E-ISSN 2250-0944
ISSN 2250-1150
doi: 10.31838/ijprt/14.01.04

Research Article

Ephemeral Resilient Signcryption and Piecewise Deep Belief Network forReliable with QoS aware Streaming Social Media Data Transmissionin 5G Network

SURESH N[1*], P KANMANI P[2]
[1]Research Scholar, Thiruvalluvar Government Arts College, Rasipuram, Namakkal dt, Tamilnadu.
[2]Assistant Professor, Department of Computer Science, Thiruvalluvar Government Arts College, Rasipuram, Namakkal Dt,Tamilnadu
*Corresponding Author

Received: 11.09.23, Revised: 13.10.23, Accepted: 09.11.23

ABSTRACT
Fifth Generation Mobile Network (5G) is supported by wireless network services to offer extensive data transmission to improve device-to-device transportation quality, as well as minimize working costs. It allows users to seamlessly access a variety of multimedia services in social network platforms such as live streaming applications like Internet live sports networks, youtube, Facebook, etc... There are various security and privacy issues related to the user's shared multimedia information. With the fast-growing 5G technology, privacy preservation of streaming data transmission in social network platforms plays a vital role for handling the attackers. In order to improve the QoS aware secure streaming data transmission in a 5G network, a novel technique called Ephemeral Resilient SchnorrSigncryptive Piecewise Damped Convolutional Deep Belief Network (ERSSPDCDBN) is introduced with higherreliability. The ERSSPDCDBN technique first collects the social media stream data. After that, secure data transmission is performed by applying an ephemeral resilient schnorrsigncryption. For enhancing security, ephemeral resilient key generation, signcryption, and unsigncryptionis carried out by using signcryption method. Followed by, the user authenticity is verified based on digital signature verification using a simple matching coefficient. If the signature is valid, the authorized user obtains the original data and avoids the attackers. During data transmission, Piecewise regressive Damped Convolutional deep belief network is developed for achieving higher throughput and minimum latency. Experimental of ERSSPDCDBN is conducted by using six metrics.

Keywords: 5G technology, social network, reliable and Qos aware streaming data transmission, Piecewise regressive Damped Convolutional deep belief network, ephemeral resilient matching schnorrsigncryption

Preamble

Social mediadomainsis connected with people fortransmitting data in suitable manner through growth of wireless network. Differentnovel social network methods are introduced during modern days with social media content. With this, users wereresponsivefor accessing delay-aware media content. An unique security risks were introduced by smart mobile devices to improve communication services by limiting any malicious attacks in the similar moment.

In order to safecommunication, a security protocol was introduced in [1] for accurately detect the attacks with aid of Elliptic Curve Cryptography (ECC). But latency was not minimized. For straight communications and social-awareness constraints, secure and Trust D2D (SeT-D2D) framework was developed in [2] to protect D2D communications and privacy. But, efficient data delivery with higher authentication was not achieved.

For conveying extremely flexible safety, and verificationtask, the software-Defined-Networking framework was developed in [3] with multimedia data communication. 5G IoT secure data transmission is performed in [4] by using a pseudo-random hash-based ECC as well as linear scaling Rock Hyraxes swarm-based CNN.

Security and data delivery ratio was improved [5] with node-oriented secure data transmission method. But it failed to detect and prevent malicious attacks.Multimedia way was identified by mixture deep learning-based anomaly determination approach. But the accurate authentication was not performed.Social-Aware D2D Video Delivery approach was developed [7] with reduce the packet loss, the higher throughput was not achieved.

In 5G multiservice systems, a novel hierarchical identity management approach was developed [8].The delay and more the bandwidth efficiency of the edge devices was minimized [9] with help of QoS-Aware optical fogassisted cyberphysical method.For a 5G-enabled healthcare network, clever QoE-aware radio access technology was developed in [10]However, secure data transmission was a challenging problem.

Major contributions

The issues of the existing literature have been addressed with developing a novel ERSSPDCDBN and the contribution is given below,

- To increase the reliability as well as QoS-aware social media data transmission in the 5G network, the ERSSPDCDBN technique is introduced with two major contributions.
- First, the ephemeral resilient schnorrsigncryption technique is employed in an ERSSPDCDBN for secure social media streaming data transmission. Followed by, the user authenticity is verified based on digital signature verification by means of a simple matching coefficient. If the signature is valid, the authorized user obtains the original data and detects the attackers. In this way, reliable data transmission is performed in a 5G network.
- The Piecewise regressive Damped Convolutional deep belief network is introduced in ERSSPDCDBN for achieving QoS-aware data transmission to achieve higher throughput and minimum latency.
- For evaluating the experiments by using several parameters, proposedas well as conventional techniqueswere estimated. The outcome of the ERSSPDCDBN is better than other traditional methods.

Paper organization

The paper is arranged into five different sections; Literature work provided in section 2. ERSSPDCDBN with a neat diagram is explained in section 3. Experimental settings of proposed and existing methods are presented in section 4. Followed by, section 5 illustrates the performance results of the proposed ERSSPDCDBN against the conventional methods with different parameters. The conclusion is presented in section 6.

LITRATURE REVIEW

A distributed architecture was introduced in [11] for D2D communications and trust management between dynamic social relationships. The designed method reduces the energy consumption over legacy in 5G cellular networks but the loss rate was not minimized. An efficient trust relay node was identiifed with Edge Collaboration Cache Trust Community Routing model was designed in [12]. The algorithm provides efficient data packet delivery but the latency was a major challenging issue. In [13], Social network data analysis was performed based on higher security. However, the data analysis with more information fromthe social network was not considered.

With 5G networks, improved primary verificationas well as key harmonyprocedure were developed [14]. However, The QoS aware data transmission was not achieved. The protected as well as unidentified transportation was ensured in [15] via Certificateless Public Key Cryptography (CL-PKC) as well as ECC. However, delay-aware group communications were not focused. To improve average transmission capability with higher throughput, an QoS-forecasting-basis of theclever flow-control method was developed [16]. But, 5G system procedure was not optimized.

In order to address these security issues by detecting DDoS attacks, safe Blockchain-based 5G validation as well as key concord was developed [17].A social-aware spectrum sharing and caching helper selection (SSC) was developed [18] for sharing records.The reliability of data transmission inside social networks was analyzed in [19]. A new trust-aware method was introduced in [20] based on deep learning to improve data transmission.

METHODOLOGY

Social media ismassiveimpact on people’s lives. In 5G, the user in online social networks permits to share multimedia streaming information with other people and enables the users to view videos. The key feature in 5G data communication is used to noticeably minimize the latency and improves the throughput of data delivery. During the streaming social data transmission, reliability as well as QoS is major challenging issues in upcoming 5G technology for achieving the wireless mobile performance.

When the same information is received atthe destination from the source and not subjected to corruption due to attackers for obtaining data transmission reliability. The data traffic is handled with QoS metric for minimizing latency.

In streaming data transmission, reliability and QoS-aware data communication are significant processes in upcoming 5G technology to enhance the performance of the wireless mobile network. Many technologies are required to manage the 5G network. Among the many technologies, reliability and QoS-aware communication are demanding concerns to enhance the performance of 5G cellular communication. Therefore a novel ERSSPDCDBN technique is introduced aiming to improve security requirements in social networks. The proposed ERSSPDCDBN technique achieves better reliability and QoS-aware streaming data transmission by means of 5G cellular communication. The streaming information shared in social networks distributes very fast with minimal latency and immediately which makes it attractive for attackers to modify the information. In this case, the proposed ERSSPDCDBN technique solves the attacker's problems by introducing the signcryption technique.

