2017 14th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC) September 6-7, 2017; Shiraz University - Shiraz, Iran

A Novel and Efficient Privacy Preserving TETRA Authentication Protocol

Behnam Zahednejad
M.A student of secure telecommunication, IHU University, Iran,
zahednejadb@gmail.com

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

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

***Abstract*— TETRA (Trans-European Trunked Radio) is the main trunking technology European standard for Private Mobile Radio systems (PMR). TETRA is one of the best choices to be implemented in SCADA environment to provide interoperability for the whole system. The authentication and privacy-preserving of users is quite critical. In addition, the system should prevent adversary from tracing the movement of mobile radio subscribers. This paper discusses the vulnerabilities of TETRA authentication protocol namely the availability and unlinkability of mobile radio subscribers. It identifies a serious linkability attack against the protocol threatening the privacy of subscribers. In the following we have fixed the protocol with a much better efficiency than other proposed schemes. The security of the proposed scheme isfurther analyzed with BAN-Logic and ProVerif analysis tool.**

Keywords— ***TETRA, SCADA, untracability, unlinkability, BAN-Logic, ProVerif***

I. INTRODUCTION

Terrestrial Trunked Radio (TETRA) has been developed by Telecommunications Standards Institute (ETSI) as a great standard for the specialized and professional users of the world. 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.

SCADA is an industrial system to control industrial processes which mainly consists of: A central host or master station and data gathering units which are called remote stations or remote terminal units (RTU) as well. The main concern of the paper is the authentication protocol between the mobile terminals and authentication server (SwMI).

Despite the use of ATSI in such network [3], a temporary identity of users changing from time to time, the authentication protocol is vulnerable against linkability attack by itself. In this paper, we present a linkability attack against TETRA authentication protocol threatening the untracability of users.

In [4] some availability attacks are presented violating the availability of the system. It is truly claimed that in emergency and safety communication networks, availability is arguably more critical than confidentiality. They have proposed a countermeasure to fix the availability attacks.

978-1-5386-6560-2/17/$31.00 ©2017 IEEE

However their solution is not so efficient. We have presented a much more efficient scheme that fixes the linkability attack and availability attacks together. We then prove the security of our scheme using Ban-Logic and ProVerif analysis tool.

The main authentication protocol of TETRA has been investigated in [4-5]. In addition to the authentication protocol, other features of TETRA including key management and location privacy has been discussed in [6] and [7] respectively. The linkability attack which is discussed in this paper has been discussed in other authentication protocols such as [8]. Other similar mobile radio standards such as P25 has been discussed in [9]. In the following we briefly describe each of them:

In [4] 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 drawn two key agreement and availability attacks against the protocol. They proposed to use message authentication code on the exchanged messages to avoid such attacks.

TETRA authentication protocol has been analyzed in other respects as well: Yong-Seok Park and colleague [5] have analyzed the threat of impersonation of infrastructure or the 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 [6] a new group key agreement scheme has been proposed for lightweight Mobile users. Lightweight mobile users only need a on-line XOR operation. It also allows the Mobile station and Infrastructure agree on a group key with 1-round complexity. In [7] it is shown than 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], the UMTS authentication and key agreement protocol had been shown to be vulnerable against linkability attack. They have proposed to use public-key encryption to avoid such attacks. However using public key encryption requires public key infrastructure (PKI) which is hard to deploy in mobile environments. Security analysis of American mobile radio standards such as P25 has been done in [9]. It identifies the jamming attack, unauthenticated messages,

denial of service etc. as vulnerabilities of such networks.

Organization of paper. After reviewing the previous related

studies in section 2, we discuss the TETRA architecture in section 3. Section 4 describes the vulnerabilities of TETRA authentication protocol. Our efficient proposed scheme is given in section 5 to be followed by its verification by ProVerif and BAN-Logic in section 6,7 respectively. Finally a conclusion is given in section 8.

II. INTRODUCTION TO TETRA

Terrestrial Trunked Radio (TETRA) is a wireless communications standard designed to meet the needs of Professional Mobile Radio (PMR) which is 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.

A. TETRA architecture in SCADA

In the following we describe the architecture of the TETRA system in SCADA environment. A schematic of TETRA architecture is shown in figure 1.The main components of the network consist of :

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.

