*Chapter 8*

# SECURITY, PRIVACY & TRUST IN 5G WIRELESS MOBILE COMMUNICATIONS

***A. Yarali, R. Yedla, S. Almalki, K. Covey, and M. Almohana***
Telecommunications Systems Management
Murray State University, Murray, KY

## ABSTRACT

The main purpose of this chapter is to identify the potential threats that can occur in 5G mobile communications systems and to discuss the possible techniques that can be implemented to avoid these threats. The design of the 5G networks must be scrutinized at the beginning phase of its implementation considering massive connectivity of M2M, D2D and new applications and services. The migration from 4G to 5G is not just a quantative transition because this generation of mobile communication expected to integrate and to connect various sectors such as smart grid, health, transportation and manufacturing. To counter such threats in 5G, cryptographic techniques and other new means of security designs for identity management, cloud, radio access and architecture need to be considered. This chapter discusses the security techniques such as cryptography using stream and block ciphers methods for data integrity.

**Keywords**: 5G mobile communication, privacy, cryptographic techniques

## INTRODUCTION

The demand for the security techniques are increasing day by day with the evolution of new products and new techniques. The hackers too could break through the system and could extract the data of the user. Our crucial bank details, passwords, transactions, and important personal data are getting into the hands third party interceptors. To counter these many algorithms have been developed from 2G to 5G. Some of the embedded security techniques that are being used still today are: A5/3 for Second Generation GSM networks, f8 and f9 for third generation UMTS networks, and A5/3 also known as Kasumi Cipher is still being used for the latest generation of cellular communication. Some say XXTEA is the replacement of the Kasumi cipher although it is too early to confirm since 5G is still at its esrly stage of considerarions. Technology is evolving, and technology like Long Term Evolution offers different services that come with speed like video conferencing downloading movies, uploading large files, and gaming etc.

Corresponding Author address
Email: ayarali@murraystate.edu

Every service they provide should be technologically secured; the security service should be integrated within the cellular technology. With every generation of the new invoked cellular technology, they create a better prominent technique that makes the data more secured. 5th Generation cellular technology is totally dependent on TCP/IP layered model. 5G is broader than the previous versions of cellular technology, and technically making it different from the previous versions (4G and 3G). In simple words, the paper first gives an overview about the next generation of mobile communications, second, about the 2020 agenda from 3GPP, third, about the threats 5G wireless mobile communications could face, fourth, techniques involved in cryptography to secure the user data, fifth, about the trust model and ends with a conclusion.

## WIRELESS ANONYMITY

Anonymity is a relatively new concept in the wireless world. Over the past decade, the public has become increasingly concerned about the privacy of their communication methods. Due to events, such as whistleblowing, hacking, and governmental corruption, society is becoming aware of malicious attackers, and their policy makers pulling the wool over their eyes. Because of this, citizens are taking certain measures to ensure that their telecommunications remain private. Whether the government likes it or not, people are not going to be as easily fooled as they once were. Luckily, there are many software and hardware engineers who have taken the task of keeping the wireless world anonymous and secure, upon themselves as their personal mission. Therefore, there have been so many accomplishments in the world of security because of these volunteers. Hence, this paper will only be scratching the surface. In this study, we will see how the public views their privacy and the steps they are taking to remain hidden - and safe - in the wireless world.

Wireless anonymity, put plainly, is ensuring by any necessary means that guarantee all information you are sending over a network remains private between you and your endpoint. All over the country, people are continuing to funnel money into programs dedicated to helping them retain their privacy online. There are solely set up communities that instruct people on how to remain anonymous over their networks. Websites, such as the Information Security section of StackExchange, are flooded with questions about remaining anonymous over the internet daily. Google is certainly searching the terms “wireless anonymity” to bring results from the aforementioned site. This goes to show that people are indeed interested in remaining private.

Companies have begun to take advantage of this recent privacy trend as well. One such company, Anonabox, has created a hardware router that connects to the Tor network so that they can keep your communications secure (explained later, for now just think of it as the ultimate private network) (Anonabox). This device is for sale on their website for $99. Any person can purchase this device and use it with their computer as long as their computer has a USB port and complies with the technical specifications of the peripheral. This is just our first example of easily accessible wireless anonymity for everyday people. The reason this device

is mentioned first because it is the easiest for people to wrap their head around. In essence, it is just a piece of hardware that you plug into your computer's USB ports (which almost all computer users are familiar with). The device then acts as your own personal computer and private router; accordingly, rerouting all of your communication messages to a separate global network before going to your destination, thus, protecting your online identity. This is a remarkable achievement towards everyday privacy. Consumers with a little knowledge of the information technology industry can ensure that their communications stay private just by purchasing a convenient and pluggable device, and running it alongside their everyday computer tasks. In the not-so-distant past, this would have only been attainable by a programmer or information technology professional manually setting up such a system catered to each individual. As you can see, however, this is no longer the case. Wireless anonymity has become such a major concern of the public in which we now have easy-to-use peripheral devices, readily available on the market, and can perform these tasks for us.

