

Each agent of the protocol such as mobile station, infrastructure etc. can be defined by processes such as P, Q, R. In the main process, you run them in parallel as P | Q. They can be run in infinite sessions by ! P. new and fresh variables such as long-term key, k, can be defined as new k. conditional and assignments are allowed as well. You can output and input messages on channel M by out (M,N), in(M,x) respectively. In the following after producing the long-term key k, we have run Infrastructure SWM and mobile station MS in parallel for infinite sessions:

process new k;(!SWM |! MS)

Proverif is able to prove if properties such as anonymity, intractability, unlinkability holds. Observational equivalence captures these notions. Informally, It refers to the fact that if two elements are indistinguishable from each other for the adversary, they are observationally equivalent. The “choice” construct serves this notion by taking two arguments and verifying if they are equivalent to the adversary or not. For example if you want to see two values such as n,h(n) are distinguishable for the adversary, choice[n,h(n)] serves this purpose.

.

5.1.Analyzing the unlinkability TETRA authentication protocol

In the following we show how to model the unlinkability property in ProVerif. Other properties have been discussed before in . Consider the following process:

S =!(new k1; (! new k2; let k = choice[k1, k2] in (SWM | MS)))

The long-term keys k1,k2 represent a system in which the system is run once or multiple times respectively.

We check if they are observationally equivalent to the adversary or not. The verification of our proposed scheme with the ProVerif tool shows that the unlinkability property holds. The verification of the original protocol, as expected, results in the breach of the unlinkability property.

Full ProVerif script on verifying the TETRA is available in [12].

6. VERIFYING THE PROPOSED SCHEME WITH BAN-LOGIC

Basically, There are two main methods to verify security protocols:

1- Formal proof

2- Informal analysis methods

Formal proof is generally done by analyzers in a manual manner. In such analysis, the probability of attacks such as MIMT, parallel session attacks, UKS attack, impersonation attack etc. is computed. Different security properties of protocols such as Known key secrecy, forward secrecy, unknown key secrecy, key confirmation etc. should be verified in a Logical manner. The analyzer has to make sure that the attacker cannot be a threat. In informal analysis, an experienced analyzer who well knows analysis methods should discuss about the security of protocols. BAN (Burrows, Abadi, Needham) [13] was first presented in 1990. There are several postulates that should be accepted by parties to interpret the protocol accordingly. Then, the final purpose of the protocol should be proved by such postulates. The analyzer should verify the performance of the protocol as well.

Basic Notation: In the following we describe the most basic notation used in protocol analysis.

P |~ X: P once said X: P at some time sent a message including the statement X. It is not known when the message was sent (in the past or in the current run of the protocol) but P believed that X was true when it sends the message.

P |=> X: P controls X. P has jurisdiction over X. P is a trusted authority on the truth of X. #(X): X is fresh. Using the Logic, time is divided into two epoch, the past and the present. The present begins with the start of the current execution of the current protocol. X is fresh if it is not contained in any message sent in the past.

A←K→B: K is a shared key for P and Q. K is a secure key for communication between P and Q, and it will never be discovered by any principal except for P or Q, or a principal trusted by either P or Q. For more information on BAN language refer to [13].

For our proposed scheme, firstly $SWMI$ believes that the other party (MS) believes in RES1 which is needed for the establishment of key. It must believe in RES2 as well. That is:

$$\frac{\mathrm{S}|\equiv\mathrm{K}}{MS|\equiv(\mathrm{RAND1,RAND2,RS})},\ \frac{S|\equiv\mathrm{k},\ \ \mathrm{S}|\equiv\mathrm{Rs}}{S|\equiv\mathrm{Ks,Ks'}},$$

$$\frac{S|\equiv\mathrm{ks},\ \ \mathrm{S}|\equiv\mathrm{RAND1}}{S|\equiv\mathrm{XRES1}},\ \frac{S|\equiv\mathrm{ks},\ \ \mathrm{S}|\equiv\mathrm{RAND2}}{S|\equiv\mathrm{RES2}}$$

$$\frac{\frac{S|\equiv\mathrm{XRES1},S\lhd\mathrm{RES1}}{S|\equiv(\mathrm{XRES1=RES1})},\mathrm{S}|\equiv(S-k\rightarrow MS)}{\mathrm{S}|\equiv\mathrm{MS}|\equiv\mathrm{RES1}},$$

$$\frac{\mathrm{S}|\equiv\#\mathrm{XRES1},S|\equiv(\mathrm{XRES1=RES1})}{S|\equiv\#\mathrm{RES1}}$$

