International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(13s) 2026 pp. 192-204
https://doi.org/10.70917/ijcisim-2026-4050
Article

Energy-Efficient Lightweight Cryptography for Secure Sensor Data Transmission in 5G IoT Networks

Kamaldeep Kaur[1*], Sabhyata Uppal Soni[2], Sarpreet Kaur[3]

[1]Electrical and Electronics Engineering, University Institute of Engineering & Technology (UIET), Panjab University, Chandigarh, India
kamal.0902@gmail.com
[2]Electrical and Electronics Engineering, UIET, Panjab University, Chandigarh, India
sabhyatauiet@gmail.com
[3]Electrical and Electronics Engineering, UIET, Panjab University, Chandigarh, India
sarpreetdua@yahoo.co.in

Abstract: The future 5G networks have to deal with the challenge of serving the global communications of the millions of devices comprising the Internet-of-Things. Conventional 4G mobile systems have a large computational capacity, thus applications that rely on the communication of sensor data (accelerators, GPS, and others) can implement heavy end-to-end securing solutions. New 5G mobile components are however normally less capable and of low clock speed. This, consequently, requires the creation of new sensor data transmission security solutions in streaming. This paper presents a light cryptography technology as a way of ensuring the safety of sensor data over radio transmission in 5G networks. The given solution is premised on the pseudorandom number generators that are specially created to address the needs of the 5G systems. It develops a simulation scenario and a first real deployment so as to test the performance of the contribution.

Keywords: 5G Networks, Internet of Things (IoT), Lightweight Cryptography, Secure Sensor Data Transmission, Pseudorandom Number Generator, Wireless Security, Resource-Constrained Devices, Streaming Data Protection

1. Introduction

The fifth generation (5G) wireless network is one of the significant developments in mobile communication technology as it provides extreme high data rate, low latency, massive connectivity of numerous devices, and better quality of service. Such features are applicable in numerous ways including autonomous vehicles, smart cities, Internet of Things (IoT), remote healthcare, and industrial automation [1]. Nevertheless, 5G networks are more complicated and more open, which means that they present important security challenges as well, especially with regard to safe data delivery. In comparison to the past generation, 5G is very dependent on software-defined networking, network slicing, cloud computing, and virtualization that increases the attack surface. Delicate user information that traverses an eclectic and shifting network setting falls under the risk of intercepting, fraud of information, personality deceit, and denial of service attacks. Assurance of confidentiality, integrity and authenticity of data is thus an important requirement by the 5G communication systems. The 5G secure data transmission mechanisms include highly advanced encryption algorithms, well-structured authentication mechanisms, key management schemes, and intrusion detection systems [2]. In addition, new technologies related to artificial intelligence and blockchain are also under investigation to support the resilience of security. As 5G keeps on changing, creating effective and scalable security is still a prerequisite to ensure the trust of users and the security of important information.

A. Key Security Challenges in 5G

Infrastructure that is critical and is facilitated through 5G networks poses a threat to the safety of the power and the society. As an example, internet power supply systems may be hacked that will lead to the interference of electrical and electronic systems that are crucial to the society. Besides that, we are aware that the decisions require data, yet what happens in the event that said data is corrupted during transmission over the 5G networks [3]. Thus, the key security threats of 5G networks should be thought over, highlighted, and mentioned, as well as a brief description of potential solutions capable of bringing safe 5G systems should be provided. LTE weaknesses are used as a loophole to every security threat present in 5G networks. They include some such as illegal consumption of data, denial of service (DoS) by type of network devices, information leakage and audio eavesdropping. An attack tree diagram that has been used to differentiate between the wireless network security threats and core network security risks is depicted in Figure 1.

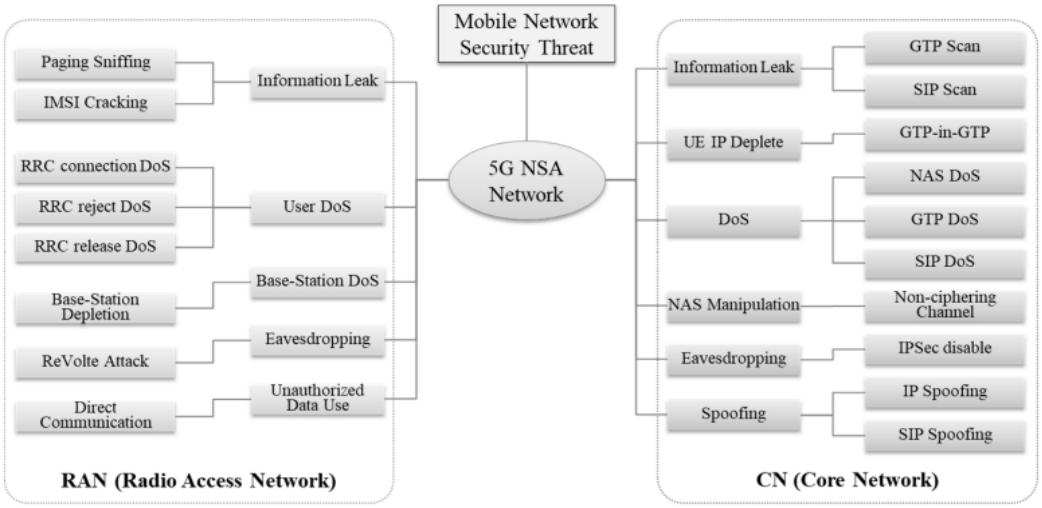

Fig 1. 5G attack tree

Types of RAN Security Threats

1. Type.R1. Information Leak: It is an attack where paging messages are used to access sensitive information including S-TMSI and IMSI. With the help of the paging cycle analysis and IMSI candidates insertion, the attackers can obtain the IMSI of the victim through the software-defined radio (SDR) and paging sniffing method.

