To Trust or Not to Trust: Data Origin Authentication for Group Communication in 5G Networks

Robert Annessi*
Institute of Telecommunications, TU Wien
Vienna, Austria
robert.annessi@nt.tuwien.ac.at

Joachim Fabini
Institute of Telecommunications, TU Wien
Vienna, Austria
joachim.fabini@tuwien.ac.at

Tanja Zseby
Institute of Telecommunications, TU Wien
Vienna, Austria
tanja.zseby@tuwien.ac.at

ABSTRACT

With the expected massive increase in high-bandwidth applications over 5G cellular networks, the efficient use of radio-network and core-network infrastructures becomes essential. Group communication is a method for transmitting data efficiently from one source to many receivers. In this paper we study the security provided in terms of authenticity and integrity for group communication in 5G networks. We identify that the current security solutions involve trusting the benignity and operational security of network operators as well as its users since the current security solutions do not provide data origin authentication. Based on this insight, we present two attack scenarios in which an adversary exploits the provided level of authenticity such that arbitrary data can be injected maliciously while receivers consider the data as if they were sent by the claimed source. We evaluate potential approaches to provide data origin authentication in 5G and show that future research is required for a general solution.

ACM Reference Format:
Robert Annessi, Joachim Fabini, and Tanja Zseby. 2018. To Trust or Not to Trust: Data Origin Authentication for Group Communication in 5G Networks. In *ARES 2018: International Conference on Availability, Reliability and Security, August 27–30, 2018, Hamburg, Germany*. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3230833.3233252

1 INTRODUCTION

From a sender-receiver multiplicity point of view one can categorize communication methods into four classes: unicast, anycast, broadcast, and multicast. Unicast denotes communication between one sender and one receiver, anycast the communication between one sender and the closest member of a group of receivers. Broadcast and multicast both convey data from one sender to a group of receivers. Broadcast targets all receivers – the group being potentially limited by physical constraints like network size or radio reception area – whereas multicast addresses a group of receivers that have explicitly joined a group, expressing their intent to receive the message. *Group communication* refers to both broadcast and multicast communication.

Unicast communication is only efficient when receivers consume different content at different times such as video on-demand but does not scale well when many receivers consume the same content at the same time such as a live video streaming. Whenever communications conform to such simultaneity constraints, group communication provides a method for transmitting data efficiently from one source to possibly many receivers without running into scalability issues. With the increasing use of high-bandwidth applications over cellular networks it will be essential to use the available resources efficiently in 5G networks. Therefore, group communication becomes necessary in order to distribute data to groups of receivers without unnecessary data duplication and transmission.

The demand for group communication services over cellular networks is rapidly increasing and this trend is expected to continue for 5G networks. Group communication services in 5G networks can be classified either as human-oriented (1) or as machine-oriented (2). Human-oriented services (1) are enhanced TV-services, for example, such as (high-definition) audio and video downloading, streaming, and distribution, news or advertising services that can be enhanced by grouping users based on their interest, preferences, or other characteristics. Other human-oriented services include location-based services range from augmented reality services that allow users to receive additional information from the surrounding environment such as for visitors in a city, or public safety services such as Mission Critical Push to Talk (MCPTT) used by police officers, fire fighters, or train operation personnel [1], or disaster recovery where users receive emergency information. Considering the huge number of connected sensors and machines expected over 5G networks, machine-oriented services (2) such as smart homes, smart industrial plants, intelligent transportation systems, or software updates also become apparent [2].

Group communication involves many issues stemming from its unidirectional nature. Some of these issues such as guaranteeing the reliable delivery of data can be solved easier on higher abstraction layers. Other issues such as efficient and secure authentication of the source tend to reoccur, no matter on which abstraction layer group communication functionality is implemented. In this paper, we address the security of group communication services in 5G networks in terms of authenticity and integrity. Guaranteeing high levels of security is crucial to the successful deployment and future use of 5G networks – not only because network operators are concerned about attacks harming their reputation

*Corresponding author.

