An encryption-encoding architecture for security enhancement in 5G communication networks

Anwesha Das[1*], *Debasis* Mishra[1], *Ashima* Rout[2] and *Suvendu Narayan* Mishra[1]

[1]Dept. of ETC Engineering, V.S.S. University of Technology, Sambalpur, Odisha, India
[2]Dept. of ETC Engineering, I. G. Institute of Technology, Saranga, Odisha, India

Abstract. This article introduces a hybrid architecture of cryptography and coding technique to provide security in 5G communication networks. There are various types of attacks in 5G communication systems. Apart from contemporary attacks, we refer some of the peculiar attacks including DOS, DDOS, bot attack, Mantis Botnet, Mirai Botnet etc. These attacks jeopardize the security systems. To overcome the situation, we propose an architecture, which makes use of modified DES encryption followed by Hamming code. In transmitter section, the 256-bit input data is encrypted by 224-bit cipher key, which is then encoded with Hamming code (448, 256) to produce 448-bit of encrypted data. The reverse scheme is applicable in receiver section. We have used Xilinx software to simulate the proposed model. Simulation results show that the duration of both the encryption and encoding are in nano seconds. The intruders shall get very less time to interfere. Therefore, the proposed architecture shall improve the security in current 5G communication systems.

Key words —Bot attack, cryptography, DES, DOS, DDOS, encryption, interim text, Hamming Code, Xilinx software

1 Introduction

Presently, 5G is becoming one of the most coveted global wireless technologies next to 4G services. 5G network potentials include more capability, flexibility, speed and lower latency in comparison to its predecessors. The ultra-fast 5G network provision results in seamless experience to its customers. It has absolutely altered the speed with which data transmission occurs. It finds numerous applications in the arena of entertainment, health sector, emergency response and weather forecasting including satellite technology. One can have the access to health experts, residing in a far off country, and may try to find medical assistance through this unique technology. The growing economic impact of 5G technology in India is projected to touch 450 billion US dollars by 2035. Stand-alone (5G SA) deployment model uses an end-to-end 5G network,

*Corresponding author:anweshadas3939@gmail.org

which delivers services, whereas non-stand-alone (5G NSA) models use a mixture of 4G LTE and 5G to deliver services [1]. The fourth industrial revolution (4.0) shall bring about different types of societal changes, where the future revelations for 5G and Internet of Things (IoT) go outside of merely associating specific gadgets. With its super-boosted wireless network, which supports download speeds ranging from 10 to 20 GBPS, 5G shall revolutionize the mobile capabilities in diverse manners.

In general, network security schemes safeguard our network and data from intruders and other potential extortions. Network security schemes protect client's information including personal data, which ensures trustworthy access, and help in guarding the data from cyber threats [2]. Network security schemes consist of protective algorithms that built into an underlying computer architecture. It also includes procedures implemented by the network manager to take safe measures of network accessible resources from illegal access, while continually monitoring and evaluating its efficiency.

5G facilitates the service providers and the enterprise industries to simply initiate new capabilities and expose them through Application Program Interfaces (API). This can be equipped at the edge of network or via 5G core Service Based Architecture (SBA). It is authenticated, and secured before being endorsed on the network and must be managed all over their life cycles to guarantee their safety. Cloud security is a set of procedures and technologies that can handle both external and internal risks to enterprise security. Organizations need cloud security as they are implementing digital renovation plans and therefore include cloud-based tools and services in their infrastructure. Software Defined Networking (SDN) and Network Function Virtualization (NFV) are at the heart of 5G network core [3]. SDN and NFV chiefly utilize HTTP and rest API protocols. These protocols are well established and regularly exploited.

