Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.022940
Article

Tech Science Press

Feature Selection Based on IoT Aware QDA Node Authentication in 5G Networks

M. P. Haripriya[*] and P. Venkadesh

Department of Computer Science and Engineering, Noorul Islam Centre for Higher Education, Kumaracoil, Tamil Nadu, 629180, India
*Corresponding Author: M. P. Haripriya. Email: haripriya023paper@gmail.com

Received: 23 August 2021; Accepted: 22 October 2021

Abstract: The coming generation in mobile networks is the fifth generation (5G), which appears to be the promoter of the upcoming digital world. 5G is defined by a single piece of cellular access technology or a combination of advanced access technologies. Rather, 5G is a true network assembler that provides consistent support for a slew of novel network topologies. Prior generations provide as a suitable starting point and give support for the security architecture for 5G security. Through authentication and cryptography techniques, many works have tackled the security issues in 3G and 4G networks in an effective manner. However, security of 5G networks while data transmission was not improved. The IoT aware Quadratic Discriminant Analysis (QDA) Node Authentication Method is proposed in order to achieve safe data communication in the 5G network. The suggested method performs feature selection using Quadratic Discriminant Analysis to identify relevant properties of mobile nodes such as trust value, residual energy level, and node cooperativeness. Simulation can be used to test the data packets, the number of mobile nodes in a security level, the computation overhead, and the authentication accuracy. The observed output clearly demonstrates that the Quadratic Discriminant Analysis Method significantly enhances the authentication accuracy of each node and the security level with less overhead than state-of-the-art-methods.

Keywords: 5G network; quadratic discriminant analysis; remote sensing; routing protocol

1 Introduction

A fifth-generation mobile network (5G) is an upgrade of 4G that features better bit rates, larger capacity, and very low latency. The next mobile network iteration is 5G, which is an upgraded design of the 3GPP (Third Generation Partnership Project) and 4G cellular systems [1]. When sending and receiving communications, 5G technology provides exceptionally low latency. The growing need for mobile data and reduced latency drives the creation of the fifth-generation network. Furthermore, the 5G network focuses for advanced features such as increased broadband user density, device-to-device communications, and lower energy consumption for better Internet of Things (IoT) application [2,3]. A mobile device is the deployment of a large number of IoT devices. The mobile nodes in this 5G network connect as directly as possible with other nodes in this huge IoT age within the range of radio transmission. When compared to previous generations of the network, mobile nodes in this network link intelligently in a short amount of time [4]. For improved outcomes in 5G networks, cryptographic techniques and authentication procedures are used in data transfer to improve security and reduce time consumption [5].

1.1 Generations of Network to 5G

From the zeroth to the fifth generation, the first zeroth generation, which was available after the Second World War in the 1970s, had precellular technology of cellular mobile telecommunications, which was the first stage of network generations. Following the zeroth generation, subsequent generations such as 1G, 2G, 3G, 3.5G, and 4G were developed and established with more efficiency when compared to one another. And now we have the fifth-generation mobile network, also known as 5G, which is an upgrade of 3GPP. Each generation's advancement was mind-blowing. The bandwidth, accuracy, and speed with are targeted to improve from one generation to the next for each generation. Fig. 1 depicts the diagrammatic representation.

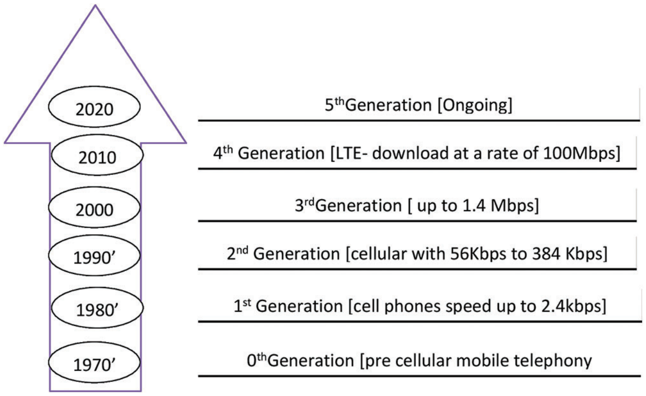
2020
5thGeneration [Ongoing]
2010
4th Generation [LTE- download at a rate of 100Mbps]
2000
3rdGeneration [up to 1.4 Mbps]
1990'
2nd Generation [cellular with 56Kbps to 384 Kbps]
1980'
1st Generation [cell phones speed up to 2.4kbps]
1970'
0thGeneration [pre cellular mobile telephony

