Journal of Engineering Technology and Applied Physics

Authentication for 5G Mobile Wireless Networks

Daphne Bunga Dwiputriane and Swee Huay Heng*
Faculty of Information Science and Technology, Multimedia University, Melaka, Malaysia.
**Corresponding author:* shheng@mmu.edu.my
https://doi.org/10.33093/jetap.2022.4.1.3
Manuscript Received: 5 January 2022, Accepted: 8 February 2022, Published: 15 March 2022

***Abstract* - Discussions regarding 5G mobile wireless networks frequently involve the impact they will create to our daily lives. Some view 5G as a disruption while some are questioning the need to deploy the network when conventional mobile networks are still performing optimally. The economic and lifestyle impact of 5G is rather subjective, but it is definite that there will be consequences to the security and privacy discussion sphere with an emphasis on authentication. As it arrives with new mechanisms, there is certainly a whole new attacking avenues to be capitalised. This paper surveys the state of 5G mobile wireless networks in terms of authentication. It further discusses the security features and challenges in the 5G mobile wireless networks, and future directions will also be charted.**

Keywords—5G, security, mobile wireless networks, cryptography, authentication

I. Introduction

The 5th generation wireless systems, or 5G, is considered to be the next generation mobile wireless networks and is viewed as a massive upgrade from the current conventional mobile wireless networks. 5G mobile wireless networks is not only an upgraded version of the 4G mobile wireless networks, it is also set to provide many new features that the conventional mobile wireless networks have failed to provide due to its limitations. It is expected that the number of subscriptions to be 100 million by the end of 2020 [1], especially with more countries ramping up the development of the wireless networks in 2020.

5G research and development aims to improve the current capabilities of the conventional mobile wireless networks, such as supporting more connected devices and higher density of devices. According to International Telecommunications Union (ITU), there will be three scenarios that users would benefit from the deployment of 5G [2]. The three scenarios are mobile broadband scenarios, massive machine type communications, and ultra-reliable and low latency communications. These scenarios greatly differ from one another, and they require networks that can support massive number of connected devices in a period of time, but also require the networks to provide low latency, high bandwidth, high throughput and ubiquitous connectivity. Specifically, 5G mobile wireless networks are set to provide 1-10 Gbps connections for end devices, 2-5 milliseconds latency, and 100-1000x number of connected devices [3, 4]. It is also reportedly set to allow 10 years of charged battery for constrained appliances.

There are various 5G use cases such as those in manufacturing automation, vehicle-to-vehicle communication, automated search, rescue missions and smart cities [4]. The new network architecture and technologies are set to bring new security and privacy challenges to the conventional mobile wireless networks.

New security requirements will be needed in order to support new use cases and network architecture. 5G is also set to be a service-oriented wireless networks and different services may have different security and privacy requirements. The security demands of 5G mobile wireless networks highlighted by the Next Generation Mobile Networks (NGMN) Alliance are as follows [5]:

- **Flash Network Traffic**: There will be a higher number of connected devices, including IoT,that may disrupt network

pattern.

- **Radio Interference**: Radio interface encryption keys are transmitted over an insecure communication channel.
- **User Plane Integrity**: User plane is not encrypted, making them unprotected.
- **Mandated Security Measures**: Some security constraints may minimise security measures.
- **Inconsistent Security Policies**: Security policies may differ from one layer to another and from one operator to another.
- **Denial of Service (DoS) Attacks on Network Infrastructure**: Attackers may target network infrastructure as more devices are connected.
- **Signal Overload**: A simultaneous and coordinated access attempts may cripple the signalling plane.
- **DoS Attacks on Users**: There are no concrete countermeasures if attackers are targeting user's devices.

In order to find compatible solutions to these issues, security must be considered as an important factor in the 5G mobile wireless networks and be placed as a high priority before deploying them to the public. Flexible security mechanisms will be needed to support a wide variety of applications. Authentication not only must take place between operators and end users, but also among service providers in the 5G mobile wireless networks. Authentication will be a key factor in the security of the 5G mobile wireless networks. Low-powered devices need a lightweight authentication scheme to support authentication process while high speed devices need to prioritise on performing with low latency. Transferring huge volume of data while maintaining a low rate of delay and a high security level is extremely critical.

As more personal information is used in 5G applications, concerns over privacy will escalate as more applications are connected over the Internet. There is also a potential shutdown to power outage and if this occurs, it may bring harm to the public. 5G security requirements need to not only consider new use cases, but also the legacy security features. Therefore, a good security architecture that could balance between providing excellent services and maintaining high standard of security is important in ensuring a successful deployment of the 5G mobile wireless networks.