As 5G starts infiltrating into all facets of life, availability, integrity and secrecy shall occupy top priorities. In terms of availability, the information produced and stored must be reachable to certified entities. This includes the preservation of hardware, technological infrastructure and systems that hoard and exhibit data. Integrity involves the modifications that are accomplished by accredited groups through authorized machinery. The most predominant feature of information security is confidentiality. When information is kept secret, it shows that other parties cannot access data. Confidentiality refers not just to preserve the information, but also to its transit. The 5G network includes new millimeter-wave and centimeter-wave bands that are new for mobile communications. However,the inclusion of new frequency bands created another problem. Short millimeter waves cannot travel well through obstacles. A probable solution is to use a huge Multiple Input Multiple Output (MIMO) antenna made up of hundreds of unified pieces of antennas. Each 5G-network client obtains a geographically and temporally tailored signal from the base station antenna, which only supplies the services required by subscriber. This practice supports more resourceful use of base stations. In the meanwhile, it also improves efficiency of 5G radio bandwidth.

2 Current age security failures

Passive attacks are those in which the attacker does not modify data or distress the system. Yet the attack may damage communications sent from the transmitter to the receiver. As a result, this sort of attack is problematic to distinguish until the transmitter or receiver realizes the leak of private information. Active assaults are those that are likely to transform data, thereby damaging the systems. An attacker can actively attack in diversified ways. They are typically easier to identify than to avoid.

There are different types of intrusions in 5G technology. Some of the modern day interferences need emergency attention of the communication engineers all over the world. We have summarized some of the peculiar attacks in the following section.

1. Denial of Service (DOS): This type of attack leads to partial slow down or complete interruption of the assured services of a system. The intruder can intercept and erase a server's reply to a customer, thereby compelling the customer to consider that the server is not replying. The attacker may well intercepts the requests from the consumers, thereby instigating the customers to send multiple requests which leads to overloading of the system.
2. Distributed Denial of Service (DDOS): This type of attack involves malicious attempts in making an online package inaccessible to genuine consumers by essentially preventing or at least deferring the host server's amenity [4]. DDOS attacks occur at the application layer or the network layer of the malevolent configurations that are associated with the systems. A number of hackers are exploiting the benefits of IoT devices with insufficient security implementation to seizure them which leads to target the victim network or server [5].
3. Bot Attack: These are programmed attacks setup by offenders and enabled by scripts (Bots) that can copy human behaviour and make duplicate copies of it. They aim at various targets including the APIs, websites and even user server. An attacker controls a bot, which comprises of computer or other networked devices. When a hacker manipulates the vulnerability in a computerized system, then a DDOS attack initiates, which leads to creation of the DDOS master bot.
4. Mantis Botnet: The Mantis Botnet is capable of generating the 26M HTTPS requests per second numbers of attacks by using merely 5000 number of Bots.
5. Mirai Botnet: This is another type of attacking malware, which targets customer devices like home routers and smartcameras. It converts them into a zombie network of remotely controlled Bots. Cyber criminals use Mirai Botnets to aim at computer systems, which results in an enormous DDOS attacks. Today security researchers and analysts are facing tragic difficulties in handling such DDOS flooding attacks. Numerous techniques to identify and stop DDOS flooding attacks have been proposed by using machine learning algorithms and other cutting-edge technologies.

3 Proposed mitigation strategy

The 5G mobile broadband networks depend upon many cryptographic techniques. In cryptography, the original message is transformed into an impenetrable message, thereby avoiding the attacker from retrieving it. Cryptography, in combination with appropriate communication protocols can provide a higher level of security in digital communication systems from intruding assaults while communicating between two distinct computers.

5G employs 256-bit encryption system, which is a major feature over the 128-bit standard used by 4G [6]. In 5G, user's identities and where-about are encrypted, making them stimulating to decide or detect from the minute they enter the network. Each consecutive release of mobile networks endeavored to lower the danger of information security.

Encryption safeguards sensitive data including personal information of individuals. This helps to protect confidentiality by minimizing possibilities of chances for criminals and government organization to keep an eye on a person. Encryption functions during data transfer or at rest, resulting in a perfect option irrespective of how or where the data is kept or utilized. 5G uses the New Radio Encryption Algorithm

(NEA) and the New Radio Integrity Algorithm (NIA) to secure the integrity and secrecy of over-the-air communication. Both algorithms support the modified Data Encryption Standard (DES) along with Advanced Encryption Standard (AES). Symmetric encryption protects the data by using a secret key to encrypt (lock) and decrypt (unlock). The key can be one from a word, a phrase or random string of letters, numbers and symbols. Hamming codes provide error detection and correction mechanism in both the situations, viz. data is stored or transmitted.

