Data Analytics and Artificial Intelligence
Vol: 2(5), 2022
REST Publisher; ISBN: 978-81-948459-4-2
Website: http://restpublisher.com/book-series/data-analytics-and-artificial-intelligence/

Deep Neural Certificate less Hessian Heap Signcryption for Secure Data Transmission in Wireless Network

***N. Shoba, V.Sathya**,
MGR, college, Hosur, Tamil Nadu, India
*Corresponding author Email: shobatiwari@gmail.com

Abstract: Systematic and well-grounded data transmission over wireless networks has been the substance of uninterrupted research over the last few years. The paramount is scrutinizing the amount of security provisioning owing to the security challenges during transmission over wireless networks. It is moderate to eavesdrop and alter data packets. Accessing the personal computer and public network possess the potential to apprehend the network traffic possibly compromising privacy. Therefore for wireless applications, it is essential to ensure data integrity during data transmission. To efficiently address the above issues, a Deep Neural Certificateless Hessian Curve Heap Signcryption (DNC-HCHS) method for secured data transmission in the wireless network is proposed. Compared with the conventional, Certificateless Signcryption DNC-HCHS method improves the data confidentiality and data integrity by generating smaller keys employing the Hessian Curve Heap function. Additionally, with the assistance of the access point or the aggregator, the sensitivity of heaped signcrypted ciphertext can improve the security of data transmission and reduce the message delivery time. Aimed at reducing the delay in data transmission, the application of Certificateless Hessian Curve Heap Signcryption in Deep Learning (i.e., Deep Neural Network) performs the overall process in a swift manner and performs much better encryption. Simulation is performed to validate the viability and efficiency of the proposed method. The results show that the data confidentiality and data integrity rate are strongly improved, while the delay is minimized.
Keywords**:** Wireless Network, Certificateless Signcryption, Hessian Curve, Deep Learning, Deep Neural, Heap

1. Introduction

Wireless network, specifically the fifth-generation (5G) network has fascinated paramount awareness in twain industry and academia in the recent few years. In order to ensure the data transmission security in network communication, a cryptosystem has to be deployed in the 5G network, hence proposing a secure heterogeneous mechanism for data transmission between different 5G network users is mandatory. In [1], a security model of heterogeneous signcryption with different system parameters (DSPHS) between certificateless cryptography (CLC) and public key infrastructure (PKI), called, PCDSPHS and CPDSPHS was proposed. The method using the Discrete Logarithm Problem (DLP) and Decisional Diffie-Hellman Problem (DDHP) ensured data transmission security. Also with these two CLC and PKI, less computation cost with minimum energy consumption was ensured. Despite improvement observed in terms of computation cost and energy consumption, the data confidentiality and data integrity involved in the data transmission was not focused. To address this issue in our work, Hessian Curve Heap function is employed during the signcrytion process by using the transformation to improve the data confidentiality and integrity in a significant manner. A secure certificateless multi-recipient signcryption scheme was proposed in [2] for addressing the issues related to security via remote downlink control commands in a multicast fashion. With the certificateless signcryption, not only confidentiality was ensured but also provided integrity with unforgeability, doesn't leak the receiving commands hence ensuring the smart meter identity. As a result, the calculation time of both was minimized with improvement observed in computational efficiency. Despite improvement found in the computational efficiency, the message delivery time and delay involved in the certificateless signcryption process were not focused. To address this issue, the aggregator or the access point obtains the heaped signcrypted ciphertext that in turn results in the improvement of the message delivery with minimum delay. In the existing literature, the important issues are shown as given below. A huge number of nodes was employed for data transmission. Due to the dissimilar types of attacks, security is a challenging task. Several existing security techniques are utilized to ensure effective communication. The data confidentiality was not focused on the conventional method. Hence, data confidentiality and data integrity need to ensure secure data transmission. The traditional method failed to perform signcryption mechanism. Motivated by the above facts, Deep Neural Certificateless Hessian Curve Heap Signcryption (DNC-HCHS) method for secured data transmission in the wireless network is designed. The designed method was to consider different processes such as partial key generation, actual key generation, and signcryption and focus the data confidentiality and integrity. In particular, the key contributions in this work are listed as follows: The proposed Deep Neural Certificateless Hessian Curve Heap Signcryption (DNC-HCHS) method is developed to improve secure data transmission. The designed method takes the source node, destination node, data packets, and their respective sizes for transmission in a heaped manner ensuring data confidentiality and data integrity. Certificateless Hessian Curve Heap Signcryption is used in the proposed DNC-HCHS method to guarantee secure data transmission in a wireless network with lesser delay and delivery time. The proposed DNC-HCHS method performs the partial key generation, actual key generation, and signcryption. The signcryption function is carried out with the innovation of the Hessian Curve Heap function for enhancing the ensure data confidentiality and data integrity. Finally, four experiments were conducted to measure the performance analysis of the

Copyright@ 2022 REST Publisher

proposed DNC-HCHS method along with conventional methods based on various performance metrics. The results show that the data transmission in wireless network performance is good with minimum delay and message delivery time, also increasing the data confidentiality and data integrity. The remainder of this paper is organized as follows. Section 2 reviews the literature. Section 3 introduces the network system model and presents the proposed Deep Neural Certificateless Hessian Curve Heap Signcryption (DNC-HCHS) method for secured data transmission in the wireless network. Section 4 provides an experimental setup and Section 5 discusses the performance evaluation through extensive simulations. Finally, Section 6 draws a conclusion

2. Related works

Information security has become the topic of research owing to the different types of cyberattacks. To be more specific, with the communication technologies in existence, security for information to be transmitted has risen. A thorough and measurable exploration of secure data transmission attained by employing one-time pad (OTP) and wireless channel in an arbitrary manner was proposed in [3]. Here, two OTP secure transmission mechanisms, an identical key and an un-identical key were designed to ensure secret transmission. However, with the increasing demand for the digital world and the inception of 5G wireless networks, authentication and key agreement model that integrates the benefits of certificateless public key cryptography (CL-PKC) and elliptic curve cryptography (ECC), to ensure secure and device to device group communications in 5G cellular networks was investigated in [4]. A thorough study on security and privacy for 5G was investigated in [5].