In this paper, a comprehensive review on the 5G mobile wireless networks is performed by investigating the features, security challenges, authentication process and identifying possible security solutions in the 5G mobile wireless networks.

II. Attacks and Security Services in the 5G Mobile Wireless Networks

New applications deployed in the network means new possible security attacks could be launched in the network ecosystem. This is why new security mechanisms are extremely important in the 5G security requirements.

A. Eavesdropping Attack

Eavesdropping occurs when an attacker received messages that are not meant for them. This type of attack falls under the category of passive attack, where normal communications between original sender and receiver goes uninterrupted, making the eavesdropping attack to be difficult to detect.

While encryption is applied over the radio access, attackers could still use analysis of the traffic to decrypt the message. It does, however, made it more difficult for attackers to decrypt the information. Attackers can uncover the encrypted information by observing the location of sender and receiver, and at the same time, understand the pattern of communication between the two parties without interrupting the communication.

With advanced technologies rolling out every year, attackers can make use of these technologies to launch a more sophisticated eavesdropping attack, which eventually will break the encryption on the radio access. The distribution of heterogeneous networks over the 5G mobile wireless networks will increase the difficulty for mobile operators to implement security mechanisms, where more scenarios need to be considered before deploying security policies. Cryptographic approaches need to be seriously considered to enhance the security of the network, particularly in the physical layer. The physical layer helps to ensure the confidentiality of data transferring from one party to another.

In the first deployment stage of 5G, researchers have found flaws in the 5G mobile wireless networks that could leave users with potential eavesdropping and Man-in-the-middle attack (MITM) attacks. The Authentication and Key Agreement (AKA) protocol used by 5G networks added a new feature to strengthen the authentication process in an effort to fight 'stingrays', or more commonly known as International Mobile Subscriber Identity (IMSI) catchers. IMSI catchers intercept communications between two parties by pretending to be a base station. Attackers could simply take advantage of the logical vulnerability in the protocol by launching replay attacks as the attack could break the protection of the sequence number [6]. The protocol can be defeated as it uses Exclusive-OR and there was a lack of randomness in its encryption algorithm.

B. Denial of Service (DoS) Attack

A DoS attack is an attack in which the attacker intends to make certain services unavailable to the end users by jamming the resources. A variation of DoS, Distributed DDoS, meanwhile, can be launched by making use of multiple devices at one time. Both DoS and DDoS attacks can be targeted towards any part of the network and the fatality could be equally damaging. DoS attack can be prevented by using a detection method. The possibility of a DDoS attack becomes higher and to a certain extent, easier, as more devices are connected to the network. Attackers can set either one of these two functions as their DoS target, which are either network infrastructure or end users. A DoS attack towards network infrastructure can be specifically targeted to the signalling plane, user plane, management plane, support systems, radio resources, and logical and physical resources. A DoS attack towards the users, meanwhile, can target battery, memory, disk, CPU, radio and sensors [5].

In relation with DoS attacks, a group of researchers have discovered three vulnerabilities in the 5G mobile wireless networks that could exploit the network in order to track user's location as well as intercepting phone calls. Hussain *et al.* uncovered a security attack that targets the paging protocol of the device [7]. The cellular paging protocol is a mechanism that informs the phone regarding an incoming message or phone calls. This attack is named as the 'ToRPEDO' attack.

The attack could simply be launched by calling a targeted individual and cancelling the call not long after. This action exploits the paging protocol as the protocol will not have enough time to inform its users regarding an incoming call. This allows the attacks to discover the location of the targeted individual and at the same time, attackers would be able to learn the time required for the phone to respond to the protocol messages, which leads them to uncover the device's International Mobile Subscriber Identity [7].

This discovery leads to two possible attacks occurring on the 5G mobile wireless networks. The first attack is the Piercer attack while the second attack is the IMSI-Cracking attack. The Piercer attack allows the device's unique 7 bits IMSI to be identified by observing the time required for the device to respond to the paging messages. The IMSI-Cracking attack, meanwhile, has the ability to brute force the encrypted IMSI in order to obtain the phone number of the device.

