International Journal of Advanced and Applied Sciences

Journal homepage: http://www.ijaas.in

Design and Evaluation of an Efficient IoT Model for 5G Applications: Enhancing Accuracy and Security through Compression and Encryption Techniques

Priya [1*]

[1] Assistant Professor, Department of Computer Science, Arya P.G. College, Panipat, India

ARTICLE INFO

Article history:
Received: 07-06-2025
Received in revised form: 13-07-2025
Accepted: 03-08-2025

Keywords:

IoT (Internet of Things), 5G Applications, Data Compression, Data Encryption, Security Enhancement, Accuracy Improvement, Network Efficiency, Bandwidth Optimization, Privacy Protection.

ABSTRACT

The rapid advancement of 5G technology has spurred the growth of Internet of Things (IoT) applications, which demand high performance in terms of data accuracy, security, and network efficiency. This paper presents the design and evaluation of an efficient IoT model tailored for 5G applications, with a focus on enhancing accuracy and ensuring robust security. The proposed model integrates advanced compression and encryption techniques to address the challenges associated with large-scale data transmission and potential cybersecurity threats in 5G environments. Specifically, data compression algorithms are utilized to reduce the volume of transmitted information, optimizing bandwidth usage and improving transmission speeds. Meanwhile, encryption methods are employed to secure sensitive data, safeguarding it from unauthorized access and ensuring privacy compliance. We evaluate the model's effectiveness through a series of simulations that measure its impact on key performance indicators such as data accuracy, transmission latency, energy consumption, and security levels. The results demonstrate that the integrated approach significantly improves IoT performance in 5G networks, offering a scalable and secure solution suitable for a wide range of applications, from smart cities to industrial automation. This study provides insights into the practical application of compression and encryption techniques to enhance the performance and security of IoT systems in the context of 5G.

Introduction

The advent of 5G technology has revolutionized the way we approach communication, providing higher speeds, lower latency, and greater connectivity. This transformation is particularly impactful for the Internet of Things (IoT), which relies on a massive number of connected devices to generate, exchange, and process data in real-time. However, the rapid proliferation of IoT devices in 5G networks presents significant challenges in terms of data accuracy, network congestion, security, and efficient data transmission. As 5G applications continue to evolve, solutions that enhance the performance and security of IoT systems are critical to realizing their full potential.

In this context, an efficient IoT model is essential to leverage the capabilities of 5G while addressing these challenges. This paper proposes a novel IoT model designed specifically for 5G environments, incorporating advanced compression and encryption techniques. The integration of data compression algorithms helps minimize the amount of data transmitted over the network, optimizing bandwidth usage and improving the overall efficiency of the system. Simultaneously, encryption techniques ensure that sensitive data remains secure, safeguarding privacy and preventing unauthorized access [1].

The primary goals of this study are to enhance the accuracy of data transmission, ensure robust security, and optimize the efficiency of the IoT model. Through a comprehensive evaluation, the proposed model is assessed based on key performance indicators, including data accuracy, security measures, transmission latency, energy consumption, and scalability. By focusing on these aspects, this research aims to provide a reliable and scalable solution for IoT applications in 5G networks, offering a significant contribution to the fields of network management, data security, and IoT performance.

This introduction sets the stage for exploring how compression and encryption can be combined to address the diverse challenges faced by IoT systems, ultimately improving the overall performance and security of 5G applications.

The quality condition of the mobile users' channel is one such major issue. The channels quality does not remain the same for all the MS. Those MS located close to Base Station enjoy better channel quality conditions and on other hand, those located at farther from BS suffer a poor channel qualities which remain a generic feature in wireless communication. However, it is not the fault of MS being located far away from BS. Other factors namely, interference from other users, obstacles, etc also influences the channel quality of the MS. The typical function of the bandwidth management schemes is to estimate the channel quality conditions and provide resources. Due to better channel conditions, the MS located in the close vicinity of the BS enjoys more system throughput and those located at the distance end do not get so much of through put in our scenario which raises the problem of Fairness [2].

Network congestion is another major challenge faced by the bandwidth provisioning mechanisms as IOT 5G systems are designed basically to handle multimedia traffic which makes the network congested easily which is a serious issue to consider. Simultaneously we have to handle different users with different bandwidth requirements and different services which complicates the task of the scheduler even more.

