Secure Keying Scheme for Network Slicing in 5G Architecture

Pawani Porambage*, Yoan Miche†, Aapo Kalliola†, Madhusanka Liyanage*‡, Mika Ylianttila*
*Centre for Wireless Communications, University of Oulu, Finland
†Nokia Bell Labs, Espoo, Finland
‡School of Computer Science, University College Dublin, Ireland
Email: *[firstname.lastname]@oulu.fi, †[firstname.lastname]@nokia-bell-labs.com, ‡madhusanka@ucd.ie

***Abstract*—Network slicing is one of the key enabling technologies of evolving fifth generation (5G) mobile communication that fulfills multitudes of service demands of 5G networks. Although the concept of network slicing, its deployment scenarios and some security aspects like slice isolation are discussed in detail, key management for network slicing based applications is still not a well-investigated research area. In this paper, we propose a secure keying scheme that is suitable for network slicing architecture when the slices are accessed by the third party applications. Since the secure keying scheme is designed using a multi-party computation mechanism, it ensures the consent of monitored use cases or devices which the data is acquired. We discuss the performance, scalability and security properties of the keying scheme to demonstrate its appropriateness under evolving 5G paradigm.**

***Index Terms*—5G, Network Slicing, Security, Key Management, Multi-Party Computation, Scalability**

I. Introduction

Fifth generation (5G) of mobile communication are expected to meet the evolution in terms of capacity, performance and spectrum access to radio-network segments [1]. More importantly, 5G will be an evolution of extreme flexibility and high programmability conversion in all non-radio network infrastructure. 5G networks will serve a multitude of use cases that have very diverse characteristics and requirements. The most mentioned 5G use cases are categorized as enhanced Mobile Broadband (eMBB), Ultra Reliable Low Latency Communication (URLLC), and massive Machine Type Communication (mMTC) [2]. To satisfy different needs of these use cases, network slicing is introduced in 5G that creates multiple logical networks over a single physical network [3].

By definition, one network slice can accommodate a separate set of network functions without interfering to support given application services [4]. In one vertical industry there can be many standalone or combined use cases running simultaneously. Each of these horizontal use cases can be served by one or multiple network slices. For instance, a smart factory environment may accommodate all types of traffic classes including eMBB (human users, Augmented Reality (AR) and Virtual Reality (VR) applications), URLLC (cobots, automated machineries), mMTC (sensor networks, IoTs) [5]. Different traffic classes can be served by one or many network slices. In these massive industrial verticals, when it is required to detect an abnormality from a given data set that has a global impact on the entire industry (i.e., smart factory), the process can be outsourced to a third party monitoring application. Under such circumstances, the monitoring application may have to access one or many network slices (i.e., the corresponding network storage resources) with the consent of the targeted use cases or the devices.

In this paper, we propose a keying scheme to securely access data from the network slices by the third party monitoring applications with the consent of the monitored use cases or devices. We discuss the retrieval of data and key management with the help of multi-party computation mechanisms. The performance of the proposed scheme is analyzed based on the involvement of the network devices as an cost analysis. Moreover, we mention the possibilities of scaling up the keying scheme for large network and discuss the security properties of the keying scheme.

The remainder of this paper is organized as follows: Section II provides the background and related work on network slicing and 5G service based architecture. Section III describes the assumptions, the threat model and the use case. Section IV presents the proposed key management scheme and its applicability in the 5G architecture. Section V and VI respectively provide performance and security analysis of the proposed solution. Finally, section VII summarizes the work and draws the conclusions.

II. Background and Related Work

5G core network is proposed to deploy in two phases [6]: well-known point-to-point connections which is similar to the current 4G-LTE (Long Term Evolution) architecture; service based architecture (SBA). According to the definition released by 3rd Generation Partnership Project (3GPP), the 5G SBA delivers the control plane functionality and common data repositories by a set of interconnected Network Functions (NFs). Therefore, SBA is more appropriate for the new cloud-native networking models and has higher flexibility for an iterative development process. 5G SBA is defined with major functional elements (or network functions) and their connecting high-level interfaces [1].