To accomplish better data security, we propose fusion of both the modified DES encryption and Hamming encoding technique, which results in lesser time consumption that may inhibits the intruder not to intercept. After closely observing the present types of attacks in the 5G networks, we propose an architecture to combat the situation. Being inspired by the concatenated coding techniques, our proposed model utilises both the systems viz. first encryption and then encoding. Fig. 1 shows the suggested architecture.

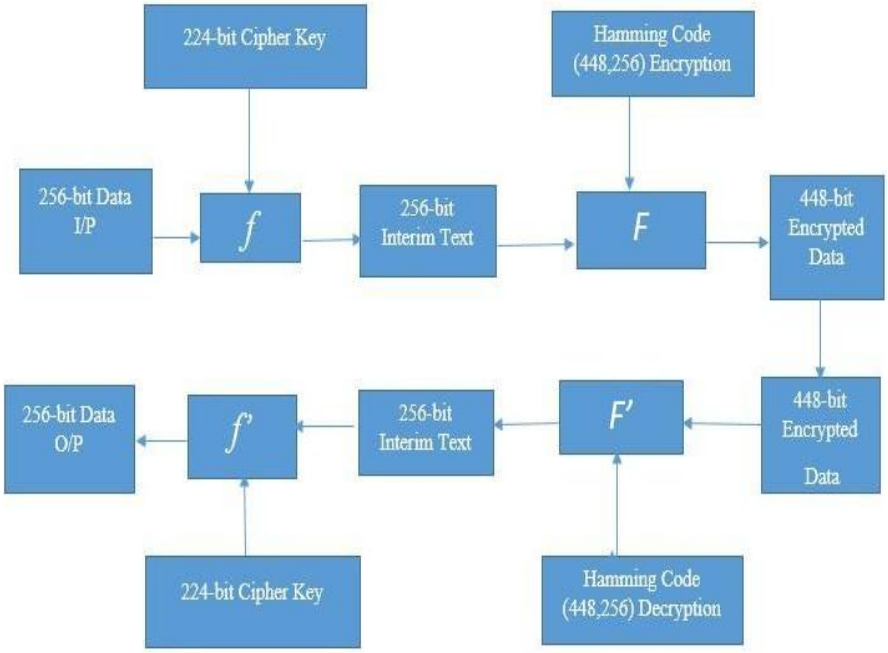

Fig.1. Proposed model of security management

4 Results and discussion

We have first encrypted 256-bit input data by using 224-bit cipher key in the block "*f*", which produces 256-bit interim text. Fig. 2 shows the simulation results of this encryption system in terms of timing diagram. Then we encodethe 256-bit interim text by using Hamming Code (448,256) in the block "*F*". After this encoding, we get 448-bit data, which is to be transmitted by the transmitter. Fig. 3 shows the simulation results of this coding system in terms of timing diagram.

