# Investigation Study On Secured Data Transmission In 5g Networks With Internet Of Things

**D.Suganya, Dr.A.V.Santhosh Babu**

**Abstract:** Mobile networks are organized in an environment where the network nodes are presented with less security protection against attacks. Internet of things (IoT) is an interconnected device used to transmit data over the network without human interface. 5G technology slices the physical network into different virtual networks for distributing right slice of network depending on the usage. Security is a keystone for 5G to construct the network infrastructure platform. Many node authentication techniques have been introduced to preserve the privacy of transmitted data over 5G mobile networks. But, the authentication accuracy was not improved and time consumption was not minimized. In order to address these problems, IoT based Multi-Objective Principal Component Regressed Emphasis Boosting Node Authentication (IoT-MOPCREBNA) method is introduced for performing secured communication in 5G wireless networks. This in turn helps to improve the security level in 5G networks. Simulation is carried out on factors such as authentication accuracy, authentication time and security level with respect to number of mobile nodes and data packets.

**Index Terms**: Mobile networks, security protection, cellular systems, principal component regressed emphasis boosting, node authentication.

## 1. INTRODUCTION

A mobile network is a communication network where mobile nodes are distributed without any access point [15, 16]. Internet of things (IoT) is a heterogeneous network compatible with mobile network for data transmission process. Fifth-Generation (5G) is the development of 4G that illustrated through higher bit rate, more capacity and low latency. 5G network aims at different advanced features like higher density of broadband users and device-to-device communications, lesser energy consumption for better IoT applications. The significant concern in 5G wireless network is to present the novel robust security solution that preserves the network from variety of routing attacks. This paper is organized as follows: Section 2 explains existing secured data transmission techniques in 5G networks, Section 3 shows the study and analysis of the existing and proposed secured data transmission techniques, Section 4 explains the simulation settings. Section 5 identifies the possible comparison between them. Section 6 presents the discussion and limitations of secured data transmission techniques. Section 7 concludes the paper.

## 2. 2 LITERATURE SURVEY

A fast mutual authentication and data transfer scheme were developed in [1] for large narrowband IoT devices to guarantee the security. The designed scheme combined the access authentication and secured data transmission process simultaneously. The designed scheme reduced the computational overhead but authentication accuracy was not improved. An Efficient, Secure network-Sliced and Service-oriented Authentication framework (ES3A) was introduced in [2, 17] for 5G-enabled IoT. However, the higher security level was not attained.


- *Mrs.D.Suganya, Assistant Professor, Department of Information Technology, Velalar College of Engineering and Technology, Erode, Tamil Nadu, India. E-mail: dsuganya55@gmail.com*
- *Dr.A.V.Santhosh Babu, Assistant Professor, Department of Information Technology, Sengunthar College of Engineering, Tiruchengode, Tamil Nadu, India. E-mail: santhoshbabu.av@gmail.com*


A certificateless multiparty authenticated encryption scheme was designed in [3] in 5G networks. The designed scheme attained multi-party authentication process and presented the identity anonymity. But, the data packet delivery ratio was not improved. Slice Specific Authentication and Access Control (SSAAC) mechanism was introduced in [4] to manage AAC with flexibility through virtualization technology. The designed mechanism performed authentication and access control of IoT devices assigned to third parties for decreasing load connectivity provider. But, an efficient authentication was not employed to enhance the security of data transmission. A new software-defined platform was introduced in [5] to allow the flexible infrastructure for 5G IoT communication. A sum-rate analysis was performed through optimization approach for data transmissions. SoftAir decoupled control plane and data plane for software-defined wireless architecture and allowed coordination among the remote radio heads with millimeter-wave for IoT access. However, the secured communication was not carried out in software-defined platform. An ultra-lightweight mutual authentication protocol termed ULMAP was introduced in [6, 18] with Bit and XOR operations to perform mutual authentication and prevent denial of service (DoS) attack. But, the time analysis remained unsolved.