As far as future communication systems are concerned, the heterogeneous network has become the development trend owing to the different types of services provided by it. In such a network, authentication remains the major concern that bestows identity authentication and hence fascinated large attention from numerous research persons. With the objective of mitigating the security concerns in Long Term Evolution-Wireless Local Area Network (LTE-WLAN), an enhanced mechanism based on hybrid cryptosystem was proposed in [6]. This hybrid cryptosystem not only ensured access authentication but also ensured identity privacy protection. Yet another certificateless signcryption method resisting different types of attacks was presented in [7] to ensure security and efficiency. For flying ad hoc networks, security concerns were addressed by employing certificate less key encapsulated signcryption model in [8]. In Secure multicast mechanism, the sender sends same message to multiple receivers in a secure and simultaneous manner, therefore ensuring an effective communication mechanism. However, in practicality still some problem persists. In a novel anonymous certificate less multi-receiver signcryption mechanism [9],the key generation center employed public channel to send pseudo partial private key and also the intended recipient also worked out on the actual partial private key to ensure even in case of multi receiver model. However, the computation and communication cost involved in the signcryption mechanism was found to be higher. To address this issue, an Elliptic Curve Disrete Logarithm was proposed in [10] to ensure secure data transmission. Yet another method for online and offline phases was designed in a distinct manner in [11] and hence was found to be highly susceptible to different attacks. With the swift development of technology, healthcare systems have been rapidly metamorphosed into a pervasive surrounding, where one and the other ultimatums and opportunities prevails. A light weight and robust secure aware device to device data transmission using certificate less generalized signcryption were proposed in [12] with the objective of reducing both the computational and communication overhead. Security in the presence of different types of attacks, using Long Short Term Memory, to enhance model stability was designed in [13]. Yet another privacy preservation authentication mechanism for secure smart health was proposed in [14] using aggregate signature. As far as wireless networks are concerned, secure authentication plays a vital role in ensuring secured communication. However, owing to the restriction in resource and the nature, globally networks are found to be highly vulnerable to different types of attacks. In [15], authentication mechanism was designed to identify the susceptibility based on the man-in-the-middle attack, Denial-of-Service (DoS) attack. Also, robust authentication mechanism was designed to ensure security while roaming in networks. A review of literature on security mechanism based on routing was investigated in [16]. In addition to the cryptographic mechanisms that are utilized in upper layers, security in physical layer has also found a major place to improve information security. In [17], security analysis for two-way relay network via intermediate relay nodes was proposed to guarantee reliable and secure communication between nodes in the network. A survey of deep learning mechanisms for secure data transmission in wireless network was investigated in [18]. The increasing network density and unexpected growth in network traffic due to large numbers of devices in the network and online services that arise a requirement of intelligent network operations. In this regard, a review of Machine Learning (ML) techniques was designed in [19] for ensuring secured data transmission. A review of data security and privacy concerns to mitigate targeted attacks was presented in [20]. Thread model: The dissimilar security attacks are considered, by using Privacy-preserving mutual authentication and key agreement protocol in [21] for handling the privacy and security problem. A systematical evaluation framework was developed in [22] for providing security, efficiency, and scalability. An efficient smart-card-based password authentication scheme was developed in [23] for achieving security. However, it failed to estimate data confidentiality. Security is an important factor in the WSNs. In data transmission, special security threats are arising in WSNs. The security mechanisms were utilized in a sensor network that is generally considered an attacker. Attackers were to compromise a node or even physically capture a node. The majority of WSN nodes are monitored owing to the high cost of sensor nodes. The attacker was proficient in stealing the key materials contained within the compromised node. Recently, wireless network networks and embedded devices have significantly improved, which unhappily presents novel dissimilar threats associated with security and privacy. But, the data confidentiality and data integrity metrics were not considered in the data transmission. In addition, the certificateless signcryption process was not performed and failed to reduce the message delivery time and delay. In order to overcome issue, the novel deep learning is to handle the security threats in WSN.

3. Methodology

With the increased use of the internet and the large number of nodes involved in data transmission over the wireless network, security has received great attention. Also owing to the reason that better scalability and lower maintenance cost, several users are doing data transmission over the wireless network. In recent years, there has been an outpouring of endeavors to apply deep learning to security. In this work, a new Deep Neural Certificateless Hessian Curve Heap Signcryption (DNC-HCHS) methods proposed by combining CL-AS with HC in the deep learning process. The Heap Signcryption performed here ensures the confidentiality and authentication of data transmission. Moreover, different verifications of collected signatures are rationalized to only one authentication in it. Also, it has the eminence of dispensing shorter key size and outrageous processing speed upon comparison with the state-of-the-art methods retaining the security aspects. Figure 1 shows the block diagram of the DNC-HCHS method.