C. Man-in the Middle (MITM) Attack

A MITM attack occurs when an attacker initiated an attack by eavesdropping two parties communicating with each other. Rather than simply observing the two parties communicating, MITM attacker plays a more active role, in which they could intercept, modify or replace the content of the transmitted data between the two parties. MITM attacks could compromise the confidentiality and integrity of the transmitted data as well as damaging the privacy of the two parties. MITM attack could occur on the mobile wireless networks when an attacker pretends to be a base transreceiver station (BTS) by creating a fake base station [8]. Conventional mobile wireless networks are known to be vulnerable to MITM attacks. Any mobile devices could be forcefully connected to the fake base station by the attacker. The attack is taking advantage of the fact that the device needs to authenticate itself with its own unique subscriber identity while the base station does not need to authenticate itself. A flaw that was described under the eavesdropping section could also be exploited in order to launch a MITM attack on the network. During the recent 2019 Black Hat conference, researchers found that a MITM attack can be deployed to illegally obtain the information of mobile phones either by launching a bidding-down attack or a battery-drain attack as new security mechanism is yet to be applied on the mobile phones.

For bidding-down attacks, attackers could remove the carrier aggregation signal, which is usually use to boost the speed of the network, by changing the information of the frequency band, preventing the device to use the roaming function [6]. As for battery-drain attack, the attack is targeted towards the low-powered NB-IoT devices, where attackers can modify or remove the power saving mode enabled on those devices [6]. The absence of power saving mode will make the device unable to function properly.

D. Smart Jamming Attack

Recent research by Arjoune and Faruque found a vulnerability on 5G mobile wireless networks that makes the network vulnerable to jamming attacks [9]. Jamming a network on purpose could stop legitimate users from using the service. A jamming attack is an attack that tries to interfere with wireless communications. There are several types of jammers, and the popular ones are constant jammers, random jammers, deceptive jammers, and reactive jammers [10]. Despite 5G mobile wireless networks being labelled as an improvement to previous networks such as 3G and 4G, it is still expected to be vulnerable to jamming attacks. 5G mobile wireless networks becomes an even more attractive avenue due to the wide range of industry and activities that could possibly be carried out via the network.

There are few vulnerabilities that might let 5G mobile wireless networks to be exposed to jamming attacks. The vulnerabilities are found on broadcast channel (PBCH), downlink control channel (PDCCH), random access channel (RACH), and massive Multiple Input Multiple Output (MIMO) [9]. PBCH, PDCCH, and RACH are some of the physical channels of a 5G mobile wireless networks while Massive MIMO is a new feature that enhances the capability of a mobile wireless network to support more devices on

the network. The jamming attacks on the physical channels capitalise on the weakness of the network architecture by taking advantage of the frequency. The attacks could target on the existing frequency and starts jamming the network from the existing component using a similar technique for jamming in older mobile wireless networks. Meanwhile, jamming attacks on Massive MIMO can be done by targeting channel estimation procedure [9]. Massive MIMO allows the segmentation of multiple data streams depending on how heavy the data consumption is on one channel. Many research studies found that massive MIMO are extremely vulnerable to jamming attacks and found that it is extremely possible to conduct such attacks [9].

III. Proposed Security Solutions

The features of the 5G mobile wireless networks require an architecture that could support its ability in order to perform optimally. This includes maximising speed, having low latency and is capable to operate in an acceptable level of energy and spectrum efficiency.

Balancing all these requirements on top of the massive number of connected devices indicates the possibility of network issues if only one traditional server is operating. This may make it tougher for users to utilise the network efficiently. There is also a security concern regarding the use of single server as it is vulnerable to attacks.

With security challenges such as signal overload and heavy network traffic, stakeholders need to come up with a solution that could address this issue, which have been a source of concern in the research sphere. Solving high network traffic also means the speed and reliability of authentication scheme need to be considered.

A. Lightweight Cryptography

The deployment of various devices in the 5G mobile wireless networks has made components such as memory, computing power and battery supply, an important successful deployment factor. These devices, mainly, IoT devices, tend to operate in low power and limited battery supply. This has made it necessary to view Moore's Law in a different perspective, in which cutting half the price for a constant computing power over 18 months is a better solution than doubling the performance of a device [11]. In a more general definition, Moore's Law allows IoT applications, which already operates on a tight cost constraint, to be easily deployed as the cost of building these devices will gradually become cheaper [12].

Hence, there is a need to come up with a lightweight cryptographic algorithm that can be implemented efficiently called 'Lightweight Cryptography'. Lightweight cryptography is cryptographic method that operates in constrained devices. One of the biggest differences between 5G and their predecessors is the speed of data transfer in the network. 5G relies on its speed to ensure excellent performance. Hence, the cryptographic method that will be implemented in the network should support the speed of the network. Lightweight cryptography is the suitable solution for this issue as it operates faster than other cryptographic methods.