Due to its ability to support multiple service requirements over a common network, network slicing is considered as a key commercial driver for 5G [3]. By definition, a network slice controls its own packet forwarding from the user end to the cloud servers in the core network [4]. The end-to-end slicing architecture has three segments including access slices, core network slices, and pairing functions that connect former two. CN (Core Network) slices are designed with the logical separation between control and user plane functions and the corresponding NFs such as Access and Mobility Management function (AMF), Session Management function (SMF), User plane function (UPF), Policy Control Function (PCF), Authentication Server Function (AUSF), Unified Data Management (UDM) and Network Slice Selection Function (NSSF).

Security considerations in network slicing are associated with many networking and communication technologies and addressed with different perspectives [7], [8]. Strong slice isolation is a main requirement to mitigate the spreading of security threats among multiple network slices. When two slices are sharing common resources, an attacker who reveals the cryptographic materials on one slice can exploit to affect the security functions running on another slice. Other security considerations are addressed on inter-networking slice communication, operations of network slice manager, slice heterogeneity, authentication of network slice instances, and key management.

Although slicing security has gained a high attention, not many works are published during the recent past. The majority of the work consider authentication and key management protocols from the user end or for the inter-slice communication. The paper [9] proposes a cross-authentication scheme for 5G heterogeneous networks by combining non-cryptographic and cryptographic algorithms. In [10], a secure service oriented authentication framework is presented to support slicing and fog computing for 5G-enabled IoT services. It guarantees the secure access of IoT services and privacy-preserving slice selection. The solution includes a service-oriented three-party key agreement to negotiate keys among IoT servers, local fog servers, and users, based on Diffie-Hellman key agreement. In [11], two heterogeneous signcryption schemes are proposed to achieve mutual communications among network slices deployed in different public key cryptosystems (i.e., e public key infrastructure and certificateless public key cryptography environment). Slice isolation, privacy, and managing trust among different stakeholder and slices also matter the most. Customizing slicing security by Software Defined Networking (SDN) using micro-segmentation is another approach to isolate traffic flows related to different applications or users [12].

However, none of those published articles address the security considerations, possible attacks and mitigation techniques related to networking slicing, when the slices are accessed by external parties. Throughout this work, we describe how multi-party computational algorithms can be used to implement secure keying scheme among the network slice resources, the served use cases (i.e., devices or users) and the external entities. Our work is inspired by the scheme in [13], a distributed approach with a hybrid cryptosystem that ensures the confidentiality in a video surveillance system. According to their setup, the recorded video-material is only available to a subset of authorized users who will finally be able to decrypt the videos. Similar to the scheme in [13], we also take the advantage of using a multi-party computation algorithm (i.e., Shamir's secret sharing) to compute keys in our security scheme.

III. Use case and Threat model

A. Use case

To elaborate the key management protocol and its necessity, we consider one particular vertical industry which is smart factory or Industry 4.0. Under the given industry vertical there are multiple horizontal use cases or services running with different requirements and specifications. For instance, a smart factory environment includes numerous cyber-physical systems such as cobots (collaborative robots), augmented reality (AR) applications and sensor networks. As illustrated in Figure 1, one factory premises may accommodate different such use cases and each can be served by single or multiple network slices. When the factories are geographically dispersed, the horizontal use cases can be also served by dedicated or shared network slices. Each network slice owns logically isolated computation and storage resources to perform data processing and storing tasks to all the use cases that receive their services.

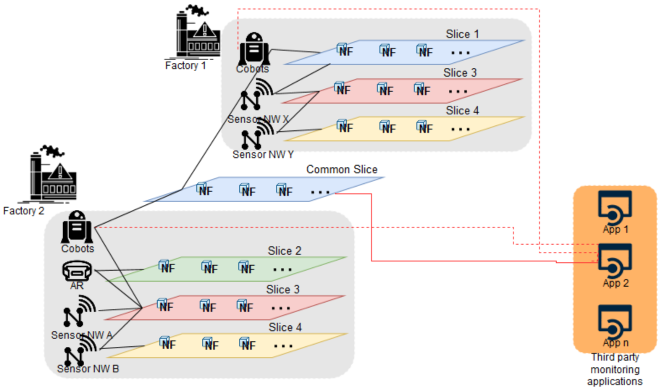

Fig. 1: Provision services for horizontal use cases in factories using dedicated and shared network slices.

