Formal Verification and Analysis of Primary Authentication based on 5G-AKA Protocol

Ed Kamya Kiyemba Edris
School of Science and Technology
Middlesex University
London, United Kingdom
EE351@live.mdx.ac.uk

Mahdi Aiash
School of Science of Technology
Middlesex University
London, United Kingdom
M.Aiash@mdx.ac.uk

Jonathan Kok-Keng Loo
School of Computer Engineering
University of West London
London, United Kingdom
Jonathan.Loo@uwl.ac.uk

Abstract—**Fifth generation mobile network (5G) is intended to solve future constraints for accessing network services. The user and network operator depend on security assurances provided by the Authentication and Key Agreement protocols (AKA) used. For 5G network, the AKA has been standardized and 5G-AKA protocol is one of the primary authentication methods that have been defined. This paper models the protocol and provides comprehensive formal analysis on 5G-AKA protocol as specified by The Third Generation Partnership Project (3GPP) standard. Using ProVerif a security protocol verification tool, we perform a full systematic evaluation of the 5G-AKA protocol based on the latest 5G specifications. We present security assumptions and properties that assists on the analysis based on two taxonomies, we find out that some important security properties are not achieved and related work ignored some crucial protocol flaws. Finally, we make some recommendations to address the issues found by our security analysis.**

Index Terms—**5G-AKA; protocol; formal methods; symbolic verification; primary authentication; ProVerif;**

I. Introduction

The development of fifth generation mobile network (5G) is intended to solve future constraints for accessing network services. It will create new network functions and user cases such as tactile internet, Internet of Things (IoT), Vehicle to Vehicle (V2V) that can be used to connect large number of devices and sensors. Mobile subscribers with their User Equipment (UE) will able to access services through New Generation Radio Access Network (ngRAN) as the access point (AP), taking advantage of various wireless technologies, therefore secure access is very paramount to 5G principle design. The security requirements have been defined by Third Generation Partnership Project (3GPP) in security architecture [1] and system architecture [2] to support these objectives.

The subscriber and Mobile Network Operator (MNO) expect security assurances from the methods used, such as the trust, authentication, data confidentiality and data integrity. The UE and the network must authenticate each other for the UE to gain access to the network, authorization and further authentication might be required for the UE to access other services. The network access security is achieved by running Authentication and Key Agreement (AKA) protocol between the UE, the Serving Network (SN) and the Home Network (HN), achieving mutual authentication and session key establishment for a secure communication over wireless channel. The 5G security standard [1] addresses the most critical security requirements in 5G network, by defining authentication procedures, like primary authentication that all UEs must perform to access the network services. This can be achieved by using 5G-AKA or an improved Extensible Authentication Protocol (EAP)-AKA' methods, in this paper we formally verify and analyse the 5G-AKA protocol to find the security guarantees that it provides.

Protocols such as 5G-AKA are complicated and challenging hence, they require formal methods and automated verifications tools for security analysis to explore its security properties. In this paper we analyse and verify the 5G-AKA protocol using ProVerif [3] an automated protocol verifier tool.

The main contributions of this work include formalization, modelling, and critical analysis. We study the security and privacy of the 5G-AKA protocol, we formally interpret the security properties. We model the protocol with symbolic modelling using ProVerif based on three and four entities models. Furthermore, we conduct a formal and comprehensive security evaluation of 5G-AKA to identify the security requirements of the 5G-AKA protocol based on two sets of taxonomies. We finally present our security consideration, our protocol modelling can serve as a basis for modelling and analysis for next generation AKA protocols.

The rest of the paper is structured as follows, section II explores related work, formal methods and automated tools. While section III discuses 5G-AKA standardisation briefly. We carry out the protocol modelling and discuss the threat model and security properties in Section IV. In Section V, we formally verify the protocol and the related security properties. We present our security analysis and discuss our recommendations in section VI. We finally conclude in Section VII.