Now, we have gotten a little technical analysis, so we can start talking about certain software technologies that have been around in recent years to help us remain secure and private in the online world. One mentionable technology is a security protocol by the name of Secure Sockets Layer, or SSL for short. It is now a standard technology that is available to use by the public with updated operating systems on their computers and smartphones. SSL is a technology based on security. What it does is setting up one-and-done secure connection between a server and a client over the internet. It can often be seen in web browsers when you visit a website with the "https" prefix. Unlike "http" counterpart, "https" uses SSL to establish a secure connection between your web browser and the server that you are trying to connect to. Usually this type of security benefits everyday communications such as credit card transactions, private passwords and keys, social security numbers, and other similar information from being sent over a network using plain text (as it is used to doing). This information, when it is sent as plain text, is in danger of being intercepted by an attacker. A malicious hacker can listen to your insecure connections and "eavesdrop" on your communications. This can lead to identity theft, stolen money, and other headaches that can be prevented by secure technologies. SSL is one solution to this problem. As a matter of fact, SSL is a protocol that lets the server and the client know how to expect the incoming data to be encoded. The data is first encrypted, using the specification supplied by SSL, into an indiscernible string of data. This data is then sent over the network and to the server where the server, knowing how to expect its incoming data, decodes it using the same specification and decides what to do with it from there (logging a user in, processing a payment, etc.). The beauty of SSL, however, is that the specification we discussed is one that is only known to the client and the server, so it is completely unique to that session. This is where the security of SSL lies. It establishes these keys between the client and the server through its initial connection between the two. After the two have identified with one another, the keys are shared, and communications can proceed. These keys are the specification as I mentioned before. They allow the two nodes to decode one another's information during transmissions (Digicert). Without this, the web would greatly be a different place. To point that out, credit card payment gateways would be much harder to trust. Forms requesting social security numbers would be dismissed as malicious phishing attacks. We certainly would not be at the level of comfort with online communications that we are today. Technologies available to protect and serve the public have made many of our daily tasks easier.

Connecting to a website using a secure connection is just as easy as a malicious individual is capturing your information when you are not on a secured connection. It seems that as long as improvements are made to help people out, just as many improvements are

made to the opposite end of the spectrum designed to hinder your everyday life and communications. Have you ever wondered how easy it is for an attacker to retrieve your information over an insecure connection? It is as easy as downloading the right software, telling it where to listen, and relaxing in your chair while you sneakily eavesdrop on someone else's private conversation over a network. Public locations like coffee shops, libraries, office buildings, and any other location with unsecure public networks are the ideal hunting ground for people to snoop into your wireless transmissions. People are able to download free software, built by others who enjoy snooping on other people's information, and lurk on the network looking for private information they can steal. Things like credit card numbers, social security numbers, passwords, and other confidential information are what these people intend to capture. This software can observe the packets being sent over the public network and capture the information being distributed. This information, often in plain text, can be used against you if the attacker chooses. Things such as the web pages you visit, the emails you send, login information, form submissions, and any other data sent over an unsecure network are completely available for an attacker to retrieve using these methods (Geier). With all of this astoundingly simple to use software specifically to monitor your confidential communications, it appears that the world is out to get the everyday internet user. There is a hope, and it comes from a place we have already visited. Using SSL, or any other similar network security protocol, you can combat network eavesdroppers by making it nearly impossible for them to decipher your information. The beauty of this technology is that it is free to public. You are not charged to keep your internet communications safe, and that is great news to anyone who is concerned about their wireless anonymity. One downside to this type of wireless security is that it is up to the company running the website to implement the SSL security layer. Without them stepping in and actively working towards the implementation of this encryption based security, you cannot utilize it. When you access a website using your browser, and the prefix of the URL is "https", then that was made possible by an IT professional. This downside, while still a valid point, truly is not that big of a negative aspect. It is free (to you), easy to use, easy enough to implement, and it is a huge player in making sure our connections stay secure.

Another secure communication protocol is the Transport Layer Security protocol (TLS). The RFC defines the main goal of the TLS protocol as "to provide privacy and data integrity between two communication applications". The TLS protocol is made up of two parts: the TLS Record protocol and the TLS Handshake protocol. TLS must be layered over the top of some transport protocol, such as TCP, to function. The lowest level functionality of TLS is the Record protocol. The Record protocol strives to provide a secure connection between two communicating devices for the length of their session together. It can be thought as a protocol providing two basic requirements:

1. A private connection secured by symmetric encryption. The data sent during the communications between the two applications is what gets encrypted. It is done so by algorithm encryption, such as AES, RC4, and others. The private connection uses keys that are uniquely generated for every connection established, which are based on a secret key that is established between the applications during the process of another protocol (Handshake protocol, in the case of TLS). Despite this, the Record protocol can function without using any encryption techniques. This is not desirable when it is concerned with the utmost security and anonymity, however.
2. A connection should be reliable. To ensure the integrity of transported messages, a keyed MAC is used. Hashing algorithms, such as SHA-1

(Secure Hashing Algorithm), are used for the MAC computations. The Record protocol does not require a MAC, but it is only used without it when there is another Record protocol being used to transport security parameters.