2. Type.R2. User DoS: RRC (Radio resource control) connection DoS attacks damage the S-TMSI (SAE-temporary mobile subscriber identity) of the victim and render them incapable of utilizing the airwaves due to the issuance of RRC connection requests over and over again. By doing this, the device used by the victim is forced to lengthen the act of disconnection nearly indefinitely and this results in the unavailability of normal services.

3. Type.R3. Base-Station DoS: Attackers complicate the work of a base station by flooding it with RRC connection requests. Such requests are made with randomly generated IMSI (international mobile subscriber identity) of the victim thereby, consuming resources of the base station hence, interfering with normal operations. This, therefore, leads to the scarcity of resources and denial of service [4].

Type.R4. Eavesdropping: Comparison of the plain and the ciphered text of the following calls provides an attacker with a repeat DRB ID (Data Radio Bearer ID) used to extract the keystream of a voice call. This permits to the finding of previously made calls and hence the voice communication of the victim is made insecure.

5. Type.R5. Unauthorized Data Use: It is only possible to use the two bearers, default bearer and committed bearer as they are created in one terminal, but not to others with different purposes. Nevertheless, the attacker can utilize them differently as per the original intention and consequently, utilize the data without authorization. Specialized carrier could be used to pass information communication between terminals, without any communication charges. This, in its turn, would lead to service provider charges. Above all, direct communication may also be used in the case of caller spoofing when it is applied properly [5].

Types of Core Network Security Threats

1. Type.C1. Information Leak: The GTP (GPRS tunneling protocol) and SIP (session initiation protocol) protocols are insecure and can be exploited by the attackers to obtain the sensitive information exchanged between the equipment of the EPC (Evolved packet core) and IMS. By injecting the packets and applying the tools like Packit, they can even find out the IP addresses of the core network equipment such as PGW (Packet Gateway) by using the GTP-C messages.

2. Type.C2. IP Depletion: Through the use of GTP-in-GTP packet injection, hackers can use a core network's IP pool by pushing GTP-C Create Session Requests with more than one IP. As a result, terminals unable to acquire IP addresses are affected and thus communication fails [6].

3. Type.C3. DoS: Attackers utilizing continuously sent attach-request messages via botnets, cause a huge traffic on 5G NSA. One attach request can trigger up to eight GTP-C messages, causing a significant traffic load on the core network.

4. Type.C4. NAS Manipulation: Attackers can deploy inebriate base stations to trick NAS attach-request messages. Through manipulating the UE network capability field, they will be able to reduce or even turn off encryption, thereby making the terminal more susceptible to attacks.

5. Type.C5. Eavesdropping: By using secret menus on 5G terminals, the attacker can turn off the IPSec settings, thus, resulting in the communication being unencrypted. If NAS (non-standalone) manipulation is used with the latter, then attackers can overhear and eavesdrop on the victim's voice traffic.

6. Type.C6. Spoofing: Attackers can conduct IP spoofing by altering data traffic IP addresses, causing invalid charges or DoS attacks. Attackers can use SIP (session initiation protocol) and MMS spoofing for voice phishing by making the outgoing number look different in the SIP packet header [7].

Fundamental Methods for Protecting 5G

Following is the description of the fundamental methods of protecting 5G environment.

1. Network Functions Virtualization NFVs and Network-Slicing: To support the 5G core, RAN, and MEC, the 5G Service-Based Architecture (SBA) is critically dependent on Network Functions Virtualization (NFV) technology. NFV turns the physical hardware into a shared resource that can perform functions like Open RAN (ORAN) and Cloud RAN (CRAN) as if it were a virtualized environment. The management and orchestration of these virtual resources are the responsibilities [10] of NFV Management and Orchestration (MANO). Besides, network slicing allows the separation of multiple slices for various services, e.g., mobile broadband or latency-critical industry applications, by modifying control and user plane network operations according to individual users or companies' requirements.

2. Mutual Authentication: Mutual authentication was first introduced in 3G because it became obvious that the 2G algorithms had authentication flaws. This is by all means, an already existing near-5G technology. Nevertheless, in the case of 5G, a device first verifies that the network it is about to connect to is not fake and then responds to any security issues posed by the network. The device sends a response to the security challenge right after the network verification and allows the core network to check if the device is really legitimate.The AUSF (Authentication Server Function) is a vital component for achieving mutual authentication and key agreement processes, as it acts as an intermediary between AMF and UDM to acquire security information from UDM. In the first place, authentication confirmation is usually performed between the UE and AMF. The fact that the secret key of the device is stored at both the UDM and the UE enables the UDM to generate the 5G authentication vector using symmetric keys. Initially, the mutual authentication process along with the creation of the authentication vector is the first step before carrying out any other security measures in 5G. Figure 2 depicts this procedure of mutual authentication.