Lightweight cryptography designers need to be aware of the difference between the implementation of the algorithm for both software and hardware, where the two items require different requirements and, in some cases, their requirements may be different to one another. Bit permutations, for example, are extremely efficient on hardware but may cause trouble and slow down the performance of a system if it is implemented on the software. Another suitable example is substitution table. Substitution table is easy to implement on software but implementing on hardware can be expensive and takes a lot of resources. In the end, the evaluation of how 'successful' the implementation of a cryptographic algorithm differs greatly between software and hardware. For software, memory requirements and clock cycles are compared, while for hardware, the chip size and clock cycles are considered as a higher priority. Comparing power consumption for hardware implementation is a difficult task to perform as the platform that the implementation runs may differ to one another and simulating them in a controlled environment may not give a consistent result. Despite this, comparing power consumption on software may be doable and could produce a rough estimation by multiplying the time taken for the process to complete with the average power consumption on the device.

There is also a need to differentiate between symmetric cryptography and asymmetric cryptography. Symmetric cryptography uses one shared key while asymmetric cryptography requires a pair of keys to perform cryptographic processes.

B. Some Existing Lightweight Cryptography Solutions

There is no algorithm that could become the solution to all the vulnerabilities and weaknesses found in the 5G mobile wireless networks. There are only algorithm solutions that could be suitable for different kind of scenarios, depending on the issue that arises from the problem. Lightweight cryptography has been lauded as a good cryptographic tool for 5G mobile wireless networks. There are a few research studies that support this claim that have given possible solutions to the weaknesses found in the 5G mobile wireless networks, majority of the research studies have chosen lightweight cryptography as their preferred cryptographic tools. The summary in Table I considered research studies that put focus on other

schemes, but the basis of their proposal still could be considered as lightweight.

Table I. Summary of Existing Lightweight Cryptographic Solutions.

Research Studies	Description	How It Works
Taleb *et al.* [13]	Proposed a lightweight MTC control plane agreement called Lightweight Evolved Packet Core (EPC-LightEPC)	- To make plane procedures simpler that allows MTC devices to go through in order to be used by network users. - Placed a single NFC function in the data centre to control the plane. - The data centre acts as a controller that groups MTC devices and helps to establish connection with MTC servers.
Pan *et al.* [14]	Proposed cross-layer security for secure interaction between mobile devices and base stations as well as the interaction between mobile devices.	- Combined traditional lightweight authentication scheme and cross-layer authentication for authentication stage. - Designed to co-exist with one another to allow the security architecture to meet different security demand.
Ying & Nayak [15]	Proposed a lightweight remote user authentication protocol using Self-certified Public key Cryptography (LASPC) for multi-server 5G networks.	- Designed to connect devices with multiple servers to ensure smooth transition.
Dubrova *et al.* [16]	Proposed a lightweight message authentication scheme based on CRC.	- Maintaining existing functions while working on to boost the capability of the functionality in error detection and data integrity protection. - Replaced the irreducible generation polynomial of CRC with a product of irreducible polynomials of lower degrees.
Wang *et al.* [17]	Proposed a new lightweight label-based access control scheme (LACS) to demand reliability in 5G caching	- The scheme allows fog nodes to be authenticated before being deployed by the users. - It is authenticated by checking the integrity of the data in the caching context.
Liu *et al.* [18]	Produced a puzzle-based co-authentication (PCA) scheme as part of the solution.	- Designed an effective hash puzzle with an appropriate level of computational complexity. - Created a mutual trust relationship in a clusters of vehicles that allows certificate verification process to be bypassed if one vehicle in that one cluster has verified the certificate before.
Fan *et al.* [19]	Proposed a lightweight RFID mutual authentication protocol (LRMAPC) with cache in the reader.	- Designed to allow a direct authentication of recently visited key of tags in the reader rather than storing them straight away. - Save a lot of computational power and transmission cost for the constrained devices.
Zhou *et al.* [20]	Proposed an authentication scheme for IoT devices with the assistance of cloud computing	- Proposed a two-factor authentication scheme for IoT-enabled devices with cloud assistance. - Introduced a robust architecture that provides critical security protection for IoT devices.
Ramadan *et al.* [21]	Proposed a secure identity-based signature scheme with Server-Aided Verification for 5G mobile systems (IBS-SAV)	- A combination of identity-based signature and server-aided verification technique. - Assign a server to help the verification process from the user equipment (UE) perspective. - 5G system will use the cloud server in order to verify the signature of user that will be using the network.
Tsu-Yang *et al.* [22]	Proposed an improved version of Wu *et al.*'s authentication protocol in a distributed cloud environment	- Previous protocol does not guarantee perfect forward secrecy (PFS) and suffers from privileged insider attacks - Enhanced the strength of the existing protocol to ensure this protocol can work in a multi-server environment.