ARES 2018, Hamburg, Germany

ACM ISBN 978-1-4503-6448-5/18/08…$15.00
https://doi.org/10.1145/3230833.3233252

and revenue but also because impersonations of group communication services may lead anywhere from inconveniences to catastrophic results, depending on the specific service attacked. Security measures for group communication services are essential and become more important as industry and critical infrastructures increasingly depend on cellular networks and future 5G infrastructures. The aim of this paper is to study whether group communication services in 5G networks are appropriately secured in terms of authenticity and integrity and to evaluate data origin authentication schemes to improve security for group communication in 5G networks.

2 BACKGROUND

2.1 Group Authentication vs. Data Origin Authentication

Receivers can assure that datagrams have been, indeed, sent by a legitimate source by using cryptographic methods. For group communication, two types of authentication have to be distinguished: group authentication and data origin authentication.

Group Authentication assures that data originates from a legitimate but unidentified group member and has not been modified by entities outside of the group. Message Authentication Codes (MACs) with a key shared by all group members are a well understood and efficient method for achieving group authentication. Nevertheless, receivers cannot distinguish between the individual group members sharing the key and therefore do not know the exact identity of the source as any group member could have generated a MAC. This is of particular importance in group communication since there are usually many receivers involved, and a single dishonest or compromised receiver is sufficient to impersonate the source. Besides this security issue, MACs are rather inefficient in group communication as the shared key needs to be renewed and redistributed every time a receiver joins or leaves.

For data origin authentication, an asymmetric cryptographic method is required that allows receivers to verify the authenticity (of datagrams) without providing means to generate valid authentication information themselves on behalf of the source. In asymmetric cryptography, keys consist of two parts: a public key shared with all receivers and a secret key that is kept private by the source. Table 1 summarizes the security properties provided by group authentication and by data origin authentication.

Table 1: Group authentication vs. data origin authentication

Security Property	Group Authentication	Data Origin Authentication
Integrity	✓	✓
Non-repudiation	✗	✓
Authenticity	Group	Source

Digital signature schemes provide data origin authentication. However, the main downside of today's digital signature schemes, such as RSA, DSA, and ECDSA, is that they come at high computational cost and, therefore, introduce substantial penalty in terms of delay, both in the source and in the receiver. Consequently, it is widely believed that digital signatures are roughly 2 to 3 magnitudes slower than MACs [3] so that signing each datagram is not a practical solution. In Section 4, we will highlight that this assumption needs to be revised as recently proposed high-performance digital signature schemes could build the foundation for data origin authentication for group communication.

2.2 Security Measures Related to Group Communication in 5G

In cellular networks, User Equipment (UE) devices such as mobile phones or mobile networked devices that perform their action without human assistance (i.e., machines) are connected to Evolved Node Bs (eNBs) over a radio network. eNBs are enhanced base stations that incorporate all radio interface related functions. eNBs receive data over the core network from the Broadcast Multicast - Service Centre (BM-SC), which practically acts as source of the group communication data. The BM-SC receives the data from the actual content provider over a unicast link. The communications between the BM-SC and the eNBs as well as between the eNB and the UEs are conducted over multicast or broadcast interfaces. Fig. 1 on the next page depicts group communication services over 5G and the related security measures. In the following, we will briefly describe these security measures.

2.2.1 Content Provider to BM-SC. The link between content provider and BM-SC usually is unicast and therefore out of the scope of this paper. Conventional security measures such as IPsec can provide integrity, authenticity, and confidentiality and therefore appropriate security for this link.

2.2.2 BM-SC to eNB. The communication between BM-SC and eNB can be secured with IPsec as long as it is conducted over a unicast link. IPsec security in terms of authenticity, integrity, and (optionally) confidentiality is mandatory between the edges of networks operated by distinct administrative authorities. This architecture basically provides a hop-by-hop security approach in which securing the communication is optional within a network (according to the standard) [4]. It needs to be stressed that IPsec can only secure unicast links[1]. For group communication, the security entirely depends on the group communication specific security measures (described in Section 2.2.4).

2.2.3 eNB to UE. The integrity of the communication from eNBs to UEs is commonly protected in terms of integrity, confidentiality, and authenticity. This protection between eNB and UE is achieved as data is scrambled with UE-specific keys such that only the UE can decode the data [6]. However, this protection is only provided for unicast but not for group communication [7]. For this reason, the security of the communication entirely depends on the group communication specific security measures (described next).