In addition to the aforementioned dedicated services required by different use cases, there are certain occasions that need them to be monitored in common by Third Party Monitoring Applications (TPMAs). For example, while detecting anomalies in a particular process in the factory, the third party application has to acquire data from multiple use cases and keep the proper co-ordination among them and the respective network slices. Under such a scenario, the third party application has to access the data from the respective network slices, however with the consent of the particular use cases (Figure 2) or their individual components (Figure 3).

To cater such secure communication links among the third party applications, the network slice resources, and the use

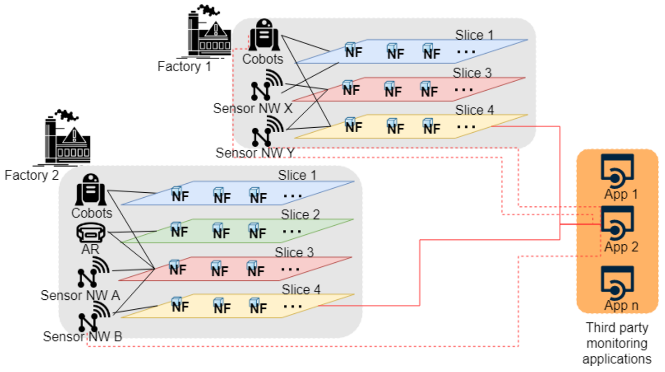

Fig. 2: Third party application access data with the consent of different use cases.

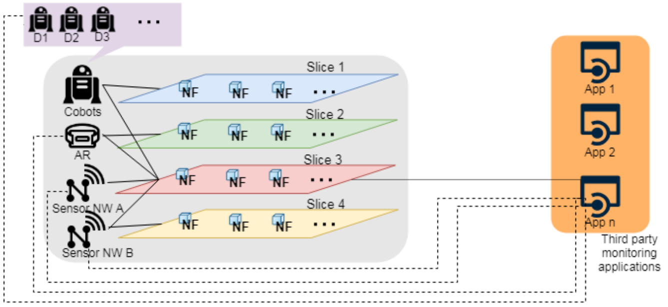

Fig. 3: Third party application access data with the consent of individual components in a given use case.

cases, we propose a secure key management scheme based on Shamir's secret sharing technique.

B. Threat model

1) Adversaries: We consider three possible adversary types.

Internal adversaries with administrative control: An internal adversary can be located in the factory premises and take the administrative control of the devices in the factory. This can be a tenant inside the factory or an external intruder who has access to a compromised device.

External adversaries with access to data transportation: An external adversary that could attack the data transportation between TPMA, factory devices and network slice.

External adversaries with access to TPMA: An external adversary that could attack a TPMA by accessing its security credentials or creating Distribute Denial of Service (DDoS) attacks.

2) Attacks on a slice while accessing by a third party:

DDoS flooding attacks: These can be launched by external adversaries on network slices (i.e., particularly on AMF) while TPMA communications in all cases are occurring across an untrusted network.

Data tampering attacks: These attacks can be launched by external adversaries when they access data obtained by TPMA. When a TPMA is compromised the attacker can deliberately modify, replay or inject bogus data stored. Moreover, tampering attacks can also be initiated by the external adversaries those who can access the data transportation.

Key-compromise impersonate attacks: These attacks may occur when an internal adversary uses a compromised device to access its keying materials use them for future communication purposes. If the long term private key shares of the devices are compromised, the attacker can use those key shares to compute the security credentials requested by TPMA.

C. Assumptions

The slice operators' network is functional as the service-based 5G core network architecture. Within the factory premises, the monitored devices are protected by a Trusted Platform Module (TPM) on each device for mutual authentication and integrity checks in all communications. The communication link establishment between the TPMA and 5G core is performed by the means of a conventional security protocol like IPSec and TLS (Transport Layer Security). Moreover, we consider an ideal situation where the proper slice implementation is achieved in such a way to avoid slice specific security vulnerabilities including slice isolation and side channel attacks.

