ANALYTICAL MODEL FOR SECURITY IN 5G NETWORK

S. Selvakumar[1], A. Jency[2], Prianka R R[3], Hilda Jerlin C M[4], Ruhi Bakhare[5], Amara S A L G Gopala Gupta[6]

[1]Department of Computer Science and Engineering, Aarupadi Veedu Institute of Technology, Vinayaka Mission Research Foundation, Salem, Tamil Nadu 636308, India. **selvakumar.avcs085@avit.ac.in**

[2]Department of Artificial Intelligence and Data Science, RMK College of Engineering and Technology, Thiruvallur, Tamil Nadu 601206, India. **jencyads@rmkcet.ac.in**

[3]Department of Artificial Intelligence and Machine Learning, New Horizon College of Engineering, Bengaluru, Karnataka 560103, India. **priankabibin@gmail.com**

[4]Department of Artificial Intelligence and Data Science, Panimalar Engineering College, Chennai, Tamil Nadu 600123, India. **ruthjerry97@gmail.com**

[5]Department of Computer Science and Engineering, Dr. Ambedkar Institute of Management Studies and Research, Nagpur, Maharashtra 440010, India. **ruhibakhare@rediffmail.com**

[6]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh 522302, India. **amara_gupta@yahoo.com**

Abstract:-

In 3GPP mobile networks, application data is sent wirelessly between a phone and an access point. The unique feature of the mobile network wireless connection is the transfer of a channel endpoint when the phone travels from one access point to another. Various publications have examined key evolution during handover, but they have not combined this study with an examination of the wireless-link application-data encryption protocol. We provide a game-based security framework for such channels to allow the formal study of the 4G/5G wireless connection. We also offer flexible key insulation security ideas for application data transmission, including forward and backward security in the provided adversary model. We integrate a bidirectional application data transfer channel with a general framework for multiparty channel evolution protocols in our modular ideas. The security of the channel-evolution protocol may depend on the security of the data transfer channel for part or all of its messages due to the interaction between these two components.

Keywords:- 3G, 4G, 5G and Wireless Networks

1. INTRODUCTION

In the context of complexity theory, we also provide the first formal model of 4G/5G wireless connection security that takes into account both handover key evolution and application data transmission. Regarding our security assumptions, we demonstrate that the model is safe. As a side effect, we come up with suggestions for

enhancing the security of next mobile network standards to accomplish critical insulation. In particular, we demonstrate that the present standards fall short of achieving forward safe encryption, despite the fact that it seems like an express aim. We demonstrate how to fix this. Around the globe, Fifth Generation (5G) testbeds are now being established to create, implement, and test 5G networks, platforms, and cutting-edge technologies. The purpose is to assess new apps' and use cases' performance as well as the interoperability of new radio equipment and mobile network components. The Third Generation Partnership Project (3GPP) is developing 5G standards, which include identity management and processes for user privacy assurance, to protect the network core, radio, and user equipment. To create new companies, guarantee that vital applications can run securely, and fully qualify and understand the risks throughout the whole eco-system, it is crucial to comprehend these linkages. Procedures for identity management and privacy assurance must be connected to user permission and data processing methods [1]-[5].

The ITU's vision for 5G defines use cases with a wide range of technical performance and system requirements, necessitating the interconnection of mobile networks with several non-3GPP network technologies. A single network operator in their own niche cannot do this. Interoperability between networks, which must also be safe and reliable, is unquestionably necessary. Despite the fact that the 3GPP has released 5G standards that outline interfaces for inter-network communications, more work is still required to advance interface functionality, performance, and security. Effective collaborations between various network operators, equipment owners, such as transportation firms, regional and municipal governments, and publically sponsored organisations are required to achieve smooth interoperability. It is necessary to safeguard network boundaries across all borders in order to provide end-to-end security [6]-[10].

The interaction of 3GPP and non-3GPP networks, new 5G use cases with various needs, new 5G technologies, and evolutionary techniques in the mobile network all contribute to the complexity of the new platforms. Due to the increased attack surface and new security vulnerabilities that result, it is critical to carefully assess the risks and vulnerabilities and develop action items to mitigate them. Additionally, there is a trade-off between network speed and security due to the many difficulties in deploying secure 5G networks and satisfying the criteria of diverse 5G use cases. Increasing network-to-network complexity, end-to-end cross-layer system security, and important applications will make it impossible to use traditional security measures. To address these issues and keep traditional security measures from jeopardising the necessary 5G performance, new technologies will be needed. Context-aware networks and artificial intelligence (AI), which can analyse context transfer patterns and correlate them with user, device, application, and security context meta-data to generate predictions, offer the UK a tremendous potential for innovation. As a result, the network will be able to foresee and pre-validate the necessary end-to-end security and connection before the UE requests the service, ensuring that the system setup is one step ahead of the dynamics of the UE behaviour and context.