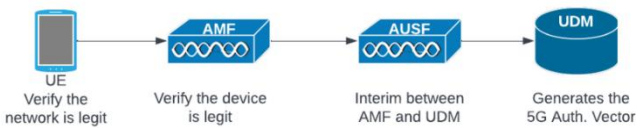

Fig 3. Mutual Authentication

3. Encryption and Integrity: As far back as the 2G, encryption and integrity check have been in place. 5G has included these functionalities for RRC, NAS, and user data plane signalling communications, in addition to other kinds of signalling messages. The UE and AMF now reveal the keys that are essential for the encryption and decryption

of these signals during the 5G mutual authentication and key agreement process. Later on, these keys are disseminated all over the system wherever necessary. However, there are some disparities in the encryption standards of these message signalling systems [11].

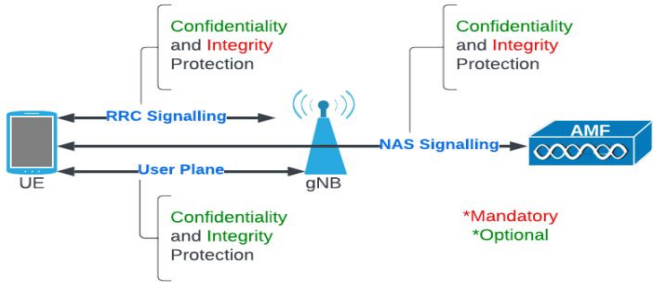

Fig 2. Encryption and Integrity

Figure 3 shows the fact that for RCC and NAS signaling messages, encryption is an optional means of protection, while integrity checking on the other hand is indispensable. For user-plane traffic, both encryption and integrity checking are optional, depending on the type of device that is connecting to the radio network and whether the encryption is necessary. In a way, the implementation of encrypting signaling messages between the user's device and network functions for confidentiality can act as a safeguard against man-in-the-middle (MITM) attacks and also against fake base station threats such as Stingray or IMSI catchers [12].

4. Service based interface protection: There are two main ways to secure 5G service-based interfaces. The first one is about protecting the protocol stack by using Transport Layer Security (TLS), which is a transport layer security protocol, between HTTP/2 and TCP. The TLS version must be 1.2 or higher. 3GPP has also clearly defined the cipher suites for TLS which are used to guarantee integrity as well as confidentiality of messages in transit. The second option is OAuth 2.0, which does not secure traffic in transit but rather protects service producers from malicious consumers who may try to invoke services with harmful requests.

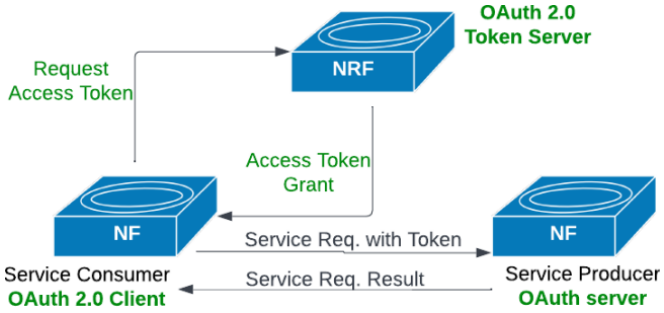

Fig 4. OAuth Token Based Authentication

OAuth 2.0 process is shown in Figure 4, which is between the service consumer and provider. OAuth 2.0 is a token-based authentication technique in which the network repository function [13] is the token server of the OAuth 2.0. A function on the network acting as a client invariably seeks an access token from the OAuth 2.0 server to access a particular service. These tokens can be limited to a certain category of network functions or very detailed so that only a specific service or operation can be executed. First, the server checks the authenticity of the token and then it gives the access. The two methods of security, TLS and token-based authentication, are used optionally.

5. Roaming and inter-connections security: Often, however, the connectivity between visited Public Land Mobile Networks (PLMN) and home PLMN is not direct. The exchange of traffic among these PLMs is mostly done via an IP Packet Exchange (IPX) provider, a third-party connection service, which the mobile operator does not own. Therefore, safeguarding traffic between these networks is a key factor. In a service-oriented architecture, this security is done by the Security Edge Protection Proxy (SEPP) service, which takes care of the control plane traffic. SEPP is the interface that provides functions such as topology hiding to obscure the sensitive addressing information, message filtering for the specific signaling messages, and traffic policing for the management of the traffic streams [14].

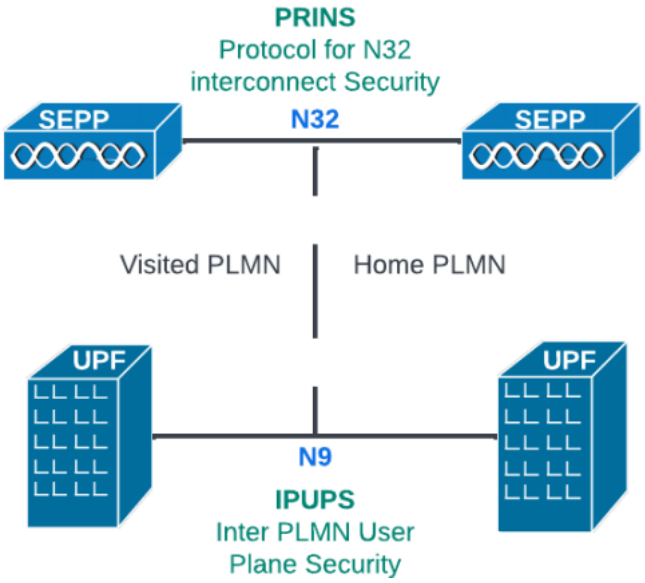

Fig 5. Roaming and inter-connections security

SEPPs, using the N32 protocol, an improvement over the 4G S6a protocol, are connected as illustrated in Figure 5. It uses TLS protection under HTTP/2 with some parts of the message optionally secured via PRINS (Protocol for N32 Interconnect Security), thus allowing protection of some parts and leaving the rest open for end-to-end routing in the interconnected network. For User Plane Function (UPF), Inter PLMN User Plane Security (IPUPS) is the used protocol which offers N9 protocol connectivity between UPFs. No traffic passes across N9 unless a pre-configured GTP v1-u tunnel is established, hence, preventing unauthorized or malicious traffic between UPFs when no tunnel is available. Moreover, both UPF should be informed about the exchanged traffic [15].