Figure 1: Various generations of network

The Fig. 1 above shows the successive generations of networks with the established period. Each generation of network, such as from 0G to 5G, increased from one to the next, with the most notable improvement being its effective data speed for mobiles. The extensive network coverage that enables more people to utilise mobile phones. Additionally, the speed, capacity, range, frequency, and bandwidth are all substantially enhanced.

1.2 IOT and 5G

The availability of a network with a broad range and low latencies is determined by the needs of each user. The Internet of Things, abbreviated as IoT, was the new face of the developing world at our fingertips. The most well-known examples of IoT are smart devices, remote sensing equipment, self-driving automobiles, and so on [6]. This smart application requires better data efficiency, more bandwidth, and less time consumption, which can only be intelligently given by 5G technology. IoT is the process of transforming the world into a smart world with less time and effort in order to make everything easier [7].

Fig. 2 shows the diagrammatic form of 5G with IoT as represented that the future world became the smart world. The standardization of 5G in the Internet of things is classified into two types of standards. The initial step defines as the technology standard which deals with wireless communication, protocols, and network technology, and another step which defines data privacy and security with the regulatory standard [8].

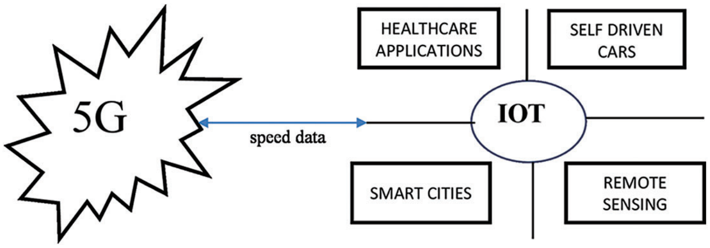

Figure 2: Represents the 5G with IoT environment

2 Feature Selection Based QDA Method

The feature selection method is one of the important and effective methods used in data pre-processing and an essential component in the Machine Learning process. In statistics and machine learning, it is also known as variable selection, attribute selection, or variable subset selection. The two most significant elements of the feature selection process are individual evaluation and subset assessment. The feature selection technique is employed to detect the relevant features, as shown in Fig. 3. Text categorization, intrusion detection, genomic analysis, image retrieval, and remote sensing are all examples of applications that use feature selection [9].

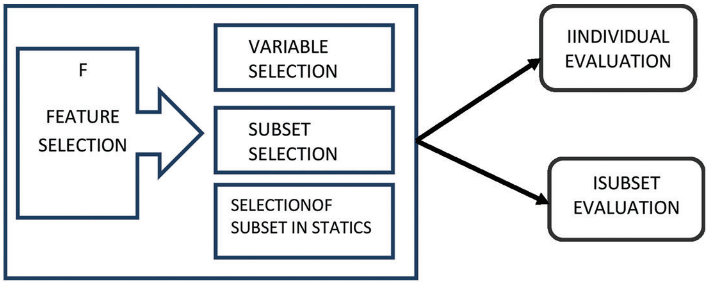

Figure 3: Feature selection method to detect relevant feature

Fig. 3 depicts the feature selection process for picking the attribute by examining its numerous aspects and then subjecting it to two sets of variables. They are the subset evaluation and the individual evaluation, which are accomplished *via* the use of various simulation methodologies and mathematical evaluations.

Several issues are raised by the existing approaches, including the lack of authentication accuracy, increased time complexity, and the failure to improve the security level for successful data communication in 5G networks, among others. Several drawbacks of existing methods are noted, and the main contribution of the IoT aware Quadratic Discriminant Analysis method is as follows. The feature selection method is done out utilising quadratic discriminant analysis to reduce the computation overhead of mobile node authentication. The probability ratio test is used to pick related features.