The Record protocol encapsulates other, higher-level, TLS protocols. One of these encapsulated protocols is the Handshake protocol mentioned earlier. The Handshake protocol allows each end in a server-client relationship to authenticate one another. It also allows them to decide upon an encryption algorithm and unique cryptographic keys before either end ever sends any data. Similar to the Record protocol, it can be defined in three attributes:

1. The identity of the peer can be authenticated using asymmetric (public key) cryptography, such as RSA or DSA. This step of authentication is optional, and it is only required for one node.
2. The reconciliation of the shared secret to be used in the connection is secure. This is an important feature because the shared secret cannot be obtained by eavesdropping. If the connection is authenticated, the shared secret cannot be obtained even if an attacker can intervene in the middle of the connection.
3. The negotiation of the shared secret is reliable. An attacker could not alter the involved communication with the negotiation without being known to the nodes involved in the communication.

An upside of the TLS protocol is that it is independent of an application protocol already existing on the system. Other higher-level protocols can seamlessly be layered on top of TLS completely transparently, and they do not interfere with one another in the process. One part of the TLS specification that is quite peculiar and makes it stand out is that TLS does not attempt to dictate the methods used to add security with TLS. Those decisions, such as how to start a TLS Handshake negotiation and how a connection will interpret authentication certificates, are left up to the engineers developing and constructing the protocols that exist on top of TLS. TLS is not an extremely ambitious security protocol. In fact, it simply aims to provide a very flexible, easy to implement, and solid security foundation for the communication between two applications. As a protocol, TLS is said to have a very simple set of goals:

1. Cryptographic security: The protocol aims to provide a secure connection, backed by cryptographic means, to two communicating nodes during their communication session.
2. Interoperability: The protocol needs to make it possible for two completely independent applications, with no prior or current knowledge of one another's' code, to communicate securely utilizing the TLS protocol extensively.
3. Extensibility: The protocol tries to create an environment where the implementers are not restricted in the types of encryption they are able to use with it. This means that the new public key and encryption methods should ideally be able to integrate smoothly with the protocol. This single goal satisfies other sub-goals: removing the necessity of a new protocol just to implement a particular method, and not having to create a brand-new security library.
4. Relative efficiency: Encryption functions are normally very CPU intensive, due to a high amount of operations that need to be executed to successfully

> encrypt the data, during the generation of public keys. Because of this, TLS utilizes a session caching scheme that reduces the amount of connections to need to be spawned. Also, the designers have taken the amount of network activity into consideration and desire to limit it as much as possible.

These overall goals for the TLS protocol can be summed up to cover the quality and speed in which it is able to operate. TLS is just one more example of the available secure communication protocols obtainable for developers to use in their applications. TLS is available for use in all realms of software, and it is used quite often. TLS options come automatically in the Microsoft web realm on their Windows Server, IIS, and Internet Explorer software suites (This section from RFC 5246 sourced below).

Having security protocols readily available is a big proponent for their continued purpose and popularity. However, just like the SSL protocol, it is up to the developers and engineers to utilize TLS for its benefit. It is a shame when extensive websites that receive copious amounts of traffic do not adhere to these security rules, but instead they choose to ignore them. These websites are putting their users at risk by denying them the right to operate their sight securely. Websites that allow their users to purchase via credit card, or event through connecting a bank account, are at risk for wireless snooping from malicious attackers. This is horrible, unsafe, and needs to be fixed. Every website that utilizes any kind of confidential information such as card numbers, social security numbers, bank accounts, or even passwords (because people often use the same password for many things, meaning if one password is snooped on, the attacker can most likely access other accounts owned by that user) should be using the free, easy to implement software found within these security packages. Until we get one hundred percent cooperation from every trafficked website on the internet, the web will continue to be a place where malicious attackers can eavesdrop on other people's communications. As long as this is true, people need to be careful with what they submit online. Anything and everything can be obtained simply from having the correct software installed, and by being in the right place at the right time.