II. Related Work

We present an updated formalization of an 5G-AKA protocol based on a 3GPP standard version v15.5.0 of TS 33.501 [1]. Some of the related work don't consider the four entities model which models HXRES that provides the HN with more home control as proof of UE participation. The authors in [4], analysed 5G-AKA protocol based on TS 33.501 v0.7.0. They discovered protocol vulnerability which would enable the attacker to impersonate another user to a SN. However, this

TABLE I
CORE LANGUAGE: SYNTAX AND INFORMAL SEMANTICS

a, b, c, k, s	name
x, y, z	variable
M,N ::=	terms
h(D1, . . . ,Dn)	function application
f(M1, . . . ,Mn)	constructor application
D ::=	expressions
fail	failure
P,Q ::=	processes
out(N,M); P	output
in(N, x : T); P	input
!P	!P replication
0	nil
P — Q	parallel composition
new a : T; P	restriction
let x : T = D in P else Q	expression evaluation
if M then P else Q	conditional

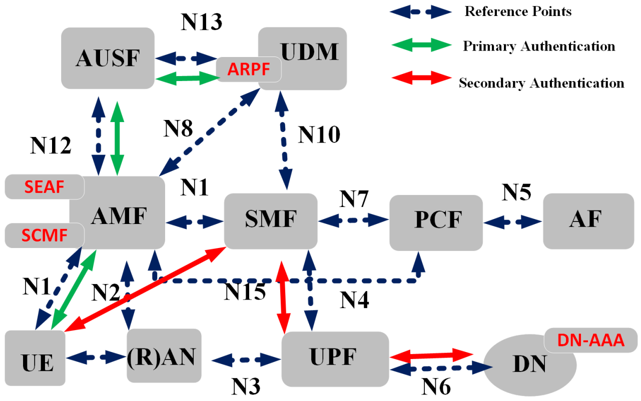

Fig. 1. 5G system and security architecture

attack is no longer possible due to the revised specification which states that SN name shall bind UE and 5G to an authentication procedure. In addition, the Subscription Permanent Identifier (SUPI) is now included when Authentication Credentials Repository and Processing Function (ARPF) is responding to Authentication Server Function (AUSF) request.

In [5], the authors provided a formal model based on TS 33.501 v15.1.0. They also conducted model security evaluation, identified the security assumptions and critical security properties that are missing. However, now the SUPI and KSEAF are sent together, the SN Name (SNN) binds Security Anchor Function (SEAF) to UE as well AUSF and ARPF, it eliminates the issue of SN assigning the KSEAF or SUPI to the wrong UE. The authors in [6] explored 5G-AKA security and stated that the protocol still suffers from all known attacks except for the IMSI-catcher attack. Partly their analysis was based on an attacker using fake BS, however due to SNN binding to UE and HN this seems unlikely. Also, the attack depended on permanent de-synchronization which can be avoided as the SEAF doesn't react to unsolicited synch failure message from UE or send new authentication request message unless it gets a response from AUSF.

A. Formal Methods and Tools

Formal methods and automated verification have been applied to AKA protocols in the past, earlier versions of AKA protocol were manually verified using tool like an enhanced BAN logic [8]. Formal methods have also been applied to assess security protocols in [9], [10]. The 5G-AKA protocol properties are very challenging due to the use of cryptographic primitive such as SQN, Exclusive-OR (XOR), its algebraic properties are tricky for symbolic reasoning [5] hence certain model checker tools are not suitable. There are many tools that can be used for AKA analysis like Automated Validation of Internet Security Protocols and Applications (AVISPA) [11], Tamarin [12] and ProVerif [13]. ProVerif focuses on unbounded sessions, uses horn-clause abstraction and supports cryptographic primitives defined by rewrite rules and equational theories that satisfy the finite variant property. It analyses security protocols, with Dolev-Yao (DY) [23] as the adversarial model, the equational theories are defined by the user and are enough to model primitives like XOR [14]. It uses applied π-calculus [15] as a formal language for describing and modelling security protocols. It also takes the security properties such as authentication, secrecy and observational equivalence to be proved as input. Cryptographic primitives are modelled as functions, messages as terms, built over an infinite set of names, variables and function symbols. For those reasons we find ProVerif suitable tool for our analysis, the grammar of ProVerif process language is shown in Table I [13].