The bootstrapping protocols were introduced in [7] with 3GPP specification to allow 5G feature of secondary authentication for constrained IoT devices. Two Extensible Authentication Protocol (EAP) lower layers, namely PANATIKI and LO-CoAP-EAP were introduced to permit secondary authentication and key establishment in NB-IoT and 4G/5G environments. The designed framework failed to offer an efficient secure end-to-end authentication. A new multimedia authentication technique was designed in [4] depending on trusted content representation (TCR) for 5G networks. The designed framework failed to present the attention for attacks and security trials. A mobility management model was introduced in [9] for triggering efficient handover and for choosing the optimal networks depending on multicriteria decision modeling. But, the reliability during communication was not improved by designed model. A new security framework was introduced in [10] to perform multitenant 5G-based IoT traffic through control loop feature. The designed framework failed to implement the cryptographic method for attaining the higher

security. The receiver-side nonlinearity compensation and symbol detection was carried out in [11] to perform transmitter task as simple and cheap. The joint maximum likelihood estimation detection issues of channel were measured through comb-type pilots in multipath fading OFDM systems. But, the complexity level was not minimized. A consensus-based algorithm were designed in [12] with selected information processing functionalities in IoT scenarios. The cooperative communication algorithms were introduced to perform the reliable communication services. Distributed timing and carrier frequency offset estimation techniques were employed to allow low-latency services. However, time complexity was not minimized by consensus-based algorithm. Two schedulers were introduced in [13] for IoT communications depending on QoS needs. The designed scheme presented the trade-off between two traffics through guaranteeing network performance and avoiding development of available resources. Though bandwidth utilization was reduced, scheduling efficiency was not performed. A real-time air pollution index measurement platform was introduced in [14] by 5G wireless network and blockchain. Blockchain technology encrypted and transmitted the data to the cloud and presented air pollution index measurement platform. However, the processing time was not minimized by real-time air pollution index measurement.

## 3. IOT BASED SECURED COMMUNICATION IN 5G WIRELESS NETWORKS

Internet-of-Things (IoTs) based networks are becoming key component for different application implementation regarding the healthcare and surveillance. IoT network are combination of objects, sensors and devices with different controllers for distribution of sensing and control information. IoT networks comprised multiple mobile nodes with capability to sense the neighboring environment. The key task within mobile network is to determine route taken between the sender and receiver for efficient data transmission. 5G directly communicate with additional mobile nodes within radio communication range. Due to dynamic movement, 5G wireless networks are susceptible to different types of routing attacks which affect the mobile nodes performance. Security is major challenging problem in wireless networks. The recent growth and conventional schemes for 5G wireless security have been discussed.

### 3.1 Fast Authentication and Data Transfer Scheme for Massive NB-IoT Devices in 3GPP 5G Networks

A fast mutual authentication and data transfer scheme was introduced to integrate the access authentication and secure data transmission process for Narrowband Internet of Things (NB-IoT) devices. The designed scheme attained authentication and data transmission of NB-IoT devices simultaneously. The designed scheme reduced the authentication process and removed load of networks and guaranteed the robust security protection with user anonymity and non-repudiation. The mutual authentication was achieved between group of NB-IoT terminals and Mobility Management Entity (MME). The data from group of NB-IoT terminals were transmitted to the core network in execution of mutual authentication process. The designed scheme minimized the signaling cost and communication cost. In addition, the designed scheme avoided the signaling overload of 3GPP 5G network and assured the QoS requirements of NB-IoT applications. The designed scheme was employed data security transmission for single NB-IoT terminal, group of NB-IoT terminals and huge NB-IoT terminals by anonymous attribute-based group establishment method. The designed scheme was authenticated through CK model and formal verification tool to provide robust security protection including identity privacy preservation and non-repudiation.

### 3.2 Efficient and Secure Service-Oriented Authentication Supporting Network Slicing for 5G-Enabled IoT

An Efficient, Secure network-Sliced and Service-oriented Authentication (ES3A) framework performed the network slicing for 5G-enabled IoT services. The users generated the connection with IoT services through network slices of 5G communication selected depending on accessing services types. The privacy preserving slice selection mechanism preserved the configured slice types and accessing service types. The session keys were described among users and IoT servers to guarantee the secure access of service data and remote servers with lesser latency. ES3A framework allowed 5G operator and IoT service provider to create anonymous delegation for subscribed users and to support slice selection for fog nodes devoid of exposing slice/service types. A privacy-preserving slice selection mechanism was introduced to select the network slices depending on allowed service type matching and configured slice types for package forwarding. The slice/service types and features differentiating network slices were preserved against fog nodes during the slice selection to break links among users and accessing services.