C. Multi-Server Architecture

Multi-server architecture, meanwhile, is a suitable framework for 5G as it allows devices to be connected with multiple services at once. Likewise, in 5G, users will be connected with multiple services at the same time. A multi-server setting is a suitable framework to test the capability of the network rather than a single server setting.

The research for multi-server architecture in the 5G mobile wireless networks started with Borcoci *et al.* [11], where it tries to solve the rising traffic issue in mobile wireless networks. Multi-server architecture allows users to be connected with multiple radio access technologies, a wider variety of services. Subsequently, multi-server setting will be more productive rather than in a single server setting. This proposal, unfortunately, allows attackers to impersonate authorised users and servers in order to control the communication channel. This is where an effective and efficient mutual authentication scheme can be considered to solve its weakness.

Some cryptographic algorithms require high computational overload, making them unsuitable to be implemented in a constrained environment. Public key cryptography has been the main choice but this requires the presence of an on-line registration centre, resulting in a higher overhead and complexity. In a

research study aligned with the concept of multi-server architecture, He *et al.* proposed a protocol to authenticate user with the presence of a self-certified public key cryptography [23]. This protocol does not require users to be present at the on-line registration centre [23].

Research development on multi-server architecture have led to Ying and Nayak's proposal regarding a lightweight user authentication protocol in a multi-server architecture [13]. Their proposed protocol, Lightweight and anonymous mutual Authentication protocol using Self-certified Public key Cryptography (LASPC) could be achieved with a basic understanding of the Elliptic Curve Cryptography [15]. This proposal has successfully provided an efficient and anonymous authentication by introducing additional features such as dynamic identities to provide anonymity to users and prevent adversaries from tracking users without figuring out the secret values.

Background and Requirements. A multi-server 5G mobile wireless networks must meet the requirements as follows [15]: mutual authentication without on-line registration centre, efficiency, user anonymity, untraceability, attacks resistance. Ying and Nayak have summarised their security analysis based on the requirements as shown below:

- **Authentication without on-line registration centre**

Users only need to sign up with Registration Centre (RC) when they use the network for their first visit. Any subsequent visit does not require any interaction with RC. Users and server are able to authenticate one another without the help of RC, proving that this protocol allows authentication process to be performed without the presence of on-line registration centre.

- **User Anonymity**

The real identity of the users is hidden in the dynamic identity produced by the protocol. Dynamic identity is used for users to communicate securely between two parties while concealing their real identity. Dynamic identity is also computed with a hash function, providing anonymity to the users.

- **Untraceability**

As the presence of dynamic identity allows users to keep their real identity confidential, this also prevents attackers from being able to link which dynamic identities belongs to which users in the system. Dynamic identities are updated frequently so users will never have the same identity like the ones they have used before. Hence, it is harder for attackers to determine whether a message was sent from the same user.

- **Mutual Authentication**

In order to prove the validity of the message, this protocol introduced a mutual authentication phase that allows both sender and receiver to compute a process that allows them to authenticate whether the message they have received is genuine or not. One important component of this phase is the presence of a secret number in the computation process.

Attackers will not be able to produce a fabricated message for the communicating parties without knowing the secret number. They are also unable to forge a valid message between two parties without knowing the secret number.

- **Attacks Resistance**

This protocol is able to resist different type of attacks in the deployment of 5G mobile wireless networks. The key in resisting attacks such as offline attack is the presence of random numbers in various phases of computation and verification processes. The randomly generated numbers will boost the security of the 5G mobile wireless networks as it adds another layer of complexity for attackers to solve before they could forge messages or obtain passwords. The security of the protocol is also contributed to the presence of a one-way hash function, which makes it tougher for attackers to gain access without coming up with the right numbers.

There is no algorithm that could become the solution to all the vulnerabilities and weaknesses found in the 5G mobile wireless networks. There are only algorithm solutions that could be suitable for different kind of scenarios, depending on the issue that arises from the problem.