ProVerif has been used to check security properties of AKA protocols [16], [17]. Some of the related work modelled the two HN entities as one [5] and re-synchronization was omitted in [4]. In others XOR was either not modelled or a different construct with simpler algebraic properties were used.

III. 5G-AKA PROTOCOL

5G-AKA protocol was developed directly from Evolution Packet System (EPS)-AKA protocol [19] with in-built home control to enable the HN to get informed when the UE is authenticated and to take the final call on authentication.

The network architecture still consists of three essential parties [20];

- UE: A mobile terminal containing the Universal Subscriber Identity Module (USIM). The USIM has cryptographic capabilities such as algorithms, encryption, Message Authentication Code (MAC), it stores SUPI, long-term key K and Sequence Number (SQN).
- Home Network (HN): It houses the database and security functions; it generates Authentication Vector (AV), stores users' subscription data and shares SUPI and the key K with UE.
- Serving Network (SN): It is the access network the UE attaches to via ngRAN.

The 5G security architecture [1] consists of UE, SEAF, AUSF, ARPF and Unified Data Management (UDM). The SEAF is located in the SN whereas AUSF, ARPF and UDM are in

TABLE II
NOTATIONS AND DESCRIPTION

Notation / Messages	Description
HNid	MMC,MNC MSIN
SNN	Service code:5G‖SNId
Ki (key K)	Symmetric key (UE, HN), Pre Shared key (PSK)
RAND	Random nonce challenge
SUPI	(MMC,MNC,MSIN)
SUCI	(MMC,MNC,enc(MSIN))
AUTN	(SQNHN ⊕ AK,MAC,AMF)
MAC,XMAC	f1(K, (SQNHN, Rand, AMF))
RES, XRES	f2(K, Rand)
RES*,XRES*	KDF((CK, IK),SNN, (Rand, RES /XRES))
CK	f3(K, Rand)
IK	f4(K, Rand)
AK	f5(K, Rand)
HXRES* / HRES*	SHA256(Rand, XRES*/ RES*) one-hash function
AMF*	Authentication management field 0-1
KAUSF	KDF((CK, IK), (SNN, SQN ⊕ AK))
KSEAF	KDF(KAUSF, SNN)
SQN	Sequence Number = (SQN ⊕ AK) ⊕ AK
SQNUE	UE SQN
SQNHN	HN SQN
MACS	f 1* (AMF, RAND, K, SQNUE)
AK*	f 5* (K, Rand)
AUTS	(SQNUE ⊕ AK) ‖ MACS

the HN as shown in figure 1. They also introduced SUPI, a UE identifier, SUPI is encrypted as Subscription Concealed Identifier (SUCI) while in transit for confidentiality and only decrypted by the HN. The key K acts as the primary source of security context. The key derivation [1] involves the UE and other entities, includes key K, cipher key (CK) and integrity key (IK) that are used to derive other keys such as KAUSF and KSEAF as illustrated in Table II.

IV. Modelling of 5G-AKA Protocol

We model the 5G-AKA protocol using four entities (UE, SEAF, AUSF, ARPF) for model A and with three entities (UE, SN, HN) for model B. The four entities modelling is significant for the calculation of HXRES and verification of RES as performed by AUSF and AUTS re-synchronization due to RAND that is exchanged between AUSF and ARPF. The value RES has been split up into halves to enable backwards compatibility. When SEAF receives RES, it can only verify the first half, because the AV contains only XRES*. However, HN can verify both RES and RES*. The AV includes RAND, AUTN to prove the challenge's freshness and authenticity while XRES* is the expected response. We consider two types of channels; (a) UE-SEAF (unsecure) and SEAF-AUSF-ARPF (secure); (b) UE-SEAF (unsecure) and SEAF-AUSF-ARPF (unsecure) and in b the channel between SN and HN channel is compromised [21], [22]. We fully model the MAC failure and sync failure message for re-synchronization.