The report reviews probable flaws and problems that might occur in 5G networks and identifies areas where standardisation organisations, business, and academics can collaborate. To this purpose, the study assesses the breadth of the security flaws that the complexity of 5G systems introduces, and it emphasises the need for end-to-end, cross-domain, and cross-layer security in 5G. The purpose of the document is to provide the first benchmarks

for security implementation and testing for 5G networks, not only for the testbeds being constructed by the Collaborators but also for comparable networks, trials, and testbeds throughout the globe aiming to integrate 5G system(s). The study highlights the importance of end-to-end security as an essential component of 5G networks, which must be in place by design, by taking into account various security layers and novel characteristics unique to 5G [11]-[14].

2. NETWORK FRAMEWORK

Without a system or framework that enables operators to commercialise the different feature sets and services, 5G networks would not be feasible. Release 15 and Release 16 papers from the 3GPP include a number of 5G standards. Figure 3 illustrates the modular structure of the 5G system architecture as released by the 3GPP in the technical specification document TS 23.501. This layout enables the core network's components to be instantiated numerous times to support virtualization and network slicing technologies. The goal of the design is to eliminate the data overlay that was usually employed in earlier versions of mobile networks. Architectural adjustments were required to support feeding a large number of devices (huge IoT), producing sporadic traffic, while managing the enormous volume of video traffic across mobile networks expected for 5G networks. The need for user plane E2E latency to be less than 5 ms also demanded an architecture modification, allowing for the involvement of just relevant network functions for individual data sessions as opposed to the core network as a whole across heavy connections. Reduced latency requirements are also a result of certain use cases, such autonomous cars, being supported by 5G. Overall, 5G is anticipated to have 5–10 times less latency than 4G.

The architecture's separation of control from user plane activities, which effectively allows user plane functions (UPF) to be dynamically programmed by a control plane entity, such as the session management function, is one of its key advantages (SMF). This makes it possible for several UPFs to be centrally programmed, disseminated, and instantiated as needed over a vast area topology. These UPF components may also be linked together via the N9 interface to create a chain of user plane processing entities, each of which can be devoted to carrying out certain tasks. The access management function (AMF), where the remaining control plane functions are now centralised, enables rapid bearer installation and change as well as simpler context management across the core network. A particular component known as the network slice selection function (NSSF) has been designed to cooperate with the control plane function AMF in order to allow network slicing activities and help assign network slices to user traffic flows.

Based on past experiences with legacy mobile systems and the extra complexity of numerous 5G technologies that will now be a component of mobile systems for 5G, a variety of possible issues and difficulties linked to 5G networks may be recognised today. Since these issues are inextricably tied to the 5G system itself (which comprises of the mobile network, the access technologies, devices, and services), it is necessary to understand its structure and operation in order to identify these issues. The goal of the various technologies utilised in the network must be understood properly as part of the whole 5G system, and the design of 5G networks must be carefully taken into account as well. Otherwise, there will be more risk. Security experts can identify system processes and components that are necessary for the network to function without their help by having a system-level

knowledge of the system. Based on the principles of information assurance, information security, and cyber security, the weaknesses of the new 5G system have been evaluated in this section. The Collaborators are looking at the security issues needed to guarantee longer-term Security by Design2 methods as they construct the testbeds. In order to handle E2E security for upcoming 5G systems, this entails implementing security measures where they are applicable and readily accessible (standardised). The design team will work closely with technical security specialists on this. Additionally, it entails seeking advice on technological security architecture and information assurance prior to each significant design choice. Security-by-design ensures that risks, included controls, mitigations, and vulnerabilities are well understood and that the design team, security organisations, and users are all aware of vulnerabilities. In turn, this helps users and operators manage risk more skillfully and enhances security testing.

3. 5G NETWORKS

The interaction of 3GPP and non-3GPP networks, new 5G use cases with various needs, new 5G technologies, and evolutionary techniques in the mobile network all contribute to the complexity of the new platforms. Due to the increased attack surface and new security vulnerabilities that result, it is critical to carefully assess the risks and vulnerabilities and develop action items to mitigate them. Additionally, there is a trade-off between network speed and security due to the many difficulties in deploying secure 5G networks and satisfying the criteria of diverse 5G use cases. Increasing network-to-network complexity, end-to-end cross-layer system security, and important applications will make it impossible to use traditional security measures. To address these issues and keep traditional security measures from jeopardising the necessary 5G performance, new technologies will be needed. Context-aware networks and artificial intelligence (AI), which can analyse context transfer patterns and correlate them with user, device, application, and security context meta-data to generate predictions, offer the UK a tremendous potential for innovation. As a result, the network will be able to foresee and pre-validate the necessary end-to-end security and connection before the UE requests the service, ensuring that the system setup is one step ahead of the dynamics of the UE behaviour and context.