6. Subscriber Identity protection: 5G networks leverage a mechanism referred to as Subscription Concealed ID (SUCI) which ensures that user devices (UE) do not send clear text IMSI (Subscription Permanent ID (SIP) in 5G). The UE encrypts the Mobile Subscriber Identification Number (MSIN) using a public key provided by the 5G network. This SUCI is the result of IMSI being transformed into SUCI via encryption. The Mobile Country Code (MCC) and Mobile Network Code (MNC) are remaining to streamline routing while protecting the MSIN.

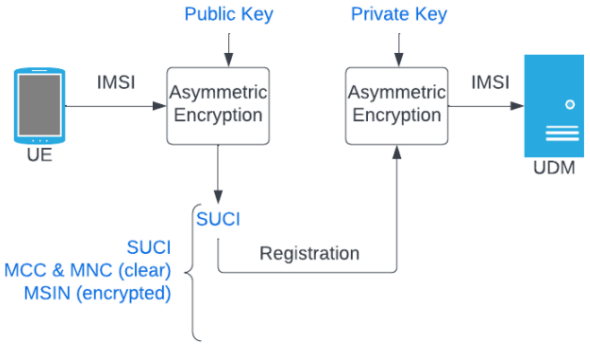

Fig 6. Subscriber Identity Protection

At the time of the registration process, the UE sends the SUCI to UDM, where it is decrypted by the corresponding private key to get IMSI. Nevertheless, including the encryption of the MSIN inside the SUCI is not an obligatory provision, and the encryption algorithm can be set to null, permitting the SUCI to be sent in clear text. Figure 6 shows the transfer process of SUCI from UE to UDM [16].

2. Literature Review

R. S. Shukla et al., (2025) introduced 5G wireless communication services and it explained that the deployment of the 5G network brought unprecedented evolution in the wireless access through the use of ultra-high-speed network

data transfer, massive connectivity rates, and ultra-low latency services [17]. The activity of such developed security features was measured in the rate of detection, reaction-time and encryption power. The results indicated that the suggested system that integrates AI-based anomaly identification improved the threat avoidance, and blockchain and cryptography that are resistant to quantum ensured the authenticity and security of the data. Upon this effort, the researchers contended that AI, cryptography and Zero-Trust policies were paramount facets to consider when developing security in new generation wireless communications. The following actions were expected to develop online threat detection, and also increase authentic quantum-safe cryptography to secure 5G networks against new cyber threats.

Y. Sun et al., (2024) suggested a generalized design of D2D relay communication [18]. The review of performance revealed that the scheme proposed had desirable efficiency relative to other related schemes. Lastly, an APP called D2DWatchmen was created to approximate the entire protocol and assess its strength and real execution time whereby the findings indicated good availability and performance. One of the resource offloading technologies in the fifth-generation (5G) network is device-to-device (D2D), which was found to be universally applicable in a wide range of scenarios in order to achieve greater speed, reduced latency, and increased capacity. Nevertheless, mobile devices were prone to security risk and privacy invasion by third parties and parties in the middle when transmitting D2D data on wireless channels. As it was observed, academia and industry had not put forth any pertinent schemes or standards in D2D relay data transmission situations.

Prakhar Consul et al., (2024) carried out three different methodologies that could help to improve the robustness and reliability of the communication architecture in 5G plus future networks [19]. Firstly, the use of the Deep Reinforcement Learning technique was supported in detecting abnormalities and defective sensors. Secondly, the consumption of energy was found as one essential attribute of the IoUT devices, and accordingly, the combination of renewable sources of energy, i.e. oxygen rechargeable batteries with nano-generators, was utilized. Also, a case study was provided, which is dedicated to the mitigation of interference in the IoUT. Finally, the article reported on the problems of research and gaps that remained in the field of IoUT.

P. Joshi et al., (2024) determined the possibility of using 5G and future versions of the network 5G (B5G) to transmit multi-sensory data, such as audio, visual, haptic, olfactory, and gustatory data [20]. With the introduction of 5G and B5G technologies, sensory information of various types can be transmitted in real-time or close to it because of the high speed, low latency, and high capacity of these technologies. This survey was aimed at concentrating on the problems associated with the transmission of multiple sensor data as part of the 5G and other network technologies and the necessity to receive this information intact. In addition, the paper solved the existing challenges of ensuring sufficient bandwidth, low latency, high quality of service, and high level of security in the transmission of multi-sensory information over the wireless networks. This was aimed at giving an introductory overview on the research, engineering and practitioners interested in exploiting 5G and B5G networks and the future scope identified potential improvements in this area.