A. Threat Model

Our threat model assumes a DY adversary in [23], the DY controls the network, can read, intercept, modify and send messages. It is also capable of initiating passive and active attacks such as eavesdropping, manipulation, interception and injection of messages. The DY can listen to signalling messages and set up a fake BS to impersonate SNs. It can also compromise secure entities such as USIM and other entities. Furthermore, the adversary can apply hashing, encryption and sign on values that are known to the attacker.

B. Security Assumption

Most assumptions are based on the specifications in [1], [24]. While the wireless channel between the UE and SN is vulnerable to both passive and active attacks. The wired channel between SN and HN is only vulnerable to the same attacks if it compromised. It is assumed functions f1, f1*, f2 provide integrity as MAC and f3, f4, f5, f5* provide integrity and confidentiality as CK, IK and AK keys respectively [24]. We also assume that the entities that run the diameter protocol or the protocol itself [21], [22] can be compromised through sophisticated cyber and virtualization related attacks. We also have to consider that the attacker may have genuine USIMs then end up compromising the UE. Initially it is assumed that key K, SUPI and SQN stored on non-compromised entities.

The desired security properties for 5G-AKA protocol are confidentiality, integrity, authenticity and privacy as specified in [1]. The security properties are informally defined, we adopt the taxonomies in [25] and [26] for precise formal analysis, referred to as set 1 and set 2 respectively in this paper.

C. Informal Analysis of 5G-AKA Protocol

The diameter base protocol is still at risk to several attacks such as man in a middle (MITM) and malware that can be used to initiate further attacks [28]. While the trust enhancement in 5G is due to attacks like routing attacks [21] and impersonation of network nodes [22]. Encryption is enabled in diameter but in practice MNO internetwork security is built on trust. Therefore, we agree with [4], [5], [6] that because the 3GPP defines the general properties of authentication which rests on successful procedures, it is very challenging, cannot all be assessed at once.

D. Protocol Messages Exchange

To illustrate the full execution of the 5G-AKA protocol, we use model A and concisely omit some of text of the message exchange, 5G-AKA consists of three phases:

Phase 1: The Authentication Initiation and Method Selection
The SEAF in SN initiates authentication with the UE that wants to connect to it. Then UE sends msg 1, an authentication request which includes SUCI.

```
Msg1. UE → SEAF: SUCI
Msg2. SEAF → AUSF:SUCI ‖ SNN
Msg3. AUSF→ ARPF: SUCI‖ SNN
```

In msg2, SEAF adds its SNN, when the UDM/ARPF receives msg3 it retrieves SUPI.

Phase 2: The Protocol

```
Msg4. ARPF → AUSF:(RAND,AUTN, XRES*,KAUSF,
SUPI)
Msg5. AUSF→ SEAF: (RAND, AUTN, HXRES*)
```

```
Msg6. SEAF → UE: (RAND ‖ (AUTN)
Msg7. UE → SEAF : RES*
Msg8.SEAF → AUSF: RES*
Msg9. AUSF→ SEAF: SUPI ‖  KSEAF
```

After retrieving SUPI, ARPF generates AV with AMF. The ARPF sends AV in msg4 to the AUSF indicating 5G-AKA is to be used. The AUSF receives msg4 and computes HXRES*. The AUSF stores XRES*, SUPI and KAUSF, derives KSEAF from KAUSF, replaces XRES and KAUSF with HRES and KSEAF respectively and send msg5 with AV to SEAF. When SEAF receives msg5 it stores HXRES* and send RAND and AUTN in msg6 to UE. When UE received msg6, the USIM verifies the AV freshness by checking if the AUTN can be accepted. First computes AK and retrieves the SQN. Then computes XMAC, checks if xMAC = MAC and checks if the SQN is SQNUE ¡ xSQNHN. If they are the expected response, USIM computes RES and then computes CK and IK. The USIM sends RES, CK and IK to the UE. The UE computes RES* from RES calculates KAUSF from CK and IK then KSEAF from KAUSF and checks that the separate bit of AMF* in AUTN is set to 1. UE returns RES* in msg7 to prove its identity and the ownership of K implicitly. SEAF calculates HRES*, after receiving msg7 and checks that it matches with the HXRES* value. If HXRES = HRES, SEAF considers the authentication a success. The SEAF sends msg8 containing the RES to the AUSF. If HRES $\neq$ HXRES then it aborts the process. AUSF shall compare RES* with XRES*. If RES* = XRES*, the AUSF considers the authentication a success. Then AUSF sends KSEAF and SUPI to SEAF in msg9.