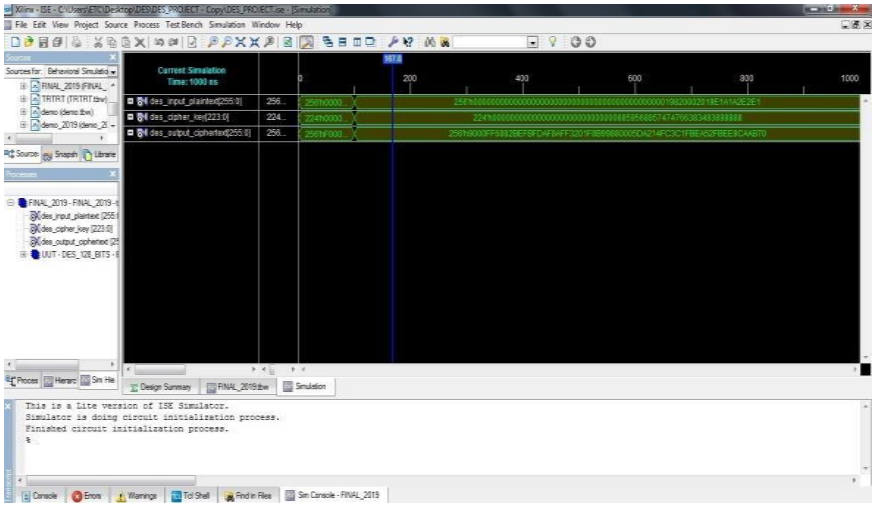

Fig.2. Simulation results of modified DES encryption process

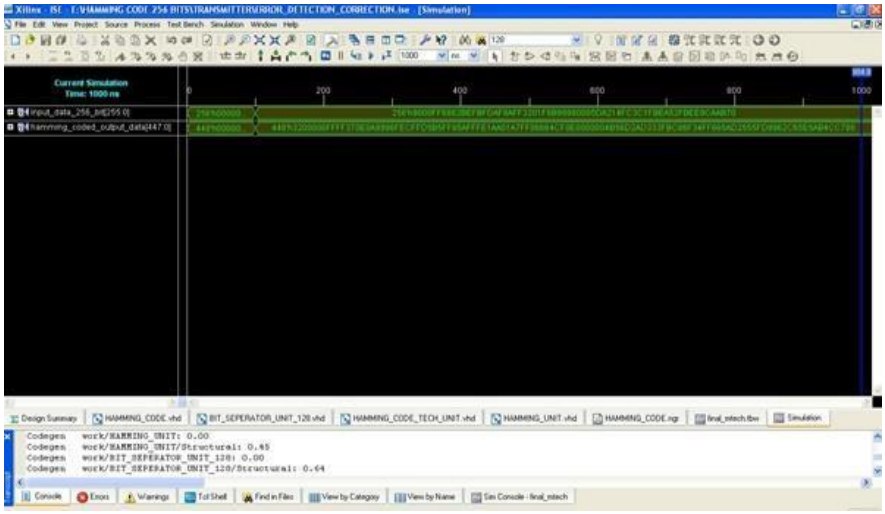

Fig.3. Simulation results of Hamming Code (448,256)encoding process

Now at the receiver, the reverse of the above procedure is maintained. Again the Hamming Code (448,256) decodes the received data in the block " F ′ ". The output of this block is also 256-bit interim text. Fig. 4 shows the simulation results of this decoding system in terms of timing diagram. This interim text is deciphered by the same 224-bit key in the block"*f ′*". This block produces 256-bit output data. Fig. 5 shows the simulation results of this decryption system in terms of timing diagram.