IV. Proposed Keying Scheme

A. Preliminaries

For all the calculations in the rest of the sections, we consider that G_q is a group of prime order q, where the Discrete Logarithm Problem and closely related problems are believed to be hard and g is a generator of G_q. All the computation in $\mathbb{Z}$ are also undergoing $mod\ q$, although it is not appeared in the text. In addition to that, the proposed security architecture exploits Shamir's secret sharing [14] technique to distribute and reconstruct the shares of private keys and ElGamal cryptosystem [15] for encryption and decryption of interval-keys. Shamir's secret sharing technique is based on a (n, k) threshold scheme [14], wherein n devices process a polynomial share and k polynomial shares being enough to reconstruct the DH keys through the Lagrange polynomial interpolation. According to [14], the (n, k) threshold scheme is selected as $n = (2k - 1)$.

B. Keying scheme

As illustrated in Figure 4, the devices $\{D_1, D_2, \ldots, D_n\}$ are accessing one particular network slice. When a TPMA needs to acquire data related to the given devices from the network slice, it also has to get the consent of those devices.

As an initial phase, the network slice and the devices will receive the corresponding cryptographic keys from a Key Distribution Center (KDC), which is co-operating with the Authentication Server Function (AUSF). For a given network slice that serves n devices (or n distinctive use cases), KDC generates a key-pair (d, e) for the ELGamal cryptosystem: d and e are private and public keys. The shares of the private key $(d_1, d_2, \ldots, d_n)$ and the public key $e = g^d$ are respectively delivered to the devices and the network slice in a secure manner. The secret key d is generated following a t-degree

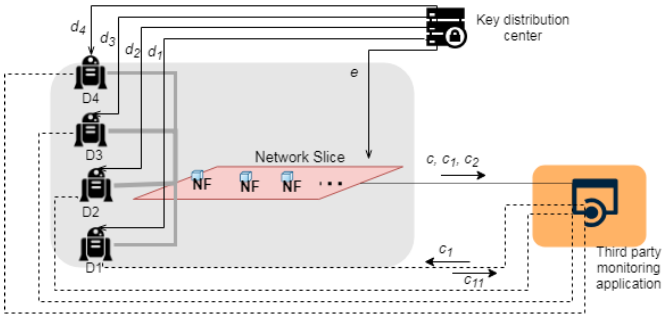

Fig. 4: Graphical representation of delivering security credentials in the key management scheme.

polynomial $f()$ (i.e., $d = f(0)$) and d_i shares are computed as follows.

$$d_i = f(i) = d + \sum_{j=1}^{t} r_j i^j, \quad r_j \in_R \mathbb{Z}_q^* \tag{1}$$

According to Shamir's Secret Sharing technique and by Lagrange interpolation, in order to reconstruct the private key d, it is necessary to have at least $t+1$ number of d_i values.

There can be multiple security and privacy issues arising when the third party application can keep the records of previously accessed data from a network slice. Therefore, it is necessary to ensure that the data released by the network slice is transferred as encoded context in an application specific format (e.g., use homomorphic encryption). There should be an entity operating at the network slice, that is responsible for encoding the data and providing it for pre-designed tasks of TPMA.

The encoded data related to a particular incident or a given period of time is named as M and encrypted with an interval-key k using symmetric encryption $E_S(M,k) = c$. The network slice generates a random interval-key k as a one-time key related to the request made by TPMA. In addition to that, the slice encrypts k with the public key e using ElGamal asymmetric encryption and computes c_1 and c_2 values: $E_A(e,k) = (c_1, c_2)$.

$$E_A(e,k) = (g^\alpha, ek^\alpha) = (c_1, c_2) \quad \alpha \in_R \mathbb{Z}_q \tag{2}$$

When TPMA accepts the received message (i.e., c, c_1, c_2), it has to follow several steps to derive k and reconstruct the encoded data. First step is to derive the ephemeral key k, using (c_1, c_2) and the consent of the devices (or the use cases) in the factory. On behalf of the TPMA, the network slice manager sends c_1 value to the devices who agree to co-operate. Then each collaborating device performs the ElGamal decryption of c_1 using its private key share d_i (i.e., equation 3) and sends back c_{1i} to TPMA through the network slice manager.