### 3.3 Certificateless Multi-Party Authenticated Encryption for NB-IoT Terminals in 5G Networks

A certificateless multiparty authenticated encryption scheme was introduced for NB-IoT terminals in 5G networks. The designed scheme attained multi-party authentication in access authentication process to offer identity anonymity and non-repudiation. The access authentication and data transmission were joined into one process. When multiple NB-IoT terminals present the access authentication, terminal information and encrypted private data were transmitted to Access and Mobility Management (AMF). AMF verified the validity and data security through authenticating the certificateless authenticated ciphertexts. Privacy identity protection scheme was carried out depending on anonymous. Every user registered with Key Generate Center to generate the registration serial number. Certificateless signcryption technique guaranteed the data security and integrity through the authentication process in data transmission.

### 3.4 A new scalable authentication and access control mechanism for 5G-based IoT

The fifth generation (5G) of mobile networks supported many needs and handled connectivity for massive Internet of Things (IoT) devices. Authenticating IoT devices and controlling their access to the network plays a vital role in the security of the devices and cellular system. Slice Specific Authentication and Access Control (SSAAC) mechanism was introduced to utilize the flexibility presented through virtualization technologies for handling the Authentication and Access Control. The designed mechanism performed authentication and access control of IoT devices allotted to the third parties for decreasing the load of connectivity provider with higher flexibility and modularity of 5G networks. The feasibility of designed mechanism was

computed with open-source platform. The designed mechanism minimized AAC signaling load on connectivity provider in Core Network (CN).

### 3.5 IoT based Multi-Objective Principal Component Regressed Emphasis Boosting Node Authentication

IoT based Multi-Objective Principal Component Regressed Emphasis Boosting Node Authentication (IoT-MOPCREBNA) method is introduced for secured communication in 5G wireless networks. In IoT-MOPCREBNA method, node cooperativeness count, trust and energy value of mobile nodes is computed for secured communication with connected IoT devices. IoT-MOPCREBNA method has two processes, namely feature selection and classification process. In IoT-MOPCREBNA method, the feature selection is performed by Principal Component Regression Analysis to select the relevant features of mobile nodes (i.e., trust, remaining energy and node cooperativeness). This helps to minimize the computation overhead of mobile node authentication in IoT-MOPCREBNA method. After feature selection process, the weighted emphasis boosting mobile node classification method is used to authenticate the mobile node as normal nodes and malicious nodes depending on the selected features. The designed ensemble classification model combines the weak learners (i.e., quadratic classifier) to make final strong classification results with lesser loss. Finally, the malicious nodes are removed and normal nodes are considered for performing the secured communication in 5G wireless networks. The architecture diagram of IoT-MOPCREBNA method is shown in figure 1.

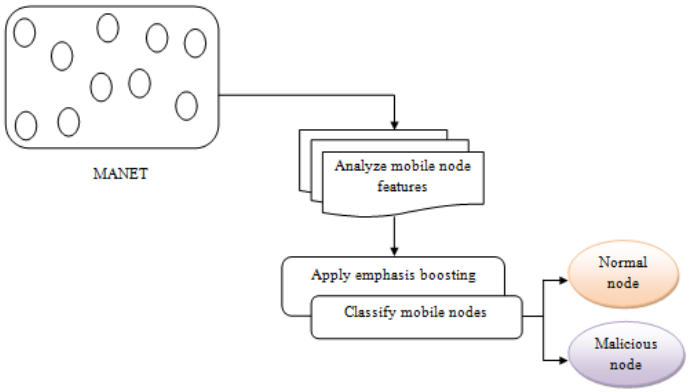


***Figure 1*** *Architecture Diagram of proposed IoT-MOPCREBNA method*

Figure 1 illustrates the architecture diagram of IoT-MOPCREBNA method to perform the node authentication for secured communication in IoT based 5G wireless networks. Let us consider, 'n' number of mobile nodes arranged in the wireless network. Then, mobile node features are identified by applying the Principal Component Regression Analysis. After finding the features of mobile node, the nodes are classified into two groups, namely normal or malicious mobile node by using emphasis boosting classification process. Therefore, the data communication is carried out through the normal node to improve the packet delivery ratio between sender and receiver mobile node.