Following the process, the trust value, energy level, and node cooperativeness attributes are taken into account while authenticating the mobile nodes. The elements listed above help to improve the quality of nodes in every transmission.

3 Related Works

In [10], a novel key exchange and authentication mechanism was devised to improve security during a mobile terminal handover. However, reducing the amount of time spent was insufficient. A Blockchain-based lightweight distributed mobile producer Authentication (BlockA*uth*) protocol was presented in [11] for secure and fast mobile user authentication. However, the performance of authentication was not adequate.

In [12], an IEWA technique was created to improve system stability and security performance. However, the packet delivery ratio was not taken into account.

Secure two-factor authentication and key agreement scheme were presented in [13] for secure user authentication and key agreement. However, the authentication accuracy was not considered.

A System Theoretic Process Analysis (STPA) technique was designed in [14] for safety analysis and STPA-sec for security analysis. However, the energy consumption was not minimized. [15] designed a novel key exchange and authentication technique to improve security during a mobile terminal handover. However, reducing the amount of time spent was insufficient.

4 Architecture Diagram for Quadratic Discriminant Analysis

This quadratic discriminant analysis method was utilised to discover the effective features of the mobile node in feature selection. Existing approaches, which have a variety of limitations, can be improved to produce improved result. To overcome this the Quadratic discriminant analysis was introduced [16].

Fig. 4 shows the flow process of the quadratic discriminant analysis to perform the feature selection method for getting the efficient features of the mobile node in the network. As shown in the above diagram the discriminant model first takes the set of input as the mobile node from the network. After getting the input the QDA (Quadratic Discriminant Analysis) method was performed for getting the efficient feature through the feature selection method [17]. Also, this feature selection method contains the relevant feature selection process as the sub-category for this analysis method.

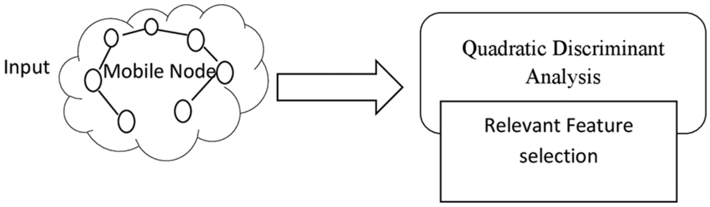

Figure 4: Architecture diagram of quadratic discriminant analysis

5 Quadratic Discriminant Analysis-Based Feature Selection

The quadratic discriminant analysis is used to choose the most relevant features of the mobile nodes from a large set of features. In general, node characteristics include node mobility, velocity, trust, cooperativeness, energy, and so on. A subset of the many attributes has been chosen for node authentication in mobile ad-hoc networks. An adhoc network is used to reduce authentication time. The flow process of Quadratic discriminant analysis-based feature selection is given below.

Fig. 5 represents the structure of the Quadratic discriminant analysis-based feature selection process for secure data communication. The IoT-QDA method uses the Quadratic Discriminant Analysis for selecting the more relevant features for node authentication. At first, Quadratic Discriminant Analysis is applied in machine learning to divide the total set into two or more subsets. As represented in the figure, in the 5G network different mobile nodes are available. Those nodes are taken as an input, then these data are divided into two or more subsets, after that feature selection process is carried out by using Quadratic Discriminant Analysis. Thus, we get the relevant feature set as an output. Here, the two subsets s_1 and s_2, are initialized with the mean value (μ_1, μ_2). The likelihood ratio test is measured between the features of mobile nodes $f_1, f_2, f_3, \ldots .f_n$ and the mean of the classes.

$$L_d(\mathrm{s_n}|\mathrm{f_1},\mathrm{f_2},\mathrm{f_3},\ldots.\mathrm{f_n}) = \frac{1}{\sqrt{(2\pi\sigma^2)^{-n}}}\exp\left(\frac{\mathrm{f_i}-\mu_\mathrm{i}}{2\sigma^2}\right) \tag{1}$$

where, L_d represents the likelihood, $\mathrm{s_n}$ denotes a subset of features $\mathrm{f_1},\mathrm{f_2},\mathrm{f_3},\ldots.\mathrm{f_n}$, μ_i denotes a mean of the subset, σ denotes a deviation. The likelihood ratio test expresses how the feature is more related to the authentication for secure data transmission. As a result, the likelihood function categorizes the features into subsets through the mean which is closer to the feature.