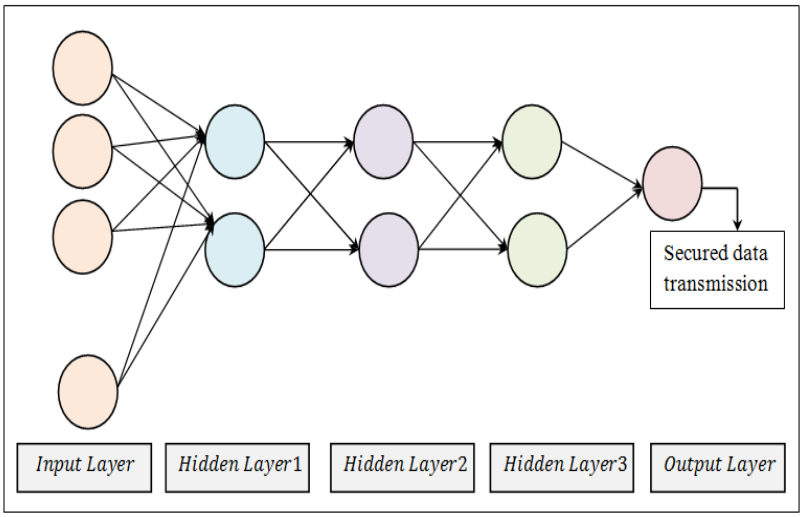

FIGURE 1. Block diagram of DNC-HCHS method

From the above figure, the Sender Node 'SID' and Receiver Node 'RID', Data Packet 'DP', Data Packet Size 'DP_{size}' are provided as input in the input layer to generate the certificateless signcryption setup. Next, three hidden layers are present. In the first hidden layer, partial key generation is performed whereas, in the second hidden layer, the actual key generation is performed. Finally, in the third hidden layer, the Heap Signcryption employing the Hessian Curve is formulated. Last, in the output layer, the actual data transmission between authenticated and validated sender-receiver nodes is performed in a secured manner. The proposed network model is elaborated in the following sections. Proposed Network model provably secure three-factor AKA protocol was introduced in [24] for mobile lightweight devices. The generic model was applied for constructing the AKA protocol to enhance security. An efficient privacy-preserving user authentication scheme was designed in [25] for providing security. The symmetric cryptographic algorithms were applied to reduce the computation cost. But, the communication cost was higher by using asymmetric cryptographic algorithm. Secure and efficient smart-card-based password authentication system called Quantum2FA was introduced in [26]. However, the security and efficiency were not improved. In order to overcome the issue, in this section, the proposed Deep Neural Certificateless Hessian Curve Heap Signcryption (DNC-HCHS) method is provided to increase the security and efficiency. Figure 2 given below shows proposed DNC-HCHS network model.

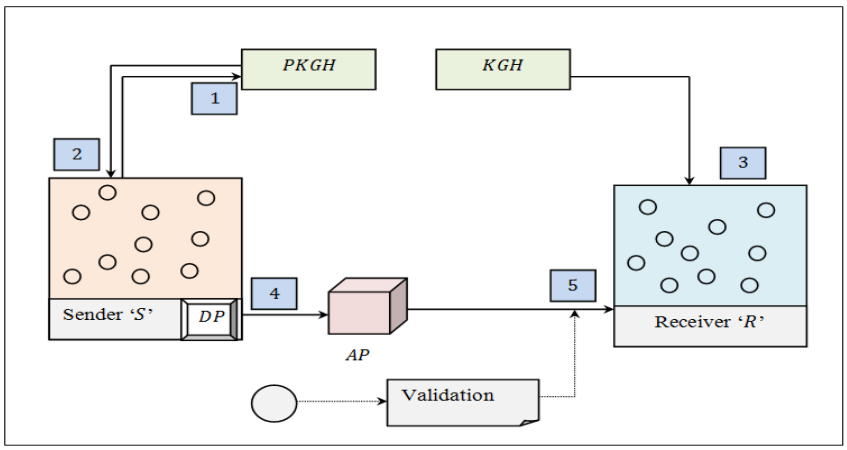

FIGURE 2. DNC-HCHS network model

As shown in the above figure, the network model consists of five entities, the Key Generation Hub 'KGH', Private Key Generation Hub '$PKGH$', Sender Node 'S', Receiver Node 'R' and the Access Point 'AP'. The Sender Node 'S' needs to be authorized by the Private Key Generation Hub '$PKGH$'. The Private Key Generation Hub '$PKGH$' generates a private key for the Sender Node 'S' and the Key Generation Hub 'KGH' generates partial private keys for Receiver Node 'R'. Then, the 'S' signcrypts the Data Packets 'DP' and transmits the signcryption ciphertext to the Access Point 'AP'. The 'AP' quantifies the signcryption authentication parameter, and transmits it with ciphertext to 'R'. Only the designated receivers precisely validate the parameter and signature, and then decrypt the respective signcryption ciphertext. In this way, the used network model provides significant and secure data transmitted between users or nodes in wireless networks. Deep Neural Certificateless Hessian Curve Heap Signcryption (DNC-HCHS) for Secure Data Transmission in Wireless Network Given a security parameter 'SP', the Key Generation Hub 'KGH' selects cyclic group 'CG' of an arbitrary prime order 'p', a generator 'G' of 'CG', a Hessian Curve 'HC' and ternary security hash functions as given below.

- $H_1: \{0,1\} * CG \rightarrow Z_p$ (1)
- $H_2: \{0,1\} \rightarrow Z_p$ (2)
- $H_3: Z_p \rightarrow \{0,1\}^{DP+ DP_{Size}}$ (3)

From the above equations (1), (2), and (3), the three hash functions 'H_1', 'H_2' and 'H_3' are modeled based on the cyclic group 'CG', arbitrary prime order 'p', number of data packets 'DP', and the data packet size 'DP_{Size}' respectively. Then, the Key Generation Hub 'KGH' selects the master key '$MK \in Z_p$' in an arbitrary fashion along with the public key '$PubK = MKG$'. Finally, the Key Generation Hub 'KGH' disperses the system parameters to each sender node with the respective identification 'SID' for secure data transmission in a wireless network as given below.