978-1-5386-6560-2/17/$31.00 ©2017 IEEE

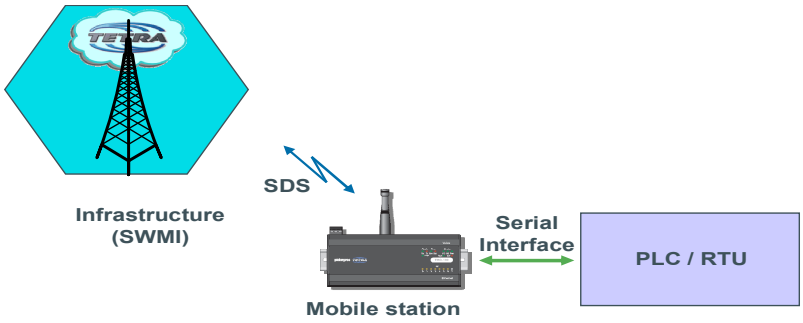

Figure 1. The main architecture of TETRA

They also communicate with each other using short data service (SDS) to provide an integrated SCADA network

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.

B. TETRA security

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

User identity confidentiality: 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 untracability: 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. To address the above properties, the ITSI is only used when registering into the network. It is then replaced by the Alias TETRA Subscriber Identity (ATSI) and the ISSI is replaced by the Alias Short Subscriber Identity (ASSI). These temporary identities are changed frequently from time to time. It should be noted that ATSI should never be derivable from ITSI.

C. TETRA authentication protocol

The security functions of TETRA include authentication, Air Interface Encryption (AIE), and End-To-End Encryption (E2EE). In TETRA, the authentication services include authentication of MS by SwMI, authentication of SwMI by MS and mutual authentication [1].

The infrastructure includes authentication center and a base station. Session key KS is generated by a random seed RS along with the long-term key K. Challenge-response is the basis of the authentication mechanism. For the mobile station (MS) to be authenticated to the infrastructure, the infrastructure retrieves the common pre-shared key k by the received ATSI of the MS. Algorithms TA11,TA21 take the pre-shared key k and a random seed RS as input to derive two session keys KS,KS'. KS is used for the authentication of MS to the infrastructure and KS' is used for the authentication of infrastructure to the MS. Infrastructure then sends a challenge RAND1 and RS to the MS. Infrastructure takes RAND1 and KS as input to the algorithm TA12 to get the expected response XRES1. The MS uses the received challenge (RAND1) as input to this algorithm which outputs RES1 to be sent to the infrastructure. This algorithm can generate DCK1 as half of the common derived cipher-key (DCK) as well. After receiving the response of MS by infrastructure, 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.