$$D_A(c_1, d_i) = c_1^{d_i} = c_{1i} \tag{3}$$

After collecting the sufficient number of decrypted values (i.e., from $t+1$ cooperative devices) from n devices, TPMA derives the interval-key k by decrypting the values as follows: First compute λ_i coefficients for each received c_{1i} in the subset P (i.e., size of $t+1$) of the participating devices.

$$\lambda_i = \prod_{i \in P, j \neq i} \frac{-j}{i-j} \tag{4}$$

Then k value is decrypted using the Lagrange formula and λ_i values.

$$\begin{aligned} D((c_{11}^{\lambda_1}, c_{12}^{\lambda_2}, \ldots, c_{1(t+1)}^{\lambda_{(t+1)}}), c_2) &= c_2(\prod_{i \in P} c_1^{d_i \times \lambda_i})^{-1} \\ &= c_2(c_1^{\sum_{i \in P} d_i \times \lambda_i})^{-1} \\ &= c_2(c_1^d)^{-1} \\ &= k \end{aligned} \tag{5}$$

Having the key k, TPMA can decrypt the encoded data by performing $D_S(c,k) = M$.

C. High-level description of proposed scheme

This section describes the high-level overview of the information flow of the proposed protocol under the umbrella of next generation core network architecture (Figure 5).

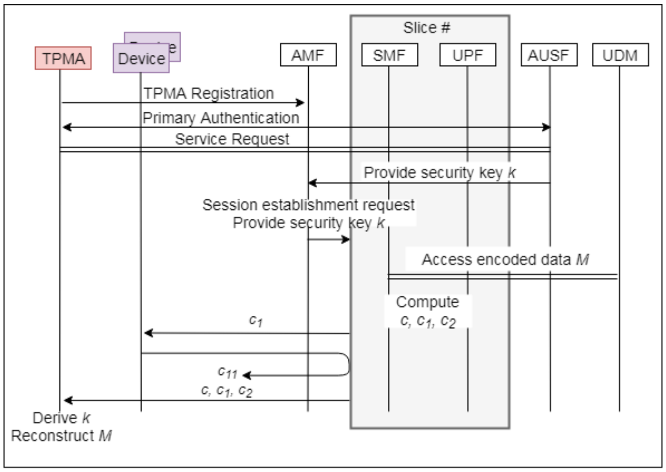

Fig. 5: Information flow of the proposed keying scheme in 5G service based architecture.

First, TPMA sends a registration request to Access and Mobility management Function (AMF). Then AMF selects an Authentication Server Function (AUSF) and interacts with User Data Management (UDM), where TPMA can perform the registration and primary authentication specified in 3GPP to access 5G network. If the authentication process is successful, TPMA can proceed with sending service request and authenticating the service to AUSF. Based on the service request, AUSF generates the ephemeral key k for the session, and shares it with AMF. Then AMF selects a network slice instance based on TPMA's service request and sends session establishment request to the corresponding Session Management Function (SMF) of the slice along with the key k. The slice specific function, User Plane Function (UPF) manages user plane traffic. Moreover, the network slice receives the service area restrictions of the serving devices and the accessibility of the stored data from UDM. Based on the accessibility policies, the slice itself accesses the encoded data M, computes c, c_1, c_2 values and sends c_1 to the devices. The devices that are willing to cooperate compute c_{1i} values and sends back to the network slice. Finally, the network slice will send c, c_1, c_2 and all the received c_{1i} values. Since there is no direct communication between the devices and TPMA, c_{1i} values are delivered via the network slice manager.

V. Performance analysis

To discuss the performance of the proposed keying scheme, we considered the behaviour of the devices in the factory premises in terms of their willingness to cooperate with TPMA to reconstruct the secrets. TPMA requests rightful access to the data, in order to provide an additional service or to detect an abnormality related to the devices. Therefore, if the devices be cooperative with TPMA each device will receive a gain (G) in return. At the same time, while contributing for the secret reconstruction, each device has to undertake a cost (C) that includes computation and communications costs.