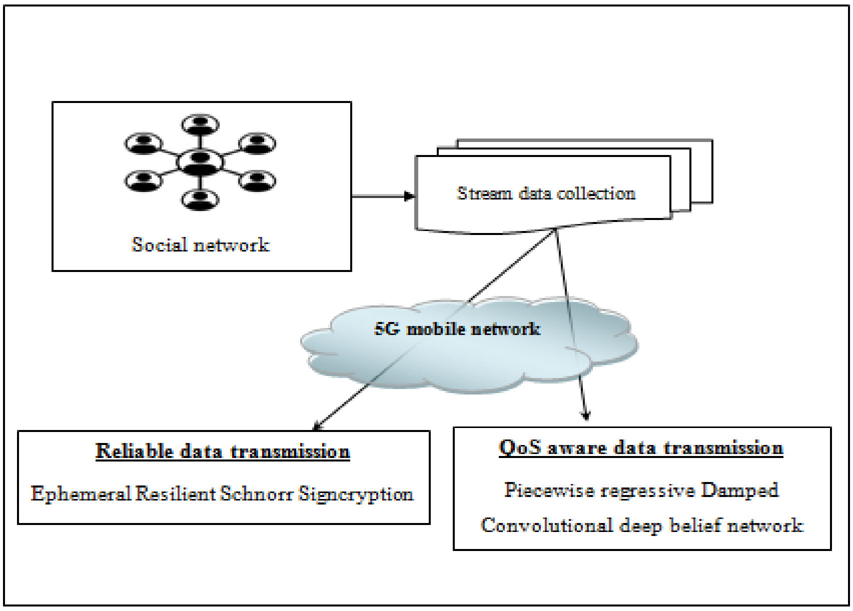

Social network
Stream data collection
5G mobile network
Reliable data transmission
Ephemeral Resilient Schnorr Signcryption
QoS aware data transmission
Piecewise regressive Damped
Convolutional deep belief network

Figure 1 Block diagram of ERSSPDCDBN

Block diagram of ERSSPDCDBN is demonstrated to perform secure and QoS-aware social media data transmission in a 5G network. The proposed ERSSPDCDBN techniquesimultaneously performs two processes namely Ephemeral Resilient Schnorr Signcryption and Piecewise regressive Damped Convolutional deep belief network. Social network is a term used to describe online web-based applications that permit individuals to create a profile and connect with other users to distribute information.

The ERSSPDCDBN organization has been described.In the social network, $G = \langle v, e \rangle$ is defined as the graphical formportrays the users as well as their associations. The online users denoted as $v = \{u_1, u_2, u_3, \dots u_n\}$ as well as the streaming data communications between the online mobile users through the 5G technology is indicated as 'e'. The proposed ERSSPDCDBN performs better reliability and QoS-aware data sharing between the users to improve the secure delivery of network services with minimum latency, data loss, and higher throughput.

Ephemeral resilient schnorrsigncryptioncryptographic methods are to handle the refuge problems with higher security aims. By using this model, thetrustworthiness of safetyas well as confidentialitytechniquesduringD2Dcommunication, as well as confirmation is improved. During the communication, Piecewise regressive Damped Convolutional deep belief network is employed in ERSSPDCDBN to achieve better QoS requirements in terms of throughput, data loss, and latency.

Ephemeral Resilient Schnorrsigncryptive secure data transmission

An online social network (OSN) includes large volumes of users' personal information. The exponential growth of users in social networks generates a large amount of information and is being shared every day conversely has encouraged attackers to increase and collect such information for malicious purposes. To ensure secure and trustworthy data transmission in social networks, it is essential to identify the various potential attacks posed by attackers. However, due to the presence of attackers, sensitive user information is often compromised. Motivated and driven by these factors, this paper develops a signcryption technique fora highly secure system for Streaming data to focus on the security of transmission. Streaming data refers to any media content seamlessly delivered to computers and mobile devices through the 5G network.

An Ephemeral Resilient Schnorrsigncryption is a public-key cryptographic technique to perform the secure streaming data transmission that simultaneously performs the digital signature as well as encryption. The signcryption typically includes different processes. In the key generation process, the private and public key of each user in the social network is generated. After that, the signcryption is performed for encrypting the sensitive data before the transmission and generating the digital signature. Finally, the Unsigncryptionprocess is performed to decrypt the data after verifying the signature. Based on the above-said processes, reliable data transmission is performed in the social network.

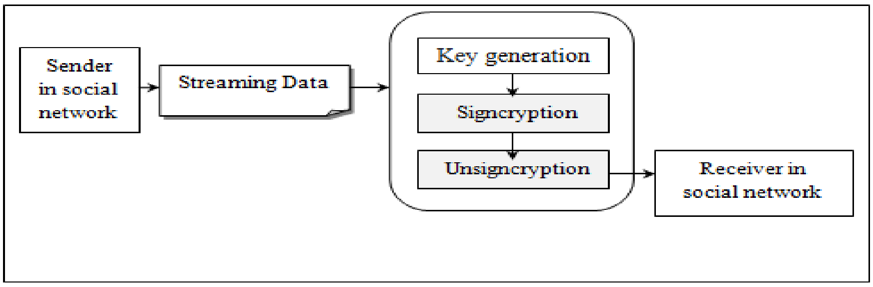


Figure 2 block diagram Ephemeral Resilient Schnorr signcryption

Figure 2 demonstrates the Ephemeral Resilient Schnorrsigncryptionwith higher confidentiality, protection of streaming transmissionand integrity. The sender transmits the streaming data to the receiver in a secure manner for preventing the streaming information as of attacks. For improving the safemessageamong sender and receiver, proposed cryptographic technique includes key generation, signcryption, and unsigncryption. These processes are explained briefly in the following subsections.

Ephemeral Resilient key generation

Ephemeral Resilient session is to execute signcryption scheme with private as well as public key generation. Ephemeral resilient session keygenerateswith each session. Also, key pair is used within a particular session. Once the session is finished, then the keys are disabled and it generates a new key for the next session. Resilient means the ability to set another key pair. Therefore, the illegal entrée is avoided to get higher confidentiality.Generated key pair has ephemeral if it is generated for each execution of a key establishment process. The generated private key has reserved secret as well as thepublic key allocation used for additionaldevelopment.

Let's consider private signing session key is a prime number 'k'. Then the public Ephemeral Resilient key is generated with the private key.

$P = B^k$ (1)

Where P indicates anEphemeral Resilient public key, 'B' indicates a large prime number. 'k' denotes a private key. As a result, pair of keys is generated for the sender and receiver.

Signcryption

After the Ephemeral Resilient key generation process, the signcryption process is carried outand it includes encryption and signature generation. In public key cryptography, encryption is the method of converting the original representation of the information into a cipher text for unreadable output with receiver's public key. Itis not understandable until it has been converted into original data using a decryption process. Let us consider the data 'D' transferred among the group of users in the social network.

$\beta_c \leftarrow E\,(P_R, D)$ (2)

Where β_c denotes a ciphertext of original data, E indicates encryption,P_R is the Ephemeral Resilient public key of the receiver. Simultaneously, the proposed cryptographic technique performs the signature generation using Schnorr digital signature algorithm by sender's private key

A digital signature is a process of verifying the authenticity of data generated by the sender. A valid signature is used to verify that the data was created by an authorized user.Create the digital signature for hash value.

Let us consider the random number 'x'.

$q = B^x$ (3)

The signature is generated as follows,

$\rho_s = H\,[q \| D]$ (4)

$z = x - k\rho_s$ (5)

Where produced signature with sender is indicated as '(ρ_s, z)', concatenation is referred as (||), cryptographic hash is denoted as ,k denotes a private key. The signature is generated as the hash value. Finally, the cipher text as well as signature istransmittedtoward receiver.

Unsigncryption

Unsigncryption is process of converting the cipher text into the original data. The signature confirmation executes with public key of sender in receiver end.