The streaming of Voice applications is the serious confront to the IOT 5G systems. Although IOT 5G-A systems are developed based on packet switching principle, they use circuit switching to stream voice packets. The explanation is very simple. IOT 5G switches to circuit switching to stream voice as the Voice packet every sensitive to delay ethics brings in all the disadvantages of circuit switching. whilst the IOT 5G networks switch to circuit switching for streaming voice applications, a large amount of precious bandwidth is wasted.

Revenue loss is the last issue of bandwidth management in IOT 5G due to serving low-revenue-generating users. Different levels of revenue losses are faced by Network operators from serving users based on their channel quality conditions, the amount of the buffered data they have at the base station and their willingness to pay for different services.

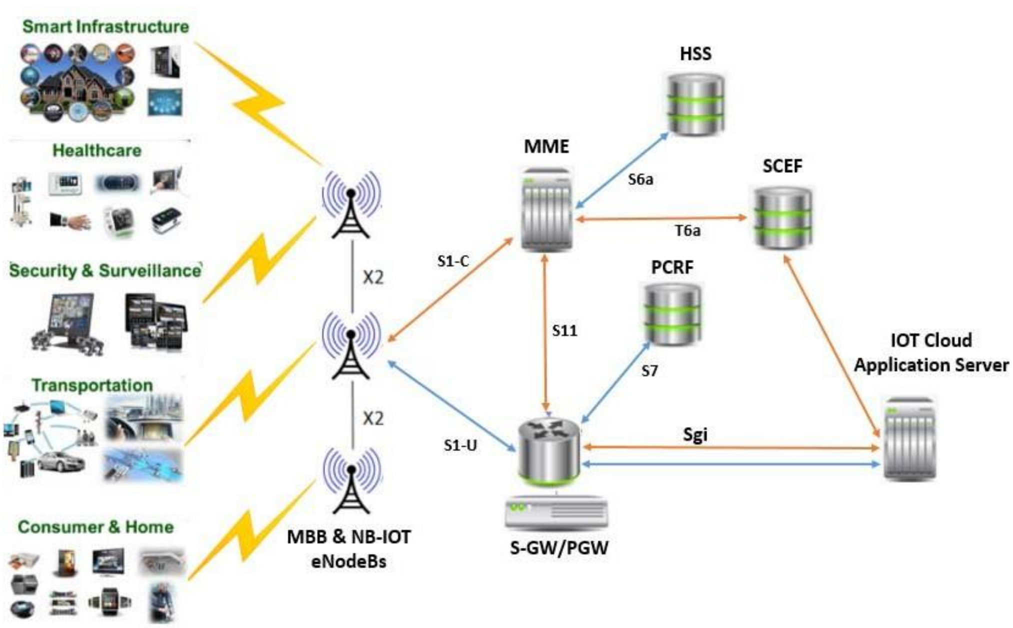

Figure 1: Existing IoT 5G network architecture

Existing schemes deal only with some of these issues, and thus neither can optimize the performance of BWASs nor can maximize the satisfaction of users. An efficient bandwidth allocation framework with a protocol stack should be able to consider all these challenges and strike an optimum balance [3].

A Simplified Protocol Stack for improved IoT support in IOT 5G

A novel protocol architecture, namely, Reduced Control Plane Protocol(RRCP) architecture suite to effectively reduce the number of signaling messages or reduce the duplication of signaling messages when an User Equipment (UE) tries to join the IOT 5G network from its sleep mode. We evaluate the performance of the proposed scheme with conventional scheme in terms of many metrics which include, number of channels allocated, delay and energy consumed and prove that the proposed architecture is much better than the existing conventional architecture.

Scheduler for IoT systems in IOT 5G

A scheduler based on sub frame Queuing model that can be effectively used for scheduling IoT traffic in IOT 5G systems. The performance of the algorithm was evaluated comparing it with existing schedulers.