2.2.4 Group Communication Specific Security Measures. Datagrams sent from the BM-SC to UEs should be protected from eavesdroppers that are not allowed to receive the data as well as from adversaries that aim to modify or inject datagrams maliciously. Since

[1]Unless Group Domain of Interpretation (GDOI) [5] is used, which itself can only provide group authentication but no data origin authentication nonetheless.

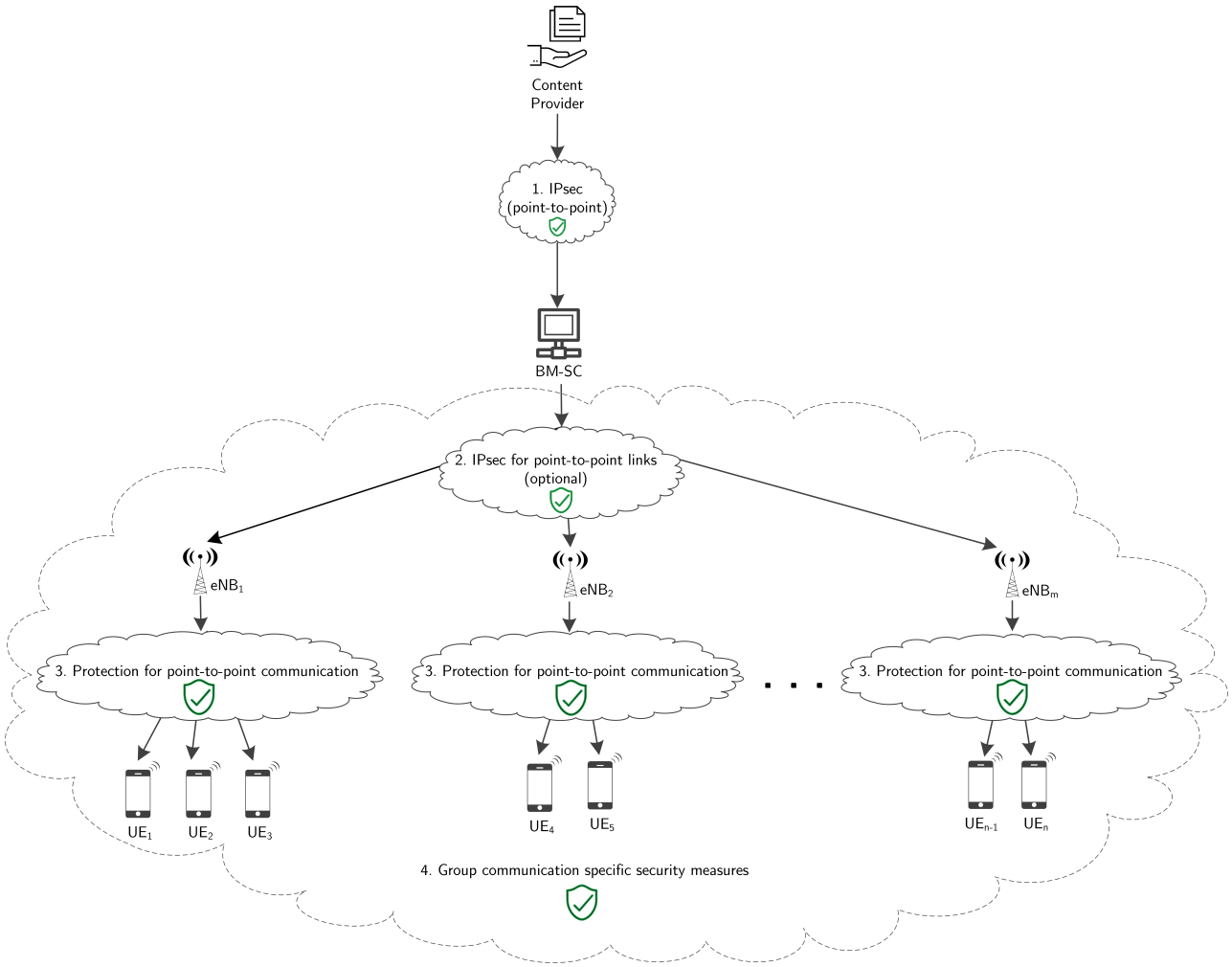

Figure 1: Security measures related to group communication in 5G.

the conventional security measures outlined before in this section cannot provide end-to-end security for group communication from the BM-SC to the UEs, additional end-to-end protection methods were introduced both for Multimedia Broadcast/Multicast Service (MBMS) and for Single Cell-Point To Multipoint (SC-PTM)[2]. These protection methods were designed to provide end-to-end integrity, authenticity, and confidentiality for group communication. The group communication specific security measures included in MBMS and SC-PTM differ but do have in common that they employ a symmetric group key to secure communications[3]. The group keys are shared between the BM-SC and every UE that has access to the particular group communication service.