- $Params = (CG, p, PubK, H_1, H_2, H_3)$ (4)

Next, with the obtained parameters '$Params$' as in the above equation (4), the partial key generation is performed in the first hidden layer. When nodes in the wireless network want to register the identity 'ID_i' to the Key Generation Hub 'KGH' the nodes in the wireless network sends 'ID_i' to the Key Generation Hub 'KGH'. Then, the Key Generation Hub 'KGH' selects arbitrary number '$AN \in Z_p$' computes the partial private key '$PPrivK_i$' and partial public key '$PPubK_i$' as given below.

- $PPubK_i = AN_i G$ (5)
- $PPrivK_i = AN_i + MKH_i(ID_i, PPubK_i)$ (6)

Finally, for each sender node in the wireless network, the Key Generation Hub 'KGH', sends the partial public key '$PPubK_i$', as in equation (5) and partial private key '$PPrivK_i$' as in equation (6) over a private and legitimate channel. Upon reception of the partial key (i.e., the partial public key and partial private key) by the intended sender node as generated by the Key Generation Hub 'KGH', the intended sender node selects the remaining portion of the key and therefore acquires the full key. This is performed in the second hidden layer. For this purpose, the intended sender node obtains a secret value '$a_i \in Z_q$' in an arbitrary manner and obtains the private key and public key is given below.

- $A_i = a_i G$ (7)
- $PrivK_i = (PPrivK_i, a_i)$ (8)
- $PubK_i = (AN_i, A_i)$ (9)

From the above equations (8) and (9), the private key '$PrivK_i$' and public key '$PubK_i$' are generated fully by the intended sender node for secure data transmission over the wireless network. In the third hidden layer, with the partial key and key generated, signcryption function is performed by means of Hessian Curve Heap function. The objective behind the employing of Hessian Curve Heap function is that smaller keys are generated in this curve requiring less memory and time. The Hessian Curve is first formulated as given below.

- $HC = P^3 + Q^3 + 1 = 0.3PQ$ (10)

Then, given three points, 'P^3', 'Q^3' and '1' in Hessian Curve 'HC' the proposed Deep Neural Certificateless Hessian Curve Heap Signcryption (DNC-HCHS) problem is to determine whether '$HC = 0.3PQ$', the output '$Out_{\mathrm{DNCHC-AS}} = 1$' if the data transmission lies within the interval (i.e., within the network) and the output '$Out_{\mathrm{DNCHC-AS}} = 0$', if the data transmission lies outside the interval (i.e., outside the network). Then within the Hessian Curve, the Heap Signcryption for 'n' nodes or users is mathematically formulated as given below.

- $ASCT = \sum_{i=1}^{n} (DP, SID_i[PubK_i, PrivK_i], RID_i[PubK_i])$ (11)

From the above equation (11), the heap signcryption text '$ASCT$', is modeled based on the data packets to be sent, 'DP', the sender public key '$SID_i(PubK_i)$', private key '$SID_i(PrivK_i)$' and the receivers public key '$RID_i[PubK_i]$' respectively. The aggregator or the access point 'AP' obtains '$SID = \sum_{i=1}^{n} SID_i$' and therefore outputs heap signcrypted ciphertext. By employing this heaped signcrypted ciphertext, not only the delay is reduced but also resulting in the improvement of the message delivery time in a significant manner. Finally, given a heap set of 'SID_i' users or 'n' sender nodes, while performing unsigncryption, the sender public key '$SID_i(PubK_i)$' and private key, the public key of receiver '$RID_i(PubK_i, PrivK_i)$', validation is performed at the access point 'AP'. Upon successful validation, returns '1' for data transmission and returns '0' for no transmission. The pseudo code representation of Deep Neural Certificateless Hessian Curve Heap Signcryption is given below.

Input: Sender Node '$\boldsymbol{SID = SID_1, SID_2, \dots, SID_n}$', Receiver Node '$\boldsymbol{RID = RID_1, RID_2, \dots, RID_n}$', Data Packets '$\boldsymbol{DP = DP_1, DP_2, \dots, DP_n}$',
Output: Robust and secure data transmission
1: Initialize data packet size '$\boldsymbol{DP_{Size}}$' arbitrary number '$\boldsymbol{AN}$', secret value '$\boldsymbol{a_i}$'
2: Begin
//Setup
3: Formulate ternary security hash functions as in equations (1), (2) and (3)
4: Generate system parameters as in equation (4)
//Partial Key Generation
5: Formulate partial public key as in equation (5)
6: Formulate partial private key as in equation (6)
//Key generation
7: Formulate private key as in equation (7)
8: Formulate public key as in equation (8)
//Signcryption
9: Formulate Hessian Curve as in equation (9)
10: Obtain Heap Signcryption Text as in equation (10)
11: Perform Heap Signcryption for '$\boldsymbol{n}$' nodes as in equation (11)
//Unsigncryption
12: If '$\boldsymbol{S1ID_i(PubK_i) = RID_i(PubK_i, PrivK_i)}$'
13: Then validation successful
14: Perform secure data transmission
15: End if
16: If '$\boldsymbol{SID_i(PubK_i) \neq RID_i(PubK_i, PrivK_i)}$'
17: Then validation not successful
18: No data transmission
19: End if
20: End

Algorithm 1 Deep Neural Certificateless Hessian Curve Heap Signcryption As given in the above Deep Neural Certificateless Hessian Curve Heap Signcryption algorithm, the deep neural learning process involves three types of layers. They are one input layer, three hidden layers and one output layer. The actual Certificateless Hessian Curve Heap Signcryption for secured data transmission in the wireless network is performed by employing deep neural learning. The sender node ID, receiver node ID, data packets to be send, and the respective size of data packets are provided as input in the input layer. Followed by three different processes, i.e., partial key generation, actual key generation, and signcryption are performed in the three hidden layers. The novelty of this algorithm remains in performing heap signcryption employing hessian curve function for secured data transmission in wireless network. By applying heap signcryption, delay in data transmission is reduced and ensures message delivery time. Also with the deployment of hessian curve function, both data confidentiality and data integrity are ensured.