## 4 SIMULATION SETTINGS

The simulation of the IoT-MOPCREBNA method and four existing methods namely fast mutual authentication and data transfer scheme [1], ES$^3$A framework [2], certificateless multiparty authenticated encryption scheme [3] and SSAAC mechanism [4] are implemented in NS2.34 network simulator. For simulation purposes, 500 mobile nodes are scattered in a squared area of 1100 m * 1100 m for performing the node authentication in 5G wireless network. The random way point model is taken as the mobility model for conducting the simulation. The simulation time is predefined as 300 seconds. DSR routing protocol is employed in the simulation to identify the normal node and malicious node for performing secured communication. The simulation parameters and their values are given in table 1.

***Table 1***

*Simulation Parameters and values*

| Simulation parameter | Value |
|---|---|
| Simulator | NS2 .34 |
| Network area | 1100m * 1100m |
| Number of mobile nodes | 50,100,150,200,250,300,350,400,450,500 |
| Protocol | DSR |
| Simulation time | 300sec |
| Mobility model | Random Way Point model |
| Nodes speed | 0-20m/s |
| Data packets | 30,60,90,120,150,180,210,240,270,300 |
| Number of runs | 10 |

### 4.1 Performance Metrics

The performance analysis of IoT-MOPCREBNA method and four existing methods namely fast mutual authentication and data transfer scheme [1], ES$^3$A framework [2], certificateless multiparty authenticated encryption scheme [3] and SSAAC mechanism [4] are discussed in this section. Three parameters are employed to compute the performance, namely

- Authentication accuracy
- Authentication time
- Security level

Impact on Authentication accuracy

Authentication accuracy is defined as the ratio of the number of mobile nodes that are correctly authenticated as normal or malicious to the total number of mobile nodes taken as input in 5G wireless networks. It is expressed as,

$$A_A = \left(\frac{Number\ of\ mobile\ nodes\ that\ are\ correctly\ authenticated}{n}\right) * 100 \quad (1)$$

From (1) '$A_A$' represents the authentication accuracy, '$n$, denotes the number of mobile nodes considered as an input. The authentication accuracy is measured in terms of percentage (%). When the authentication accuracy is higher, the method is said to more efficient.

**Impact on Authentication Time**

Authentication time '$T_A$' is defined as the amount of time

consumed for authenticating the mobile nodes in 5G network. It is defined as the difference of ending time and starting time of mobile node authentication. It is formulated as,

$$T_A = Ending\ time - Starting\ Time\ of\ Mobile\ Node\ Authentication \quad (2)$$

From (2), the authentication time is calculated. It is measured in terms of milliseconds (ms). When the authentication time is lesser, the method is said to be more efficient.

Impact on Security Level

Security level '$S_L$' is computed by means of packet delivery ratio. It is defined as the ratio of data packet that correctly received at the receiver node to the total number of data packets sent in a 5G wireless network. The packet delivery ratio is computed as,

$$S_L = \left(\frac{Number\ of\ data\ packets\ correctly\ received\ at\ receiver\ node}{Total\ number\ of\ data\ packets\ sent}\right) * 100 \quad (3)$$

The security level is measured in terms of percentage (%). When the security level is higher, the method is said to be more efficient.

## 5 RESULTS COMPARISON

In this section, the performance results of proposed IoT-MOPCREBNA method is computed in terms of authentication accuracy, authentication time and security level with other related existing methods. The performance of existing and proposed techniques is estimated using table and graphical analysis. In order to compute authentication accuracy, the numbers of mobile nodes are considered as an input ranging from 50 to 500.

***Table 2***

*Tabulation for Authentication Accuracy*

| Number of Mobile Nodes (Number) | Authentication Accuracy (%) | | | | |
|---|---|---|---|---|---|
| | Fast mutual authentication and data transfer scheme | ES$^3$A framework | Certificateless multiparty authenticated encryption scheme | SSAAC mechanism | IoT-MOPCREBNA method |
| 50 | 67 | 75 | 78 | 81 | 89 |
| 100 | 69 | 77 | 80 | 83 | 90 |
| 150 | 70 | 79 | 81 | 85 | 92 |
| 200 | 72 | 81 | 84 | 87 | 94 |
| 250 | 71 | 79 | 82 | 84 | 93 |
| 300 | 68 | 78 | 80 | 82 | 91 |
| 350 | 65 | 76 | 79 | 81 | 89 |
| 400 | 67 | 77 | 82 | 85 | 92 |
| 450 | 69 | 80 | 84 | 88 | 93 |
| 500 | 71 | 82 | 86 | 90 | 95 |