MS believes that SWMI has said RES2 once. Due to the equality of XRES2 with RES2, it makes sure that both of them are fresh values. Thus, it makes sure that SWMI believes in RES2.

$$\frac{\mathrm{MS}\,\big|\equiv\mathrm{XRES2},\mathrm{MS}\lhd T,MS\,\big|\equiv\mathrm{S}\leftarrow\mathrm{K}\rightarrow MS}{MS|\equiv\mathrm{S}|\sim\mathrm{RES2}}$$

$$\frac{\mathrm{MS}\,\big|\equiv\#\mathrm{XRES2},\mathrm{MS}\,\big|\equiv(\mathrm{RES2}=\mathrm{XRES2})}{MS|\equiv\#\mathrm{RES2}}$$

$$\frac{\mathrm{MS}\,\big|\equiv\mathrm{S}\,\big|\equiv\mathrm{RES2},\mathrm{MS}|\equiv\#\mathrm{RES2}}{MS|\equiv\mathrm{S}|\equiv\mathrm{RES2}}$$

SWMI also believes that MS has the RES2 required for the establishment of keys. Due to the fact that SWMI believes that MS accepted RES1, it makes sure over the establishment of key with MS.

$$\frac{S|\equiv\mathrm{MS}|\equiv(\mathrm{Rs,RAND2}),\mathrm{S}\ |\equiv\#\mathrm{RAND2},\mathrm{S}\leftarrow\mathrm{K}\rightarrow MS}{S|\equiv\mathrm{MS}|\equiv\mathrm{RES2}}$$

$$\frac{S|\equiv\mathrm{MS}|\equiv\mathrm{RES1},\mathrm{S}\ |\equiv MS\ |\equiv\mathrm{RES2}}{S|\equiv\mathrm{MS}|\equiv\mathrm{sharedkey}}$$

For the full script of verification of the protocol with BAN-Logic refer to [12].

7. CONCLUSION

TETRA is the main European digital transmission mobile radio standard used in industry, emergency, rescue service organizations etc. as a general national safety communication network. It is being adopted extensively in manufacturing, oil and gas and utility sectors. Apart from authentication and availability, in industrial environments, confidential critical missions of security organizations, military, police forces, etc. it is vitally critical that the anonymity and untracability of users be preserved. Violation of this property enables all kinds of undesirable behaviors such as tracing mobile users. In this paper we have analyzed the vulnerabilities of TETRA authentication protocol. Despite the use of ATSI in such network, a temporary identity of users changing from time to time to hide the real identities of users, the execution of the authentication protocol paves the way for the attackers to trace TETRA subscribers. Lack of perfect forward secrecy is another vulnerability of the protocol we then proposed an improved privacy preserving authentication protocol resistant against such vulnerabilities. Further the security of the proposed scheme is verified using BAN-Logic and ProVerif analysis tool.

Reference

[1] Hai-chen, X. U, “Analysis on Security Architecture for TETRA Digital Trunking Network,” *Communications Technology,* no. 7, 2010.

[2] Ozimek, I and Gorazd. K, “SCADA system using TETRA communication network,” *Recent advances in computers, computing and communications* , pp. 164-166, 2002.

[3] Duan.S,Mjølsnes.S.F, “Security analysis of the Terrestrial Trunked radio (TETRA) authentication protocol,” in *Norwegian Information Security Conference,* Stavanger, 2013.

[4] Yong-Seok.P,Kim.S, “The vulnerability analysis and improvement of the TETRA authentication protocol,” in *The 12th International Conference on Communication Technology (ICACT),* 2010.

[5] Lee, S., Lee, S., & Lee, D., “Efficient group key agreement for dynamic TETRA Networks,” *Theory and Practice of Computer Science,* pp. 400-409, 2007.

[6] Pfeiffer, M., Kwiotek, J. P., Classen, J., Klose, R., & Hollick, M, “nalyzing TETRA Location Privacy and Network Availability,” in *Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices* , 2016.

[7] Arapinis.M, “New privacy issues in mobile telephony: fix and verification,” in *ACM conference on Computer and communications security.* , 2012.

[8] MullaZadeh.M,Farash.S, “formal verification of TETRA authentication protocol with automated tools,” *cyber and electronics defense magazine,* no. 4, pp. 109-129, 2017.

[9] “ETSI EN 300 392-7, “Voice plus Data (V+D); Part 7: Security”,” 2017. [Online]. Available: http://www.etsi.org/deliver/etsi_en/300300_300399/30039207/03.04.01_60/en_30039207v030401p.pdf. [Accessed 12 December 2017].

[10] Tilborg.W, Encylopedia of cryptography and security, Springer, 2013.