4. Experimental setup

Simulation of the Deep Neural Certificateless Hessian Curve Heap Signcryption (DNC-HCHS) method for secured data transmission in wireless network state-of-the-art data transmission methods, PCDSPHS and CPDSPHS [1], certificateless multi-recipient signcryption scheme [2] are implemented using the NS2.34 network simulator. In order to conduct the simulation, 500 nodes are deployed in a squared area '$(1200\,m * 1200\,m)$' in wireless network. To improve the data transmission, a Random Waypoint model is used as a mobility model. Nodes in the wireless network are moved with a speed of 0 to 35m/sec with a total simulation time of 250 sec. Table 1 given below lists the stimulation parameter settings.

TABLE 1 Simulation parameters settings

Simulation parameters	Values
Network Simulator	NS2.34
Simulation area	1200 m * 1200 m
Number of nodes	50,100,150,200,250,300,350,400,450,500
Number of data packets	80,160,240,320,400,480,560,640,720,800
Mobility model	Random Waypoint model
Speed of sensor nodes	0 – 35m/s
Simulation time	250sec
Routing Protocol	DSR
Number of runs	10

5. Discussion

The performance analysis of the DNC-HCHS method are compared with the existing PCDSPHS and CPDSPHS [1], certificateless multi-recipient signcryption scheme [2] in terms of data confidentiality, data integrity, message delivery time and delay. Performance analysis of data confidentiality A Framework for Comparative Evaluation of Web Authentication Schemes was introduced in [27] to provide security benefits. The designed method comprises password organization software, graphical password systems, cognitive authentication schemes, one time passwords, phone-aided methods and biometrics. In [23], the efficient smart-card-based password authentication scheme to obtain security. But, data confidentiality was not considered. In order to overcome the issue, DNC-HCHS method is introduced. Data confidentiality is important factor to ensure the secure data transmission. Data confidentiality refers to the confidentiality rate with which the data packets are received at the intended recipient. In other words, it is measured as the ratio of number of data packet being protected from unauthorized user to total number of data packets. It is formulated as given below.

$$DC = \frac{DP_{prot}}{DP} * 100 \qquad (12)$$

From the above equation (12), data confidentiality 'DC' is measured based on the data packet protected 'DP_{prot}' and the overall data packets 'DP' involved in the simulation process. It is measured in terms of percentage (%).Table 2 shows the data confidentiality of the proposed method DNC-HCHS when compared with the existing methods [1] and [2]. It is clear from the table that DNC-HCHS is a unique solution that utilizes the certificateless signcryption via deep learning in correlation with the wireless network for secure data transmission.

TABLE 2. Tabulation for data confidentiality

Data packets	Data confidentiality		
	DNC-HCHS	PCDSPHS and CPDSPHS	certificateless multi-recipient signcryption
80	92.55	88.75	87.55
160	92	87.25	85.25
240	91.85	86	84
320	91.35	85.45	83.15
400	91	85	81
480	91	83.15	79.55
560	90.55	82	76.25
640	90	80.35	74
720	88.25	78.55	73.15
800	88	75	72

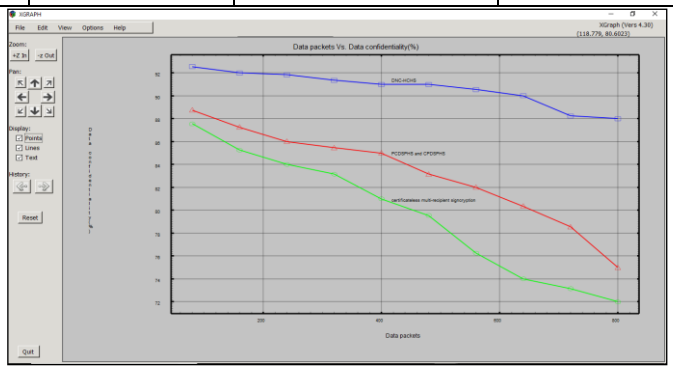

FIGURE 3 Graphical representation of data confidentiality

Figure 3 given above illustrates the data confidentiality rate with respect to data packets involved in the simulation for secure data transmission in the range of 50 to 500 collected at different time instances. From the figure, it is inferred that the data confidentiality is inversely proportional to the data packets involved in the simulation. In other words, increasing the data packets causes an increase in the congestion in the network traffic and obviously a small portion of data packet is compromised while performing data transmission. Therefore, the data confidentiality is found to be in the decreasing trend using all the three methods with the increase in the data packets. However, with simulations conducted using 80 data packets, 74 data packets were protected using DNC-HCHS, 71 data packets were protected using [1] and 70 data packets were protected using [2]. From the results, the overall data confidentiality using the three methods was observed to be 92.5%, 88.75% and 87.55% respectively. From this result it is inferred that the data confidentiality using DNC-HCHS was observed to be better than [1] and [2]. The reason behind the improvement was due to the application of Hessian Curve Heap function while performing signcryption process that in turn protected the data packet to be sent to the intended recipient. Owing to this reason, the data confidentiality using DNC-HCHS method was observed to be better than 9% compared to [1] and 14% compared to [2]. Performance analysis of data integrity the second parameter of significance for secured data transmission in wireless network is the data integrity rate. In other words, data integrity refers to the number of data packets that are not altered by unauthorized users to the total number of data packets involved in the simulation process. It is measured as given below.

$$DI = \frac{DP_{NA}}{DP} * 100 \left[\frac{Numberofdata\ not\ altered\ by\ \text{unauthorized user}}{Totalnumberofdata}\right] * 100 \quad (13)$$

From the above equation (13), the data integrity 'DI' refers to the data packets not altered 'DP_{NA}' to the data packets involved in the simulation process 'DP'. It is measured in terms of percentage (%).Table 3 shows the comparison between data integrity rates using three different methods, DNC-HCHS, PCDSPHS and CPDSPHS [1], certificateless multi-recipient signcryption scheme [2] respectively.