Earlier in this paper I mentioned a technology known as Tor. Tor is perhaps one of the coolest and the most intriguing technology that has emerged as a result of the wireless anonymity craze. Tor, a project started in the early 2000's (approximately 2003, this is as far back as their issue tracking tickets go) is short for "The Onion Router". It is called The Onion Router because the onion (the vegetable, not the fictitious news network) is used as the project's mascot. The thing that is similar to the two is the fact that both of them are made up of layers upon layers. An onion, if you have never had to peel one before, is made up of layers expanding outward from its core. To get to the core (or out of the core, probably a better analogy, but I digress), you must traverse these layers by either peeling them away, for the sake of this analogy, piercing the layers, or traveling through them until you get to your destination. This analogy is perfect for what the Tor project aims to do! The Tor project, in essence, masks your online identity anonymously (in a way that will be described shortly) so that you can travel the web and pass through all networks attached to it. It does this in a very unique and innovative way. The Tor network is developed, operated, and maintained by a group of volunteers determined to keep the internet a place of private travels. Basically, these volunteers take on many tasks to benefit the project, such as contributing development to its repository (it is open source, go figure), using the software and reporting any bugs, or by running a relay for the network. The latter option is the true heart and soul of Tor. Volunteers can maintain and operate relays to be used by nodes traversing the Tor network. So basically, imagine if you have a spare computer that you have never been using (or going to use), and

you were a big advocate for wireless anonymity. You could play a significant part in helping the internet to become more anonymous by "donating" your unused computer to the Tor project as a relay. All you would have to do is download a certain software of the Tor project's website (do not worry, they use SSL), install the software on your computer, and as long as the computer is connected to the internet it would contribute to the cause! The software that continuously runs on the relay stays in constant contact with other relays on the Tor network. Each node on the Tor network is aware of other nodes in their proximity (proximity is relative of course). This allows a node to seamlessly communicate with any other node on the network. Because of this, the nodes on the network are able to leapfrog to and from one another without a hitch. This, for lack of a better phrase, is where the magic happens. Since each relay is aware of other relays that are also connected to Tor, and Tor acts as a closed network consisting of only these relays, they are able to select a random path from one node to an end server (routing it through the random path of Tor relays) outside of the Tor network. In a broader sense, each Tor relay is open to receive communications from any other Tor relay. So, one Tor relay is able to accept a communication from a Tor user (for the sake of our earlier example, think of this as your PC running the Tor client software) and hand those packets off to another Tor relay, essentially making sure that your packets end up coming from such different locations across the globe that they are virtually impossible to track down. As a Tor user, all you have to do is download the Tor client software, install it, and start surfing the web (or however else you intend to connect remotely to servers across the planet). It is really that simple. The software will continuously watch for outgoing packet transmissions and make sure to route them through a randomly selected chain of Tor relays ultimately ending at your desired end point (most likely a web server serving you a file to your browser). Thanks to projects such as this one, everyday people are able to take their privacy into their own hands. After all, using software such as this, we are able to rely on ourselves instead of rely on a third party. As long as a person is running Tor, Tor relays stay open, and the Tor project stays alive, and wireless anonymity will be free to use for anyone who needs it (Tor: Overview).

One thing that I continually mentioned throughout this paper is open source software. Open sourcing software is the act of releasing the code that makes up your software for the world to see, contribute to, and use at no cost. These projects are often released under some license (such as the MIT, Apache, etc.), and are protected in terms of other's taking credit for the work of someone else. Open source software, however, is another big movement that is helping wireless anonymity and security much more than other things. When a project is released as open source software, anyone who has access to the internet has access to the code that makes up the software. This is an incredible advantage for the developers who maintain the project. It is so because those people who view the code are able to notice potential bugs in the software. A bug in software is often times synonymous with a "hole", which allows someone to maliciously take advantage of the software's weak points. Holes are obviously not good, and often small software teams are not able to spot every hole that may be lying in their project's code. However, thanks to open source software communities, it is becoming a much easier thing to handle. Projects can go open source, allow an extremely large amount of people to view, contribute to, and use the software, and everyone ends up benefitting in the long run. Holes are patched, features that once seemed too daunting of a task are implemented, and projects become more than they ever would have been without the open source contributions. To give an example of some famous open source software, I will use Chromium as a prime candidate. Chromium is the foundation software for the Google Chrome web browser as well as the Google Chrome OS. It is known as safe and secure, and it is mainly used for these aspects along with its user friendliness. Most people who are not in

the development community do not know that it is also open source software. Chromium is made to be safe, secure foundation for other software (particularly web browsers). Anyone can go and use the Chromium project as the foundation for their own web browser if they wish. A large part of Chromium's success as a secure and a reliable piece of software is due to the fact that it is an open source. Without such an idea, and a community, there is no way to tell how far along secure software would be today. As citizens who are concerned about our privacy and security, we owe many thanks to the open source community (The Chromium Projects).

As a person who is aware of the importance of wireless anonymity and security, I am glad to see that there is a rapid growth being made in the information technology industry. Thanks to large companies who have considerable influence in the software development industry spreading the importance of such awareness (such as. Google, Mozilla, etc.), more big players are starting to pay attention and give citizens what they deserve. The events that people, such as Edward Snowden, brought to light are inexcusable. No government should ever be allowed to spy on their people without proper cause, especially, a government built upon the foundation of freedom and democracy. It is despicable to think that our own policy makers are citizens themselves, and would do such a thing to their country. Because of open source security projects, we are beginning to get past this phase of wireless privacy infringement. Eventually, people will no longer be able to snoop in on other people's communications. We owe our thanks to these teams that have made such a thing possible, lest we take them and their service for granted.