Table 2 describes the comparison of our proposed IoT-MOPCREBNA method with other existing schemes in terms of authentication accuracy. The authentication accuracy is computed for different number of mobile nodes. As described in results, authentication accuracy of IoT-MOPCREBNA method is higher than the four existing approaches fast mutual authentication and data transfer scheme [1], ES$^3$A framework [2], certificateless multiparty authenticated encryption scheme [3] and SSAAC mechanism [4]. While conducting the experimental work with 250 mobile nodes, IoT-MOPCREBNA method achieves 93% authentication accuracy whereas existing fast mutual authentication and data transfer scheme [1], ES$^3$A framework [2], certificateless multiparty authenticated encryption scheme [3] and SSAAC mechanism [4] achieves 71%, 79%, 82% and 84% respectively. From that, it is observed that authentication accuracy using proposed IoT-MOPCREBNA method is higher when compared to existing methods [1], [2] [3] and [4] for performing secured data communication. The comparative result analysis of authentication accuracy is described in figure 2.

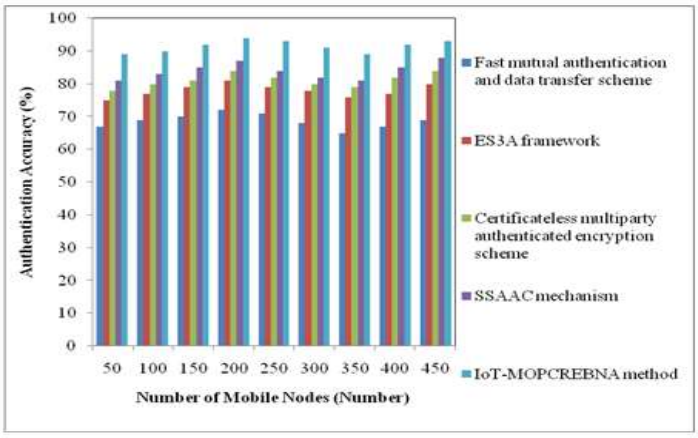


***Figure 2*** *Measure of Authentication Accuracy*

As illustrated in figure 2, the authentication accuracy of five methods is represented by five different colors. The above graphical results confirm that the authentication accuracy is improved using IoT-MOPCREBNA method than the existing methods. This is because of applying emphasis boosting classification process to categorize the mobile nodes as the normal node or malicious nodes. Emphasis boosting classification process combines the results of all weak learners for improving the accuracy performance. The comparision resutls proves that the authentication accuracy of IoT-MOPCREBNA method is increased by 33%, 17%, 13% and 9% as compared to existing methods [1], [2], [3] and [4] respectively. The second metric is the authentication time which helps to identify the amount of time consumed for authenticating the mobile nodes in 5G network. The simulation results of authentication time are shown in table 3.

***Table 3***

*Tabulation for Authentication Time*

| Number of Mobile Nodes (Number) | Authentication Time (ms) | | | | |
|---|---|---|---|---|---|
| | Fast mutual authentication and data transfer scheme | ES$^3$A framework | Certificateless multiparty authenticated encryption scheme | SSAAC mechanism | IoT-MOPCREBNA method |
| 50 | 45 | 38 | 32 | 25 | 13 |
| 100 | 47 | 40 | 34 | 27 | 14 |
| 150 | 49 | 42 | 37 | 29 | 17 |
| 200 | 51 | 45 | 39 | 31 | 18 |
| 250 | 53 | 47 | 41 | 33 | 21 |
| 300 | 55 | 49 | 44 | 35 | 23 |
| 350 | 57 | 51 | 46 | 37 | 25 |
| 400 | 59 | 54 | 48 | 40 | 27 |
| 450 | 61 | 57 | 50 | 42 | 29 |
| 500 | 63 | 59 | 52 | 45 | 32 |

Table 3 explains the comparison of our proposed IoT-MOPCREBNA method with other existing schemes in terms of

authentication time. The authentication time is determined for different number of mobile nodes. As shown in table results, authentication time of IoT-MOPCREBNA method is lesser than the four existing approaches fast mutual authentication and data transfer scheme [1], ES$^3$A framework [2], certificateless multiparty authenticated encryption scheme [3] and SSAAC mechanism [4]. While conducting the experimental work with 150 mobile nodes, IoT-MOPCREBNA method consumes 17ms authentication time whereas existing fast mutual authentication and data transfer scheme [1], ES$^3$A framework [2], certificateless multiparty authenticated encryption scheme [3] and SSAAC mechanism [4] gets 49ms, 42ms, 37ms and 29ms respectively. It is clear that authentication time using proposed IoT-MOPCREBNA method is lesser when compared to existing methods [1], [2], [3] and [4] for performing secured data communication. The comparative result analysis of authentication time is described in figure 3.