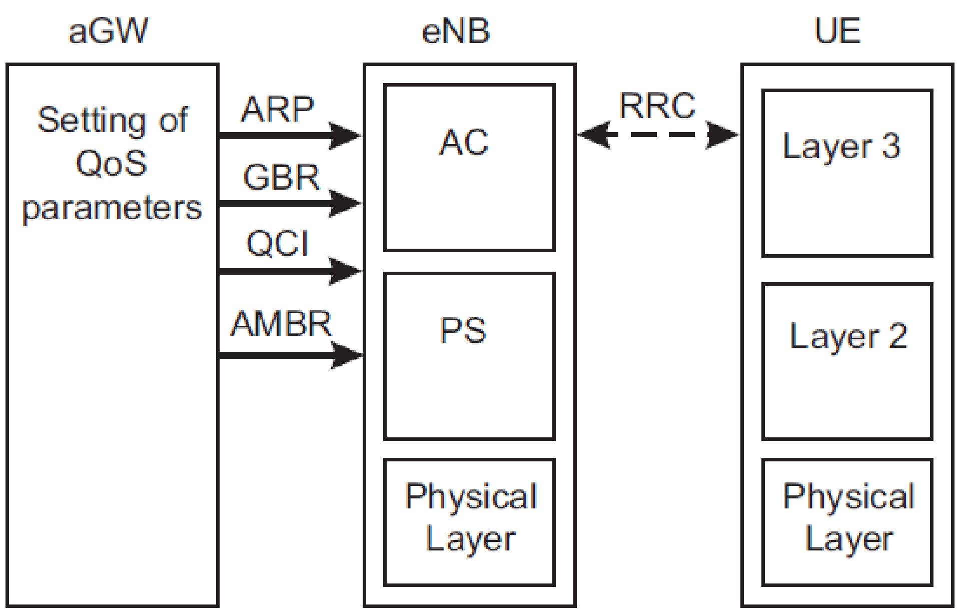

Figure 2: QoS Parameter setting IOT 5G

Literature review

PMI

The Precoding matrix determines how the individual data streams are mapped to the antennas. Skillfully selecting this matrix yields a maximum number of data bits, which the UE can receive together across all layers. However, this requires knowledge of the channel quality for each antenna in the downlink, which the UE can determine through measurements. If the UE knows what the allowed Precoding matrices are, it can send a PMI report to the BS and suggest a suitable matrix.

RI

The channel rank indicates the number of layers and the number of different signal streams transmitted in the downlink. Single Input Multiple Output (SIMO) uses one layer whereas 2x2 MIMO uses two layers. An optimized RI shall effectively maximize the channel capacity of the entire downlink channel by completely utilizing the advantage of full channel rank. However, the CSI of the IOT 5G systems is not completely evaluated on RI. CQI and PMI area accounted while taking scheduling decisions, since the value of the RI also influences the allowed Precoding matrices and CQI values [3].

Reference signal received power (RSRP)

The entire process of cell selection, reselection and handover is based on the RSRP value. The handover mechanisms and cell reselection mechanisms are also based on the RSRP values. In other words, RSRP may be defined as the received signal power at the UE. However, it must be noted that RSRP only provides the signal strength and not describe signal quality. The UE measures the RSRP and reports the same to the eNodeB through the RRC messages. However, The UE does not report the exact value that is measured. It indeed sends a non-negative value ranging from 0 to 97 to the eNodeB.

It is a very important factor that influences the scheduling as the value of the RSRP is used to estimate the distance between the UE and eNodeB. It is used in both RRC idle / connected mode for measuring inter frequency and intra frequency bands. The physical layer interface used in the IOT 5G A systems is OFDMA. OFDMA provides an opportunity for the cellular service providers to allocate different power channels to different users based on the proximity of the user. This feature may be definitely exploited by the scheduling scheme in order to save some power [4]. Further, the modulation technique employed though mostly decided by the quality of the channel, the RSRP may also be used by the scheduler to take a decision because sometimes the channel quality may be affected briefly because of external factors and may be restored immediately. It is not necessary that the channel quality is only affected by the distance between the UE and eNodeB.

Reference Signal Received Quality (RSRQ)

The measurements in the numerator and denominator shall be made over the same set of resource blocks. E-UTRA Carrier Received Signal Strength Indicator (RSSI), is the linear average of the total received power (in [W]) observed only in OFDM symbols containing reference symbols for antenna port 0, in the measurement bandwidth, over N number of resource blocks by the UEfrom all sources, including co-channel serving and non-serving cells, adjacent channel interference, thermal noise etc. RSRQ indicates the quality of the received reference signal.

RSRQ = N×RSRP/(E-UTRA carrier RSSI)

UE usually measures RSRP or RSRQ based on the direction (RRC message) from the network and report the value [5]. The measurement is usually carried out at the front end of the antenna. It is measure every transmission receiving cycle. It provides additional information to the scheduling scheme apart from the RSRP about the quality f the channel and facilitates the scheduling process decision making.