978-1-5386-6560-2/17/$31.00 ©2017 IEEE

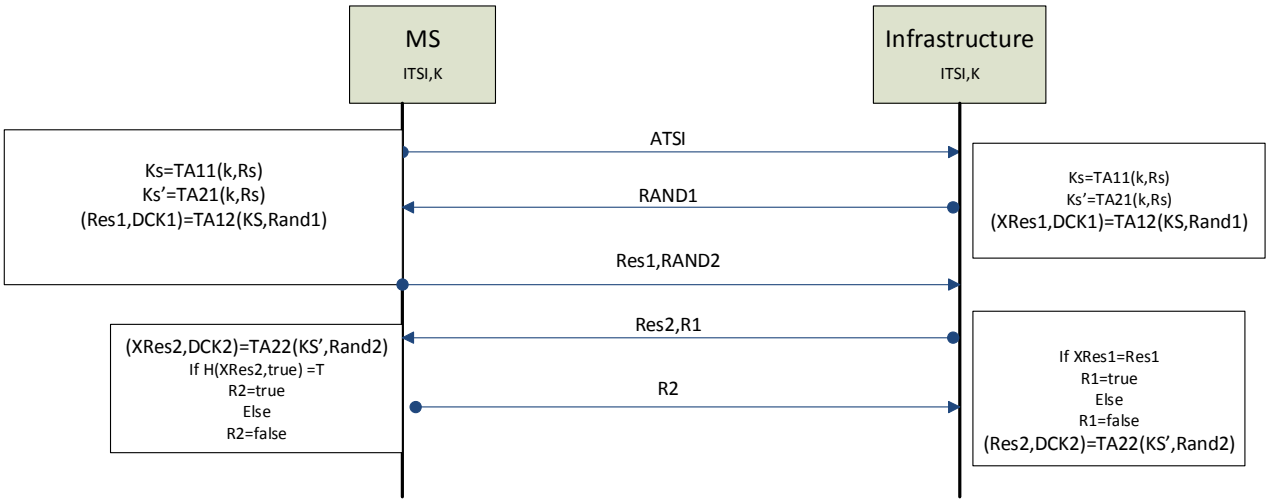

Figure 2. Mutual authentication of the main TETRA authentication protocol

In the mutual authentication scenario, the two entities namely MS and infrastructure authenticate each other by using two different challenges RAND1, RAND2. The parameters RAND1, RES1 are responsible for the authentication of MS to the infrastructure as said before. However RES1 is sent together with the challenge RAND2 to get the respective response namely RES2 which is used for the authentication of infrastructure to the MS. They each check whether the response they receive equals the one expected for. The session keys KS, KS' are different. KS is used to compute response RES1 while KS' is used to compute response RES2. Figure 2 shows a schematic of this scenario.

III. VULNERABILITIES OF TETRA AUTHENTICATION PROTOCOL

The attacks threatening the TETRA authentication protocol are listed below. A key agreement attack and availability attacks were first introduced in [4]. While linkability attack is introduced in this paper which is captured by ProVerif analysis tool. In the following, we describe each of them in detail.

A. Key agreement attack against mutual authentication protocol

As described in [4], the attacker makes mobile station run two parallel sessions with the Infrastructure, while the Infrastructure just participates in a single session. After the infrastructure sends challenge RAND1 to the MS in the first run, the attacker intercepts the response of the MS namely the Res1 (leaving out its challenge RAND2) and begins a parallel session (run 2) with the same MS with a different challenge i.e RT. The MS in run 2 gives REST as a response and produces Rand2' to authenticate infrastructure. The attacker then gives the intercepted RES1 from the first run of MS and the challenge RAND2' from the second run of MS to the infrastructure to be answered by a response RES2' which corresponds to RAND2'. It is then given to the MS in the second run. Obviously, the MS in the second run and the infrastructure

agree on different challenges namely Rand1 and RT. As a result their common cipher-key DCK1 will be different accordingly. In [4], it has been proposed to use message authentication code (MAC) on the (Rand2, Res1), but this solution is not so efficient, as for each session a MAC should be verified separately.

B. Availability attack

As said in [4], if the MS/Infrastructure are not authenticated the values of R1/R2 are set to false The attacker can easily change the value of the acknowledgement "R1/R2" from false to true to deceive the infrastructure/MS thinking that the other party has computed the common derived cipher-key (DCK).

C. Linkability attack

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.

978-1-5386-6560-2/17/$31.00 ©2017 IEEE

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. An active attacker is able to intercept the authentication triplet (Rs, RAND1, RES1) sent and received by the infrastructure 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. The linkability attack is shown in figure 3.

V. THE PROPOSED SCHEME

As shown in figure 4, we propose not to send challenges Rand1, Rand2, 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 as (Rs, Rand1, Rand2)=RGF(k) for the first session. For the next sessions the RGF produces the new challenges (Rs', Rand1', Rand2') seeded from the previous challenges namely Rand1, Rand2 as (Rs', Rand1', Rand2') = RGF (Rand1, Rand2). In addition, the value of H (Res2, R1) is sent to the Infrastructure. The value R2

should be changed to H (R2, Rand2) as well. Other procedures of the protocol are the same as before. The improvement made to the new authentication protocol is shown in table 1. As you can see our proposed scheme reduces the number of messages transmitted from 5 messages to 3 messages for the mutual authentication scenario. It also reduces the number of messages transmitted from 4 messages to 2 messages for the unilateral authentication scenario. In addition, the number of times the hash value has to be computed and verified is reduced from 3 times to 2 times. Assuming the equal computation costs of Random Generation Function (RGF) and Key Derivation Function (KDF), the number of times they are invoked or the number of their output values is reduced from 7 outputs to 6 outputs. The attacker has no way to change the common derived cipher-keys (DCK) of the parties as he has no control over the challenges Rand1, Rand2. In addition, she/he cannot trace mobile users as he/she never knows the challenges to see which party gives the same response as the one intercepted before. In the next two sessions we prove the security of our scheme using BAN-Logic and ProVerif analysis tool.

Table 1. comparison of performance and efficiency of the proposed scheme with Duan's scheme in [4].

Mutual authentication schemes	**Performance**	
	Computation cost	No. of messages transmitted
Duan's Scheme [4]	$8T_s$+$3T_h + 7T_{RGF}$	5
Our scheme	$8T_s + 2T_h + 6T_{RGF}$	3

T_s: Computation cost of symmetric encryption

T_h: Computation cost of hash function.