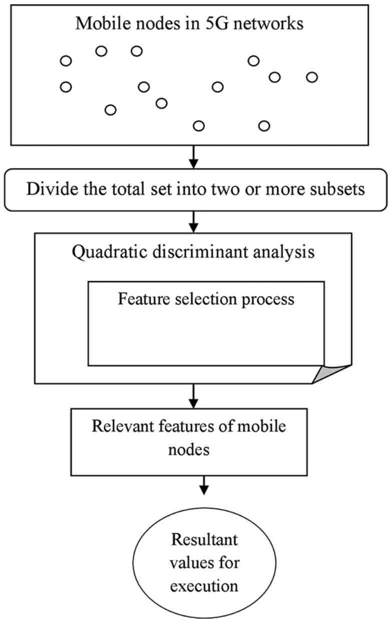
Mobile nodes in 5G networks
Divide the total set into two or more subsets
Quadratic discriminant analysis
Feature selection process
Relevant features of mobile nodes
Resultant values for execution

Figure 5: Structure of quadratic discriminant analysis

Fig. 6 represents the IoT-QDA method selecting three more relevant features namely node trust, energy, and cooperativeness. The features are described as follows.

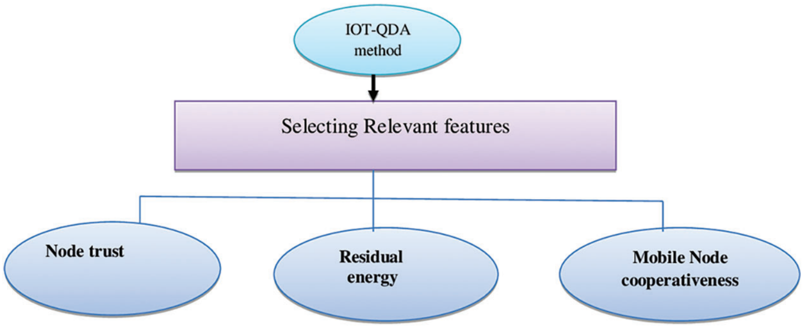

Figure 6: Selecting relevant features for the QDA method

5.1 Node Trust

The number of mobile nodes $Mn_i = Mn_1, Mn_2,\ Mn_3 \ldots Mn_n$ are placed in a wireless network. Based on the history of that node the trust value is calculated for each mobile node (MN). It means that the number of data forwarded and received as well as dropped by the sensor node. The trust value is calculated by the equation,

$$T_{Mn} = \left(\frac{D_f - D_{dr}}{D_R}\right) \tag{2}$$

where, T_{Mn} indicates a trust value of the MN, D_f denotes a data packet forwarded, D_{dr} indicates a data packet dropped, D_R refers to received data packets from the mobile node.

5.2 Residual Energy

Energy is one of the significant features of the mobile node during the data packet transmission. As based on the time and Product of the power the energy is mathematically calculated as given below by the expression,

$$E_{Mn} = power * time \tag{3}$$

where, E_{Mn} represents the energy of the mobile node and Joules (J) is the term used for measuring. Based on the energy, the total energy, and the residual energy is calculated to depend on the amount of energy utilized by the mobile nodes after receiving data packets and transmitting data packets. The residual energy of the node is measured as below,

$$R_{Mn} = T_E - T_u \tag{4}$$

where, R_{Mn} represents the mobile nodes residual energy, T_E represents the total energy of the mobile node (i.e., initial energy), T_u denotes an amount of energy utilized by the mobile node.