MAC's HARQ Processing

The MAC is responsible for managing the HARQ. HARQ stands for Hybrid ARQ or Hybrid automatic repeat request. The HARQ is a result of error detection that happens through two mechanisms namely, the Forward error Correction (FEC) and the Cyclic Redundancy Check (CRC). When these mechanisms are not able to retrieve the data at the transmitter then a HARQ is performed.

Data transfer in any form (both uplink-PUSCH / and downlink-PDSCH) between UE and eNBis handled by HARQ. For uplink synchoronous HARQ is used, for downlink asynchronous HARQ is used [6]. Every transmission and reception of data is associated with a particular HARQ process identifier.

The MAC receives a Negative Acknowledgment (NACK) when there is a CRC failure. The physical layer usually indicates the failure to the MAC. When the MAC at the eNodeB receives the NACK it retransmits the block using a different type of coding to the receiver. The coding once sent is maintained in the buffers of the eNodeB. After one or two retransmissions the receiver will be successfully be able to build the transmitted signal or decode the transmitted signal.

RLC Segmentation Process

The RLC layer in the Layer 2 is responsible for Segmentation and Reassembly (SAR). It performs SAR in three modes, namely, Transparent Mode, Acknowledged Mode and Unacknowledged Mode. On receiving the PDUs the duplicates are discarded; the PDU's are reordered; the resulting RLC SDUs are reassembled and delivered it to higher layer. It discards any remaining PDUs that cannot assembled. The ARQ procedures are only performed by an automatic mode RLC entity [7].

In Acknowledged Mode the transmitting RLC entity can poll the receiving AM RLC entity. Based on the results it sends a Status report to get information about whether the PDU's is acknowledged or Unacknowledged. The Status PDU consists of a one Acknowledged Serial Number and a one or more Unacknowledged NACK Serial Number. The receiving RLC sends the serial number of the last PDU received before the first NACK and one or more NACK SNs for either a whole PDU or a portion of an AMD PDU. The transmitting RLC on receiving the NACK initializes a counter 'RETX_COUNT' and retransmits the PDU; if necessary it may re- segment the PDU and retransmits the PDU. On receiving successive retransmit request for the same PDU it increments the counter and retransmits.

PDCP Layer

In the 3G and earlier cellular systems, the PDCP was only used for the packet data processing as the protocol stack in the previous versions was based on circuit switching between the host and the RLC layer. The IOT 5G has migrated into a completely IP based systems and hence the PDCP processing has moved to higher layers [8]. The PDCP functions include decryption, ROHC header decompression, sequence numbering and duplicate removal. PDCP functions in the control plane include decryption, integrity protection, sequence numbering and duplicate removal. There is one PDCP occurrence per radio bearer. The radio bearer is similar to a logical channel for user control data. The SDUs are discarded on their successful delivery. Every SDU is associated with ad is card timer; when the timer expires, that SDU can be discarded and is informed to the lower layers.

HARQ's is an important process which contributes to packet delay as the whole process will come to a halt until the packets are retrieved. Hence it is crucial, that HARQ re-transmissions are provided higher priority over the other process. The effectiveness of the systems to do error correction will directly impact the retransmission time of the scheduler. Repeated re- transmissions increase the delay in packet delivery. The HARQ feedback also provides an estimate of the packet delay. Packet delay is a very important factor that affects decisions in scheduling as it is known that many applications like VoIP are very sensitive to delay. capacity to do error correction reduces the retransmission time for the scheduler.

Research Methodology

Reduced signaling

It may note that the functions of each module of the IOT 5G system are redefined. Much of the signaling of the control plane has been reduced drastically saving precious bandwidth of the air interface. In this section we highlight the key reductions in the signaling mechanism. In the usual Attach process the Authentication message is sent from the UE to eNOdeB. However, in the proposed scheme the Authentication message is no longer sent over the air interface. The same is for the Authentication Response message. Similarly, you will find the RRC SMC message was communicated between the UE and the eNOdeB. However, in the proposed scheme this is avoid edas well.

Simulation Scenario

We now present the IoT-5G system architecture designed for the simulation and evaluation of the RRCP protocol. The environment was modeled to accurately replicate a realistic IoT-5G scenario characterized by diverse traffic types, including voice, video, and other data streams. Each partial cell hosts numerous IoT devices connected simultaneously. The total number of IoT devices per cell ranges from 1,000 up to 50,000 within a coverage area of 50 m² to 1 km². The typical distance between two IoT devices is defined as d=2log(n/k)d = 2 \log(n/k)d=2log(n/k), where nnn represents the total number of devices and kkk the active subset. It is assumed that at least 300 devices in each cell are active at any given time. The number of scheduling requests per sub frame varies between 1 and 18, while the number of radio blocks per frame takes values of 4, 8, 16, or 32. The transmission power is set to 200 mW, and the corresponding received power is set to 100 mW.