## 3RD GENERATION PARTNERSHIP PROJECT

3rd Generation Partnership Project is an integration of seven telecommunications standard development organizations as 'Organizational Partners'. Seven telecommunications standards ARIB, TTC, ETSI, TSDSI, TTA, ATIS, and CCSA and these standards combinedly develop a dominant common standard. The collaboration of these standard organizations has standardized our mobile communication previously, and their progressive results were: GSM, GPRS, EDGE, HSPA, HSPA+ and LTE. 3GPP's main areas of interest were: on the service, concentrating on core networks and radio interfaces. The multiple access techniques were used to evolve Time Division Multiple Access to Code Division Multiple Access to Orthogonal Frequency Division Multiple Access, and the OFDMA access technique is what is used in LTE.

3GPP introduced LTE to the cellular market, and it is only the system which made a unified approach in telecommunications industry. It is widely spread in telecom market due to 3GPP. 3GPP released its first version of LTE in the year 2008 as 'Release 8'. The main strategies 3GPP considering for the future: Increase in the robustness for the future smart phones trending traffic flow, Improving the capacity and performance of LTE standard, opening the windows of LTE towards new business segments. Now, they are collaborated to evolve our cellular mobile communication to the next level '5G'.

The body of 3GPP has disintegrated the 5G into four major areas to concentrate more on the area. The major areas to concentrate: Massive Internet of Things, Enhanced Mobile

Broadband, Critical Communications, and Network Operations. Like, 3GPP other bodies which are working towards the 5G are: NGMN (Next Generation Mobile Networks): it associates leading operators, vendors, manufacturers, and universities. GSMA, 5G-PPP 'public private partnership' initialized by European Commission, IETF, and IEEE. 3GPP believes that LTE (Long-Term Evolution) will only be the standard that they are depending on. There is a possibility that they are going to reach the maximum limits of LTE, but they must improvise the current standard of LTE, such that they are compatible with the 5th Generation Mobile Communication. LTE will remain as a key factor for wide area broadband coverage of 5G era.

## 5G: THE NEXT GENERATION MOBILE COMMUNICATION

The next generation of mobile communication is about the connectivity to every electronic device. Unlike the predecessors of the cellular communications the main agenda that the 5G cellular communication is considering is to: provide better coverage, greater connectivity, higher reliability, greater mobility range, higher throughput, and lower latency. These features will be featured by different network layers, implies directly to the need of provision of an identity, security, trust, and privacy. Currently, we have IMT-Advanced/4G standard in the market. 5G standard plans to accommodate more number of users per unit area than that of the 4G, it aims for greater capacity with faster internet connections. Allowing greater speeds of internet service, for example, in gigabytes for every user without any latency in the service, thus allowing user to stream the HD videos for hours long without any interruptions. The internet of things is what the 5G is about, for instance, end to end communication; machine to machine communication is what 5G is targeting. Till now the 5G is just a theory without a standard, but there are some basic requirements 5G is going to be based on, like:

- Lower latency duration, for example, less than 1ms.
- Greater battery efficiency of the device
- Internet of things: Connectivity to everything, i.e., smart homes, machine to machine connectivity.
- Cloud based data storage and retrieval, big data.
- Improved security, privacy, and storage.
- Connectivity of millions of devices around the world to the world-wide web at speeds of gigabits per second.
- Greater connectivity and mobility to the networks with reduced call drops and increased handover capabilities.

## GEARING UP FOR 2020 & BEYOND

The technological innovations that lead the world to move forward in a faster pace, 90's of the hippies have changed the digital world. Now, our handheld devices have: Processing speeds clocking at 1 Gigahertz, Some GB's of storage space, 1920 X 1080 Pixels per inch screens, high performance OS, Artificial Intelligence, and anywhere accessibility to

the world-wide web and much more. The data hungry devices need more data, greater speeds, and security. Every year the number of internet users increases, and the time they spend on the internet are increasing as well as the network traffic is increasing; therefore, people are expecting the best innovative technique ever to make their work in a simple manner. The thought of 5G has evolved with evolution of their technological innovations, and 5G defined the standards that must be based on the requirements that they have defined. The deadline that has been set by the Next Generation Mobile Networks Alliance is around 2020. The Next Generation Mobile Networks Alliance feels that the 5G evolution is set to change the industries to evolve for a new era of chip designing and base stations with new, fast, and sleek application processors. The evolution the cellular communication has progressed through first generation to fourth generation. 1981: The first-generation mobile communication which is analogous in nature. 1991: The second generation used GSM and introduced MMS & SMS services, data rates of 64kbps. 2001: After 10 years of 2G service, the introduction of smartphones which are more addicted to data usage, the speeds introduced were of 2Mbps. The 3G era was web based applications and video files. 2012: Current cellular communication speeds up to 1Gbps, principled with the concept of mobile broadband everywhere. 2020: International Telecommunication Union planning to launch the fifth-generation mobile communication which speeds some thousand times faster than that of the 4G. South Korea is planning to localize trail during Winter Olympics. Many companies are involved in the research and development of 5G, recently, Samsung has made its first steps of achievement in attaining the speeds of 7.5Gbps in a 'stationary environment' & speeds of 1.3Gbps uninterrupted service while travelling at a speed of 63mph.