$q_s = B^z P^{\rho_s}$ (6)

$\rho_r = H[q_s \| D]$ (7)

Where, $\rho_r$is the new signature onreceiver.If the created signature confirmed and it is matched by signature generated in the sender 'ρ_s' by using simple matching coefficient (SMC) is a statistical function used to compare the similarity and diversity of sample sets (i.e. signatures).

$$M = \frac{Matc\hbar ing\ word\ in\ \rho_s\ and\ \rho_r}{Lengt\hbar of\ signature} \quad (8)$$

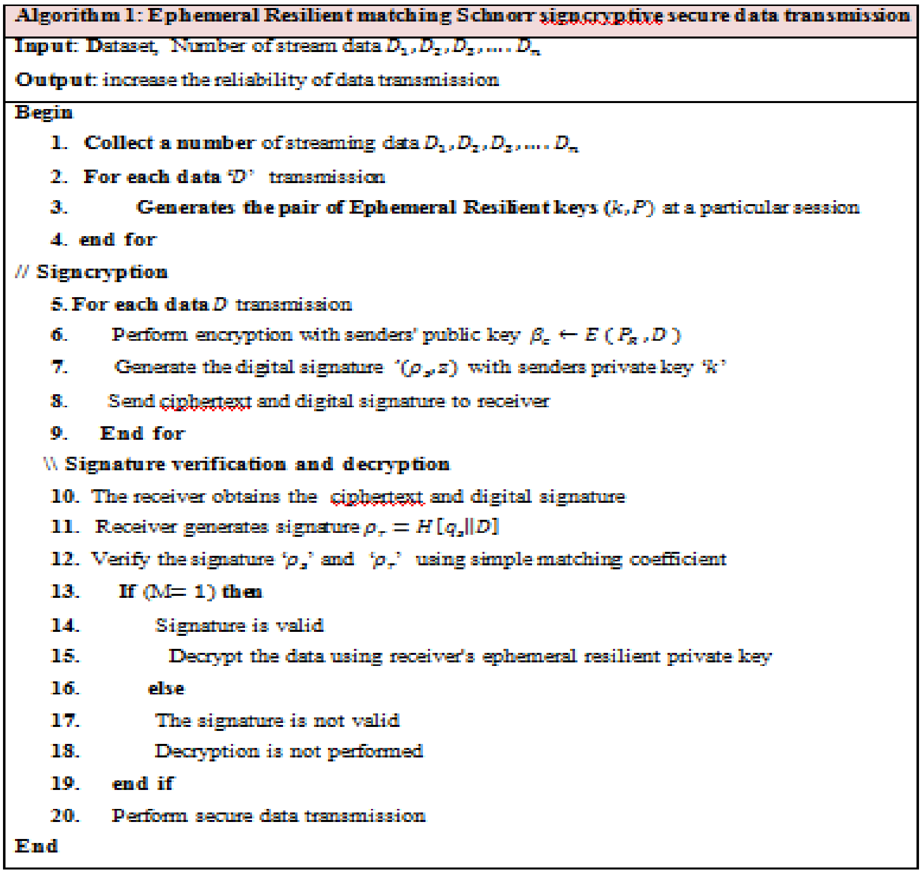
Where M indicates a simple matching coefficient that returns '1' for accurate matching and '0' for not matched

$$M = \begin{cases} 1, & \rho_s = \rho_r \\ 0, & \rho_s \neq \rho_r \end{cases} \quad (9)$$

When both signatures get matched, then the receiver is authenticated as an authorized user and obtains the ciphertext.Or else, the signature hasunacceptable as well asreceiver did not get the original data. These processes enhance the refuge. The decryption process is obtained as given below,

$D \leftarrow dec(k_r, \beta_c)$ (10)

From (10),D denotes original data,dec indicates the decryption, k_r denotes a private key of the receiver, β_c is the ciphertext. In this way, secure streaming data transmission is carried out with higherprivacy. The TIPBRSCSBT algorithm has given below.



Algorithm 1: Ephemeral Resilient matching Schnorr signcryptive secure data transmission

Input: Dataset, Number of stream data $D_1, D_2, D_3, \dots D_n$

Output: increase the reliability of data transmission

```
Begin
    Collect a number of streaming data $D_1, D_2, D_3, \dots D_n$
    For each data 'D' transmission
            Generates the pair of Ephemeral Resilient keys $(k, P)$ at a particular session
    end for
// Signcryption
    For each data $D$ transmission
        Perform encryption with senders' public key $\beta_c \leftarrow E\,(P_R, D)$
        Generate the digital signature '$(\rho_s, z)$ with senders private key 'k'
        Send ciphertext and digital signature to receiver
    End for
  \\ Signature verification and decryption
    The receiver obtains the ciphertext and digital signature
    Receiver generates signature $\rho_r = H\,[q_s \| D]$
    Verify the signature '$\rho_s$' and '$\rho_r$' using simple matching coefficient
        If (M= 1) then
            Signature is valid
              Decrypt the data using receiver's ephemeral resilient private key
           else
            The signature is not valid
            Decryption is not performed
      end if
      Perform secure data transmission
End
```

The above process describes a secure stream data transmission using the ephemeral resilient matching schnorrsigncryption technique. First, the streaming data are collected from the dataset. Then the cryptographic techniques generate the pair of ephemeral resilient keys for each session. Then the data encryption as well as signature generation based on the schnorr algorithm is performed on the sender side. The encrypted data and generated digital signature are sent to the receiver end. Followed by, the unsgncryption process is carried out at receiver through the signature verification and decryption. The receiver generates a new signature for that particular data. The signature verification process is done by applying a simple matching coefficient (SMC). If the two signatures get matched, then the matching coefficient returns '1' and the receiver perform decryption to obtain the original data. This helps to improve the reliability of data transmission interms of achieving higher security by avoiding the attacks

Piecewise regressive Damped Convolutional deep belief network based QoS aware data transmission in social network

During the data transmission in 5G social networks, the seamless delivery of streaming information is maintained with minimum latency and higher throughput. Owing to significant mobility necessities, as well as irregular network situations, delivering QoS has difficult for 5G. Hence, Convolutional deep belief network-basedQoS-aware data transmission is introduced with minimum latency and data loss to incessant contact of data on several times.

A Convolutional deep belief network includes various units such as two visible units input and output and more than one hidden unit. The advantage of a convolutional deep belief network is less computational complexity while considering numerous units.

Figure 3 depicts the schematic construction of the Convolutional deep belief network with visible units and more than one hidden unit. In a schematic deep belief network, the input unit receives the given input as a node or device and transforms it into the hidden unit for deep learning. Finally, the output unit displays the processed outcomes from the hidden units. The units are connected in a feed-forward manner.