Phase 3: Re-synchronization

In Msg6, if the verification of the AUTN to UE fails, then the USIM indicates reason whether it is MAC or synchronization failure.

```
Msg10.UE → SEAF:(mac_failure,
Synch_failure,AUTS)
Msg11.SEAF → AUSF:(Synch_failure,AUTS)
Msg12.AUSF → ARPF:(Synch_failure, AUTS,
Rand)
```

The UE sends msg10 to SEAF with MAC and synch failure messages with AUTS. When SEAF receives msg10, it may request re-identification from UE in case of mac_failure or initiate new authentication in case of sync_failure then SEAF sends msg11 to AUSF. The AUSF sends msg12 to the ARPF, with the RAND sent in msg4 and AUTS received in msg11. The ARPF retrieves SQNUE from AUTS, checks if SQNUE is in the correct range and whether the next SQN generated using SQNHN would be accepted. If SQNHN is in the correct range, the UDM/ARPF generates new AV, otherwise it verifies AUTS. If the verification is successful, the ARPF resets the value of the counter SQNHN to SQNUE. Then ARPF sends new AV to AUSF for the UE. Where by the AUSF processes a new authentication procedure with the UE but this out of scope of this paper.

V. Verification of the 5G-AKA Protocol

A. *Formal Verification using ProVerif*

The modelling of a protocol in ProVerif is composed of declaration, process macros and main processes. For the XOR translation problem for horn theories, the equation `xor(m1,xor(m1,m2)) = m2` is used. The queries are carried out to rectify the correctness and secrecy of a protocol. The ProVerif code is used to specify the protocol concisely using declaration of types, functions, queries and events such as:

```
processUE, free pubChannel :channel,
type key, fun f2(key, nonce): bitstring,
free Secret:bitstring[private]
query attacker(S),
query x1:id,x2:id,x3:key;
event (endUE(x1, x2, x3)) ==>
event (begUE(x1, x2, x3)).
```

B. *Formal Analysis of the 5G-AKA Protocol*

We simulated the protocol using two models:

- Model A the four parties' protocol (UE-SEAF-AUSF-ARPF)
  ```
  ((!processUE(supi,hnid_ue,ki))
  (!processSEAF(snn_sn))
  (!processAUSF)
  (!processARPF(supi,ki,amf)))
  ```
- Model B the three parties' protocol (UE-SN-HN)
  ```
  ((!processUE(supi,hnid_ue,ki))
  (!processSN(snn_sn))
  (!processHN(supi,ki,amf)))
  ```

For the deep analysis we focus on model A, since most related work based their arguments on model similar to model B. When we run the protocol on the compromised public channel, we found an attack whereby the authentication doesn't hold as assumed by the related work. The attack occurred on both model A and model B.

ProVerif Results Out of Model A:

The secrecy of the secret, supi,ki, kseaf holds, authentication of UE to SN holds but authentication of SN to UE does not hold on both non-injective and injective agreements.

```
/proverif protocols/5G_AKA_4ent_pub.pv |
grep RES
RESULT not attacker(Secret[]) is true.
RESULT not attacker(supi[]) is true.
RESULT not attacker(ki[]) is true.
RESULT not attacker(kseaf[]) is true.
RESULT event(endUE(x1,x2,x3)) ==>
event(begUE(x1,x2,x3)) is true.
RESULT event(endSN(x1_80)) ==>
event(begSN(x1_80)) is false.
RESULT inj-event(endUE(x1_81,x2_82,x3_83))
==> inj-event(begUE(x1_81,x2_82,x3_83))
is true.
RESULT inj-event(endSN(x1_84)) ==>
```