The report reviews probable flaws and problems that might occur in 5G networks and identifies areas where standardisation organisations, business, and academics can collaborate. To this purpose, the study assesses the breadth of the security flaws that the complexity of 5G systems introduces, and it emphasises the need for end-to-end, cross-domain, and cross-layer security in 5G. At the 3GPP workshop held in September 2015, the creation of standards for 5G networks as well as future specifications plans got under way. Phase 1 specifications were to provide the architecture for satisfying service needs, and Phase 2 specifications were to provide procedures for putting that architecture into practise. Phase 1 was divided into two sections during planning. The non-autonomous, or Non-Standalone, architecture for 5G New Radio (NR), was finished standardising in December 2017. The wireless air interface for integrating with the current LTE base networks is defined by this first official set of 5G

specifications. Due to the ability to merge 4G LTE and 5G NR networks, user data transfer now has better latency and capacity. The first phase of 5G Phase 1 standardisation was finished in July 2018. The NR Standalone architectural standards, which were made available as part of 3GPP Release 15, describe how the anticipated 5G radio network would function with a 5G network core. In addition to standardising radio networks, the structure of the majority of the 5G network core was defined in 3GPP Release 15. Current work on 3GPP Release 16 is focused on standardising Phase 2 of the 5G network's fundamental structure and use cases, which is due to be finished by December 2019 is shown in Figure 1. Nobody has a complete understanding of 5G network security yet since the 5G network core is still being standardised. But we can already draw some early judgements based on the requirements that have been made public thus far. It is important to first study the main use cases that 5G standards take into consideration in order to fully grasp the difficulties at hand.

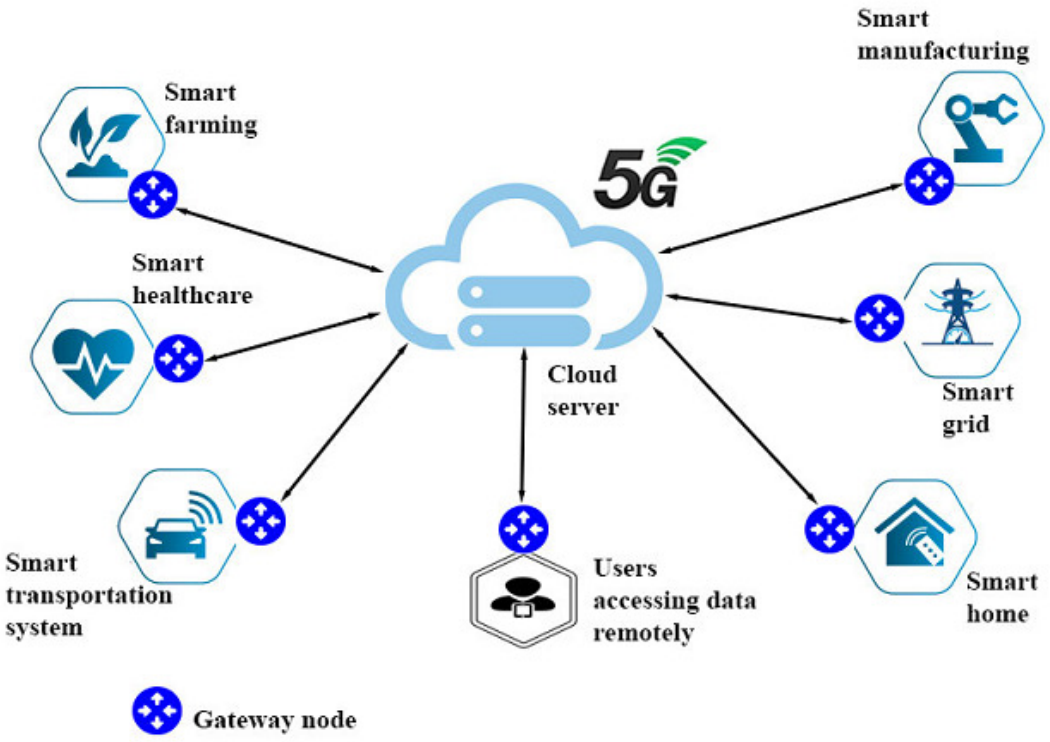

Figure.1. 5G Network

Modern civilization is based on mobile networks, which provide wireless internet access to more than 5 billion people. Their security is crucial since they are a component of important infrastructure. Secure application data transfer between the mobile phone and the network when the phone is in motion is one of its main functions. To the best of our knowledge, this safe transmission and the key evolution methods that go along with it have not yet undergone a rigorous analysis or even a defined security model. Mobile networks, which are segmented into several portions, provide wireless connectivity to mobile phones and Internet of Things devices. The serving network and the home network are the two primary components. The former offers wireless connectivity, while the latter manages the subscription and authentication for the phone. When the serving network is run by a different operator