On September2015, ITU- Radio Communication finalized its views towards International Mobile Telecommunications, for instance, encompassing both IMT-Advanced and IMT-2000 of 4G into IMT-2020 for 5G. The approved spectrum for 5G by Federal Communications Commission (FCC) USA in the bands of 28Gigahertz, 37 Gigahertz and 39 Gigahertz, it was approved on 14$^{th}$ July 2016. ITU set deadlines for the launch 5G service worldwide. Standardization details deadlines are:

- 2017 as the year for the submission of templates, evaluating the requirement and methods to follow.
- 2018-2019 for proposal submissions.
- 2019 for evaluating the submitted proposals before standardizing.
- 2020 for IMT-2020 publication.

## 5G SECURITY

The security issue is a major concern from the beginning of the time of cellular mobile communication. The security in the systems has tremendously improved and yet remains a vital concern in the industry. 5G is wider than 3G, 4G, or any mobile generation because everything we see in the 5G is completely profound to the online internet world, 5G attracts more number of cyber-attacks. Main qualities of 'Security' involves: integrity, privacy & availability. That implies that high level sorts of security prerequisites can be

recognized as: Security of service layer, Privacy, Integrity & Authenticity of transmission of data over different network layers, Security of network application.

Technological changes, abilities, services, regulatory requirements, and new security concerns will surface with a new beginning of 5G just as every new product in the market. More and more security standards will be under developing stage until a standard of good security ability is finalized. The current 4G security standards are confined to 4G itself since the use of virtualization and cloud in 5G encourages the telecommunication industry to develop a better secured and trusted model to be developed. The whole agenda again must consider the efficiency and performance since it should degrade the efficiency and performance of the system. The security should be considered between end to end communication, such as machine to machine and not just confining to one device alone.

## DENIAL OF SERVICE ATTACKS & DISTRIBUTED DENIAL OF SERVICE IN 5G

It is an attack on the network, which floods the networks with unwanted traffic and making the network congested. Teardrop and Ping of Death attacks are examples of DoS attacks. The flooding of traffic is caused by one computer, and one internet connection on the target whereas, in DDoS the flooding of unwanted traffic is from the multiple computers and multiple internet connections on the targeted source or user. There are different types of DDoS attacks such as on the attacks on traffic, bandwidth, and application. These attacks are originating from the machines that maybe located far away; moreover, DoS tends to steal and deplete the logical and physical resources of the target. The attacks are categorized into two types: From a network manager perspective: supporting network infrastructure will be exhausted because of these attacks on the targeted network. This will make the network users who are connected through this network indirectly suffer. From the user or devices perspective: These attacks are targeted to deplete the information of the user or on large number of users which can indirectly effect the operator resources.

- The physical resource DoS attacks on the users: CPU, Memory, Battery, Sensors, etc...
- The logical resource DoS attacks on ‘users’: Configuration, Applications, OS, etc...

## 5G SECURITY REQUIREMENTS

5G security requirements includes identifying and defining application, user, device, network, service, ability to handle security for the operations that require less latency period, authenticity, privacy, and integrity of data with less complexity. Encrypted data movement acroases the nodes without any decryption capability from any third party in the network is a basic requirement. These requirements can be backed up or the strategy that should be based on:

- Management of credentials and identity,

- Protection towards user data,
- Assuring security,
- Strong monitoring,
- Security update and management mechanisms.

## CRYPTOGRAPHIC TECHNIQUES

With few resources in hand, building a security standard for 5G is a difficult task, for example, the system built should be compact, sleek, efficient, and powerful, building a cryptographic system with limited resources is a complex job and difficult to estimate. The data traffic is set to increase in the coming years as more and more number of device connectivity is expected in the coming years. 5G has greater data speed (in Gbps) and expecting higher traffic, for example, something around thousand times greater than that of the present LTE, and low latency should be considered in building a secure system. In general, there will be a tradeoff between speed and size of hardware for building a secure system which is a severe setback. Ciphers like 'Grain' has high propagation delay and Ciphers like 'Trivium' use too many 'flip flops' to maintain the security level, such as cryptography must compromise w.r.t speed or size of the hardware.