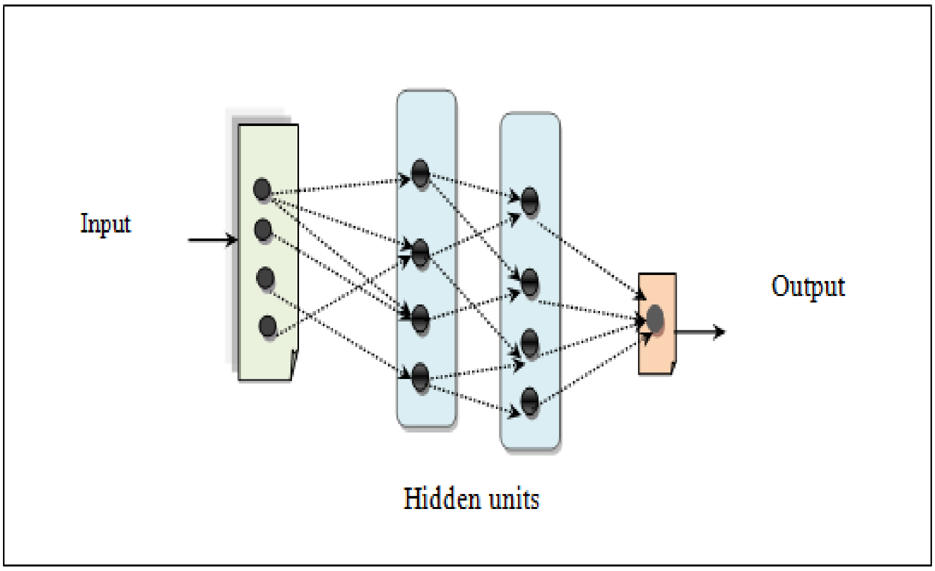


Figure 3 schematic construction of the Piecewise regressive Convolutional deep belief network

Let us consider the number of nodes or device$M_1, M_2, M_3, \ldots . M_n$in 5G network taken as input. Then the input is transferred hidden unit. The signal strength of the device in a 5G network is analyzed by piecewise regression.

Piecewise regression examines the signal strength in which the independent variable is partitioned into different segments by setting the threshold value.In the hidden units, received signal strength of the devices or nodes'Rss' estimated,

$$Rss = \left[\frac{g_t * g_r * k_t^2 * k_r^2}{r^4}\right] * t_r \qquad (11)$$

Where, g_t and $g_r$designates a sender and receiver antenna gain,k_t^2represents the height ofthe senderantenna, k_r^2 indicates the height of the receiver (i.e. device), r indicates the distance between sender and receiver, $t_r$indicates a transmitted signal power of the device. The piecewise regression is applied to a hidden layer for analyzing the signal strength of the device in a 5G network.

$$Y = \begin{cases} \mathrm{Rss} > th & ; \quad strong \\ \mathrm{Rss} < th & ; \quad weak \end{cases} \qquad (12)$$

Where 'Y' indicates an output of the piecewise regression, Rss indicates a received signal strength of the device, th denotes a threshold. If the received signal power of the mobile device is greater than the threshold, then the device has strong received signal strength. If the attained signal power is lesser than the maximum threshold and higher than the minimum threshold, the mobile device is classified as having weak signal strength. The mobile device weaker signal strength is connected innearest base station in improving the data delivery with higher throughput and minimizing the latency.

Let us consider the location of mobile nodes is $(\mathrm{x}_1, \mathrm{y}_1)$ and the location of the base station $(\mathrm{x}_2, \mathrm{y}_2)$. Therefore, the distance from themobile nodes to the base station is measured as given below,

$$\mathrm{d} = \sqrt{(\mathrm{x}_2 - \mathrm{x}_1)^2 + (\mathrm{y}_2 - \mathrm{y}_1)^2} \qquad (13)$$

Where, distance is computed. A damped least-squares method is applied used tofind the minimum distance.

$$\mathrm{Z} = \arg\min\ \mathrm{d} \quad (14)$$

Where, Z indicates anoutput of the damped least-squares method, an argument of the lowest method is represented as '$\arg\min$'. As a result, the mobile device is connected to the nearest base station for continuously delivering the data to minimize the latency and increase the throughput.

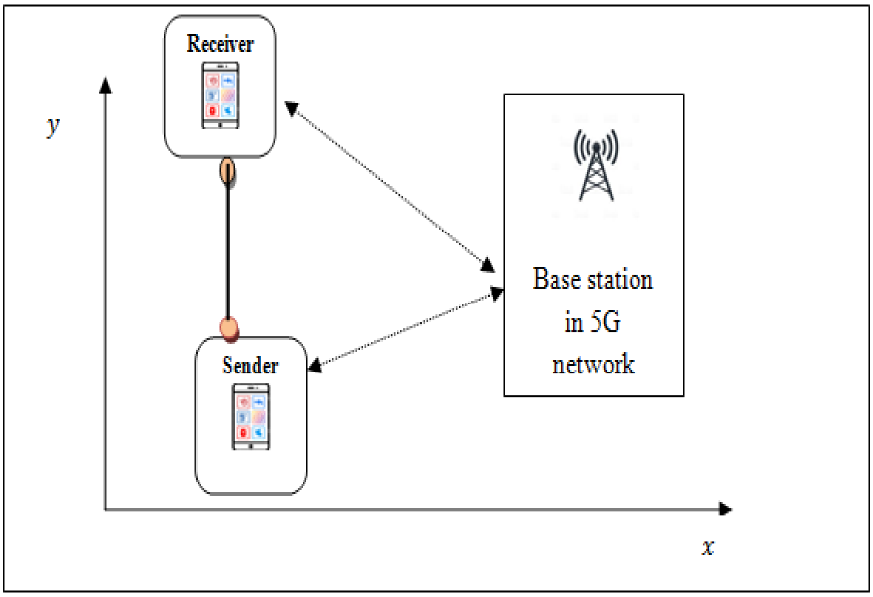
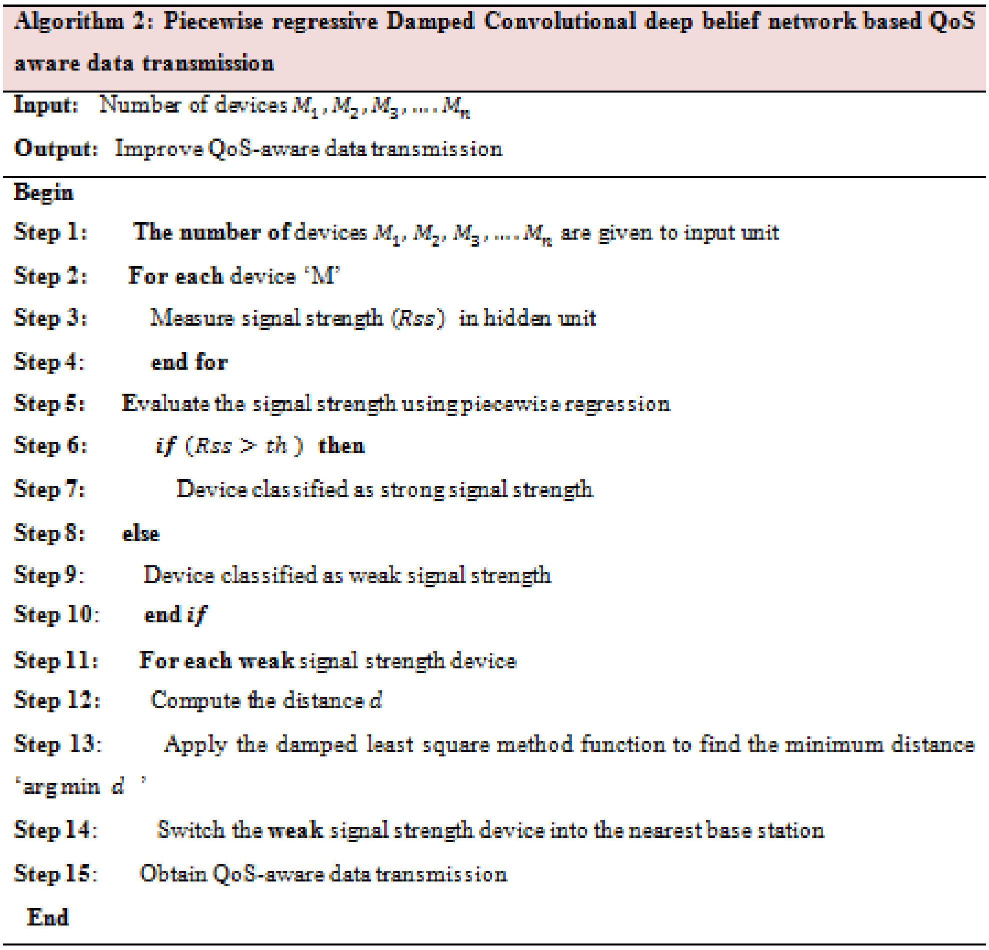