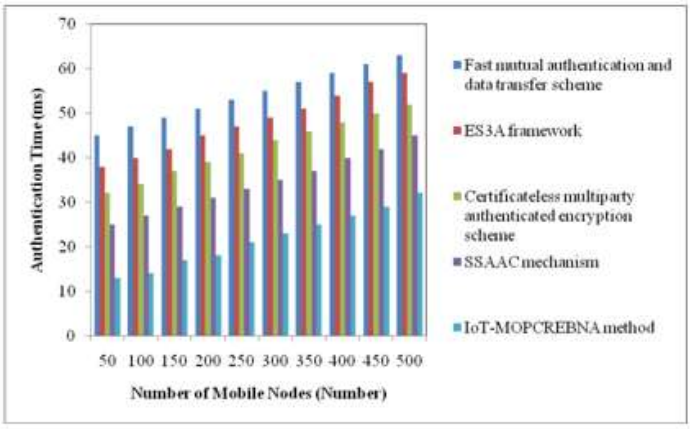


***Figure 3*** *Measure of Authentication Time*

Figure 3 illustrates the comparison of authentication time obtained by using the proposed IoT-MOPCREBNA method and other related works. For enhanced representation, ten iterations are carried out. While increasing the number of mobile nodes, the authentication time consumption gets increased correspondingly. The graphical illustration illustrates that the authentication time is minimized than the other four existing methods. The reason is application of principal component regression analysis for performing the feature selection of mobile nodes in IoT-MOPCREBNA method. The analysis determines the eigenvalues and eigenvectors for covariance matrix. After that, eigenvalues of features are arranged. Consequently, principal component (i.e. features) with larger eigenvalues is selected for performing the node authentication. This in turn helps to minimize the authentication time. With this, the authentication time is considerably reduced by using IoT-MOPCREBNA method by 60% when compared to [1], 55% when compared to [1], 4% when compared to [1] and 37% when compared to [4]. The third metric is security level which is measured in terms of packet delivery ratio depending on the number of packets being sent from sender node to receiver node. In order to compute security level, the numbers of data packets sent are considered as an input ranging from 30 to 300.

***Table 4***

*Tabulation for Security Level*

| Number of data packets sent (Number) | Security Level (%) | | | | |
|---|---|---|---|---|---|
| | Fast mutual authentication and data transfer scheme | ES$^3$A framework | Certificateless multiparty authenticated encryption scheme | SSAAC mechanism | IoT-MOPCREBNA method |
| 30 | 68 | 73 | 75 | 83 | 92 |
| 60 | 70 | 75 | 77 | 85 | 93 |
| 90 | 71 | 77 | 78 | 87 | 95 |
| 120 | 73 | 79 | 81 | 89 | 97 |
| 150 | 72 | 77 | 79 | 86 | 96 |
| 180 | 69 | 76 | 77 | 84 | 94 |
| 210 | 66 | 74 | 76 | 83 | 92 |
| 240 | 68 | 75 | 79 | 87 | 94 |
| 270 | 70 | 78 | 81 | 90 | 95 |
| 300 | 72 | 80 | 83 | 92 | 96 |

As designed in table 4, the simulation analysis of security level is described depending on number of data packets sent. The observed results prove that security level is improved using the IoT-MOPCREBNA method when compared to four existing methods. When considering the 210 data packets sent from sender node, the security level is 92% using IoT-MOPCREBNA method and security level of fast mutual authentication and data transfer scheme [1], ES$^3$A framework [2], certificateless multiparty authenticated encryption scheme [3] and SSAAC mechanism [4] are 66%, 74%, 76% and 83% respectively. The graphical representation of the security level is shown in figure 4.