In cryptography for encryption purpose, there are different types of cyphers and those are categorized as stream and block ciphers. Block ciphers research started some fifty years back, and the development led to Advanced Encryption Standard (AES) algorithm, which is secured and it can withstand different kinds of attacks. The most recent ciphers are known as Stream ciphers as binary additive stream ciphers. At this point, the plain text, the key, and the cipher text are all in binary sequences. The key is generated by a keystream generator in which it attains a secret key and initial value as a source, and these generate a random sequence of 1's and 0's. The ultimate cipher text is, thus, attained by the bit-wise addition of the generated key and the plain text. Stream ciphers are sleeker and faster than block ciphers as in the case of Trivium and Grain.

Recent innovations and research made the block ciphers too in the size of Trivium and Grain. Examples of block ciphers which are almost the same capabilities as Grain and Trivium are Piccolo, LED, PRESENT, TWINE, and KATAN. The block codes are mostly for radio frequency identification tags and they can be clocked at frequencies of 100KHz, yet some of them can be clocked even faster up to 1Gbps. However, stream ciphers are naturally the best choice when considering compact size and higher throughput. Global System for Mobile Communications (GSM) ciphers A5/1 and A5/2 belong to stream ciphers category. As we have seen that the stream ciphers are sleek and fast, yet they were found susceptible to attacks. So, later they were replaced with more secure stream cipher A5/3 in place of A5/1 and A5/2 was restricted from any further use.

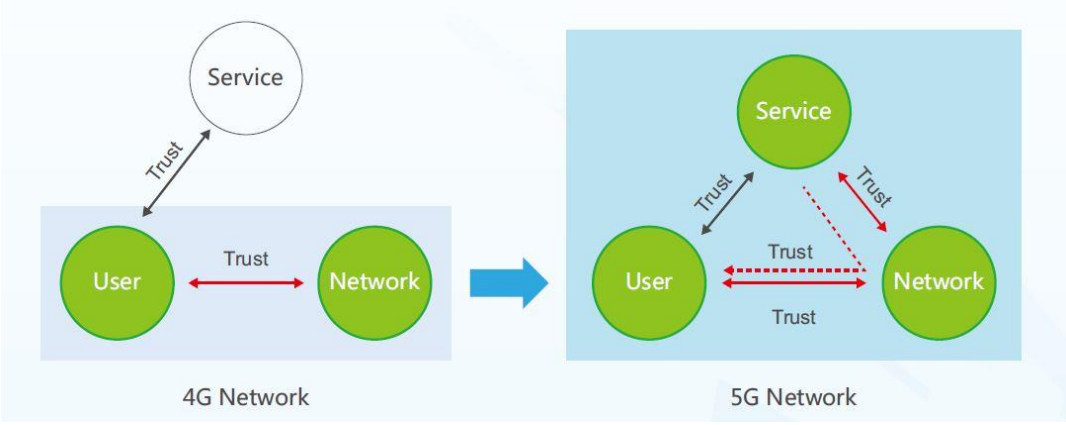
KASUMI belongs to the block cipher category which is used in GPRS, UMTS and GSM cellular mobile communication systems. GPRS uses 'GEA3' as 'keystream generator'; GSM uses 'KASUMI' in 'A5/3' keystream generator and UMTS where KASUMI is used for

'integrity' and 'confidentiality' as 'f9 and f8' algorithms as UIA1 and UEA1. KASUMI has a key size of 128 bits and a block size of 64bits. The Kasumi cipher is replaced by AES in 4G-LTE. 802.11 used something called RC4 especially for 'secure wireless networks'; nevertheless, the drawback was used for the same keystream twice. Therefore, basing on the results from previous standards, it was replaced by AES in 802.11i and the latest standards. 4G LTE mobile network used 128-bit AES algorithm after a careful observation and simulation, LTE-SAE security uses EIA2 or EEA2 as its options and these are based on AES. WiMAX uses168-bit digital encryption because, in WiMAX, the transmitting data should be secured when used air as a medium. The concept of combining the encryption models with the AES is now a trend among the researchers to produce more secured system. 4G-LTE uses three cipher suites which were introduced by 3GPP for UMTS system. One from block cipher and two from stream cipher, and block cipher used KASUMI; the two stream ciphers are SNOW 3G and ZUC.

The A5/3 cipher can be replaced by much advancement such as in block cipher. XXTEA is a block cipher, which is a 'Corrected Block TEA'. It was designed to counter the weakness of Block TEA, and it is dependability on variable-length blocks that are multiples of 32 bits in size and the minimum acceptability in size is 64 bits. However, the acceptance rate is higher in stream ciphers.

## TRUST MODEL

Previous versions of cellular mobile communication networks and the authentication process to the network for a user is the responsibility of the telecommunication networks.




2. Trust Model Evolution, Koteswararao, 2016.

In previous version, a trust is formed between the network and the users but not between the network and the service providers. Unlike the trust model in the 5G networks, the trust is only between the user and the network just as in the 4G. The trust model of 5G is more secured in which the networks communicate with the service providers, and it establishes a secured connection between the user and the network, making it more efficient and secured way of identity management.