As highlighted in the beginning of this section, security measures based on symmetric keys can only provide group authentication, and therefore neither MBMS nor SC-PTM provide data origin authentication. This shortcoming of the group communication specific security measures in MBMS and SC-PTM together with the conventional security measures that are not applicable to group communication become important in the attack scenarios presented in the next section (when the security and benignity of the network operator cannot be trusted).

3 ATTACK SCENARIOS

As pointed out before, group communication comprises unique security challenges compared to unicast communication, specifically with regard to authenticity and integrity. In this section, we present two attack scenarios to group communication services in 5G, which are facilitated because only group authentication and not data origin authentication is provided by the current group communication specific security measures. We focus on the major threat of impersonating the group communication service through

[2]MBMS [7] and SC-PTM [1] are radio access methods that provide group communication functionality. SC-PTM is optimized for mid-size groups while MBMS is optimized for large groups. In this way, both methods are complementary.
[3]In case of MBMS the symmetric group key is called MBMS Traffic Key (MTK), and for SC-PTM it is called Radio Network Temporary Identifier (RNTI).

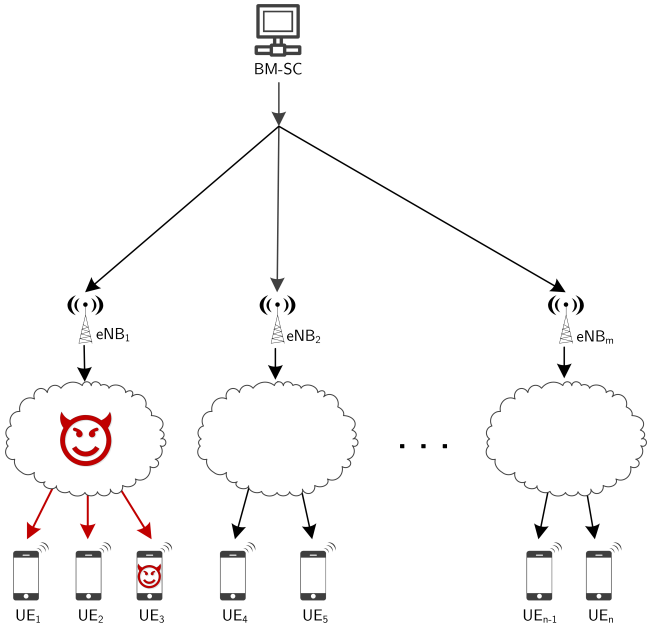

Figure 2: First (short-range) attack scenario on group communication services due to the lack of data origin authentication.

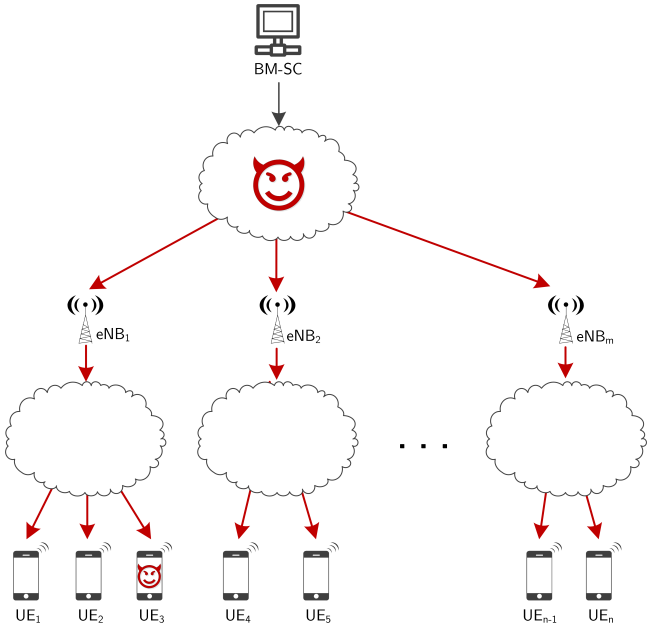

Figure 3: Second (long-range) attack scenario on group communication services due to the lack of data origin authentication.

injection or modification of datagrams although less severe Denial of Service (DoS) attacks can be equally conducted by the adversary[4].