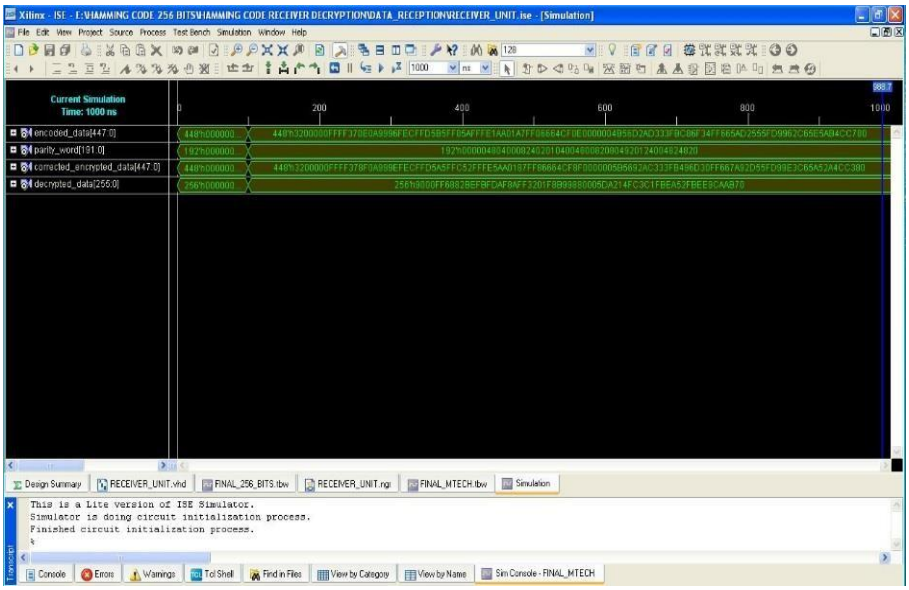

Fig.4.Simulation results of Hamming Code (448,256)decoding process

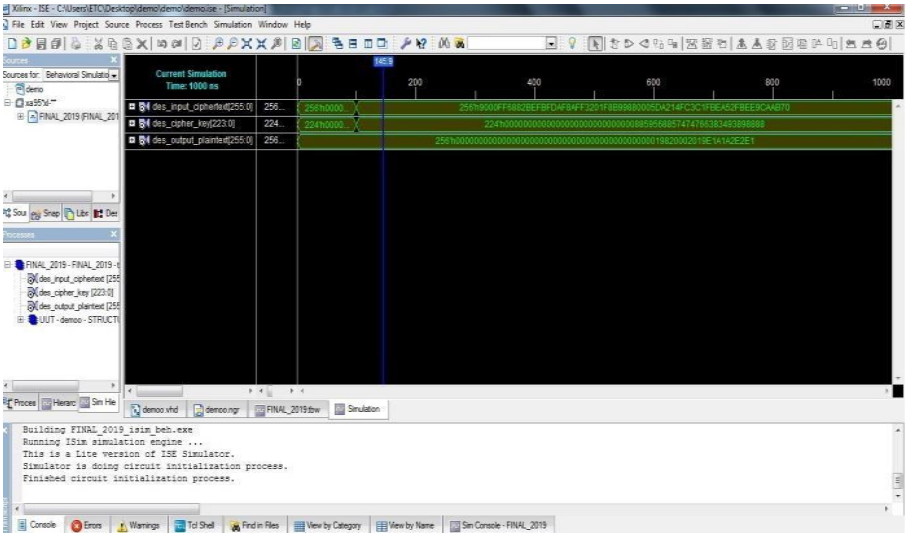

Fig.5. Simulation result of modified DES decryption process

The timing diagrams, obtained after simulation of Xilinx software, suggest that the ciphering of 256-bit plain text in to 256-bit interim text takes only 10.763 ns. Similarly, the Hamming code encoding process requires 19.231 ns of time to convert 256-bits of interim text into 448-bits of cipher text.

5 Conclusion

Here, both the durations of encryption and encoding are of the order of nanoseconds. This will reduce the risk of various types of attacks in the 5G communication networks. The intruders shall get much less time to interfere in the system. Apart from concatenated coding, we suggest that lesser duration of encryption and encoding shall add a new dimension to 5G communication systems. In future, combinations of other encryption algorithms and encoding techniques may lead to design networks that are more robust in terms of security.

References

1. J. Metzler, "Security implications of 5G Networks", CLTC White Paper Series, UC Berkeley, pp 1-30 (September 2020).
2. "5G Security Issues", White Paper, Positive Technologies (2019).
3. C. Mei, et. al., "5G Network Slices Embedding with Sharable Virtual Network Functions," Journal of Communications and Networks, vol.**22**, No.5, pp-415-427, (October 2020).
4. A. Cheema, et.al., "Prevention Techniques against Distributed Denial of Service Attacks in Heterogeneous Network: A systematic Review," Security and Communication Network, Hindwai, Wiley, vol.**2022**, pp.1- 15 (May 2022).
5. J. Sun, et. al., "A Tamper-Resistant Broadcasting Scheme for Secure Communication in Internet of Autonomous Vehicles", IEEE Transaction on Intelligent transportation system, pp.1-10 (Future Issue)
6. Y. N. Alswailem, M. S. Alhilal, et.al., "5G Security Risk and Mitigation Measures", Nokia White Paper, pp.1-19.