5.3 Mobile Node Cooperativeness

Because of the arbitrary mobility of mobile nodes, node collaboration is critical in MANETs for achieving improved communications. The cooperativeness of a node is determined by its behaviour when communicating with other nodes in the network [18]. The cooperativeness is utilised to determine the node connection over the time interval. As a result, each mobile node in the network is responsible for maintaining a connection to its whole neighbourhood in order to communicate effectively. End-to-end connectivity is guaranteed to improve data transmission if the connections between neighbouring nodes are kept. Here we consider that the two mobile nodes Mn_i and Mn_j in the network. Before transmitting the data, it has a connection in between the mobile nodes that are organized through the distributed message namely *req* and *rep*. The Mn_i sends the request message to another neighboring node as follows,

$$Mn_i \overset{req}{\rightarrow} Mn_j \tag{5}$$

where, Mn_i is the mobile node sends the request *req* to the other mobile node Mn_j. After receiving the request message, the other mobile node sends the reply back to the node. This indicates that these two nodes are connected and cooperatively working together at a particular time instant.

$$Mn_i \overset{rep}{\leftarrow} Mn_j \tag{6}$$

where the mobile node Mn_j sends reply *rep* message back to the mobile node Mn_i. If the node Mn_i did not receive any reply message from the node Mn_j, then the mobile node Mn_j are not cooperate to Mn_i with particular time‘t’. And based on cooperativeness of the particular node is identified. The algorithm for the feature selection process is given as follows,

```
Algorithm for Quadratic discriminant analysis-based feature selection,
Input: ‘n’ number of mobile nodes $Mn_i = Mn_1, Mn_2,\ Mn_3 \ldots Mn_n$
Output: To select the more relevant feature
Begin
For each mobile node $mn_i$
 Measure the likelihood function using Eq. (1) then
    Group the features into subsets $(s_1, s_2)$ with the mean value $(\mu_1, \mu_2)$
  Relevant features are selected using Quadratic discriminant analysis
    Calculate node trust using Eq. (2)
    Calculate residual energy of the node using Eq. (3)
    Calculate node cooperation using Eq. (4)
End for
End
```

The above table represents the algorithm that shows the process feature selection using Quadratic Discriminant Analysis. In this area of wireless network, there are mobile nodes in ‘n’ numbers that are randomly deployed. Then, the likelihood function is calculated for each mobile node. Based on this function features are divided into two subsets with mean. After that, the proposed IoT-QDA method selects more relevant features of the mobile node (i.e., trust value, residual energy level, and node cooperativeness) by using the Quadratic discriminant analysis model.

6 Simulation Setup and Parameter Settings

The IoT-QDA method simulation and the existing method namely fast mutual authentication and data transfer scheme [19] and ES^{3}A framework [20] implemented in an NS2.34 network simulator. Here 500 MN are distributed in a squared area of A^2 (1100 m * 1100 m) for performing the node authentication to improve the security of data communication in the 5G mobile ad-hoc network for simulation purposes.

For conducting the simulation, the mobility model uses the model called the random waypoint model. Here the time to be set as 300 seconds to undergo simulation. The Distance Source Routing protocol is effectively used in the simulation to identify the normal node and malicious node for secure communication. The list of simulation parameters and their values are described in Tab. 1.

Table 1: Simulation parameters and values

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

The above Tab. 1 contains the simulation parameter used to find out that the node ae normal or malicious during data communication [21]. The number of nodes which are taken as from 50 to 500 with the simulation time of 300 sec and by using DSR protocol [it's a protocol that can be used in a mesh network, where in an ad-hoc network the on-demand protocol is used to restrict the bandwidth consumed by control packets And the DSR which stands for dynamic source routing] the execution of the process been calculated with 10 number of runs with the speed of 20 m/s.

7 Comparative Analysis

This section discusses the performance study of the IoT-QDA technique [22] as well as existing approaches such as the rapid mutual authentication and data transmission scheme and the ES3A framework. The three parameters utilised to evaluate performance are security level, authentication accuracy, and authentication time. The performances are analysed using graphical representations and tables. Each section displays the performance results.