***Figure 4*** *Measure of Security Level*

Figure 4 describes the packet delivery rate performance for different number of data packets ranging from 30 to 300. The number of data packets is considered as input which is given in horizontal axis. The packet delivery ratio results are given in vertical axis. From the figure, it is noticed that the performance of IoT-MOPCREBNA method is higher than the other four methods. This is because; IoT-MOPCREBNA method improves the security level during the data packet transmission through identifying the normal mobile nodes in 5G network. With these normal nodes, data packets transmission is performed to attain higher security. This helps to increase the successful data packets received at receiver node with minimum packet loss. The average results of security level of the proposed IoT-MOPCREBNA method improved by 35%, 24%, 20% and 9% as compared to existing

methods.

## 6 DISCUSSION ON LIMITATION OF SECURED DATA COMMUNICATION IN 5G NETWORKS WITH IOT

A fast mutual authentication and data transfer scheme integrated the access authentication and secure data transmission process. The designed scheme reduced the signaling and communication cost. But, authentication accuracy was not improved by designed scheme. ES3A framework supported the privacy-preserving slice selection and service-oriented anonymous authenticated key agreement for 5G-enabled IoT. However, the higher security level was not attained. In certificateless multiparty authenticated encryption scheme, IoT connected to the 5G core network to reduce the communication overhead and computational complexity for improving system efficiency. But, the data packet delivery ratio was not improved. The slice specific AAC approach was introduced with Radio Access Network for 5G mobile networks. Through managing AAC of devices under responsibility of 3rd parties, connectivity provider signaling load gets minimized. But, an efficient authentication was not employed to enhance the security of data transmission. From the discussion, it is clear that proposed IoT-MOPCREBNA method improves the security level on data transmission in 5G networks with higher authentication accuracy and minimum time consumption.

## 7 CONCLUSION

A comparison of different existing and proposed secured data transmission techniques in 5G wireless network with IoT is studied. From the study, it is clear that the existing techniques not improved the authentication accuracy. The survival review shows that the existing ES3A framework not attained the higher security. In addition, an efficient authentication process was not employed to enhance the data transmission security. In order to address these problems, IoT-MOPCREBNA method is introduced with higher authentication accuracy and lesser time consumption. The wide range of experiments on existing and proposed methods determines the performance of the secured data transmission techniques in 5G wireless network techniques with its limitations. Finally from result, the proposed IoT-MOPCREBNA method increased the authentication accuracy and reduced time consumption during secured data transmission techniques in 5G wireless network.

## REFERENCES


[1] Jin Cao, Pu Yu, Maode Ma, Weifeng Gao, “Fast Authentication and Data Transfer Scheme for Massive NB-IoT Devices in 3GPP 5G Network”, IEEE Internet of Things Journal, Volume 6, Issue 2, 2019, Pages 1561-1575

[2] Jianbing Ni, Xiaodong Lin, Xuemin Sherman Shen, “Efficient and Secure Service-Oriented Authentication Supporting Network Slicing for 5G-Enabled IoT”, IEEE Journal on Selected Areas in Communications, Volume 36, Issue 3, 2018, Pages 644 -657

[3] Yinghui Zhang, Fangyuan Ren, Axin Wu, Tiantian Zhang, Jin Cao, Dong Zheng, “Certificateless Multi-Party Authenticated Encryption for NB-IoT Terminals in 5G Networks”, IEEE Access, Volume 7, 2019, Pages 114721 – 114730

[4] Shanay Behrad, Emmanuel Bertin, Stephane Tuffin and Noel Crespi, “A new scalable authentication and access control mechanism for 5G-based IoT” Future Generation Computer Systems, Elsevier, Volume 108, July 2020, Pages 46-61

[5] Luis Tello-Oquendoa, Shih-Chun Linc, Ian F. Akyildiz, Vicent Pla, “Software-Defined architecture for QoS-Aware IoT deployments in 5G systems”, Ad Hoc Networks, Elsevier, Volume 93, 2019, Pages 1-11

[6] Kai Fan, Panfei Song, and Yintang Yang, “ULMAP: Ultralightweight NFC Mutual Authentication Protocol with Pseudonyms in the Tag for IoT in 5G”, Mobile Information Systems, Hindawi Publishing Corporation, Volume 2017, April 2017, Pages 1-7