Fig. 2 and 3 depict the attack scenarios. For both attack scenarios, we assume that the adversary knows the shared group key (MTK or RNTI for MBMS and SC-PTM respectively). The adversary can get knowledge of the group key through a collaborating UE, by operating a legitimate UE, or by compromising a UE. The assumption that the adversary is in possession of the group key is reasonable especially in the case of group communication because the more UEs exist the more likely it is that at least one gets compromised, collaborates with, or is operated by the adversary. In our specific example (Fig. 2 and 3), it is UE_3 that (deliberately or not) cooperates with the adversary but it could equally be any of the other UEs that are subscribed to the group communication service.

For the first attack scenario (Fig. 2), the adversary only needs additional access to the air interface in order to inject arbitrary data maliciously, which will be received by all UEs in range as authentic since the adversary knows the correct group key. The adversary can get access to the air interface through the collaborating or compromised UE, by operating a UE, or by compromising the specific eNB. The potential impact of the attack highly depends on the specific group communication service and the content of the injected data and can be anywhere between inconvenient and catastrophic. Unless the attack is concerted in a distributed fashion on multiple locations, the attack is physically limited to the UEs within range.

[4]The adversary can, for example, inject a single datagram (that is considered authentic by the receivers) that includes the maximum possible sequence number such that UEs will discard any other future datagrams for that service from the legitimate source.

In the second attack scenario (Fig. 3), the adversary also needs additional access to the communication medium between the BM-SC and the eNBs (instead of access to the air interface needed in the first attack). The communication medium may be accessed through an individual network access that was not properly secured or through a compromised network device, for example. This time, however, the adversary needs to break additional security measures.

There can be three kinds of additional security measures: (1) there may not exist additional security at all if unicast communication is used between the BM-SC and the eNBs and all operate in the same network. In this case all preconditions are fulfilled, meaning that the attacker does not need to circumvent any additional security measures to gain access. (2) If group communication is used between the BM-SC and the eNBs, they use the group communication specific security measures (as described in Section 2.2.4). For this reason, the security measures again fall short of providing a decent level of authentication if the attacker gets access to the group key shared between the BM-SC and the eNBs. In this case, the attacker needs to compromise an eNB, which is likely significantly harder than compromising (or operating) a UE but, on the other hand, the attack also has significantly more impact, which may justify this additional effort. (3) The communication between BM-SC and eNB consists of multiple unicast links that are secured with IPsec. Then, the attacker would need to break IPsec, which is commonly considered unfeasible. For this reason, mandatory IPsec-secured unicast links between BM-SC and eNBs can be considered an interim solution. The downside, however, is that the communication between BM-SC and eNBs is rather inefficient then in terms of computational and communication overhead. In any case, the impact of the

second attack is significantly larger than that of the first attack scenario since the data is propagated from the BM-SC via the eNBs to UEs, and therefore every single UE that is subscribed to the service may receive the maliciously injected data.

To counter both attack scenarios, conventional security measures are apparently inadequate. Data origin authentication is required in order to allow the BM-SC to secure the data without giving the UEs means to construct valid authentication information on behalf of the BM-SC. Each UE can then verify the authenticity of the data without having the necessity to trust the benignity as well as the operational security of the network operators and its users. Given the trend on attacks on critical infrastructures and its users, we argue that requiring trust into users and networking infrastructures is no longer appropriate nor acceptable today.

4 DATA ORIGIN AUTHENTICATION APPROACHES FOR GROUP COMMUNICATION IN 5G NETWORKS

Data origin authentication schemes for group communication have matured for more than 25 years, and many ideas were proposed to solve this challenging problem. None of the proposed schemes, however, satisfies all constraints and requirements of applications so that naming a single superior scheme seems non-trivial. In the sheer number of data origin authentication schemes that have been proposed for group communication, we identified three conceptional distinct approaches [9]. The first approach aims to extend symmetric schemes to data origin authentication. The other two approaches aim to overcome the computational intensive nature of public-key based authentication schemes: reducing the cost of conventional signatures schemes and designing fast authentication schemes.