7.1 Simulation Analysis of Security Level

The security level is measured in terms of packet delivery ratio refers to the percentage ratio of the data packet that receives the destination to the data packet send in a network. The mathematical formula for calculating the packet delivery ratio is expressed as follows,

$$DR_{dp} = \left(\frac{N_{dp}\ correctly\ received}{N_{dp}}\right) * 100$$

where, DR_{dp} refers to the packet delivery ratio, N_{dp} is the number of data packets. The packet delivery ratio is measured in terms of percentage (%).

Fig. 7 shows the performance of the packet delivery rate which was ranged from 30 to 300. The horizontal axis shows the number of data packets considered as the input whereas the vertical axis shows the result of the packet delivery ratio. The above Fig. 7 represents the performance of the IoT-QDA method is better than the existing method.

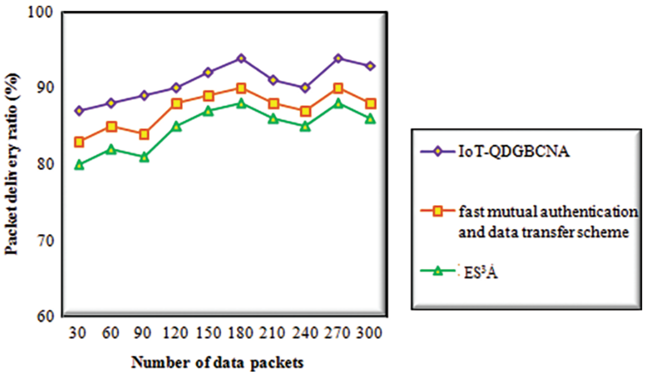

Figure 7: Graphical results of packet delivery ratio

7.2 Simulation Analysis of Authentication Accuracy

Authentication accuracy refers to the percentage ratio of the number of MN, mobile nodes that are perfectly authenticated as malicious or normal to the total number of MN's taken as input in a 5G wireless network. It is mathematically expressed as given below.

$$A_{acc} = \left(\frac{n_{CA}}{n}\right) * 100 \tag{7}$$

From Eq. (7), A_{acc} denotes an authentication accuracy, n denotes the number of mobile nodes (MN) taken as input, n_{CA} denotes correctly authenticated MN. The accuracy is measured in terms of percentage (%) is the term that is used to measure accuracy. Whereas, higher the authentication accuracy, the method is said to be more efficient.

7.3 Sample Calculation

Here the sample calculation process has been carried out by using the following three steps with a mathematical expression such as

1. Proposed IoT-QDA
2. Existing fast mutual authentication and data transfer scheme
3. Existing ES^{3}A framework

7.3.1 Proposed IoT-QDA

The number of mobile nodes correctly authenticated is 46 and the total number of mobile nodes taken as input is 50. Therefore, the authentication accuracy is mathematically calculated as follows,

$$A_{acc} = \left(\frac{46}{50}\right) * 100 = 92\%$$

7.3.2 Existing Fast Mutual Authentication and Data Transfer Scheme

The number of mobile nodes correctly authenticated is 44 and the total number of mobile nodes taken as input is 50. Therefore, the authentication accuracy is mathematically calculated as follows,

$$A_{acc} = \left(\frac{44}{50}\right) * 100 = 88\%$$

7.3.3 Existing ES^{3}A Framework

The number of mobile nodes correctly authenticated is 43 and the total number of mobile nodes taken as input is 50. Therefore, the authentication accuracy is mathematically calculated as follows,

$$A_{acc} = \left(\frac{43}{50}\right) * 100 = 86\%$$

The above Tab. 2 explains the simulation results of authentication accuracy for data communication. The authentication accuracy is calculated based on the number of IoT devices i.e., mobile nodes. For simulation purposes, the number of mobile nodes is taken from 50 to 500. The simulation graph is shown in Fig. 7.