T_{RGF}: Computation cost of Random Generating Function.

VI. 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.The language is converted to horn clause to be compiled by the machine to automatically verify our security protocols based on the queries.

978-1-5386-6560-2/17/$31.00 ©2017 IEEE

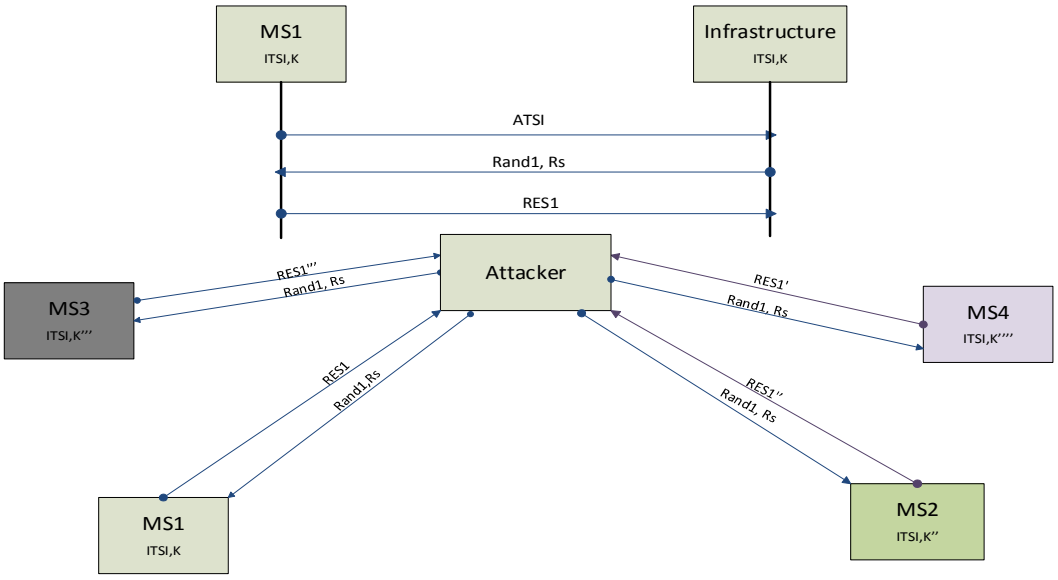

Figure 3. The linkability attack against TETRA authentication protocol

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 $P \mid Q$. 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)

B. Observational Equivalence

Proverif is able to prove if properties such as anonymity, intractability, unlinkability, offline guessing attack 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.

B. Verifying TETRA authentication protocol by ProVerif

This section describes the modelling of the TETRA authentication protocol in ProVerif.
Unlinkability . In the following we show how to model the unlinkability property in ProVerif. We consider two cases S-*UNLINK* and S.

Then we check if they are equivalent or not. *S-UNLINK* is the system consisted of infrastructure SWMI and MS with the long term identity key K, defined as S*UNLINK* =!new k; (*SWM* | *MS*). The system *S-UNLINK* represents the authentication protocol that is run at most once. We assume another system S that can be run multiple times.
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 S,S UNLINK are observationally equivalent to the adversary or not: $S \approx$ *S-UNLINK*.
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].

VII. VERIFYING THE PROPOSED SCHEME WITH BAN-LOGIC

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.