TABLE III
SECURITY ANALYSIS OF SET 1 PROPERTIES

Properties	UE -SN	SN-UE	UE-HN	HN-UE
Secrecy	H	H	H	H
Aliveness	H	X	H	H
Weak Agreement	H	X	H	H
Non-Injective Agreement	H	H	H	H
Injective Agreement	H	X	H	H

```
(inj-event(begSN(x1_84)) && (inj-event
(e3(x1_84)) ==>
(inj-event(e2(x1_84)) ==>
inj-event(e1(x1_84,x2_85))))) is false.
RESULT (even event(endSN(x1_5702)) ==>
(event(begSN(x1_5702)) &&
event(e3(x1_5702))) is false.)
```

The event endSN means that the SN has completed the protocol, the UE received msg4 and sent msg5, e1 means that the SN sent msg4. These events take as arguments all parameters of the protocol; the AUTN and RAND, except e2 which has to check if `xsqn xor (xored_sqn, ak)`, `xmac = f1((xsqn, xrand), ki)` and if `xmac =mac` then if `xsqn = sqn_ue`. If the arguments are true then RES is sent otherwise it sends MAC_failure or synch_failure. The direct proof of correspondence fails in ProVerif because msg4 can be replayed, yielding several e2 for a single e1. We prove the correspondence and conclude the desired correspondence by noticing that event e2 which has RES as argument cannot be executed before AUTN and RAND have been sent and before e1 has been executed, Which fails in ProVerif with false.

VI. SECURITY ANALYSIS

A. Protocol Security Analysis

In addition, with the discovered attack in this paper, 5G-AKA protocol's long-term Key K might be leaked due to eavesdropping on communication channel or hacking of the USIM card. This vulnerability would allow an attacker to masquerade another user in a roaming mode to a SN. Hence allowing the attacker to bill legitimate users with expensive access and phone calls charges [4]. The analysis of the protocol is based on security requirements in sets 1 and 2, Table 3 show the analysis of set 1.

The Analysis using security properties of Set 2:

- Mutual Entity Authentication: The UE is authenticated to the SN if `RES = HRES` and to HN if `RES = XRES`. Since the SNN includes the SNid this enforces weak agreement and implicit authentication from HN after a successful authentication and KSEAF confirmation. In addition, when SUPI and SNN are sent to the HN, proved to hold and they enforced this requirement. Moreover, the creation of SNN, links the UE to SEAF and SEAF to AUSF. However, the SN to UE authentication fails to hold.
- Mutual Key Authentication: Since the authentication between UE and HN is based on secrecy of KSEAF, it also gets implicitly authenticated by including KAUSF and SNN in its derivation parameters.
- Mutual Key Confirmation: The successful AKA roundtrip between the UE, SN and HN ending with KSEAF confirmation enforces this requirement.
- Key Freshness: ProVerif has no function to check key freshness however during the authentication process the UE checks the validity of the AV data and freshness of SQN, checks if `xSQN > SQNUE` which also facilitates the derivation of KSEAF. In 5G, KSEAF from previous session cannot be reused in new session as every KSEAF is linked to particular session and SN by SQN and SNN respectively. And since the secrecy of KSEAF is not violated, it implies the key is fresh.
- Unknown-Key Share: The reachability property in ProVerif is used to check aliveness. The entities ID and Key binding prevents this attack. The inclusion of SUPI in the authentication process and the SNN in the KDF of KSEAF links it to SN and since it is derived from the key K that is preshared between UE and HN proves this requirement. Also, the KSEAF is only sent to SEAF after the RES* verification by AUSF.
- Key Compromise Impersonation Resilience: Since the KSEAF is derived from key K and both their secrecy holds hence it enforces this requirement. 5G ensures that knowing KSEAF from a certain session is not enough to deduce KSEAF that has been generated in old session or that will be established in a new session. Backward secrecy and Perfect Forward Secrecy (PFS) on key K are possible. KSEAF established in a particular session remains a secret even when the KSEAF keys established in all other sessions[5] are known to the adversary. However that PFS and Post Compromise Secrecy (PCS) do not hold, if the key K is compromised [29], the adversary can compute feature and past keys as the secrecy of session key is accessed when long-term key material is compromised.