Figure 4 Social media data communication in 5G network

Figure 4 demonstrates the social media data communication between the devices in the 5G network. Two mobile devices directly communicate with each other and the higher signal strength is provided by the base station. The algorithmic process of the piecewise regressive damped convolutional deep belief network is given below.



```
Algorithm 2: Piecewise regressive Damped Convolutional deep belief network based QoS aware data transmission
Input: Number of devices $M_1, M_2, M_3, \ldots M_n$
Output: Improve QoS-aware data transmission
Begin
Step 1:  The number of devices $M_1, M_2, M_3, \ldots M_n$ are given to input unit
Step 2:  For each device 'M'
Step 3:      Measure signal strength $(Rss)$ in hidden unit
Step 4:      end for
Step 5:  Evaluate the signal strength using piecewise regression
Step 6:      if $(Rss > th)$ then
Step 7:          Device classified as strong signal strength
Step 8:  else
Step 9:      Device classified as weak signal strength
Step 10:     end if
Step 11: For each weak signal strength device
Step 12:     Compute the distance $d$
Step 13:         Apply the damped least square method function to find the minimum distance 'arg min $d$ '
Step 14:         Switch the weak signal strength device into the nearest base station
Step 15:     Obtain QoS-aware data transmission
  End
```

Piecewise regressive damped convolutional deep belief network based QoS-aware transmission algorithm is explained. First, the mobile devices are given to the input unit of the convolutional deep belief network. Signal strength estimates for each device at hidden unit. Then,piecewise regression is applied to find the strong and weak signal. Followed by, nearest base station is identified through the damped least square method from the available base station to perform the continuous data delivery with higher throughput and minimum latency.

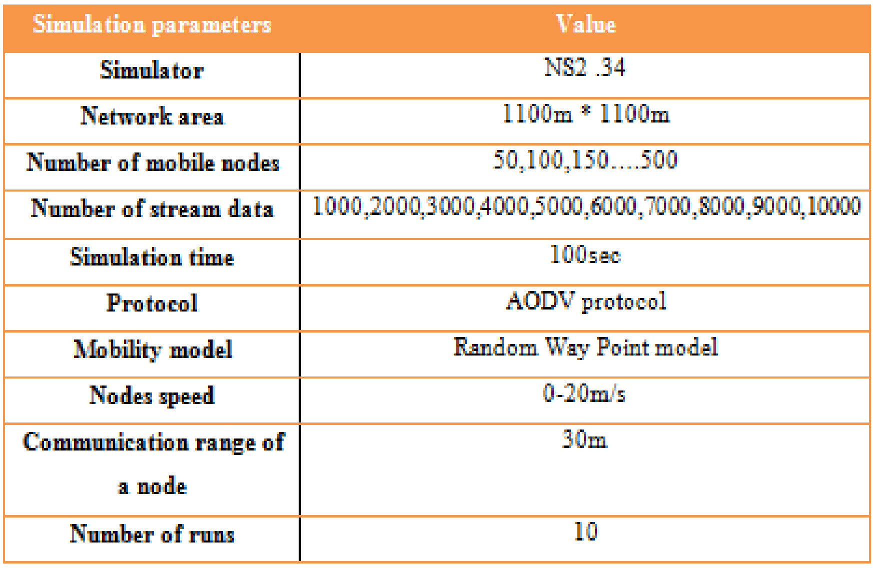
Case scenario 1: Reliance Jio has started for providing 5G services to mobile users with the latest communication technology. The Jio 5G technology provides seamless exposure, maximumin formation rate, minimum latency, as well as extremely trust worthy transportation scheme. Jio 5G network gives the highest impressive download speed (i.e. throughput) of 1085Mbps. The latency of Jio 5G networks is 11ms and 9ms jitter.

Simulation settings

Simulation assessment of three different methods namely proposed ERSSPDCDBN and existing security protocol [1], SeT-D2D [2] are implemented in the NS2 network simulator. For the simulation purposes, a totally of 50,100 …500 nodes or devices are considered in the square area A^2 (1100 m * 1100 m) for reliable and QoS-aware social media streaming data transmission n a 5G network by suing Web page phishing detection dataset [21]. The provided dataset includes 11430 URLs with 89 extracted features. The URLs links include different social media stream data includes, including facebook, youtube, Instagram, and tweet. The collected data is securely transmitted by avoiding phishing attacks.

Table I demonstrates the simulation metrics as follows.

Table I Simulation Parameters



Simulation parameters	Value
Simulator	NS2 .34
Network area	1100m * 1100m
Number of mobile nodes	50,100,150….500
Number of stream data	1000,2000,3000,4000,5000,6000,7000,8000,9000,10000
Simulation time	100sec
Protocol	AODV protocol
Mobility model	Random Way Point model
Nodes speed	0-20m/s
Communication range of a node	30m
Number of runs	10

Performance Results Analysis

In this section, the ERSSPDCDBN as well as conventionalsecurity protocol [1], SeT-D2D [2] approaches are discussed with authentication accuracy, loss rate, throughput, latency,data delivery rate, as well as jitter.

Authentication accuracy: the number of legitimate users and attackers are correctly identified for enhancing the security of stream data transmission with number of nodes. Therefore, the accuracy is estimated in percentage (%) and as given below,

$$\mathrm{AAcc} = \left\{\frac{\text{Numberof nodes or devices correctlyauthenticated}}{\mathrm{n}}\right\} * 100$$

(15)

Where AAcc denotes authentication accuracy, 'n' indicates the number of nodes or devices considered as input for experimentation.

Data delivery rate: The number of social data establishedwith receiver based on number of data sent from sender is computed as data delivery rate$\mathrm{DD}_{\mathrm{rate}}$. It is computed in percentage (%).

$$\mathrm{DD}_{\mathrm{rate}} = \left(\frac{\text{Number of social data received}}{\text{Number of social data sent}}\right) * 100 \quad (16)$$

Data loss rate: Theproportion of number of data lost because of weak signal strength is defined as data packet loss R. It is calculated in percentage (%).

$$\mathrm{DLR} = \left(\frac{\text{Number of social data lost}}{\text{Number of social data sent}}\right) * 100 \qquad (17)$$

Throughput: It is defined as the size of stream data delivered to the receiver in a given amount of time. Throughput is measured as follows,

$$\text{Throughput} = \left(\frac{\text{Amount of stream data delivered (Mb)}}{\text{time (sec)}}\right)$$

(18)

The throughput is estimated in terms of bits per second (Mbps).

Latency: The time considered to deliver the data is defined as latency from the sender to the receiver.

$$\mathrm{Lat} = \mathrm{n} * \text{time}\,[\mathrm{DD}] \qquad (19)$$

Where 'Lat' indicates latency, n indicates the number of stream data, and $\text{time}\,[\mathrm{DD}]$ denotes the time consumed in delivering the information. It measured in milliseconds (ms).