978-1-5386-6560-2/17/$31.00 ©2017 IEEE

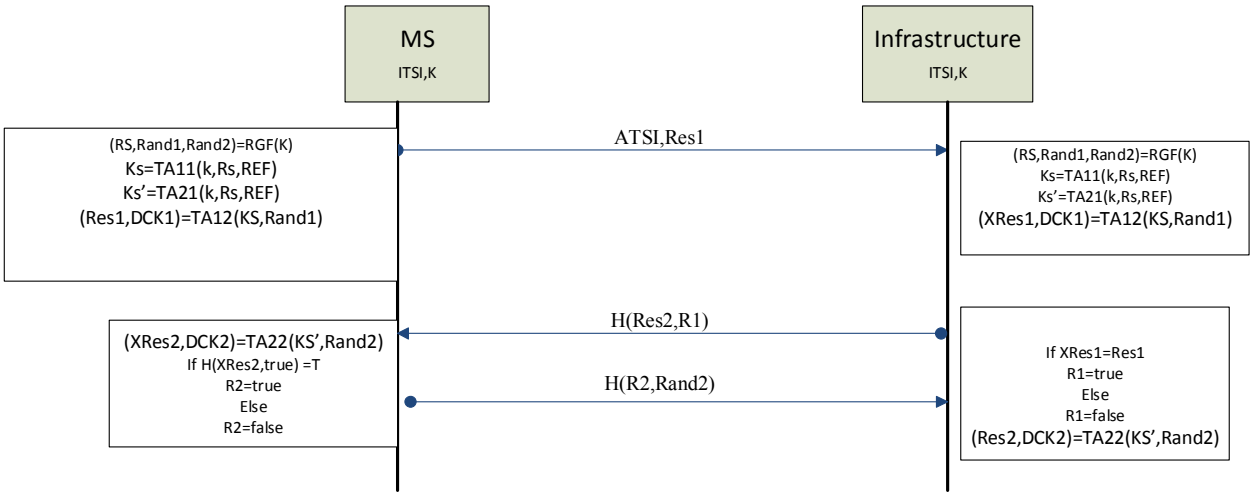

Figure 4. Our proposed scheme.

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:

$$\frac{S|\equiv K}{MS|\equiv(RAND1,RAND2,RS)}, \frac{S|\equiv k,\ S|\equiv Rs}{S|\equiv Ks,Ks'}, \frac{S|\equiv ks,\ S|\equiv RAND1}{S|\equiv XRES1}, \frac{S|\equiv ks,\ S|\equiv RAND2}{S|\equiv RES2}$$

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

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.

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

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

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

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.

978-1-5386-6560-2/17/$31.00 ©2017 IEEE

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

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

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

VIII. 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 unlinkability of TETRA authentication protocol with ProVerif. 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. After describing the potential linkability attack as a vulnerability of TETRA protocol, we proposed a novel efficient privacy preserving authentication protocol resistant against this kind of attack. The efficiency of the proposed scheme is significantly much better than the previous proposed scheme. Further the security of the proposed scheme is verified using BAN-Logic and ProVerif analysis tool.

References

[1] Hai-chen, X. U. "Analysis on Security Architecture for TETRA Digital Trunking Network [J]." Communications Technology 7 040, 2010.

[2] Ozimek, Igor, and Gorazd Kandus. "SCADA system using TETRA communication network." Recent advances in computers, computing and communications 164-166, 2002.

[3] Dunlop, John, Demessie Girma, and James Irvine. Digital mobile communications and the TETRA system. John Wiley & Sons, 2013.

[4] Duan, S., Mjølsnes, S.F., Tsay, J.-K.: Security analysis of the Terrestrial Trunked radio (TETRA) authentication protocol. In: Norwegian Information Security Conference, Stavanger, 18th–20th Nov 2013.

[5] Park, Yong-Seok, Choon-Soo Kim, and Jae-Cheol Ryou. "The vulnerability analysis and improvement of the TETRA authentication protocol." Advanced Communication Technology (ICACT), The 12th International Conference on. Vol. 2. IEEE, 2010.

[6] Lee, S., Lee, S., & Lee, D. (2007). Efficient group key agreement for dynamic TETRA Networks. SOFSEM 2007: Theory and Practice of Computer Science, 400-409.

[7] Pfeiffer, M., Kwiotek, J. P., Classen, J., Klose, R., & Hollick, M. (2016, October). Analyzing TETRA Location Privacy and Network Availability. In Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices (pp. 117-122). ACM.

[8] Arapinis, Myrto, et al. "New privacy issues in mobile telephony: fix and verification." Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012.

[9] A Security Analysis of the APCO Project 25 Two-Way Radio System." USENIX Security Symposium. 2011.

[10] Blanchet, Bruno, et al. "Proverif: Cryptographic protocol verifier in the formal model." 2012-07-03)[2013-09-28] http://prosecco. gforge. inria.fr/personal/bblanche/proverif,2010.

[11] Sangiorgi, Davide, and David Walker. The pi-calculus: a Theory of Mobile Processes. Cambridge university press, 2003.

[12] Online verification scripts at:
http://uploadboy.me/70611hbwlvtk/Proof.rar.html

[13] Mao, Wenbo, and Colin Boyd. "Towards formal analysis of security protocols." Computer Security Foundations Workshop VI, 1993. Proceedings. IEEE, 1992

978-1-5386-6560-2/17/$31.00 ©2017 IEEE