Moreover, the adversaries nowadays are more sophisticated and use adaptive techniques, these assumptions were ignored in related work or assumed that security mechanisms would protect diameter protocol, the channel and HN entities, so we assumed that even the secure network can be compromised in number of ways which creates a wider attack vector. Since the non-injective and injective agreement SN to UE fails to hold that indicates that replay attack is possible between SN and UE. The secure protocol results are shown below:

ProVerif Results for Model A:

```
/proverif protocols/5G_AKA_4ent_pubsec.pv|
grep RES
RESULT not attacker(Secret[]) is true.
RESULT not attacker(supi[]) is true.
RESULT not attacker(ki[]) is true.
RESULT not attacker(kseaf[]) is true.
RESULT event(endUE(x1,x2,x3)) ==>
event(begUE(x1,x2,x3)) is true.
```

```
RESULT event(endSN(x1_78)) ==>
event(begSN(x1_78)) is true.
RESULT inj-event(endUE(x1_79,x2_80,
x3_81)) ==>
inj-event(begUE(x1_79,x2_80,x3_81))
is true.
RESULT inj-event(endSN(x1_82)) ==>
(inj-event(begSN(x1_82)) && (inj-event
(e3(x1_82)) ==>
(inj-event(e2(x1_82)) ==>
inj-event(e1(x1_82,x2_83))))) is true.
```

B. Security Consideration

The UE's data privacy is put at risk if the standard is underspecified or if the USIM is compromised, KSEAF can be revealed using only K and the message with RAND and AUTN which has been sent from SEAF to UE in plain text. PFS can be achieved if a Diffie-Hellman (DH) key exchange is applied. DH is already being used by Elliptic Curve Integrated Encryption Scheme (ECIES) in the generation of the UE. Authentication based on the AUSF and KAUSF provides weaker security guarantees but an authentication process that involves the ARPF and the USIM as direct participant gives stronger guarantees.

Cryptographic techniques are not enough to address the SS7 and diameter vulnerabilities, it requires secure communication protocols and other measures such as a multi-layer security techniques that leverage the existing signaling transport points (STP) and adding signaling firewall functionalities for context-sensitive assessment on SS7 messages. Additionally, diameter sessions protection should also be enhanced. The 5G standard should be strengthened to prevent active attacks on the privacy properties by using encryption and randomness. The sequence and unlikability problem can be solved after the replayed message has made roundtrip to the HN. Even though the main security properties haven't been changed much, certain specifications have been updated since then. Therefore, this paper discussed some of the changes made in the recent revised version of the standard.

VII. Conclusion

We have formally analysed 5G-AKA protocol, identifying the security properties, a formal model of the protocol was illustrated as per revised 5G standard using two models. We conducted a formal security analysis using ProVerif and findings were given. The analysis was based on two security properties taxonomies which showed the properties that were violated when we changed the channel assumption from secure to unsecure channel. This is due the diameter sessions not being able to secure the channels hence making attacks possible. We concluded that 5G-AKA is still vulnerable to linkablity and replay attacks, with cyber attacks getting sophisticated we cannot just assume that communication channels are secure without accurately anticipating the adversary capabilities. The future work should consider the increasing sophistication of the adversaries and how the primary authentication affects services in other domains.

References

[1] 3GPP, "Security architecture; procedures for 5G system," 2019.

[2] 3GPP, "System architecture for the 5g system," 3rd Generation Partnership Project, Tech. Rep., 2018.

[3] B. Blanchet, "Automatic verification of correspondences for security protocols," *J. Comput. Secur.*, vol. 17, no. 4, p. 363?434, December 2009.