For the successful key reconstruction, at least there should be $t + 1$ cooperative devices. Consequently, the total profit which one device can gain will also depend on the likelihood of the other devices to cooperate with key reconstruction. We consider that each device is willing to cooperate (i.e., $D_i = 1$) with an equal probability of a: the probability that a device will not cooperate is $1 - a$ (i.e., $D_i = 0$). Then the probability of success or the probability that at least $t + 1$ devices are contributing among n devices (i.e., $D_1, ...D_i, ...D_n$) will be:

$$\begin{aligned} Pr_{success} &= Pr\{\sum_{i=1}^{n} D_i \geq (t+1)\} \\ &= \binom{n}{t+1} a^{(t+1)}(1-a)^{(n-(t+1))} + \cdots + \binom{n}{n} a^n \\ &= \sum_{i=t}^{n-1} \binom{n}{i+1} a^{(i+1)}(1-a)^{(n-(i+1))} \end{aligned} \tag{6}$$

Therefore the expected net profit (P_{avg}) at a device would be the difference between its expected net gain and the expected cost:

$$P_{avg} = G \sum_{i=t}^{n-1} \binom{n}{i+1} a^{(i+1)}(1-a)^{(n-(i+1))} - Ca \tag{7}$$

The graphs in Figure 6 show the behaviour of the expected net profit (P_{avg}) with the variation of the probability of device cooperation (a). We keep a fixed gain value as $G = 20$ and changed the cost value C. Thereby we observe that P_{avg} is increasing with the decremented C. In each case, the maximum P_{avg} is observed for the probability of a between 0.8 and 0.9.

A clustering mechanism with a hierarchical key distribution scheme can be used to tailor the proposed keying scheme in such a way to provide higher scalability for the given use case. As described in Section III, network slices can be assigned under multiple scenarios (i.e., dedicated or shared slices) or TPMA may request data from the devices served by different slices. Moreover, when the number of devices served by one network slice drastically increases from hundreds to thousands (e.g., sensor networks), it will be challenging to adjust the values of n and t accordingly. One responsible node (e.g., cluster head) can be assigned to a group of devices and each of those cluster heads can provide the consent to the TPMA on behalf of their leaf nodes (i.e., end devices).

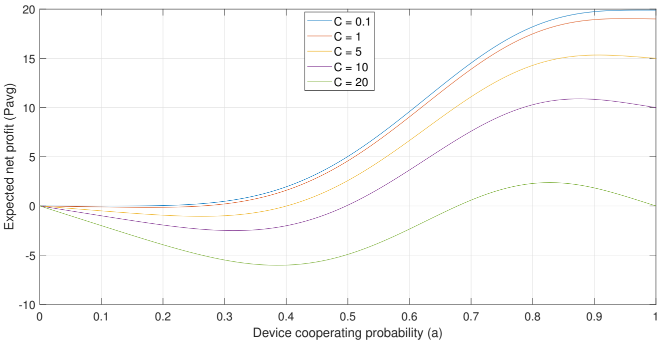

Fig. 6: The behaviour of the expected net profit with the probability of device cooperation at different costs

VI. Security properties

Security properties of the keying scheme are described considering the threat model mentioned in Section III. The keying scheme takes the advantage of multitude secret shares to reconstruct key k generated by AUSF. Since the scheme takes the consent of the devices (or use cases), it can be easily adopted for a group of users and the protocol may provide an implicit assurance for privacy-protection of the monitored users.

1) DDoS flooding attacks: Although the devices provide their consents to the key reconstruction process, they do not have direct communication with TPMA. Instead the message is coming from the slice itself, which is assumed to deliver securely. Therefore, on the networking devices, the protocol will clearly prevent the DoS attacks created by the external parties. However, since all the TPMA communications are occurring across an untrusted network, it is necessary to apply some conventional protection mechanisms such as IPSec and TLS. Standard DDoS defensive mechanisms should be implemented at the network slice manager which is the first contact point of the TPMA [16].