Table 1: Simulation Scenario

System Specifications	**Range**
Total number of IoT devices per small cell	1000/upto50,000
Coverage area of eNodeB	$50m^{2/}1km^2$,n=50,000
Active devices per cell	300/30 to 300
Neighbour definition	d=2log(n/k)
Scheduling requests per subframe	18/ 1 to 18
Radio blocks per subframe	32/{4,8,16,32}
Transport block size per radio block	408bits/16to584
Memory replicasize (l)	512bytes/16 to2048 bytes
Memory replicasparsity (s)	0.1l/0.1lto0.3l
Compressed replicasize	2slog(l/s)
Power during receive	100mW
Power during transmit	200mW
Consumed power during inactivity	10mW
Average collision freedelay	50ms
Time to schedule	10ms

Configuration of the Modeler

As we implement the proposed algorithm in the mobile station, the entire process requires modification. The updated process model reflects the implementation of the algorithm within the IoT-5G system .

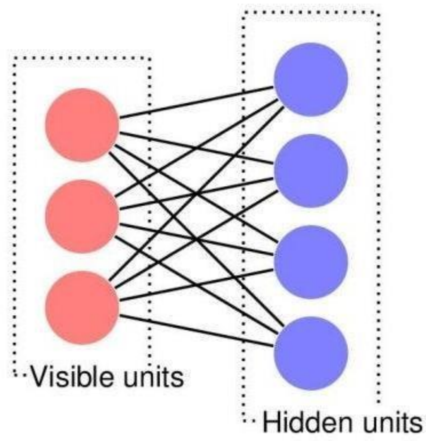

Figure 3: Visible Nodes and Hidden Nodes of BM Machine

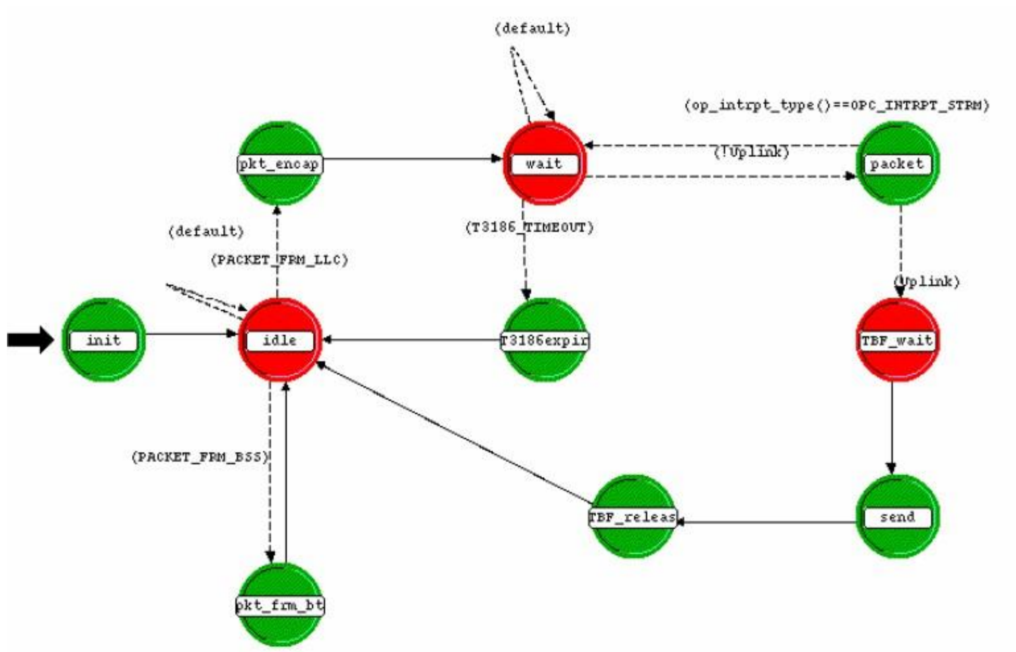

Figure 4: Process Model of the MS after implementation of the Algorithm

Packet Modification

The packets scheduled for transmission must also be encapsulated or modified. The details of these packet modifications are as follows: First, the TCP header is adjusted to align with the proposed algorithm, followed by modifications to the TCP process function. These changes are essential to integrate the proposed protocol stack effectively.