Performance Analysis. LASPC is able to perform computationally faster than other protocols that have been proposed for a multi-server environment. As it performs faster, this proves that concerns on the speed of authentication scheme in constrained devices could be resolved without sacrificing security and effectiveness. Table II provides a comparison of computational overhead for users and servers between four protocols serving a multi-server architecture. This table is a compilation of studies that are relevant in evaluating the performance of LASPC.

Table II. Comparison of Computational Overhead.

Protocol	Computational Overhead for Users (ms)	Computational Overhead for Servers (ms)
Lightweight remote user authentication protocol [15]	1.77	1.77
Anonymous mutual authentication protocol [23]	3.52	4.4
Robust Biometrics-based authentication scheme [24]	1.33	1.33
Biometrics-based multi-server authentication protocol using smart cards [25]	1.33	0.89

He and Wang [23] and Odelu *et al.* [24]'s protocols had a lower computational overhead compared to protocol proposed by Ying and Nayak [13] but they focus more on biometrics implementation rather than mobile wireless networks. It requires a built-in fingerprint scan before it could operate [24, 25] and this might incur additional costs, making it as a less attractive option [15].

With a fast authentication speed, LASPC is able to fend off heavy network traffic and signal overload challenges posed by the 5G mobile wireless networks. It could also resist a wide range of attacks, making the protocol an effective and efficient authentication scheme that can be attached in the 5G mobile wireless networks. Further intensive testing should be performed to prove the reliability of the network.

Pros and Cons. Based on their research study, Ying and Nayak are clear proponent of implementing a lightweight authentication scheme in the upcoming mobile networks. They are less favourable towards the idea of using a single server in the network infrastructure due to various disadvantages that could endanger the security and privacy of many parties involved. There are, indeed, few disadvantages of using a single-server architecture, such as the issue of signal traffic, geographical difficulties and lastly, security [15]. Signal traffic has become a major issue in the conventional 4G/LTE with more devices are using the network and operators have to adjust their infrastructure to support these devices. If things remain unsolved by the time of 5G deployment, these issues will be brought forward to the latest network, potentially hindering the growth and full potential of the network.

Deploying single server may also cause connectivity issues. 5G mm Wave will travel in a shorter distance as compared to the conventional wave. Hence, more base stations will be built to overcome this liability, avoiding any kind of connectivity disruption to the users, who are expecting seamless connectivity when they travel from one point to another. Users will also have their device to be connected to the nearest base stations, allowing their devices to access servers close to them rather than accessing servers that are located far away from their position.

Lastly, security issues are also hampering single server. Conducting a maintenance work on a single server will need the server to be switched off for a complete diagnosis. Multiple servers allow the network to be available at all time even if one of the servers is malfunctioning. Single server is also vulnerable to attacks. As communication channels are operating in an open environment, single server could be easily taken down by attackers. As everyone would be connected with the same server, there is a possibility that attackers would exploit their own credentials in order to forge identities to obtain other information regarding users who are using the networks.

These disadvantages have helped the Ying and Nayak to shape a view that a lightweight protocol relying on a multi-server architecture would be better than a single server. Hence, they have proposed a mutual authentication scheme that could verify the real users and servers, and rejecting any attempts made by unauthorised users and servers to create harm in the network. They have also put in the mind that computational complexity must be lower compared to other cryptographic protocols as lightweight devices in the upcoming networks will not be able to handle complex computational power. Any attempts to implement cryptographic protocol with large computational power into the network will fail as this will slow down the speed of the network as more power is used to solve cryptography schemes rather than transmitting information from one server to one user. To support the Ying and Nayak's claim, they have come up with a lightweight authentication scheme with a low computational overhead. The scheme has also proven its ability to produce and protect identities given to the users, generated dynamically and randomly. This has cleared any doubts on whether this protocol could protect users from having their identities forged by malicious attackers, which is partly due to the presence of a one-way hash function that was performed when the identities are generated.

This protocol fared better than other multi-server authentication protocols in terms of average traffic load. Unfortunately, LASPC has performed slower than other multi-server authentication protocols in terms of computational overload. This may be due to the fact that the other two protocols are relying on a biometric scheme, which could produce results faster compared to a cryptographic scheme. The evidence presented has supported the authors' claim of proposing a fast and efficient mutual authentication scheme.