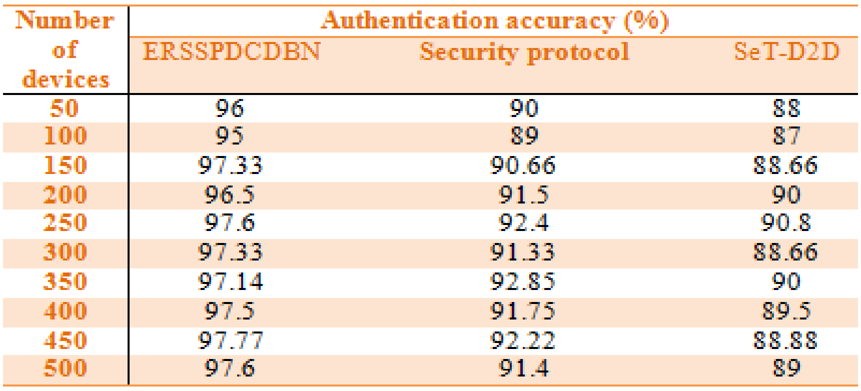
Jitter: Differenceduring time delay of data transmission with sender to receiver **is** defined as jitter as well as measuredwithin milliseconds (ms).

$$\mathrm{JT} = |\mathrm{de}(\mathrm{i}) - \mathrm{de}(\mathrm{i}-1)|$$

(15)

Where, jitter is specified as 'J',current delay is designated as $\mathrm{de}(\mathrm{i})$, earlier delay of packet transmission is denoted as $\mathrm{de}(\mathrm{i}-1)$.

Table II Authentication accuracy



Number of devices	Authentication accuracy (%)		
	ERSSPDCDBN	Security protocol	SeT-D2D
50	96	90	88
100	95	89	87
150	97.33	90.66	88.66
200	96.5	91.5	90
250	97.6	92.4	90.8
300	97.33	91.33	88.66
350	97.14	92.85	90
400	97.5	91.75	89.5
450	97.77	92.22	88.88
500	97.6	91.4	89

Table II provides the experimental results of authentication accuracy using three different methods namelyERSSPDCDBN and existing security protocol [1], SeT-D2D [2]. The authentication accuracy is measured with respect to the number of devices 50, 100, 150…500. As illustrated in Table II, the authentication accuracy is found to be higher using ERSSPDCDBN than the conventional methods.

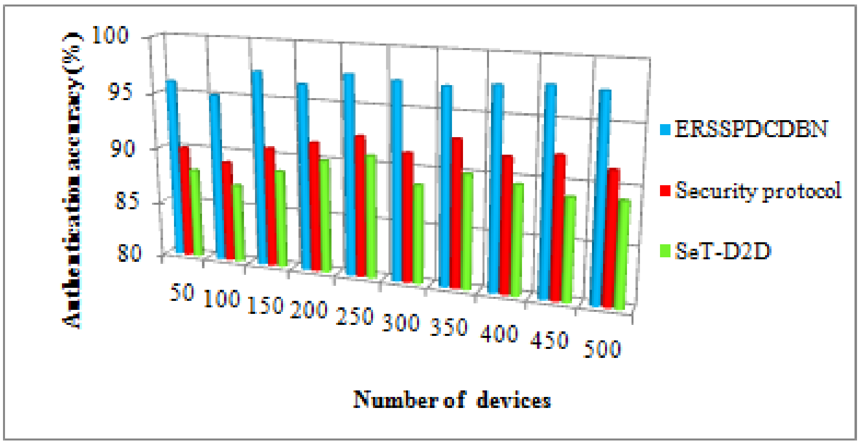


Figure 5 Performance results of authentication accuracy

Figure 5 given above reveals the graphical illustrations of authentication accuracy versus the number of mobile nodes or devices that are varied from 50 to 500 for conducting the simulation. As shown in the graphical results, the authentication accuracy of the ERSSPDCDBN gets increased when compared to all the other two existing methods. This is because of the applying an ephemeral resilient matching schnorrsigncryption technique. First, the streaming data are collected from the dataset. Then the signcryption techniques generate the pair of ephemeral resilient keys for each session of data transmission. Then the sender performs data encryption as well as signature generation based on a schnorr algorithm. In receiver, unsigncryption process is carried out signature verification and decryption. The receiver generates a new signature for that particular received data. The signature verification process is done through the simple matching coefficient (SMC). If the two signatures get matched, then the matching coefficient returns '1', and the receiver is said to be authorized and uniqueinformation is obtained. This helps to improve the reliability of data transmission interms of achieving higher security. The authentication accuracy of ERSSPDCDBN is improved by 6% and 9% when compared to the security protocol [1], SeT-D2D [2].

Table III comparison of Data delivery rate

Number of stream data	Data delivery rate (%)		
	ERSSPDCDBN	Security protocol	SeT-D2D
1000	97.5	93.6	91
2000	97	92.5	90
3000	97.33	93	91.33
4000	97.5	93.12	91.25
5000	96.4	92.4	90.4
6000	97.83	92	90.16
7000	97.28	93.02	91.57
8000	97.12	93.12	90.62
9000	96.88	92.5	90.02
10000	96.75	92.53	90.25

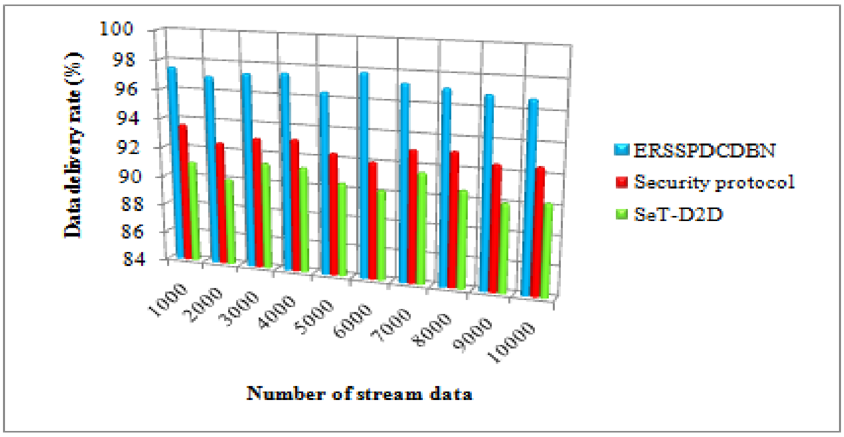


Figure 6 Performance results of Data delivery rate

The outcome of data deliverybased ondifferent streaming data in the range from 1000 to 10000 is displayed in Table III and figure 6. From this, ERSSPDCDBN provides improved performance than the existing methods of security protocol [1], SeT-D2D [2]. The significant reason for the improvement of data delivery using ERSSPDCDBN is to apply the piecewise regressive damped convolutional deep belief network. First, the mobile devices are given the input of a convolutional deep belief network. For each device, the signal strength is estimated and analyzed by applying the piecewise regression in the hidden unit. Based on piecewise regression results, the weak signal strength device is identified and it connects to the nearest base station for seamless data delivery from sender to receiver. The overall performance of ERSSPDCDBN is improved by 5% as well as 7% thanthe [1] [2].

Table IV comparison of data loss rate

Number of stream social data	Data loss rate (%)		
	ERSSPDCDBN	Security protocol	SeT-D2D
1000	2.5	6.4	9
2000	3	7.5	10
3000	2.66	7	8.66
4000	2.5	6.87	8.75
5000	3.6	7.6	9.6
6000	2.16	8	9.83
7000	2.71	6.97	8.42
8000	2.87	6.87	9.37
9000	3.11	7.5	9.97
10000	3.25	7.47	9.75