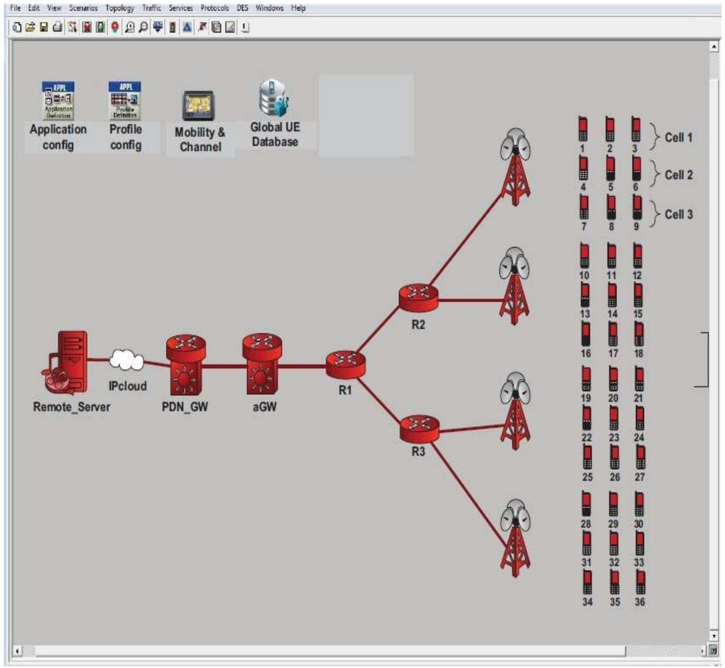

Figure 5: IOT 5G OPNET Simulation Model

The **eNodeB** serves as a bridge node connecting the User Equipment (UE) to the underlying transport systems. Acting as an interface, the eNodeB is responsible for coordinating and managing communication protocols between nodes on both sides [9]. Another key component of the model that significantly influences the algorithm's performance is the **Gateway Node Model**. This node functions as an intermediary between the eNodeB and the Packet Data Network Gateway (PDN-GW), ensuring proper traffic management. It receives data packets from the PDN-GW and forwards them to the eNodeB, thereby maintaining stable and efficient network traffic conditions.

Total Number of Channels Allocated: Since RRCP has a buffer which is introduced in the control plane, eNodeB allocates less control channels for processing the conventional IOT 5G systems as illustrated in Figure 4.Each IoT device will continues RRC signaling channels for establishing communication with eNodeB and separate NAs channels for establishing connection and authentication with the MME. Since many of this control plane processing is taken care of by the BUFFER, the b=number of control channels consumed by the RRCP scheme has reduced significantly thereby saving precious radio resources. It may be noted in Figure 4, because of the reduced signaling in the control plane the number of control channels employed for RRCP measures in a logarithmic fashion. On the other hand, the conventional scheme will require a linear increase in number of channels. When the devices use the Sleep to Active Mode the scheduling scheme will allocate all the resources to the network whether it uses the resources or not which is a total waste of resources. This behavior may reduce the delay and power consumption. The cost in achieving the same is very high though.

Result analysis

The Jain Fairness Index [JFI] is an important factor to estimate the performance of non-real time traffic. In terms of JFI it may be noted that there are other schemes that perform better than the proposed scheme for the simple reason that the proposed scheme does not prioritize the resources and takes the average transmission rate for allocating resources for a particular frame. In addition, it may also be noted that the traffic modelling is carried out in such a way that there are bursts of traffic for real time data streaming and hence the case.

Table 2: Performance analysis of Proposed RSA with others

Name of Modified RSA	Time taken to generate Keys	Time taken to Encrypt Message	Time taken to Decrypt Message	Total Time to Generate Keys, Encryption & Decryption
Proposed RSA	178	1236	2712	4126
HRSA	220	1635	3120	4975
MRSA	210	1582	3526	5318
R-RSA	188	1248	2734	4170

Link Failure Management

A network could be designed considering initial factors, but network conditions such as load and traffic characteristics change with time. Network resources also vary due to new resource requests or topology changes (e.g., node or link failures). One important part of designing a quality of service (QoS) network is the reliability of the network. This reliability could be provided with different fault management mechanisms [13],[14],[15] applied at different network levels and timescales.