C. Haitao et al., (2024) introduced the hybrid of unmanned flying cars (UAVs) as relay nodes as a promising method to increase coverage and minimize the use of data transmission [21]. The efficacy and dependability of data transmission in the enhanced 5G networks were enhanced in this study, by considering the orthogonal frequency division multiplexing (OFDM) technology alongside the sophisticated time and frequency synchronization algorithms and a special training sequence linear approach. The proposed system architecture with a dedicated signal processing algorithm demonstrated a high data throughput and a low rate of packet loss by means of intensive system simulation. Simulation outcomes showed that the efficiency of data transmission was augmented by 30 per cent and the rate of packet losses was diminished by 20 per cent in the varying environmental conditions which proved the resiliency and versatility of the system. These results demonstrated the revolutionary nature of drones in the optimization of 5G network and created the prospects of further improvements in mobile communications technology.

P. Zhang et al., (2023) suggested the quasi-real-time virtual key pool construction strategy that enhanced the framework of encryption service bearing through the quasi-real-time virtual key pool and presented the safe transmission of horizontal and vertical quantum keys at the point of distribution [22]. The new generation of 5G was described as the one with high capacity, high speed and low latency as communication technology kept on developing. Having become the common practice to promote and use 5G communication technology in industrial automation, smart cities, smart grids, healthcare, and other areas, the problem of the security of transmission in 5G networks was gaining more and more relevance. The use of strong encrypted communication algorithms to facilitate secure transfer of heterogeneous information data among large devices was found to be a critical issue that needs to be resolved.

R. Ma et al., (2022) created a common model of vehicle multicast service and offered a service authentication and data transmission scheme of multicast based on groups using this model [23]. The scheme involved building massive vehicles into a group under the same RAN coverage and connecting them to the content provider to have multicast services with the help of distributed keys safely through the 5G home network. The multicast service key was then sent to every vehicle to secure multicast service data that was being sent in a point to multipoint mode. The outcomes of security analysis with the help of formal verification tools and informal analysis demonstrated that the suggested scheme allowed supporting multicast service authentication and authorization, data protection, key distribution protection, anonymity, unlinkability, and resistance to protocol attacks. Signaling, computational, and communication overheads performance analysis proved that the scheme was better than other approaches associated with it.

X. Ren et al., (2022) used physically unclonable functions (PUFs) to provide a unique group authentication and data transmission strategy for NB-IoT. To achieve mutual authentication and key agreement, the PUF output was considered as a shared root key [24]. This solution reduced the signalling and communication costs associated with large device access requests by using a Group Leader to collect and convey authentication information. Using individual truncated authentication codes, the network side was able to identify phoney devices and, in cases when aggregated authentication codes were invalid, identify legitimate devices with a high likelihood. Additionally, the security of the scheme was assessed using an updated security model and the formal verification tool Scyther. The suggested solution attained the required efficiency, according to performance analysis results.

B. Shilpa et al., (2022) described a method for compressing videos utilising the H.265 standard and a LE [25]. Compared to modern encoders, this architecture offered compression with lower bandwidth requirements and was compatible with the latency and transmission speed of 5G networks. By adding LE to the H.265 protocol design, buffering latency was decreased and efficiency was raised. Metrics including PSNR, SSIM, and VMAF were used to assess the quality of video streaming. The suggested architecture performed better when the compression ratio and latency were compared with and without the H.264 architecture. Therefore, it was demonstrated that optimised data transfer based on deep learning increased accuracy and decreased computing complexity.

3. Research Methodology

An IoT scenario with 5G technologies s_{iot} is defined by a pair of sets of elements $s_{iot} = \{B, N\}$. B is the set of 5G base stations and N is the set of mobile nodes of the scenario. It can then be assumed, without losing any generality, that there is just a single base station in the scenario, i.e. $card(B) = 1$.

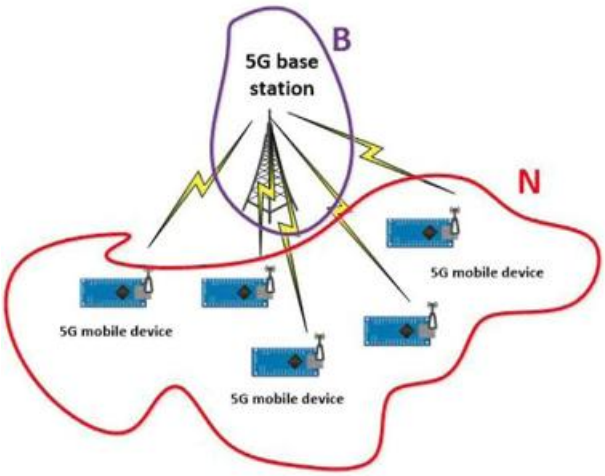

Fig 7. Study scenario

Next, two cryptographic functions are specified. Pseudorandom number generator, f_{svm} is a symmetric cipher and f_{asvm} defines a KPI, where the base station plays a central node (the element which disseminated its public key).

To start the symmetric cipher some parameters K must be shared between the transmitter and the receptor. These parameters can be interpreted as the secret key of the cipher message, since any party that is granted the same key can

get the secured messages through the encrypted message. Like that, the transmission of such parameters also needs to be secure. In addition, to ensure the presence of the secure link, an acknowledgement message must be sent, which is in accordance with the 5G mobile networks.