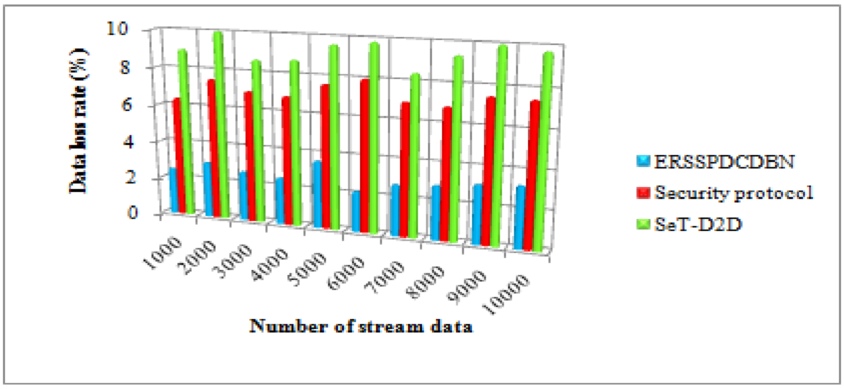


Figure 7 Performance results of Data loss rate

The outcomes of the data loss versus stream data transmission in the 5G network is illustrated in Table IV and figure 7. As shown in figure 7, the numbers of stream social data packets are taken in the horizontal direction 'x' axis and 'y' direction is observed the data loss outcome. The ERSSPDCDBN of data loss rate is considerably minimizedas compared to other existing security protocol [1], SeT-D2D [2]. The considerable reason is due to the applying thepiecewise regression to the deep neural network for finding the weak signal. Some amount of data may be lostbecause ofweak signal strength during the communication. In this case, the nearest base station is identified using the damped least square method, and the weak signal strength mobile device connected to that base stationcontinuously transmits the data to receiver and reduces the data loss. Overall performance outcomes of ERSSPDCDBN minimize data loss up to 60% as well as 70% than the [1] [2] respectively.

Table V comparison of throughput

Number of stream social data	Throughout (Mbps)		
	ERSSPDCDBN	Security protocol	SeT-D2D
1000	1012	965	895
2000	1033	975	930
3000	1042	998	950
4000	1055	1012	962
5000	1060	1020	1002
6000	1064	1032	1011
7000	1067	1037	1015
8000	1075	1043	1022
9000	1080	1047	1034
10000	1083	1049	1036

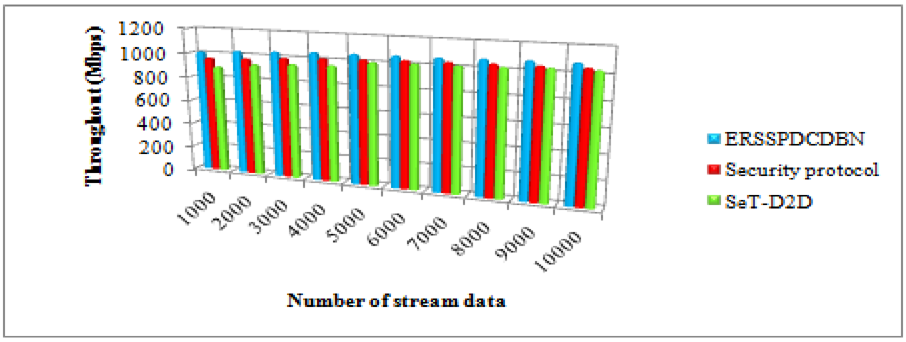


Figure 8 Performance results of throughput

Throughput outcome using ERSSPDCDBN and existing security protocol [1], SeT-D2D [2] is established in Table V and figure 8. As shown in figure 9, the throughput of all three methods gets increases while increasing the number of stream social data. ERSSPDCDBN is better than existing methods. This is proved using statistical estimation and the results are obtained based on Reliance Jio 5G network. By applying Reliance Jio 5G network, the downloading speeds of the 1085Mbps. Based on this, the simulation results of throughput are obtained. The reason for higher throughput is to implement data transmission in ERSSPDCDBN. The different results are obtained with various numbers of inputs. The performance of throughput of ERSSPDCDBN is increased by 4% and 7% when compared to security protocol [1], and SeT-D2D [2] respectively.

Table VI comparison of latency

Number of stream social data	latency (ms)		
	ERSSPDCDBN	Security protocol	SeT-D2D
1000	8.5	8.9	9.2
2000	8.9	9	9.45
3000	9.1	9.3	9.7
4000	9.55	9.7	10
5000	9.78	9.9	10.07
6000	9.86	10	10.15
7000	9.92	10.05	10.22
8000	10.05	10.22	10.32
9000	10.1	10.28	10.45
10000	10.13	10.33	10.58

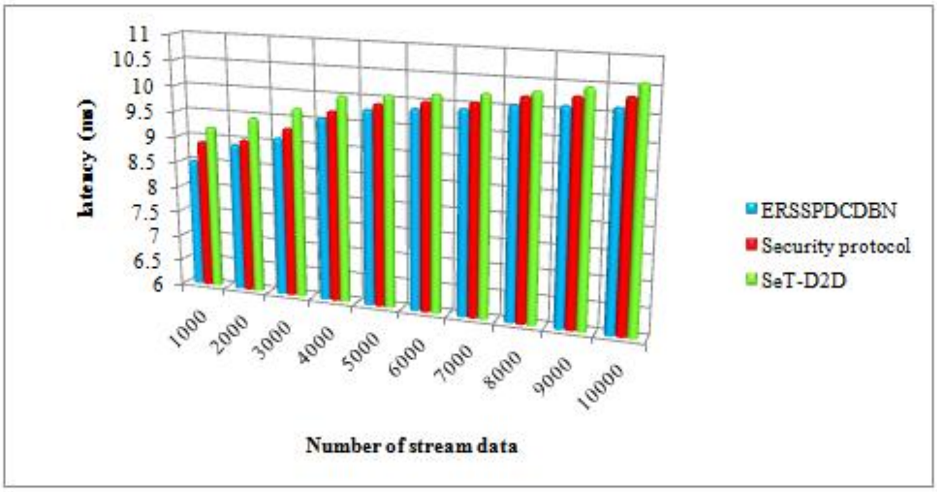


Figure 9 Performance results of latency

Table VI and figure 9 illustrate the simulation analysis of the latency of data transmission from sender to receiver. As revealed in figure 9, the latency of the three methods gets increases while increasing the number of stream social data. But comparatively, the ERSSPDCDBN technique consider lesser the latency than the other conventional approaches. This is proved using statistical estimation and the results are obtained based on Reliance Jio 5G network. By applying Reliance Jio 5G network, latency is 11ms. Based on this, the simulation analysis is obtained. In the first run, the simulation is conducted with 1000 stream social data, the latency of data delivery from sender to receiver using the proposed ERSSPDCDBN technique is 8.5ms where the latency of existing security protocol [1], SeT-D2D [2]are 8.9ms and 9.2msrespectively. The ERSSPDCDBN reduces latencyup to2% as well as 4% when compared to [1] [2] respectively. This significant improvement is attained by continuously connecting the mobile device to the base station.

Table VII comparison of jitter

Number of stream social data	Jitter (ms)		
	ERSSPDCDBN	Security protocol	SeT-D2D
1000	6.7	7.8	8.2
2000	7.4	7.95	8.27
3000	7.62	8.2	8.29
4000	7.85	8.25	8.38
5000	8.05	8.28	8.4
6000	8.12	8.33	8.42
7000	8.2	8.41	8.55
8000	8.24	8.52	8.6
9000	8.3	8.57	8.65
10000	**8.55**	8.68	8.77