The protection method employed follows a cycle, starting when the fault is detected and finishing when the LSP is recovered. This cycle involves the development of two main components: a method for selecting the working and protection paths, and a method for bandwidth reservation in these paths. A fault detection mechanism along a path and a fault notification mechanism are also necessary to convey information to the network entity responsible for reacting to the fault and taking appropriate corrective actions

.

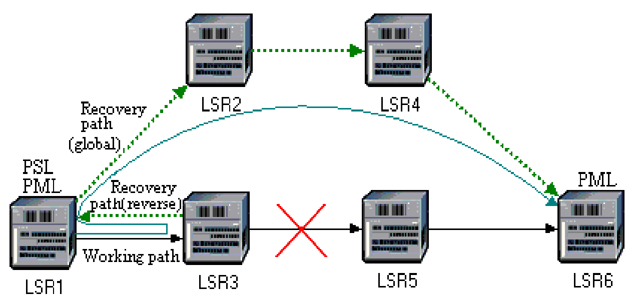

Figure 6: The reverse model, LSP backup utilization

A Network Processor is a programmable microprocessor optimized for processing network data packets. Many independent packets will be available, providing opportunities for parallel processing. Data rates for network processors range from 1.2Gbps (dual OC-12 data rate) to 40Gbps [11].

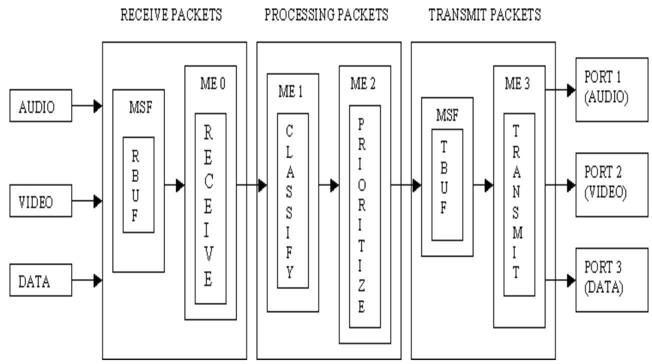

Figure 7: Block diagram of the system designed

This micro block reassembles the packet received in the receive buffer, writes the packet data to a buffer in DRAM, and queues the packet buffer handle on a Micro engine scratch ring for processing. The packet processing scratch ring holds the DRAM address where the start of each new packet is located [13].

Table 3: Initialization

Component	**Description**
Objective	Develop a scalable and secure IoT model for 5G applications by enhancing data accuracy, reducing transmission costs, and ensuring secure communication.
IoT Devices	The range of IoT devices used in the 5G network, such as sensors, actuators, and edge devices, which generate and send data.
Compression Techniques	Methods used to reduce the data size to improve bandwidth utilization, such as lossless and lossy data compression algorithms.
Encryption Techniques	Techniques to secure the data transmitted across the network, ensuring privacy and integrity. Examples include AES, RSA, and elliptic curve encryption methods.

Data Accuracy Enhancement	Methods like data fusion, noise fiIoT 5Gring, and predictive models to improve the accuracy of sensor readings in the IoT system.
Security Mechanisms	Mechanisms to prevent unauthorized access, including encryption, authentication protocols (e.g., TLS/SSL), and secure boot mechanisms.
5G Network Architecture	Design of the 5G infrastructure for IoT, including edge computing, network slicing, and low-latency communication.
Data Integrity Check	Ensuring that data is not aIoT 5Gred or tampered during transmission using techniques like hash functions or digital signatures.
Scalability	The model should be designed to handle an increasing number of IoT devices efficiently, without significant performance degradation.
Quality of Service (QoS)	Metrics to ensure that data transmission meets certain thresholds for latency, throughput, and reliability in a 5G network.
Privacy Preservation	Techniques like homomorphic encryption or anonymization to ensure that sensitive data remains private during processing or transmission.
Edge Computing Integration	Utilize local edge processing to reduce latency and load on central servers while improving data processing efficiency for real-time applications.

The Packet classification microblock receives DRAM locations from the receive microblock through the scratch ring [14]. By performing atomic operations the payload type field from the RTP header is extracted from the data payload and the packet size is retrieved from the header. Based on the PT value the received packet is identified as an audio or video packet, else considered as a data packet. The DRAM addresses of audio, video and data packets are written in separate scratch rings for further packet processing [15].