Challal, Bettahar, and Bouabdallah identified six distinct classes of data origin authentication schemes [8]: deferred signing[5], signature propagation, signature dispersal, secret-information asymmetry, time-based asymmetry, and hybrid asymmetry. In addition to these six classes, a new class was suggested – high-speed signing – where recently proposed high-speed signature schemes are employed [9]. Table 2 shows all seven classes assigned to the three approaches we identified. This table also briefly includes our evaluation results of data origin authentication schemes with regard to their suitability to secure group communication in 5G networks. In this section, we briefly introduce all classes of data origin authentication schemes, show that each class comprises a trade-off from a specific point of view, and discuss their potential to secure group communication in 5G networks.

4.1 Extending Symmetric Schemes for Data Origin Authentication

4.1.1 Secret-Information Asymmetry. With secret-information asymmetry schemes, such as k-MAC [10], the source shares a set of keys with receivers instead of a single key. The source knows the entire set of keys and can generate valid authentication information but each receiver's partial view allows just to verify (but not to generate) generally valid authentication information. The k-MAC scheme uses different keys to calculate receiver-specific MACs. Then, all MACs together are appended to every datagram. Upon reception of a datagram, each receiver can verify one MAC but cannot create valid authentication information on behalf of the source as the other keys are unknown. Nevertheless, secret-information asymmetry schemes require substantial computational resources for verification (and for signing) and introduce significant communication overhead, which makes them unsuitable for 5G applications that involve low-power devices.

[5]Challal, Bettahar, and Bouabdallah used the term differed signing in their publication [8]. Based on the method description and context we presume a spelling error and argue that deferred signing is the correct term to be used for this method.

4.2 Reducing the Cost of Conventional Signature Schemes

4.2.1 Deferred Signing. With schemes from the deferred signing class, such as offline/online signing [11], the signing process is split into two steps: a slow offline and a fast online step. In the online step, each datagram is signed using a one-time signature scheme, which is computationally very efficient. To ensure that the one-time keys originate from the claimed source, a (conventional) digital signature scheme with a certified public key is used in the offline step to sign every one-time key. The generation and signing of the one-time keys is independent of the actual datagram to be signed and therefore can be conducted (offline) in advance. High performance in the online signing part can be achieved because datagrams are signed with a computationally very efficient one-time signature scheme, and the computationally expensive part (precomputing and signing the one-time keys) is conducted offline. However, the computational effort required in the offline part at the source is substantial, and the communication overhead is large because of the one-time signature's size. Nevertheless, the deferred signing class could suite the group communication scenario in 5G in case the computational resources at the receivers should be reduced even at the expense of increased communication overhead.

4.2.2 Signature Propagation. Schemes in the signature propagation class, such as Receiver driven Layered Hash-chaining (RLH) [12], follow another approach to reduce the cost of conventional signatures. Instead of signing each datagram individually, a signature from a (conventional) digital signature scheme is appended to only one datagram, the signature datagram. Hashes of non-signature datagrams are included in preceding datagrams so that a chain of datagrams is built where each datagram carries the hash of the subsequent datagram. In this way, the digital signature propagates through all datagrams so that its computational cost is amortized as hash operations are computationally inexpensive. Signature propagation schemes rely on the successful reception of signature datagrams and are, therefore, hardly resistant to the loss of datagrams, which makes this class of schemes unsuitable for group communication services in 5G networks.

4.2.3 Signature Dispersal. The basic idea behind signature dispersal schemes, such as [13], is that datagrams are divided into fixed-size blocks, and each block is signed independently with a digital signature. The signature of a block is split and appended to the datagrams within the block. Additional information is added to each datagram to help receivers reconstruct the signature even if some datagrams were lost. In this way, signature dispersal schemes

Table 2: Evaluation of Data Origin Authentication Approaches for 5G Networks

Approach	Class	Computational Efficiency	Low Communication Overhead	Resistant to Loss of Datagrams
Extend symmetric schemes to data origin authentication	Secret-information asymmetry	✗	✗	✓
Reduce the cost of conventional signature schemes	Deferred signing	~	✗	✓
	Signature propagation	✓	~	✗
	Signature dispersal	~	~	~
Design fast authentication schemes	Time-based asymmetry	✓	✓	✓
	Hybrid asymmetry	✓	~	✓
	High-speed signing	✓	✓	✓

improve resistance to the loss of datagrams compared to signature propagation schemes. Computational efficiency is reduced, however. While the signature dispersal class could be somewhat suitable to secure group communication services in 5G networks, the following approach - design fast authentication schemes - includes more promising classes of data origin authentication schemes.