than the home network, roaming takes place. A radio access network (RAN) and a core network (CN) are further divisions of the serving network (RAN). The RAN in 4G and 5G mobile networks is made up of a collection of access points that are linked to the CN. The phone uses what we'll refer to as the wireless connection to connect to one of the access points. This name was selected based on its location in the architecture, not on any unique radio qualities. Roaming is out of scope since we are interested in how the phone and serving network interact.

4. CONCLUSION

Data transmission confidentiality and integrity have not been explicitly examined, despite important establishment and identifier-privacy characteristics of mobile networks. One significant factor is the dearth of suitable cryptographic channel models for the wireless connection, an issue we attempt to solve in this study. We started the investigation of secure anycast channels in this publication. We introduced the first secure channel concept with interparty endpoint transmission. By building a model of 3GPP 4G/5G wireless connection security and demonstrating the model's security, we demonstrated its applicability. Our model comes quite close to the requirements. We exposed a flaw in 4G/5forward G's security and suggested a fix, outlining how future mobile networks might accomplish critical insulation and compartmentalise harm to specific access points in the event of a breach.

REFERENCES

[1] C. Yoon, S. Lee, H. Kang, T. Park, S. Shin, V. Yegneswaran, P. Porras, and G. Gu, “Flow wars: Systemizing the attack surface and defenses in software-defined networks,” IEEE/ACM Trans. on Networking, vol. 25, no. 6, pp. 3514–3530, 2017.

[2] S. Lal, T. Taleb, and A. Dutta, “NFV: Security threats and best practices,” IEEE Communications Magazine, vol. 55, no. 8, pp. 211–217, 2017.

[3] V. A. Cunha, E. da Silva, M. B. de Carvalho, D. Corujo, J. P. Barraca, D. Gomes, L. Z. Granville, and R. L. Aguiar, “Network slicing security: Challenges and directions,” Internet Technology Letters, vol. 2, no. 5, p. e125, 2019.

[4] X. Ou, S. Govindavajhala, and A. W. Appel, “Mul- VAL: A logic-based network security analyzer,” in Proc. USENIX Security Symp., vol. 8, 2005, pp. 113–128.

[5] A. T. Al Ghazo, M. Ibrahim, H. Ren, and R. Kumar, “A2G2V: Automatic attack graph generation and visualization and its applications to computer and SCADA networks,” IEEE Trans. Systems, Man, and Cybernetics: Systems, vol. 50, pp. 1–11, 2019.

[6] J. Brown, T. Saha, and N. K. Jha, “GRAVITAS: Graphical reticulated attack vectors for Internet-of-Things aggregate security,” IEEE Trans. Emerging Topics in Computing, 2021.

[7] S. R. Hussain, M. Echeverria, I. Karim, O. Chowdhury, and E. Bertino, “5GReasoner: A property-directed security and privacy analysis framework for 5G cellular network protocol,” in Proc. ACM SIGSAC Conf. on Computer and Communications Security, 2019, pp. 669– 684.

[8] Brzuska, C., Fischlin, M.,Warinschi, B., Williams, S.C.: Composability of bellare-rogaway key exchange protocols. In: ACM CCS. pp. 51–62. ACM (2011)
[9] Brzuska, C., Smart, N.P., Warinschi, B., Watson, G.J.: An analysis of the EMV channel establishment protocol. In: ACM CCS. pp. 373–386. ACM (2013)
[10] Canetti, R., Krawczyk, H.: Analysis of key-exchange protocols and their use for building secure channels. In: EUROCRYPT. pp. 453–474. LNCS, Springer (2001)
[11] Copet, P.B., Marchetto, G., Sisto, R., Costa, L.: Formal verification of LTE-UMTS handover procedures. In: IEEE ISCC. pp. 738–744. IEEE Computer Society (2015)
[12] Diffie, W., van Oorschot, P.C., Wiener, M.J.: Authentication and authenticated key exchanges. Des. Codes Cryptography (2), 107–125 (1992)
[13] Dodis, Y., Katz, J., Xu, S., Yung, M.: Key-insulated public key cryptosystems. In: Advances in Cryptology - EUROCRYPT. pp. 65–82. LNCS, Springer (2002)
[14] Dodis, Y., Luo, W., Xu, S., Yung, M.: Key-insulated symmetric key cryptography and mitigating attacks against cryptographic cloud software. In: ACM ASIACCS. pp. 57–58. ACM (2012)