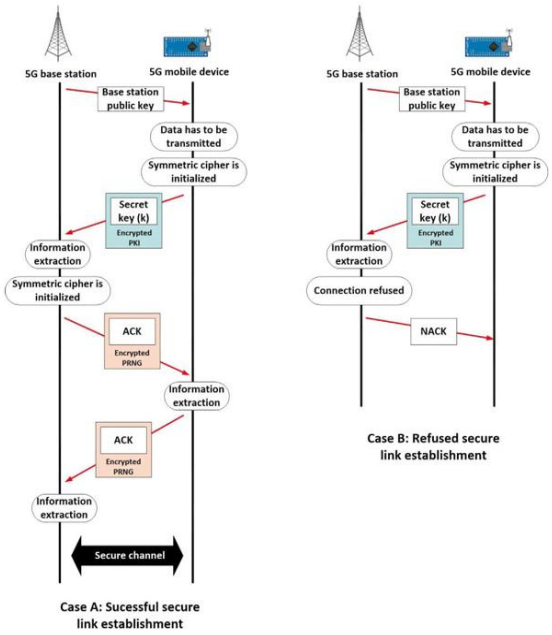

Fig 8. Message sequence chart (a) successful establishment (b) refused establishment

Specifically, the creation of a communication channel (secure or not), as numerous various works point out, must be accompanied by a triple handshaking. Nevertheless, this technology solution must be developed in the sufficient manner, since it could be a significant tool utilized by cyber-attackers to compromise the encryption.

In a nutshell, the suggested handshaking process is the following. The 5G station must publish its public key, so as to avail it to all mobile devices. After that, in case a sensor node would like to send information to the Internet it should start the work of the symmetric cipher. With the help of the public key of the base station, the secret key that is used is secured and sent. After that, base station will extract the secret key of the symmetric cipher and initialize it.

The base station at this stage builds an acknowledgment message, which is encrypted by the symmetric cipher. Attempts to obtain the secret information when the remote sensor node obtains this secure message. In case, and it is an acknowledgment message, the remote sensor node transmits the final confirmation also with the symmetric cryptographic solution. In case of error, a second round of the model is followed. At the end of this second interaction should the error still occur or the base station reject the communication the secure link is not established.

Figure 8(a) shows a message sequence chart describing a successful secure link establishment.

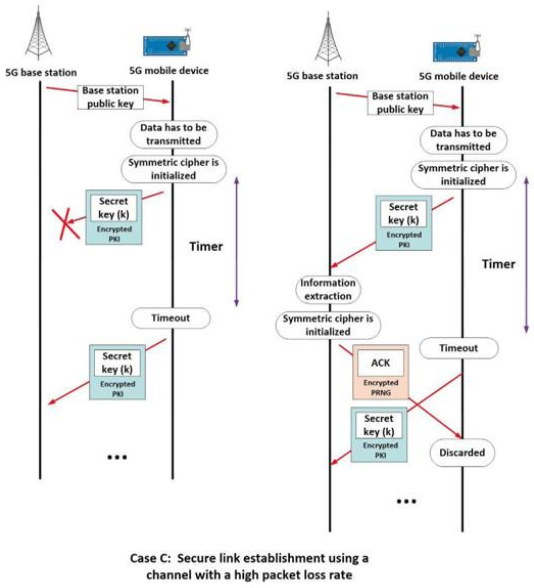

Fig 9. Message sequence chart: secure link establishment using a channel with a high packet loss rate

The data format used to send the secret key of the symmetric cipher is not tied to the proposed solution, although the IoT devices are likely to have limited resources and are not able to use high-computation power, and light information representation schemes (e.g., JSON) are desirable.

Conversely, it is sometimes possible, see Figure 8(b), that the base station will deny the connection of the secure link. In this scenario the non-acknowledgment message will be transmitted in a plain text format to the remote node which is expected to save the acquired data and wait until the remote base station is ready.

However, the failure of the procedure of establishing a secure link is not possible solely because of the refusal decisions of the base station. This process may also be impacted by problems attributed to high packet loss rate in the communication channel (among other things). To that end, a methodology of dealing with such issues is needed (see Figure 9 and Figure 10). In essence, a second iteration is done in case there arises any problem. The latter version can be invoked by a time to kill in case the base station has not responded by the time the user gets the time-out notification (Figure 9). Since a communication channel with a vast delay might be in use, every message within the initiation process must comprise a transaction number (so that, any got message comprising a previous transaction is lost), and that timer noted must be adjusted to the circumstances of the communication channel (in order to create success safe connections).

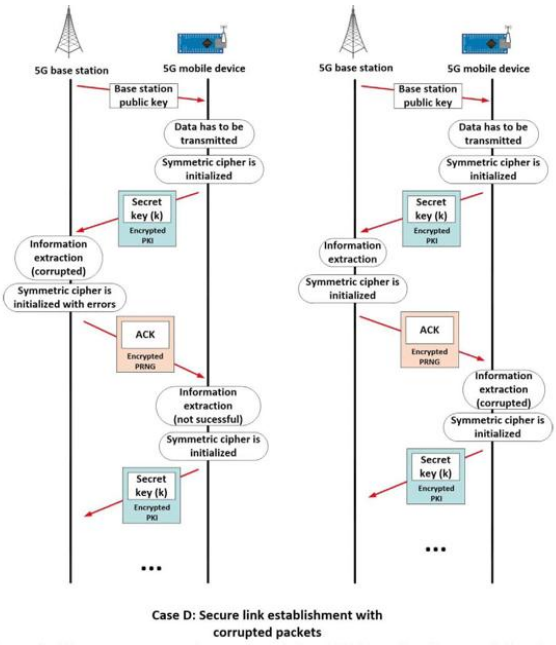

Fig 11. Message sequence chart: secure link establishment with corrupted packets

But in other occasions, communication channel does not pose a significant delay but it is much noisy medium and data packets become corrupted. A second encounter of the establishment process it is also induced in this case (see Figure 11).