4.3 Designing Faster Authentication Schemes

Compared to reducing the computational cost of digital signature schemes, a conceptionally different approach is designing fast authentication schemes. We distinguish three different classes that follow this approach: time-based asymmetry, hybrid asymmetry, and high-speed signing.

4.3.1 Time-based Asymmetry. In Timed Efficient Stream Loss-tolerant Authentication (TESLA) [14] and other time-based asymmetry schemes public and secret keys are identical - only separated through time. The keys are associated by a one-way chain so that only the initial key needs to be signed with a (certified) key from a conventional signature scheme and receivers can recover if some datagrams were lost. However, the clocks of the source and of receivers are assumed to be synchronized so that they can agree on which key is valid at a specific point in time. The accuracy of clock synchronization, therefore, becomes a security requirement. Since clock synchronization is already part of cellular networks, time-based asymmetry schemes may be well suitable for group communication in 5G networks – accuracy of clock synchronization becomes a security requirement then, however.

4.3.2 Hybrid Asymmetry. Schemes in the hybrid asymmetry class, such as Time Valid Hash to Obtain Random Subsets (TV-HORS) [15], aim to combine the strengths of secret-information asymmetry and time-based asymmetry approaches while mitigating their limitations. Hybrid asymmetry schemes are also computationally efficient but introduce an increased communication overhead. Although hybrid asymmetry schemes are potentially suitable to provide data origin authentication for group communication in 5G networks, they do not provide any specific advantages over time-based asymmetry schemes in this context.

4.3.3 High-Speed Signature Schemes. As mentioned in the beginning, signing each datagram individually is commonly perceived to be impractical due the computationally expensive nature of conventional signature schemes. Employing novel, high-performance signature schemes, however, mitigates that negative performance impact. For this purpose, signature schemes that offer previously unrivaled performance are required, such as Ed25519 [16], an elliptic-curve signature scheme *carefully engineered at several levels of design and implementation to achieve very high speed without compromising security* [16], or - as one example of multivariat signature schemes - MQQ-SIG [17], a signature scheme based on multivariate-quadratic quasigroups. Since many multivariate signature schemes have been broken, however, (some of them have been fixed and broken again), it is safe to say that the multivariate group involves serious security challenges. Nevertheless, a data origin authentication scheme based on a high-speed digital signature scheme seems very promising to secure group communication in 5G networks.

5 CONCLUSION

Group communication uses radio-network and core-network resources efficiently, which is essential in 5G networks as the use of group communication services is expected to increase massively. In this paper, we analyzed the security these group communication services can provide in the context of 5G, specifically integrity and authenticity. We highlighted the difference of group authentication and data origin authentication and showed that the current security solutions provide group authentication only - and not data origin authentication.

We presented two attack scenarios in which an adversary aims to inject or modify arbitrary data maliciously by exploiting the (low) level of authenticity provided by current group communication specific security solutions in 5G networks. In this way, the malicious data would be perceived as if they were sent by the claimed source. Depending on the specific group communication service and the data injected, results may be anywhere from inconvenient to catastrophic. Both attack scenarios are facilitated if only group authentication is provided and the implicitly assumed trust in the benignity and operational security of the network operators and its users is violated.

Data origin authentication prevents both attack scenarios as receivers cannot generate valid authentication information on behalf of the source but can still verify the authenticity of the data such that injected or modified data can be recognized as such. Data origin authentication schemes, however, are a research field on their own, and there is no single scheme that is generally applicable yet. One approach is most suitable to provide data origin authentication for group communication in 5G networks: designing fast authentication schemes. This approach of designing fast authentication schemes contains three distinct classes: time-based asymmetry, hybrid-asymmetry, and high-speed signing. Of these three classes, we argue that time-based asymmetry and high-speed signing are the most promising candidates to secure group communication in 5G networks. The deferred signing class might be used in addition to reduce the computational resources required at the receiver at the expense of a substantially increased communication overhead.