Fig. 8 illustrates a graphical representation of authentication accuracy concerning several mobile nodes as IoT devices in 5G cellular networks. As shown in the graph, it represents colors of lines such as violet, orange, and green for implementing the authentication accuracy of three methods namely IoT-QDA, fast mutual authentication and data transfer scheme, and ES^{3}A framework. From graph representation, the number of mobile nodes is given as input at $'x'$ axis whereas the simulation results of authentication accuracy are obtained at the $'y'$ axis. The above results confirm that the authentication accuracy of the IoT-QDA method is said to be improved than the other two existing methods. This improvement is achieved by applying the subtractive gradient boost clustering technique. The ensemble clustering techniques use subtractive clustering as a weak learner to group the mobile node likea normal or malicious. The ensemble technique correctly group the nodes based on the features with minimum error. As a result, the ensembled technique accurately identifies the mobile nodes in the 5G network are normal or malicious. Here with the existing techniques, a comparison takes place with the ten various results of the IoT-QDA method. The comparison results prove that the authentication accuracy is said to be improved by 4% as compared to fast mutual authentication and data transfer scheme and 7% as compared to ES^3A framework.

Table 2: Authentication accuracy

Number of mobile nodes	Authentication accuracy (%)		
	IoT-QDA	Fast mutual authentication and data transfer scheme	ES^3A
50	92	88	86
100	89	86	84
150	90	87	83
200	91	88	85
250	88	86	84
300	92	87	83
350	89	86	82
400	91	88	85
450	93	89	87
500	92	88	86

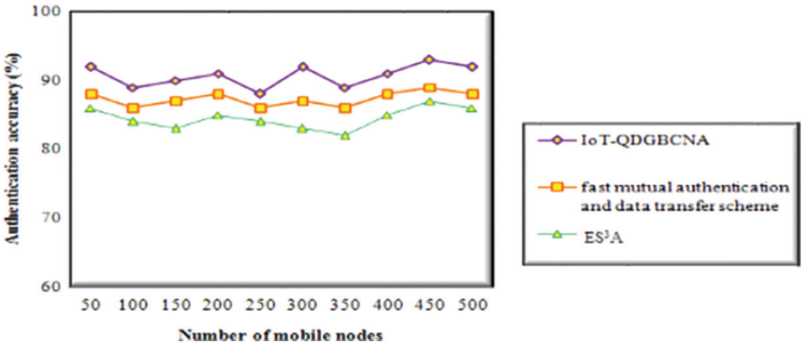

Figure 8: Graphical results of authentication accuracy

8 Conclusion

The IoT aware Quadratic Discriminant Analysis (QDA) approach performs mobile node authentication in IoT aware 5G networks. Initially, the attributes of the mobile nodes are chosen using quadratic discriminant analysis. The ensemble technique classifies mobile nodes as normal or malicious based on their characteristics in order to reduce the time spent authenticating mobile nodes in the network. The mobile nodes are authorised in the 5G network based on these results. Simulation can be used to test data packets, the number of mobile nodes in a security level, computation overhead, and authentication accuracy. The simulation results show that the proposed IoT-Quadratic Discriminant Analysis approach outperforms state-of-the-art methods in terms of higher packet delivery ratio, lower computing overhead, and higher authentication accuracy.

Acknowledgement: The authors with a deep sense of gratitude would thank the supervisor for his guidance and constant support rendered during this research.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] K. Munir, E. Zahoor, R. Rahim, X. Lagrange and J. H. Lee, "Secure and fault-tolerant distributed location management for intelligent 5G wireless networks," *IEEE Access*, vol. 6, pp. 18117–18127, 2018.

[2] M. P. Haripriya and P. Venkadesh, "Investigation study on secured data communication on 5g cellular networks," *Journal of Advanced Research in Dynamical and Control Systems*, vol. 11, no. 11, pp. 323–330, 2019.

[3] R. Devi, R. K. Jha, A. Gupta, S. Jain and P. Kumar, "Implementation of an intrusion detection system using adaptive neuro-fuzzy inference system for 5G wireless communication network," *AEU-International Journal of Electronics and Communications*, vol. 74, no. 8, pp. 94–106, 2017.

[4] B. H. Khudayer, M. Anbar, S. M. Hanshi and T. C. Wan, "Efficient route discovery and link failure detection mechanisms for source routing protocol in mobile ad-hoc networks," *IEEE Access*, vol. 8, pp. 24019–24032, 2020.