[4] M. Dehnel-Wild and C. Cremers, "Security vulnerability in 5G-aka draft."

[5] D. Basin, J. Dreier, L. Hirschi, S. Radomirović, R. Sasse, and V. Stettler, "A formal analysis of 5g authentication," 2018, iD: proquest2073641667.

[6] A. Koutsos, "The 5g-aka authentication protocol privacy," 2018, iD: proquest2135414227.

[7] L. Lamport, "The temporal logic of actions," *ACM Trans. Program. Lang. Syst.*, vol. 16, no. 3, p. 872–923, May 1994.

[8] C. Boyd and W. Mao, "On a limitation of ban logic." Berlin, Heidelberg: Springer-Verlag, 1994, p. 240–247.

[9] N. Kobeissi, K. Bhargavan, and B. Blanchet, "Automated verification for secure messaging protocols and their implementations: A symbolic and computational $approach,'' pp.435--450, 2017, iD : ieee_s7961995.$

[10] M. Aiash, "A formally verified initial authentication and key agreement protocol in heterogeneous environments using casper/fdr," 2013.

[11] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Drielsma, P. C. Heam, O. Kouchnarenko, J. Mantovani, S. Modersheim, D. V. Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Vigano, and L. Vigneron, "The avispa tool for the automated validation of internet security protocols and applications," *Computer Aided Verification, Proceedings*, vol. 3576, pp. 281–285, 2005, iD: wos000230755800027.

[12] S. Meier, B. Schmidt, C. Cremers, and D. Basin, "The tamarin prover for the symbolic analysis of security protocols," vol. 8044. Springer, 2013, pp. 696–701.

[13] B. Blanchet, "Modeling and verifying security protocols with the applied pi calculus and proverif," *Found. Trends Priv. Secur.*, vol. 1, no. 1-2, p. 1–135, October 2016.

[14] R. Kusters and T. Truderung, "Using proverif to analyze protocols with $diffie-hellmanexponentiation,'' pp.157--171, 2009, iD : ieee_s5230620.$

[15] M. D. Ryan and B. Smyth, "Applied pi calculus," 2011.

[16] C. Tang, D. A. Naumann, and S. Wetzel, "Analysis of authentication and key establishment in inter-generational mobile telephony," pp. 1605–1614, 2013, $iD : ieee_s6832108.$

[17] G. L. Adversarial Testing of, "Lteinspector: A systematic approach for," 2018.

[18] M. Arapinis, E. Ritter, and M. Ryan, "Formal analysis of umts privacy," 2011, iD: proquest2086863476.

[19] 3GPP, "System architecture evolution (sae)security architecture," Technical Specification Group Services and System Aspects, Tech. Rep., 2017.

[20] 3GPP, "Study on the security aspects of the next generation system," Technical Specification Group Services and System Aspects, Tech. Rep., 2017.

[21] T. Engel, "Ss7: Locate. track. manipulate," 2014.

[22] G. RIFS, "Diameter roaming security - proposed permanent reference document," GSMA, Tech. Rep., 2016.

[23] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 30, no. 2, pp. 198–208, 1983, iD: $gale_ofa564876.$

[24] 3GPP, "3g security; security architecture," *Technical Specification Group Services and System Aspects*, 2018.

[25] G. Lowe, "A hierarchy of authentication specifications," pp. 31–43, 1997, $iD : ieee_s596782.$

[26] A. J. A. Menezes, P. C. V. Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. Boca Raton, Fla. ;: CRC, 2001, includes bibliographical references and index.; ID: alma991001301199704781.

[27] T. Q. Thanh, Y. Rebahi, and T. Magedanz, "A diameter based security framework for mobile networks," pp. 7–12, 2014, iD: 1.

[28] Enisa, "Signalling security in telecom ss7/diameter/5g," 2018.

[29] K. Cohn-Gordon, C. Cremers, and L. Garratt, "On post-compromise security," $pp.164 - -178, 2016, iD : ieee_s7536374.$