Lastly, in case the second interaction triggered leads to an error as well, corrupted packets are received, or no response is received by the base station, the establishment procedure is canceled by the remote sensor node (see Figure 12).

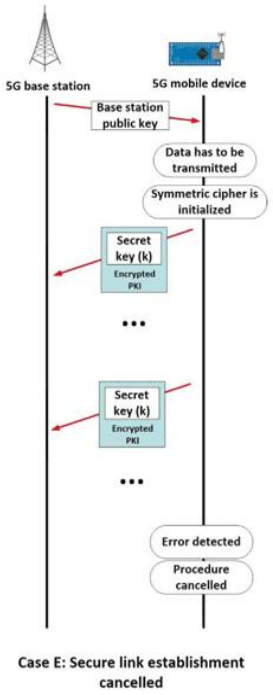

Fig 12. Message sequence chart: secure link establishment cancelled

4. Result and Discussion

To confirm the suggested solution as a legitimate technology in the context of security provision in IoT case leveraging 5G networks and resource constraint devices a pilot implementation of our proposal was created. The received results, however, depend on how many devices can be involved in the scenario and as (in the proposed solution) base stations can become points of congestions provided that an adequate network design and scaling it is not carried out. A simulation scenario was built on the NS3 simulator in order to test this dependency. The suggested algorithm was made available to base stations and mobile devices in the intended simulation, which was set up in a similar way as the prototype described earlier. In this experiment, the number of the considered IoT devices in the simulation case was extended. Each number of IoT devices was simulated twelve times. The success rate of creating the desired secure link was determined with the obtained information. The results are obtained and illustrated in figure 13.

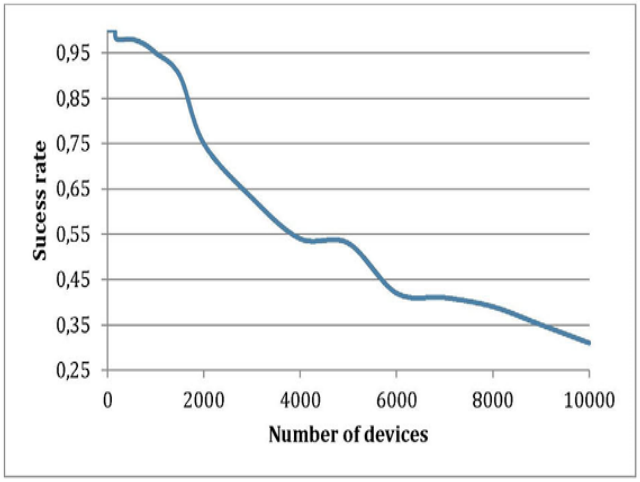

Fig 13. Success rate. Simulation results

As it can be observed, the success rate is approximately 100 percent until the count of devices taken into consideration is one thousand. The success rate is at this point approximately 90%. Henceforth, the large number of devices connecting to a same base station introduces delays of transmissions upwards, and whenever it gets increasingly difficult to complete secure connection between mobile devices and the 5G station. When ten thousand devices are taken into consideration the success rate will go down to 30 percent (approximately). Nevertheless, the future 5G networks are not designed to introduce such a great device density within a special cell. Thus, the received findings can be considered as the first sign that the suggested technology is a good solution to provide security in IoT systems using 5G mobile networks.

5. Conclusion and Future Work

The paper presents a light implementation of security provision in the IoT context using 5G networks. The next generation engineered systems will be founded on pervasive hardware platforms comprising of resource constrained devices, which are incapable of running the traditional heavy encryption algorithms. New and sufficient techniques are required in that regard. The proposed solution consists of an asymmetric cryptography-based protocol of initializing, and a symmetric cipher-based protocol of pseudorandom number generators. The given contribution, therefore, will allow the IoT devices to create a reliable connection between themselves and 5G base stations. To assess the effectiveness of the proposed technology, a preliminary prototype, which is built on the Arduino microcontrollers, has already been built, and a simulation case has been used to find out the scalability of the offered solution and the operation limits of the proposed solution. The validity of the described security solution is demonstrated through obtained results as a first evidence. Subsequent studies should take into account improved prototypes (such as wireless communication) and deal with a few practical issues that are not covered in this first work. As an illustration, to find out the security of the whole proposal, information of the chosen pseudorandom number generator (including the seeds used) must be taken into consideration, because resource constraint devices can also have a constraint in this respect.