ACKNOWLEDGMENT

The content provider icon used in Fig. 1 was created by Creative Stall. The lock icon used in Fig. 1 was created by Green Store. The evil icon used in Fig. 2 and 3 was created by Freepik.

REFERENCES

[1] J. Kim, S. W. Choi, W. Y. Shin, Y. S. Song, and Y. K. Kim. Group communication over LTE: a radio access perspective. *Ieee communications magazine*, 54(4):16–23, Apr. 2016. ISSN: 0163-6804. DOI: 10.1109/MCOM.2016.7452261.

[2] G. Araniti, M. Condoluci, P. Scopelliti, A. Molinaro, and A. Iera. Multicasting over Emerging 5G Networks: Challenges and Perspectives. *Ieee network*, 31(2):80–89, Mar. 2017. ISSN: 0890-8044. DOI: 10.1109/MNET.2017.1600067NM.

[3] J. Katz. *Digital Signatures*. Springer US, Boston, MA, 2010. ISBN: 978-0-387-27711-0 978-0-387-27712-7.

[4] 3GPP. TS 33.210 Network Domain Security (NDS); IP network layer security, Rel. 14. Dec. 2016.

[5] B. Weis, S. Rowles, and T. Hardjono. The Group Domain of Interpretation. RFC 6407 (Proposed Standard). Internet Engineering Task Force, Oct. 2011. URL: http://www.ietf.org/rfc/rfc6407.txt.

[6] 3GPP. TS 33.401 3GPP System Architecture Evolution (SAE), Rel. 15. June 2017.

[7] 3GPP. TS 33.246 Security of Multimedia Broadcast/Multicast Service (MBMS), Rel. 14. Dec. 2016.

[8] Y. Challal, H. Bettahar, and A. Bouabdallah. A taxonomy of multicast data origin authentication: Issues and solutions. *IEEE Communications Surveys & Tutorials*, 6(3):34–57, 2004. ISSN: 1553-877X. DOI: 10.1109/COMST.2004.5342292.

[9] R. Annessi, T. Zseby, and J. Fabini. A new Direction for Research on Data Origin Authentication in Group Communication. In *To appear in: Proceedings of the 16th International Conference on Cryptology and Network Security*. In CANS '17, 2017.

[10] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas. Multicast Security: A Taxonomy and Some Efficient Constructions. In. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM '99. Vol. 2, Mar. 1999, pp. 708–716. DOI: 10.1109/INFCOM.1999.751457.

[11] S. Even, O. Goldreich, and S. Micali. On-line/off-line digital signatures. *Journal of cryptology*, 9(1):35–67, 1996.

[12] Y. Challal, A. Bouabdallah, and Y. Hinard. RLH: receiver driven layered hash-chaining for multicast data origin authentication. *Computer communications*, 28(7):726–740, 2005.

[13] C. Tartary, H. Wang, and S. Ling. Authentication of Digital Streams. *IEEE Transactions on Information Theory*, 57(9):6285–6303, Sept. 2011. ISSN: 0018-9448. DOI: 10.1109/TIT.2011.2161960.

[14] A. Perrig, D. Song, R. Canetti, J. D. Tygar, and B. Briscoe. Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction. RFC 4082 (Informational). Internet Engineering Task Force, June 2005. URL: http://www.ietf.org/rfc/rfc4082.txt.

[15] Q. Wang, H. Khurana, Y. Huang, and K. Nahrstedt. Time Valid One-Time Signature for Time-Critical Multicast Data Authentication. In *IEEE INFOCOM 2009*, Apr. 2009, pp. 1233–1241. DOI: 10.1109/INFCOM.2009.5062037.

[16] D. J. Bernstein, N. Duif, T. Lange, P. Schwabe, and B.-Y. Yang. High-speed high-security signatures. *Journal of cryptographic engineering*, 2(2):77–89, 2012.

[17] D. Gligoroski, R. S. Ødeg\a ard, R. E. Jensen, L. Perret, J.-C. Faugere, S. J. Knapskog, and S. Markovski. MQQ-SIG. In, *Trusted Systems*, pp. 184–203. Springer, 2011.