2) Data tampering attacks: When there is a request coming from a TPMA, the slice will always share the encoded data which are associated with that stand-alone request. Since the data is in encoded form, it will be hard to an external attacker to retrieve any useful information out of it for future attacks. Moreover, sending encrypted data will prevent the tampering attacks during the data transportation.

3) Key-compromise impersonate attacks: According to the Lagrange polynomial interpolation $t + 1$ number of private key shares out of n shares are used to reconstruct the key k. Therefore, as long as an internal adversary is not able to solve discrete logarithm problem and do not compromise at least $t+1$ devices in the factory, he is not able to get any information about the private key (d) and reconstruct the key k. Regular updates of key shares and the polynomials will also increase the security strength of the scheme and mitigate the risk of key-compromise attacks.

VII. Conclusion

In summary, we proposed a key scheme for network slicing based systems that provide secure accessibility for third party monitoring applications with the consent of the networking devices. The keying scheme is discussed considering its performance, scalability and security properties along with its high-level integration in 5G service based architecture. According to the performance analysis of the keying scheme, the devices will receive the maximum average net profit on a cooperation probability between 0.8 to 0.9. The proposed solution has great flexibility to tailor its behavior and characteristics based on the required security strength and use case scenario. Our future research is focused on implementing the proposed keying scheme and analyzing its behaviour with respect to the delay and scalability.

Acknowledgment

This work has been performed under the framework of 6Genesis Flagship (grant 318927), 5GEAR, SecureConnect, Cost Action CA17124 and RESPONSE 5G (Grant No: 789658) projects. This research is funded by the Academy of Finland, Business Finland and the European Union.

References

[1] 3GPP, "System Architecture for the 5G Systems," Technical Specification, June 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/15.02.00_60/ts_123501v150200p.pdf

[2] A. Gupta and R. K. Jha, "A survey of 5g network: Architecture and emerging technologies," *IEEE access*, vol. 3, pp. 1206–1232, 2015.

[3] 3GPP, "Study on management and orchestration of network slicing for next generation network," Technical Specification, June 2018. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3091

[4] International Telecommunication Union, "Terms and definitions for IMT-2020 network: ITU-T Y.3100 (09/2017)," Sep 2017.

[5] Y. Siriwardhana, P. Porambage, M. Liyanage, J. S. Walia, M. Matinmikko-Blue, and M. Ylianttila, "Micro-Operator driven Local 5G Network Architecture for Industrial Internet," in *IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2019, pp. 1–8.

[6] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2429–2453, 2018.

[7] NGMN Alliance, "5G security recommendations package 2: Network slicing," Apr 2016.

[8] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions," *IEEE Communications Surveys & Tutorials*, 2019.

[9] C. M. Moreira, G. Kaddoum, and E. Bou-Harb, "Cross-layer authentication protocol design for ultra-dense 5g hetnets," in *IEEE International Conference on Communications (ICC)*, 2018, pp. 1–7.

[10] J. Ni, X. Lin, and X. S. Shen, "Efficient and secure service-oriented authentication supporting network slicing for 5g-enabled iot," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 3, pp. 644–657, 2018.

[11] J. Liu, L. Zhang, R. Sun, X. Du, and M. Guizani, "Mutual heterogeneous signcryption schemes for 5g network slicings," *IEEE Access*, vol. 6, pp. 7854–7863, 2018.

[12] J. Suomalainen, K. Ahola, M. Majanen, O. Mämmelä, and P. Ruuska, "Security Awareness in Software-Defined Multi-Domain 5G Networks," *Future Internet*, vol. 10, no. 3, p. 27, 2018.

[13] M. Schaffer and P. Schartner, "Video Surveillance: A Distributed Approach to Protect Privacy," in *Communications and Multimedia Security*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2005, vol. 3677, pp. 140–149. [Online]. Available: http://dx.doi.org/10.1007/11552055_14

[14] A. Shamir, "How to Share a Secret," *Communication ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[15] T. El Gamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," in *Proceedings of CRYPTO 84 on Advances in Cryptology*, 1985, pp. 10–18.

[16] J. Mirkovic and P. Reiher, "A taxonomy of ddos attack and ddos defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39–53, 2004.