References

1. Y. Duan, Q. Wu, X. Zhao, and X. Li. "Mobile Edge Computing Based Cognitive Network Security Analysis Using Multi Agent Machine Learning Techniques in B5G", Computers & Electrical Engineering, vol. 117, pp. 109181, 2024.
2. S. Gupta and Sonia. "An Analysis of Edge Computing with Multi Access in 5-G Technology", in Proceedings of the 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, pp. 1641-1644, 2023.
3. S. Wijethilaka, A. K. Yadav, A. Braeken, and M. Liyanage. "Blockchain-Based Secure Authentication and Authorization Framework for Robust 5G Network Slicing", IEEE Transactions on Network and Service Management, vol. 21, no. 4, pp. 3988-4005, 2024.
4. T. Saha, N. Aaraj, and N. K. Jha. "Machine Learning Assisted Security Analysis of 5G-Network-Connected Systems", IEEE Transactions on Emerging Topics in Computing, vol. 10, no. 4, pp. 2006-2024, 2022.
5. A. K. Bhagat and J. Gandhi. "A Comprehensive Analysis of 5G Security Core Technologies and Services: Conceptual Frameworks, Challenges, and Solutions", in Proceedings of the International Conference on Artificial Intelligence and Smart Communication (AISC), Greater Noida, India, pp. 1273-1281, 2023.
6. M. A. Hasnat, S. T. A. Rumee, M. A. Razzaque, and M. Mamun-Or-Rashid. "Security Study of 5G Heterogeneous Network: Current Solutions, Limitations & Future Direction", in Proceedings of the International Conference on Electrical, Computer and Communication Engineering (ECCE), Cox's Bazar, Bangladesh, pp. 1-4, 2019.
7. S. Gupta, B. L. Parne, and N. S. Chaudhari. "Security Vulnerabilities in Handover Authentication Mechanism of 5G Network", in Proceedings of the First International Conference on Secure Cyber Computing and Communication (ICSCCC), Jalandhar, India, pp. 369-374, 2018.
8. V. Adat Vasudevan, C. Tselios, and I. Politis. "On Security Against Pollution Attacks in Network Coding Enabled 5G Networks", IEEE Access, vol. 8, pp. 38416-38437, 2020.
9. V. Adat, I. Politis, C. Tselios, P. Galiotos, and S. Kotsopoulos. "On Blockchain Enhanced Secure Network Coding for 5G Deployments", in Proceedings of the IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, pp. 1-7, 2018.
10. A. Bozorgchenani et al. "Intrusion Response Systems for the 5G Networks and Beyond: A New Joint Security-vs-QoS Optimization Approach", IEEE Transactions on Network Science and Engineering, vol. 11, no. 3, pp. 3039-3052, 2024.
11. M. S. Siddiqui et al. "Policy Based Virtualised Security Architecture for SDN/NFV Enabled 5G Access Networks", in Proceedings of the IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Palo Alto, CA, USA, pp. 44-49, 2016.
12. R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage. "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions", IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 196-248, 2020.
13. W. Niewolski, T. W. Nowak, M. Sepczuk, and Z. Kotulski. "Security Architecture for Authorized Anonymous Communication in 5G MEC", Journal of Network and Computer Applications, vol. 218, pp. 103713, 2023.
14. H. Sharma and N. Kumar. "Deep Learning Based Physical Layer Security for Terrestrial Communications in 5G and Beyond Networks: A Survey", Physical Communication, vol. 57, pp. 102002, 2023.
15. T. Madi, H. A. Alameddine, M. Pourzandi, and A. Boukhtouta. "NFV Security Survey in 5G Networks: A Three-Dimensional Threat Taxonomy", Computer Networks, vol. 197, pp. 108288, 2021.
16. G. Amponis et al. "Generating Full-Stack 5G Security Datasets: IP-Layer and Core Network Persistent PDU Session Attacks", AEU - International Journal of Electronics and Communications, vol. 171, pp. 154913, 2023.
17. R. S. Shukla and A. M. Alatawi. "Enhanced Security Protocols for 5G Networks: Addressing Vulnerabilities and Opportunities in High-Speed Data Transmission", in Proceedings of the International Conference on Networks and Cryptology (NETCRYPT), New Delhi, India, pp. 1574-1577, 2025.
18. Y. Sun et al. "An Anonymous and Secure Data Transmission Mechanism With Trajectory Tracking for D2D Relay Communication in 3GPP 5G Networks", IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 8, pp. 9733-9748, 2024.
19. P. Consul, I. Budhiraja, and D. Garg. "Deep Reinforcement Learning Based Reliable Data Transmission Scheme for Internet of Underwater Things in 5G and Beyond Networks", Procedia Computer Science, vol. 235, pp. 1752-1760, 2024.
20. P. Joshi. "Multi-Sensory Data Transmission Using 5G and B5G Enabled Network for Healthcare: Survey", Discover Internet of Things, vol. 4, no. 1, 2024.
21. C. Haitao, W. Zezhao, W. Chao, L. Fuxing, and W. Wenbin. "Research on 5G Network Coverage Optimization Data Transmission System with UAV Relay Enhancement", in Proceedings of the IEEE 2nd International Conference on Electrical, Automation and Computer Engineering (ICEACE), Changchun, China, pp. 1642-1647, 2024.
22. P. Zhang, Y. Zheng, and Z. Chen. "Research on Distribution Terminals' Horizontal and Vertical Quantum Keys Secure Transmission Algorithm Based on 5G Communication Networks", in Proceedings of the 3rd International Conference on Electronic Information Engineering and Computer Science (EIECS), Changchun, China, pp. 1009-1013, 2023.

23. R. Ma, J. Cao, Y. Zhang, C. Shang, L. Xiong, and H. Li. "A Group-Based Multicast Service Authentication and Data Transmission Scheme for 5G-V2X", IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 12, pp. 23976-23992, 2022.
24. X. Ren, J. Cao, M. Ma, H. Li, and Y. Zhang. "A Novel PUF-Based Group Authentication and Data Transmission Scheme for NB-IoT in 3GPP 5G Networks", IEEE Internet of Things Journal, vol. 9, no. 5, pp. 3642-3656, 2022.
25. B. Shilpa, A. K. Budati, L. Koteswara Rao, and S. B. Goyal. "Deep Learning Based Optimised Data Transmission Over 5G Networks with Lagrangian Encoder", Computers and Electrical Engineering, vol. 102, pp. 108164, 2022.