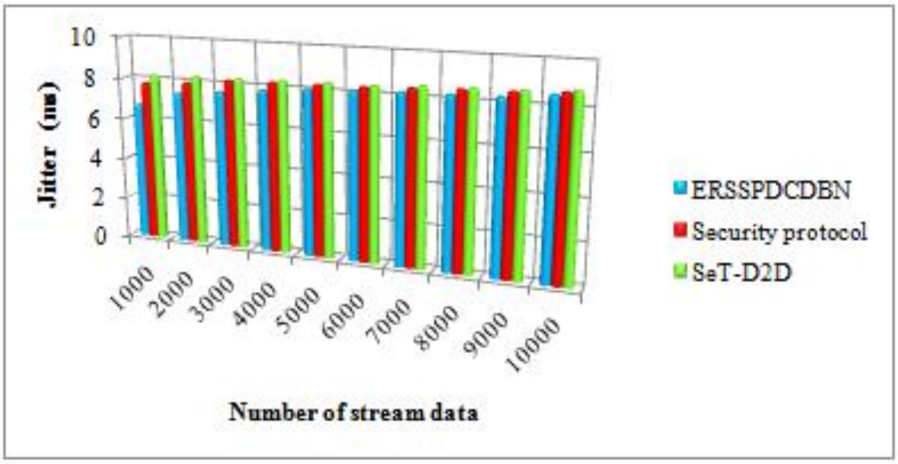


Figure 10 Performance results of Jitter

Table VII and figure 10 illustrate the performance results of jitter that obtains with respect todissimilar stream data. The obtained results indicate that the jitter of the ERSSPDCDBN lowest compared to baseline methods. As shown in above figure, for each iteration owing to the data being transmitted getting increased, then the jitter is increasedwith all three methods. '1000' data is taken to estimate experiments, performance of jitter is observed '6.7ms' using ERSSPDCDBN and 7.8ms' 8.2ms' jitter was found to be using security protocol [1], SeT-D2D [2]. TheERSSPDCDBNdecreases the jitter up to 5% as well as 7% than the conventional [1] [2] respectively.

CONCLUSION

ERSSPDCDBN is introduced in 5G Network to achieve two major contributions by applying an ephemeral resilient schnorrsigncryption and Piecewise regressive Damped Convolutional deep belief network. First, ephemeral resilient schnorrsigncryption is employed to improve the reliable stream by identifying attackers. During data transmission, the QoS is achieved through the Piecewise regressive Damped Convolutional deep belief network. The comprehensive simulation is conducted by authentication accuracy, throughput, as well as latency and jitter by varying the number of mobile devices and stream social data. ERSSPDCDBN technique improved than both reliable as well as QoS-aware streaming social data transmission over other existing schemes.

REFERENCES

1. R. Kishore, I. Ioannou, C. Christophorou, N. Prabagarane, V. Vassiliou, S. Vignesh, H. Vinayak, S. Venkatesh & A. Pitsillides, “A security protocol for D2D communications in 5G networks using elliptic curve cryptography”, International Journal of Information Security, Springer, 2022, Pages 1-13
2. C. Suraci, S. Pizzi, D. Garompolo, G. Araniti, A. Molinaro, A. Iera, “Trusted and secured D2D-aided communications in 5G networks”, Ad Hoc Networks, Elsevier, Volume 114 , 2021, Pages 1-15
3. Prabhakar Krishnan, Kurunandan Jain, Pramod George Jose, KrishnashreeAchuthan, Rajkumar Buyya, “SDN Enabled QoE and Security Framework for Multimedia Applications in 5G Networks”, ACM Transactions on Multimedia Computing, Communications, and Applications, Volume 17, Issue 2, 2021, Pages 1-29
4. Kusum Yadav, Anurag Jain, Yasser Alharbi, Ali Alferaidi, Lulwah M. Alkwai, Nada Mohamed Osman Sid Ahmed, Sawsan Ali Saad Hamad, “A secure data transmission and efficient data balancing approach for 5G-based IoT data using UUDIS-ECC and LSRHS-CNN algorithms”, IET communications, Wiley, Volume 16, Issue 5, 2022, Pages 571-583
5. Xiaoli Li and Jia Wu, “Node-Oriented Secure Data Transmission Algorithm Based on IoT System in Social Networks”, IEEE Communications Letters, Volume 24, Issue 12, 2020, and Pages 2898 – 2902
6. Sahil Garg,Kuljeet Kaur, Neeraj Kumar, Joel J. P. C. Rodrigues, “Hybrid Deep-Learning-Based Anomaly Detection Scheme for Suspicious Flow Detection in SDN: A Social Multimedia Perspective”, IEEE Transactions on Multimedia , Volume 21, Issue 3, 2019, Page(s): 566 - 578
7. Ruiling Zhang, Shijie Jia, Youzhong Ma, Changqiao Xu, “Social-Aware D2D Video Delivery Method Based on Mobility Similarity Measurement in 5G Ultra-Dense Network”, IEEE Access , Volume 8, 2020, Pages 52413 - 52427
8. YurongLuo , Hui Li, Ruhui Ma, and Zhenyang Guo, “A Composable Multifactor Identity Authentication and Authorization Scheme for 5G Services” , Security and Communication Networks, Hindawi, Volume 2021, April 2021, Pages 1-18
9. Kiran Deep Singh and Sandeep K. Sood, “QoS-Aware Optical Fog-Assisted Cyber-Physical System in the 5G Ready Heterogeneous Network”, Wireless Personal Communications, Springer, Volume 116, 2021, Pages3331–3350
10. Bhanu Priya &Jyoteesh Malhotra, “5GhNet: an intelligent QoE aware RAT selection framework for 5G-enabled healthcare network”, Journal of Ambient Intelligence and Humanized Computing, Springer, 2021, Pages 1-22
11. Farooque Hassan Kumbhar, Navrati Saxena & Abhishek Roy, “Social Reliable D2D Relay for Trustworthy Paradigm in 5G Wireless Networks”, Peer-to-Peer Networking and Applications, Springer, Volume 13, 2020, Pages 1526–1538
12. Xiaomin Wu, Liu Chang, Jingwen Luo, Jia Wu, “Efficient Edge Cache Collaboration Transmission Strategy of Opportunistic Social Network in Trusted Community”, IEEE Access (Volume 9, 2021, Pages 51772 – 51783
13. Francesca Cerruto, Stefano Cirillo, Domenico Desiato, Simone Michele Gambardella & Giuseppe Polese, “Social network data analysis to highlight privacy threats in sharing data”, Journal of Big Data, Springer, volume 9, 2022, Pages 1-26.
14. Yuelei Xiao and Yang Wu, “5G-IPAKA: An Improved Primary Authentication and Key Agreement Protocol for 5G Networks”, Information, Volume 13, 2022, Pages 1-17
15. Zhengyi Shang, Maode Ma, Xiaohong Li, “A Secure Group-Oriented Device-to-Device Authentication Protocol for 5G Wireless Networks”, IEEE Transactions on Wireless Communications, Volume 19, Issue 11, 2020, Pages 7021 – 7032
16. Xinran Ba, “QoS-Forecasting-Based Intelligent Flow-Control Scheme for Multi-Connectivity in 5G Heterogeneous Networks”, IEEE Access, Volume 9, 2021, Pages 104304 – 104315
17. Man Chun Chow and Maode Ma, “A Secure Blockchain-Based Authentication and Key Agreement Scheme for 3GPP 5G Networks”, Sensors, Volume 22, 2022, Pages 1-26

18. Nguyen-Son Vo, Thanh-Minh Phan, Minh-Phung Bui, Xuan-Kien Dang, Nguyen Trung Viet; Cheng Yin, “Social-Aware Spectrum Sharing and Caching Helper Selection Strategy Optimized Multicast Video Streaming in Dense D2D 5G Networks”, IEEE Systems Journal, Volume 15, Issue 3, 2021, Pages 3480 – 3491
19. Zhixue Wan, “Reliability Analysis of Social Network Data Transmission in Wireless Sensor Network Topology”, Journal of Sensors, Hindawi, Volume 2022, January 2022, Pages 1-10
20. Liangtian Wan, Feng Xia, Xiangjie Kong, Ching-Hsien Hsu, Runhe Huang, Jianhua Ma , “Deep Matrix Factorization for Trust-Aware Recommendation in Social Networks”, IEEE Transactions on Network Science and Engineering , Volume 8, Issue 1, 2021, Pages 511 – 528
21. Web page publishing detection dataset: https://www.kaggle.com/datasets/shashwatwork/web-page-phishing-detection-dataset