[7] Jesus Sanchez-Gomez, Dan Garcia-Carrillo, Rafael Marin-Perez and Antonio F. Skarmeta, “Secure Authentication and Credential Establishment in Narrowband IoT and 5G”, Sensors, Volume 20, Issue 3, 2020, Pages 1-19

[8] Ling Xing, Qiang Ma, Honghai Wu, and Ping Xie, “General Multimedia Trust Authentication Framework for 5G Networks”, Wireless Communication and Mobile Computing, Hindawi Publishing Corporation, Volume 2018, June 2018, Pages 1-9

[9] Sadia Din, Awais Ahmad, Anand Paul, Seungmin Rho, “MGR: Multi-parameter Green Reliable communication for Internet of Things in 5G network”, Journal of Parallel and Distributed Computing, Elsevier, Volume 118, 2018, Pages 34-45

[10] Pablo Salva-Garcia, Jose M. Alcaraz-Calero, Qi Wang, Jorge Bernal Bernabe and Antonio Skarmeta, “5G NB-IoT: Efficient Network Traffic Filtering for Multitenant IoT Cellular Networks”, Security and Communication Networks, Hindawi, Volume 2018, December 2018, Pages 1-21

[11] Ehsan Olfat and Mats Bengtsson, “A general framework for joint estimation-detection of channel, nonlinearity parameters and symbols for OFDM in IoT-based 5G networks”, Signal Processing, Elsevier, Volume 167, February 2020, Pages 1072-1098

[12] Gloria Soatti, Stefano Savazzi, Monica Nicoli, Maria Antonieta Alvarez, Sanaz Kianoush, Vittorio Rampa and Umberto Spagnolini, “Distributed signal processing for dense 5G IoT platforms: Networking, synchronization, interference detection and radio sensing” Ad Hoc Networks, Elsevier, Volume 89, June 2019, Pages 9-21

[13] Ahlem Saddoud, Wael Doghri, Emna Charfi and Lamia Chaari Fourati, “5G radio resource management approach for multi-traffic IoT communications”, Computer Networks, Elsevier, Volume 166, January 2020

[14] Yohan Han, Byungjun Park and Jongpil Jeong, “A Novel Architecture of Air Pollution Measurement Platform Using 5G and Blockchain for Industrial IoT Applications”, Procedia Computer Science, Elsevier, Volume 155, 2019, Pages 728-733

[15] Santhosh Babu A V, Meenakshi Devi P, Sharmila B & Suganya D 2019, ‘Performance Analysis on Cluster based Intrusion Detection Techniques for Energy Efficient and Secured Data Communication in MANET’, International Journal of Information Systems and Change Management, (E ISSN No: 1479-3121), vol. 11, no. 1, pp. 56-69. RG Journal Impact: 0.53 - SCOPUS Indexed Journal. A Journal Indexed in Scopus (Elsevier) DOI NUMBER: 10.1504/IJISCM.2019.101649

[16] Santhosh Babu A V & Meenakshi Devi P 2019, ‘Swarm Optimized Energy Hubness Clustering to Detect And Respond Intrusive Attack Variants in MANET’, International Journal of Business Innovation and Research, (E ISSN No: 1751-0260), vol. 18, no. 3, pp. 369-391.RG Journal Impact: 0.64 - SCOPUS Indexed Journal, Google Scholar Indexed. A Journal

Indexed in Scopus (Elsevier) DOI NUMBER: 10.1504/IJBIR.2019.098253

[17] Santhosh Babu A V, Meenakshi Devi P & Sharmila B 2018, 'Efficient enhanced Intrusion identification and response system for MANETs', International Journal of Business Information Systems, (E ISSN No: 1746-0980), vol. 29, no. 4, pp. 535-546. RG Journal Impact: 0.72 - SCOPUS Indexed Journal, Google Scholar Indexed
A Journal Indexed in Scopus (Elsevier) DOI NUMBER: 10.1504/IJBIS.2018.096036

[18] Santhosh Babu A V, Meenakshi Devi P & Sharmila B 2016, 'Comparative Study of MANET Routing Protocols', Asian Journal of Research in Social Sciences and Humanities, (E ISSN No: 2249-7315), vol. 6, no. 6, pp. 1924-1934. Scientific Journal (SJ) Indexed Journal A Journal Indexed in Indian Citation Index, DOI NUMBER: 10.5958/2249-7315.2016.00337.3