TABLE 3. Tabulation for data integrity

Data packets	Data integrity		
	DNC-HCHS	PCDSPHS and CPDSPHS	certificateless multi-recipient signcryption
80	96.25	91.25	88.75
160	95.15	90.35	87.15
240	94.35	89.15	86.15
320	93.25	88.35	85
400	92.15	87.25	84.15
480	92	86.35	82
560	91.55	85.15	81.55
640	90.35	84.15	80
720	89.15	83.35	78.55
800	88	82	76

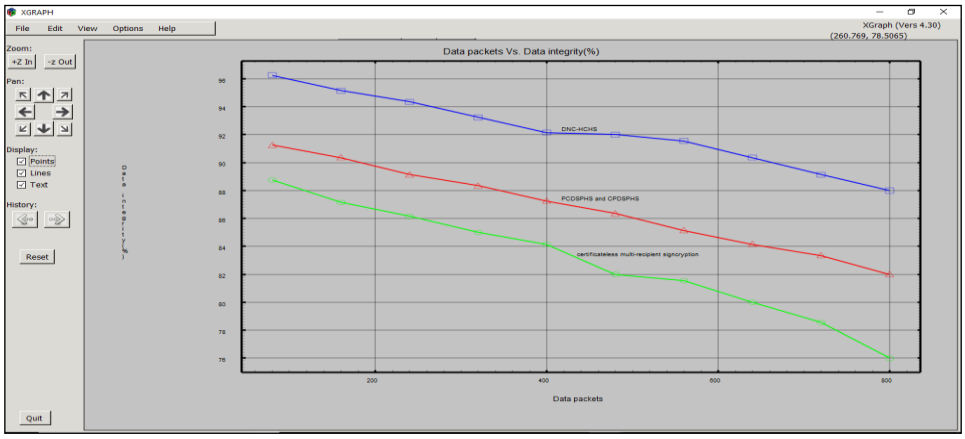

FIGURE 4. Graphical representation of data integrity

Figure 4 shows the performance analysis of data integrity. In the above figure, the horizontal axis refers to the data packets ranging from 50 to 500 and the vertical axis denotes the data integrity rate obtained at different time instances. Also from the above figure, the data integrity rate is found to be inversely proportional to the data packets. In other words, increasing the number of data packets causes an increase in the number of source and destination node involved in the secure data transmission in wireless network. This in turn increases the data to be altered by unauthorized user. However, with simulations conducted using 80 data packets 77 data packets were altered by unauthorized user, 73 data packets were altered by unauthorized user using [1] and 71 data packets were altered using [2]. As a result, the data integrity using the three methods, NC-HCHS, PCDSPHS and CPDSPHS [1], certificateless multi-recipient signcryption scheme [2] was observed to be 96.25%, 91.25% and

88.75% respectively. With this result, the data integrity using DNC-HCHS was found to be comparatively better than [1] and [2]. The reason behind the improvement was Hessian Curve Heap function in the deep learning process owing to the reason that the arithmetic operations involved during heap is faster and also requires less memory operation that standard than Hessian Curve Heap function of an Elliptic curve. This in turn minimizes the data packet alteration using DNC-HCHS, therefore improving the data integrity rate by 6% compared to [1] and 11% compared to [2] respectively. Performance analysis of message delivery time the message delivery time is defined as the time consumed in delivery of the data packets or message. It is mathematically formulated as given below.

$$MD_{time} = \sum_{i=1}^{n} DP_i * Time\ [MD] \quad (14)$$

From the above equation (14), the message delivery time 'MD_{time}' is measured based on the data packets involved in the simulation process 'DP_i' and the time consumed in delivery of the corresponding messages '$Time\ [MD]$' to the intended recipients. It is measured in terms of milliseconds (ms).Table 4 shows the comparison between delivery time using three different methods, DNC-HCHS, [1] and [2].

TABLE 4. Tabulation for message delivery time

Data packets	Message delivery time (ms)		
	DNC-HCHS	PCDSPHS and CPDSPHS	certificateless multi-recipient signcryption
80	12.4	15.2	19.6
160	16.35	21.45	30.15
240	21.55	30.35	45.35
320	35.35	41.55	60.35
400	45.55	53.25	81.35
480	53.25	75.35	105.45
560	70.15	85.25	125.35
640	85.25	110.25	140.15
720	105.45	145.55	173.25
800	125.35	152.35	190.45