Conclusion

This study presents the design and evaluation of an efficient IoT model tailored for 5G applications, focusing on enhancing both data accuracy and security through the integration of advanced compression and encryption techniques. The proposed model effectively addresses the critical challenges of large-scale data transmission, network congestion, and cyber security concerns inherent in 5G networks. By employing data compression algorithms, the model significantly optimizes bandwidth usage, reduces transmission latency, and improves the overall efficiency of IoT systems. At the same time, the incorporation of encryption ensures robust protection for sensitive data, enhancing privacy and mitigating the risks of unauthorized access.

The performance evaluation demonstrates that the proposed IoT model yields notable improvements in key performance indicators, including data accuracy, energy consumption, and system security. Furthermore, the scalability of the model makes it well-suited for a wide range of 5G applications, from smart cities to industrial automation, where real-time data processing and secure communication are paramount.

In conclusion, this research contributes valuable insights into the design of secure and efficient IoT systems for 5G environments. The integration of compression and encryption techniques offers a promising approach to enhancing the overall performance and security of IoT applications, paving the way for the successful deployment of next-generation IoT solutions in 5G networks. Future work can explore the optimization of these techniques and their potential application in emerging use cases, ensuring that IoT systems continue to evolve in line with the growing demands of 5G technologies.

Reference

1. **3GPP TS 36.321**, *Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) Protocol Specification.*
2. **3GPP TS 36.323**, *Evolved Universal Terrestrial Radio Access (E-UTRA); Packet Data Convergence Protocol (PDCP) Specification.*
3. **3GPP TS 36.201**, *Evolved Universal Terrestrial Radio Access (E-UTRA); IoT 5G Physical Layer; General Description.*

4. **3GPP TS 36.211**, *Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and Modulation.*

5. B. Clerckx, H. Joudeh, C. Hao, M. Dai, and B. Rassouli, "Rate Splitting for MIMO Wireless Networks: A Promising PHY-Layer Strategy for IoT 5G Evolution," *IEEE Communications Magazine*, vol. 54, no. 5, pp. 98–105, May 2016.

6. W. Yu, Y. Qi, K. Liu, Y. Xu, and J. Fan, "Radiated Two-Stage Method for IoT 5G MIMO User Equipment Performance Evaluation," *IEEE Transactions on Electromagnetic Compatibility*, vol. 56, no. 6, pp. 1691–1696, Dec. 2014.

7. Q. Liu, H. Yu, and C. W. Chen, "Proactive Interference Avoidance for Mobile-to-Mobile Communication in IoT 5G Networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 9, pp. 7064–7077, Sept. 2016.

8. J. G. Torres and R. Bustamante, "Analysis of the Effects of CQI Feedback for IoT 5G Networks on ns-3," *IEEE Latin America Transactions*, vol. 13, no. 11, pp. 3538–3543, Nov. 2015.

9. M. Masiuk, M. Beshley, O. Lavriv, and Y. Deschynskiy, "Common Radio Resource Management Model for Heterogeneous Cellular Networks," *IEEE International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET'2016)*, Lviv, Ukraine, Feb. 23–26, 2016, pp. 661–663.

10. M. Klymash, M. Beshley, B. Strykhalyuk, and T. Maksymyuk, "Research and Development of Methods for Quality of Service Provision in Mobile Cloud Systems," *2014 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, Odessa, 2014.

11. M. Klymash, O. Lavriv, T. Maksymyuk, and M. Beshley, "State of the Art and Further Development of Information and Communication Systems," *2016 International Conference Radio Electronics & Info Communications (UkrMiCo)*, Kiev, 2016, pp. 1–6.

12. J. Cao, M. Ma, H. Li, and Y. Zhang, "A Survey on Security Aspects for IoT 5G and IoT 5G-A Networks," *IEEE Communications Surveys &*

Tutorials, Apr. 2013.

13. A. Mehaseb, Y. Gadallah, A. Elhamy, and H. Elhennawy, "Classification of IoT 5G Uplink Scheduling Techniques: An M2M Perspective," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1310–1335, 2nd Quarter 2016.

14. J. M. Liang, J. J. Chen, H. H. Cheng, and Y. C. Tseng, "An Energy-Efficient Sleep Scheduling with QoS Consideration in 3GPP IoT 5G-Advanced Networks for the Internet of Things," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 3, no. 1, pp. 13–22, Mar. 2013.

15. J. Gozalvez, "New 3GPP Standard for IoT [Mobile Radio]," *IEEE Vehicular Technology Magazine*, vol. 11, no. 1, pp. 14–20, Mar. 2016.