IV. Future Research Directions

With the development of research in quantum computing, both quantum computing and 5G will be slowly integrated to the society and to prevent any misalignment, it is best to make sure the two emerging technologies could work well together. Public key cryptography, long relied to be an effective cryptographic method could be an ineffective tool once quantum computers are deployed due to its incredible speed in solving computational overhead, leaving a space of vulnerability that could be exploited. One direction research could go is to dig deeper into the concept of Quantum Key Distribution (QKD), a secure communication method that requires the involvement of quantum mechanics theories. QKD allows cryptographic keys to be exchanged in the

presence of quantum computing with absolute security. QKD can be tested whether its component can be integrated in conventional cryptographic system [26].

Another possible direction is by working on a three-phase approach in post-quantum-secure 5G environment. Rather than replacing all existing cryptographic algorithms which may cause unnecessary issues for operators, this method is developed to equip the SIM card with 256-bit key that could immediately be used with the existing devices. The cloning of SIM card could be performed faster with the help of quantum computing, hence, by increasing the size of the key from 128-bit key to 256-bit key, SIM card will be harder to clone. Cloning a SIM card can be done by deriving the anchor 128-bit key which has long been a favoured key to be implemented.

There is also other way that attack prevention on 5G mobile wireless networks could be done. From Mazurczyk *et al.*, the authors summarised a study titled "A Secure Federated Learning Framework for 5G Networks" from Liu *et al.* in which Liu *et al.* proposed a blockchain-based framework to defend against poisonous attacks [27, 28]. This approach discussed on how a market can be created to exchange model updates based on smart contracts in blockchain to verify the model and automatically protects them against poisoning attacks. While blockchain is still in a development stage, there are other way besides establishing blockchain in 5G mobile wireless networks. Mazurczyk *et al.* also found that government-enforced security policies and prevention measures could be introduced to allow the standardisation of measures and protection to raise awareness on the importance of securing the 5G mobile wireless networks [27, 29].

V. CONCLUSION

This paper has discussed the features and security challenges in 5G mobile wireless networks, particularly on issues regarding authentication. It then analysed some popular security methods that could be implemented in the 5G mobile wireless networks needs to be considered in order to fit the demands and requirements of the features provided by 5G. Suitable cryptographic solutions are then discussed in the latter part of the paper. For future directions of security trends in 5G, the concept of quantum computing could be tested and applied in a 5G ecosystem.

ACKNOWLEDGEMENT

This work was supported by the Ministry of Higher Education of Malaysia's Fundamental Research Grant Scheme (FRGS/1/2018/ICT04/MMU/01/01).