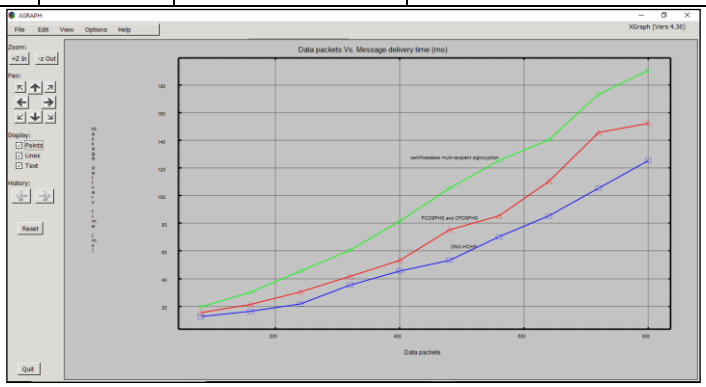

FIGURE 5. Graphical representation of message delivery time

Figure 5 given above shows the message delivery time involved in the secure data transmission process in wireless network. The x axis in the above figure represents the data packets involved in the simulation process ranging between 50 and 500 and on the other hand y axis denotes the message delivery time. From the above figure, the message delivery time is found to be directly proportional to the number of data packets involved in the simulation process. In other words, increasing the number of data packets causes increase in the data packets to be transmitted and this in turn results in the increase in the message delivery time also. However, simulation results for 80 data packets found message delivery time of 12.4ms using DNC-HCHS, 15.2ms using [1] and 19.6ms using [2]. From the results the message delivery time was found to be comparatively minimum using DNC-HCHS method. The reason behind the minimum message delivery time was owing to the application of certificateless signcryption process via deep neural learning. With the distinct process performed separately in different hidden layers, the message delivery time was found to be comparatively lesser using DNC-HCHS method by 22% compared to [1] and 43% compared to [2]. Performance analysis of delay Finally, delay is defined as the time consumed between the sender nodes sending the data packets to the receiver node received it. In other words, it is defined as the difference between the actual and expected arrival time of data packet. The overall delay is measured as given below.

$$Delay = \sum_{i=1}^{n} N_i * ([t_{act}] - [t_{ex}]) \quad (15)$$

From the above equation (15), delay '$Delay$' is measured based on the actual arrival time '$[t_{act}]$' of the data packets to the intended recipient and the expected arrival time '$[t_{ex}]$' as mentioned by the sender node. It is measured in terms of milliseconds (ms). Table 5 shows the tabulation results of delay involved in data transmission using DNC-HCHS, PCDSPHS and CPDSPHS [1] and certificateless multi-recipient signcryption [2] respectively.

TABLE 5. Tabulation for delay

Nodes	Delay (ms)		
	DNC-HCHS	PCDSPHS and CPDSPHS	certificateless multi-recipient signcryption
50	62.5	87.5	102.5
100	90.35	115.55	125.35
150	105.15	135.55	155.15
200	130.45	175.85	195.35
250	145.55	190.25	235.25
300	190.25	215.55	275.15
350	210.35	245.55	315.35
400	225.55	290.35	335.55
450	240.85	310.35	350.15
500	265.35	335.55	395.55

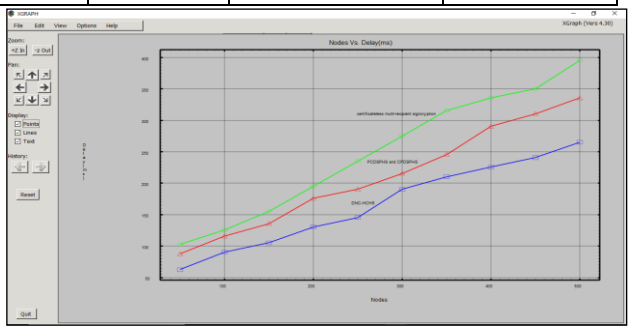

FIGURE 6. Graphical representation of delay

Finally, figure 6 given above shows the delay involved in the data transmission process. From the above figure, increasing the nodes involved in the data transmission process causes an increase in the number of data packets also. As a result the delay consumed in reaching the intended recipients also increases proportionately. But, simulations performed with 50 nodes using the three methods were observed to be 62.5ms, 87.5ms [1] and 102.5ms [2] respectively. From the result, the delay in transmitting data or data packets using DNC-HCHS is comparatively lesser than [1] and [2]. The reason behind the minimization of delay was due to the incorporation of Deep Neural Certificateless Hessian Curve Heap Signcryption algorithm. By applying this algorithm, secured transmission in the proposed work was performed using the Certificateless Hessian Curve Heap Signcryption by employing deep neural learning. Next, three distinct processes i.e., partial key generation, actual key generation and signcryption were done in the respective hidden layers. This in turn minimized the delay in data transmission using DNC-HCHS by 21% compared to [1] and 33% compared to [2].

6. Conclusion

In this paper, Deep Neural Certificate less Hessian Curve Heap Signcryption (DNC-HCHS) method is proposed for secured data transmission in wireless network from senders to the intended receivers. In this process, deep neural learning Certificate less Hessian Curve Heap Signcryption is applied for secured data transmission in wireless network. First, input details were provided in the input layer. Followed by which in the three hidden layers, partial key generation, key generation and signcryption process using Hessian Curve function was applied to the conventional elliptic curve to ensure data confidentiality and data integrity. The efficiency of the method is evaluated by using various performance measures and the obtained results are compared with the state-of-the-art methods. Therefore, on the whole, proposed DNC-HCHS method was found to be more advantageous than the existing methods. Also, as far as performance analysis is concerned, our data transmission method had the shortest delay and the maximum data confidentiality, data integrity and message delivery rate compared with the two existing data transmission method utilizing signcryption via deep learning. Hence, it is more suitable for secured data transmission in wireless network.

References

[1]. Ming Luo, Yusi Pei, Wei Huang, “Mutual heterogeneous signcryption schemes with different system parameters for 5G network slicing”, Wireless Networks, Springer, Jan 2021

[2]. Baoyi Wang, Jieqi Rong, Shaomin Zhang, Li Liu, “Research on data security of multicast transmission based on certificateless multi-recipient signcryption in AMI”, Electrical Power and Energy Systems, Elsevier, Apr 2020

[3]. Guyue Li, Zheying Zhang, Junqing Zhang and Aiqun Hu,” Encrypting Wireless Communications On the FlyUsing One-Time Pad and Key Generation”, IEEE Internet of Things Journal, Aug 2020