## AUTHENTICATION MODEL

The 5G era would change the businesses around the world with abundant of services they provide. Different businesses require different authentication techniques. The service providers try their best to provide their service at lower costs with simplicity. The possible authentication models that could exist in the 5G era for different business needs:

- Network Authentication:
  Service providers must first pay to the networks, and then the service authentication will be granted so that the users can access through the services through single authentication. This procedure incurs costs on service providers.
- Service Provider Authentication:
  Networks relay on the authentication from the service providers, and there is no necessity for any network access authentication. It implies the incurred costs on operating the networks are lowered.
- Service Provider and Network Authentication:
  In this case, networks are undertaken by the network access and services providers stick with the service access.

## CONCLUSION

5G security and privacy design must be integrated along with 5G system, moreover, 5G cellular mobile communications is vast, and it can encounter more threats from the third-party intruders. The need for stable cryptographic techniques is necessary when developing 5G mobile communication. The researchers and many academic institutions have a keen interest in the prospering field of 5G. As we can see a combination of cryptographic technique with Rijndael to form a more secure system or some say corrected block, TEA is better than the previous versions of A5/3 as in 4G. The ciphers should be sleek and fast, as we cannot compromise on either one of them alone. The latency time in 5G is too low that the ciphers must act quickly. Although there have been an extensive research and considerations for building a copmrehensivcve and secured sysetms by vendors, and academicians, but at present, there is still uncertainty about privacy and security concerns from the stakeholders. It is the right time to act upon the mistakes of the past; furthermore, the system design of 5G is new, and it will be efficient if the feature is considered in the early stage of 5G. 3GPP has decided to use LTE system with release 15, for instance, upgradation of LTE to utilize it in 5G mobile communications, and 5G is set to launch 5G by 2020.

# REFERENCES

"Anonabox | Tor Hardware Plug and Play Onion Router." Anonabox. Web. 16 June 2015.

Geier, Eric. "Here's What an Eavesdropper Sees When You Use an Unsecured Wi-Fi Hotspot." PCWorld. PCWorld. Web. 17 June 2015.

"What Is SSL (Secure Sockets Layer) and What Are SSL Certificates?" What Is SSL (Secure Sockets Layer)? Digicert. Web. 17 June 2015.

"Tor: Overview." Project: Overview. Tor. Web. 18 June 2015.

"RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2." RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2. Web. 20 June 2015.

"The Chromium Projects." The Chromium Projects. Web. 23 June 2015.

Fragkiadakis, Alexandros, Antonis Makrogiannakis, and Stefanos Papadakis. “Signal Processing Techniques for Energy Efficiency, Security, and Reliability in the IoT Domain”. *Internet of Things (IoT) in 5G Mobile Technologies*. Ed. Elias Tragos. N.p.: Springer, 2016. 416-448. Print.

Sima, Ion., D. Tarmurean, V. Greu, and A. Diaconu. "XXTEA, an Alternative Replacement of KASUMI Cipher Algorithm in A5/3 GSM and F8, F9 UMTS Data Security Functions." *Communications (COMM), 2012 9th International Conference* (2012): n. pag. IEEE. Web.

Dubrova, Elena. "Espresso: A Stream Cipher for 5G Wireless Communication Systems." *Cryptography and Communications*. Ed. Martin Hell. Vol. 8. N.p.: Springer Link, n.d. 1-17. Print.

Kaul, Vikas, Bhushan Nemade, Vinayak Bharadi, and Narayan Khedkar. "Next Generation Encryption Using Security Enhancement Algorithms for End to End Data Transmission in 3G/4G Networks.": 1051-059. *Science Direct*. 2016. Web.

Yan, Zheng, Peng Zhang, and Athanasios V. Vasilakos. "A Security and Trust Framework for Virtualized Networks and Software-defined Networking." *Security and Communication Networks* 9.16 (2016): 3059-069. Wiley Online Library. Web.

Jungnickel, Volker, Kai Habel, Michael Parker, Stuart Walker, and Carlos Bock. "Software-defined Open Architecture for Front- and Backhaul in 5G Mobile Networks." (2014): n. pag. *IEEE Xplore Digital Library*. IEEE. Web.

Chitimalla, Divya, Koteswararao Kondepu, Luca Valcarenghi, and Biswanath Mukherjee. "Reconfigurable and Efficient Fronthaul of 5G Systems." *Advanced Networks and Telecommunications Systems (ANTS)* (2016): n. pag. *IEEE Xplore Digital Library*. IEEE. Web.

Marcus, Michael J. "5G and "IMT for 2020 and Beyond" [Spectrum Policy and Regulatory Issues]." *IEEE Wireless Communciations* 22.4 (2015): n. pag. *IEEE Xplore Digital Library*. IEEE. Web.