[5] A. Celik, J. Tetzner, K. Sinha and J. Matta, "5G device-to-device communication security and multipath routing solutions," *Applied Network Science*, vol. 4, no. 1, pp. 1–24, 2019.

[6] X. Ge, R. Zhou and Q. Li, "5G NFV-based tactile internet for mission-critical IoT services," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6150–6163, 2019.

[7] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi and M. Mustaqim, "Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios," *IEEE Access*, vol. 8, pp. 23022–23040, 2020.

[8] M. P. Haripriya and P. Venkadesh, "Subtractive gradient boost clustering for mobile node authentication in the internet of things aware 5G networks," *Journal of Computational and Theoretical Nanoscience*, vol. 18, no. 4, pp. 1287–1293, 2021.

[9] S. B. Pooja, R. S. Balan, M. Anisha, M. S. Muthukumaran and R. Jothikumar, "Techniques tanimoto correlated feature selection system and hybridization of clustering and boosting ensemble classification of remote sensed big data for weather forecasting," *Computer Communications*, vol. 151, no. 2, pp. 266–274, 2020.

[10] B. Ying and A. Nayak, "Lightweight remote user authentication protocol for multi-server 5G networks using self-certified public-key cryptography," *Journal of Network and Computer Applications*, vol. 131, no. 1, pp. 66–74, 2019.

[11] M. Conti, M. Hassan and C. Lal, "Block auth: Block chain based distributed producer authentication in ICN," *Computer Networks*, vol. 164, no. 5, pp. 106888, 2019.

[12] H. Huang, L. Hu, J. Chu and X. Cheng, "An authentication scheme to defend against UDP DRDOs attacks in 5G networks," *IEEE Access*, vol. 7, pp. 175970–175979, 2019.

[13] S. Shin and T. Kwon, "Two-factor authenticated key agreement supporting unlikability in 5G-integrated wireless sensor networks," *IEEE Access*, vol. 6, pp. 11229–11241, 2018.

[14] I. Friedberg, K. M. Laughlin, P. Smith, D. Laverty and S. Sezer, "STPA-safe sec: Safety and security analysis for cyber-physical systems," *Journal of Information Security and Applications*, vol. 34, no. 1, pp. 183–196, 2017.

[15] V. Sharma, I. You, F. Y. Leu and M. Atiquzzaman, "Secure and efficient protocol for fast handover in 5G mobile Xhaul networks," *Journal of Network and Computer Applications*, vol. 102, no. 11, pp. 38–57, 2018.

[16] C. Zhuang, H. Zhao, C. Sun and W. Feng, "Detection and classification of GNSS signal distortions based on quadratic discriminant analysis," *IEEE Access*, vol. 8, pp. 25221–25236, 2020.

[17] K. Elkhalil, A. Kammoun, R. Couillet, T. Y. A. Naffouri and M. S. Alouini, “A large dimensional study of regularized discriminant analysis,” *IEEE Transactions on Signal Processing*, vol. 68, pp. 2464–2479, 2020.

[18] Y. Zhang, R. Deng, E. Bertino and D. Zheng, “Robust and universal seamless handover authentication in 5G HetNets,” *IEEE Transactions on Dependable and Secure Computing*, vol. 1, pp. 123–129, 2019.

[19] J. Cao, P. Yu, M. Ma and W. Gao, “Fast authentication and data transfer scheme for massive NB-IoT devices in 3GPP 5G network,” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1561–1575, 2018.

[20] J. Ni, X. Lin and X. S. Shen, “Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT,” *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 3, pp. 644–657, 2018.

[21] A. Appathurai and P. Deepa, “Radiation-induced multiple-bit upset prediction and correction in memories using cost-efficient CMC,” *Informacije MIDEM*, vol. 46, no. 4, pp. 257–266, 2016.

[22] A. J. G. Malar, C. A. Kumar and A. G. Saravanan, “IoT based sustainable wind green energy for smart cities using fuzzy logic based fractional order darwinian particle swarm optimization,” *Measurement*, vol. 166, no. 2, pp. 108208, 2020.