[4]. Zhengyi Shang, Maode Ma, Xiaohong Li, "A Secure Group-Oriented Device-to-DeviceAuthentication Protocol for 5G Wireless Networks", IEEE Transactions on Wireless Communications, Aug 2020
[5]. Qin Qiu,Shenglan Liu,Sijia Xu,Shengquan Yu, "Study on Security and Privacy in 5G-Enabled Applications", Wireless Communications and Mobile Computing, Wiley, Dec 2020
[6]. VipindevAdatVasudevan, Christos Tselios,IliasPolitis," On Security Against Pollution Attacks in NetworkCoding Enabled 5G Networks", IEEE Access, Mar 2020
[7]. Liling Cao, Yuqing Liu, Shouqi Cao, "An Authentication Protocol in LTE-WLAN Heterogeneous Converged Network Based on Certificateless Signcryption Scheme With Identity Privacy Protection", IEEE Access, Sep 2019
[8]. Muhammad Asghar Khan, Insaf Ullah, Shibli Nisar, Fazal Noor, Ijaz Mansoor Qureshi, Fahim Ullah Khanzada, Noor Ul Amin, "An Efficient and Provably Secure Certificateless Key-Encapsulated Signcryption Scheme for Flying Ad-hoc Network", IEEE Access, Mar 2020
[9]. Liaojun Pang, Man Kou, Mengmeng Wei, Huixian Li, "Anonymous Certificateless Multi-Receiver Signcryption Scheme Without Secure Channel", IEEE Access, Jul 2019
[10]. Caixue Zhou, "An improved lightweight certificateless generalized signcryption scheme for mobile-health system", International Journal of Distributed Sensor Networks, Sep 2019
[11]. VankamamidiSrinivasa Naresh, SivaranjaniReddi, SaruKumari, V. V. L. Divakar Allavarpu, SachinKumar, Ming-Hour Yang, "Practical Identity Based Online/Off-Line SigncryptionScheme for Secure Communication inInternet of Things", IEEE Access, Feb 2021
[12]. Aiqing Zhang, Lei Wang, Xinrong Ye, Xiaodong Lin, "Light-weight and Robust Security Aware D2D-assistData Transmission Protocol for Mobile-HealthSystems", IEEE Transactions on Information Forensics and Security, Oct 2016
[13]. ZengguangLiu, XiaochunYin, "LSTM-CGAN: Towards Generating Low-RateDDoS Adversarial Samples for Blockchain-BasedWireless Network Detection Models", IEEE Access, Jan 2021
[14]. Sunday Oyinlola Ogundoyin, IsmailaAdeniyiKamil, "PAASH: A privacy-preserving authentication and fine-grained access control of outsourced data for secure smart health in smart cities", Journal of Parallel and Distributed Computing, Elsevier, May 2021
[15]. R. Shashidhara, SanjeetKumar Nayak, Ashok Kumar Das, YounghoPark, "On the Design of Lightweight and Secure MutualAuthentication System for Global Roaming inResource-Limited Mobility Networks", IEEE Access, Jan 2021
[16]. AslihanCelik, Jessica Tetzner, Koushik Sinha, John Matta, "5G device-to-device communicationsecurity and multipath routing solutions", Applied Network Science, Jul 2019
[17]. Duy-Hung Ha, Tan N. Nguyen, Minh H. Q. Tran, XingwangLi, Phuong T. Tran, Miroslav Voznak, "Security and Reliability Analysis of a Two-WayHalf-Duplex Wireless Relaying Network UsingPartial Relay Selection and Hybrid TPSR EnergyHarvesting at Relay Nodes", IEEE Access, Oct 2020
[18]. Mahmoud Abbasi, Amin Shahraki, Amir Taherkordi, "Deep Learning for Network Traffic Monitoring and Analysis (NTMA): ASurvey", Computer Communications, Elsevier, Jan 2021
[19]. Ijaz Ahmad, ShariarShahabuddin, Hassan Malik, ErkkiHarjula, TeemuLeppanen, Lauri Loven, Antti Anttonen, Ali Hassan Sodhro, Muhammad MahtabAlam Markku Juntti, Antti Yla-Jaaski, ThiloSauter, Andrei Gurtov, Mika Ylianttila, Jukka Riekki, "Machine Learning Meets Communication Networks: Current Trends and Future Challenges", IEEE Access, Dec 2020
[20]. BelalAli, Mark A. Gregory, ShuoLi, "Multi-Access Edge Computing Architecture, Data Security and Privacy: A Review", IEEE Access, Feb 2021
[21]. TrupilLimbasiya, Sanjay Kumar Sahay, and Bharath Sridharan "Privacy-Preserving Mutual Authentication and Key Agreement Scheme for Multi-Server Healthcare System", Information Systems Frontiers, March 2021
[22]. Ding Wang,Wenting Li, Ping Wang, "Measuring Two-Factor Authentication Schemes for Real-Time Data Access in Industrial Wireless Sensor Networks", IEEE Transactions on Industrial Informatics, May 2018
[23]. Ding Wang, Ping Wang, "Two Birds with One Stone: Two-Factor Authentication with Security Beyond Conventional Bound", IEEE Transactions on Dependable and Secure Computing, September 2018
[24]. ShumingQiu, Ding Wang, Guoai Xu, Saru Kumari "Practical and Provably Secure Three-Factor Authentication Protocol Based on Extended Chaotic-Maps for Mobile Lightweight Devices", IEEE Transactions on Dependable and Secure Computing, September 2020
[25]. Chenyu Wang, Ding Wang, Guoai Xu, and Debiao He "Efficient Privacy-Preserving User Authentication Scheme with Forward Secrecy for Industry 4.0",SCIENCE CHINA: Information Sciences, August 2021
[26]. Qingxuan Wang, Ding Wang, Chi Cheng, and Debiao He "Quantum2FA: Efficient Quantum-Resistant Two-Factor Authentication Scheme for Mobile Devices", IEEE Transactions on Dependable and Secure Computing, November 2021
[27]. Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, Frank Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes", 2012 IEEE Symposium on Security and Privacy, July 2012