REFERENCES

[1] "Ericsson Mobility Report," *Ericsson*, no. June, p. 28, 2019.
[2] "Recommendation ITU-R M.2083-0," *International Telecommunication Union*, 2015. [Online]. *Available: https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf.*
[3] E. Hossain and M. Hasan, "5G Cellular: Key Enabling Technologies and Research Challenges," *IEEE Instrum. Meas. Mag.*, vol. 18, no. 3, pp. 11–21, 2015.
[4] G. Arfaoui *et al.*, "A Security Architecture for 5G Networks," *IEEE Access*, vol. 6, pp. 22466 - 22479, 2018.
[5] "5G security recommendations Package # 1," *NGMN Alliance*, no. May, pp. 1–13, 2016.
[6] A. Shaik and R. Borgaonkar, "New Vulnerabilities in 4G and 5G Cellular Access Network Protocols: Exposing Device Capabilities,"in *Proc. of the 12th Conf. on Secur. and Priv. in Wirel. and Mobile Netw.*, pp. 221–231, 2019.
[7] S. R. Hussain, M. Echeverria, O. Chowdhury, N. Li and E. Bertino, "Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information," in *The Netw. and Distrib. Sys. Secur. (NDSS) Symp.*, doi: 10.14722/ndss.2019.23442, 2019.
[8] M. Conti, N. Dragoni and V. Lesyk, "A Survey of Man in the Middle Attacks," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016.
[9] Y. Arjoune and S. Faruque, "Smart Jamming Attacks in 5G New Radio: A Review," in *10th Annual Comput. and Commun. Workshop and Conf.*, doi: 10.1109/CCWC47524.2020.9031175, 2020.
[10] S. V. Manikanthan and T. Padmapriya, "Detection of Jamming and Interference Attacks in Wireless Communication Network Using Deep Learning Technique," in *Proc. of the First Int. Conf. on Comput., Commun. and Contr. Sys.*, doi: 10.4108/eai.7-6-2021.2308599, 2021.
[11] D. Schinianakis, "Alternative Security Options in the 5G and IoT Era," *IEEE Circuits Syst. Mag.*, vol. 17, no. 4, pp. 6–28, 2017.
[12] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann and L. Uhsadel, "A Survey of Lightweight-cryptography Implementations," *IEEE Des. Test Comput.*, vol. 24, no. 6, pp. 522–533, 2007.
[13] T. Taleb, A. Ksentini and A. Kobbane, "Lightweight Mobile Core Networks for Machine Type Communications," *IEEE Access*, vol. 2, pp. 1128 - 1137, 2014.
[14] F. Pan, H. Wen, H. Song, T. Jie and L. Wang, "5G Security Architecture and Light Weight Security Authentication," in *2015 IEEE/CIC Int. Conf. on Comm.,* doi: 10.1109/ICCChinaW.2015.7961587, 2017.
[15] B. Ying and A. Nayak, "Lightweight Remote User Authentication Protocol for Multi-server 5G Networks Using Self-certified Public Key Cryptography," *J. Netw. Comput. Appl.*, vol. 131, pp. 66–74, 2019.
[16] E. Dubrova, G. Selander, M. Näslund and F. Lindqvist, "Lightweight Message Authentication for Constrained Devices," in *WiSec 2018 - Proc. 11th ACM Conf. Secur. Priv. Wirel. Mob. Networks*, pp. 196–201, 2018.
[17] Q. Wang, D. Chen, N. Zhang, Z. Qin and Z. Qin, "LACS: A Lightweight Label-Based Access Control Scheme in IoT-Based 5G Caching Context," *IEEE Access*, vol. 5, pp. 4018 - 4027, 2017.
[18] P. Liu, B. Liu, Y. Sun, B. Zhao and I. You, "Mitigating DoS Attacks Against Pseudonymous Authentication Through Puzzle-based Co-authentication in 5G-VANET," *IEEE Access*, vol. 6, pp. 20795–20806, 2018.
[19] K. Fan, Y. Gong, C. Liang, H. Li and Y. Yang, "Lightweight and Ultralightweight RFID Mutual Authentication Protocol with Cache in The Reader for IoT in 5G," *Secur. Commun. Networks*, vol. 9, no. 16, pp 3095–3104, 2016.
[20] L. Zhou, X. Li, K. H. Yeh, C. Su and W. Chiu, "Lightweight IoT-based Authentication Scheme in Cloud Computing Circumstance," *Futur. Gener. Comput. Syst.*, vol. 91, pp. 244–251, 2019.
[21] M. Ramadan, Y. Liao, F. Li and S. Zhou, "Identity-based Signature with Server-aided Verification Scheme for 5G Mobile Systems," *IEEE Access*, vol. 8, pp. 51810 - 51820, 2020.
[22] T. Y. Wu, Z. Lee, M. S. Obaidat, S. Kumari, S. Kumar and C. M. Chen, "An Authenticated Key Exchange Protocol for Multi-

Server Architecture in 5G Networks," *IEEE Access*, vol. 8, pp. 28096 - 28108, 2020.

[23] D. He, S. Zeadally, N. Kumar and W. Wu, "Efficient and Anonymous Mobile User Authentication Protocol Using Self-Certified Public Key Cryptography for Multi-Server Architectures," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 9, pp. 2052 - 2064, 2016.

[24] D. He and D. Wang, "Robust Biometrics-Based Authentication Scheme for Multiserver Environment," *IEEE Syst. J.*, vol. 9, no. 3, pp. 816 - 823, 2015.

[25] V. Odelu, A. K. Das and A. Goswami, "A Secure Biometrics-Based Multi-Server Authentication Protocol Using Smart Cards," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 9, pp. 1953 - 1966, 2015.

[26] C. Mitchell, "The Impact of Quantum Computing on Real-world Security: A 5G Case Study," *Comput. Secur.*, vol. 93, no. 101825, 2020.

[27] W. Mazurczyk, P. Bisson, R. P. Jover, K. Nakao and K. Cabaj, "Challenges and Novel Solutions for 5G Network Security, Privacy and Trust," *IEEE Wirel. Commun.*, vol. 27, no. 4, pp. 6 - 7, 2020.

[28] Y. Liu, J. Peng, J. Kang, A. M. Iliyasu, D. Niyato and A. A. A. El-Latif, "A Secure Federated Learning Framework for 5G Networks," *IEEE Wirel. Commun.*, vol. 27, no. 4, pp. 24-31, 2020.

[29] J. M. Batalla *et al.*, "Security Risk Assessment for 5G Networks: National Perspective," *IEEE Wirel. Commun.*, vol. 27, no. 4, pp. 16-22, 2020.