Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.018953
Article

Lamport Certificateless Signcryption Deep Neural Networks for Data Aggregation Security in WSN

P. Saravanakumar[1], T. V. P. Sundararajan[2], Rajesh Kumar Dhanaraj[3], Kashif Nisar[4,*], Fida Hussain Memon[5,6] and Ag. Asri Bin Ag. Ibrahim[4]

[1]Department of Electronics and Communication Engineering, Bannari Amman Institute of Technology, India
[2]Department of Electronics and Communication Engineering, Sri Shakthi Institute of Engineering and Technology, India
[3]School of Computing Science and Engineering, Galgotias University, India
[4]Faculty of Computing and Informatics, Universiti Malaysia Sabah, Jalan UMS, 88400, KK, Malaysia
[5]Department of Mechatronics, AMM Lab Jeju National University, Korea
[6]Department of Electrical Engineering Sukkur IBA University, Pakistan
*Corresponding Author: Kashif Nisar. Email: kashif@ums.edu.my
Received: 27 March 2021; Accepted: 31 August 2021

Abstract: Confidentiality and data integrity are essential paradigms in data aggregation owing to the various cyberattacks in wireless sensor networks (WSNs). This study proposes a novel technique named Lamport certificateless signcryption-based shift-invariant connectionist artificial deep neural networks (LCS-SICADNN) by using artificial deep neural networks to develop the data aggregation security model. This model utilises the input layer with several sensor nodes, four hidden layers to overcome different attacks (data injection, compromised node, Sybil and black hole attacks) and the output layer to analyse the given input. The Lamport one-time certificateless signcryption technique involving three different processes (key generation, signcryption and unsigncryption) is adopted to achieve secure data transmission between the sender and receiver. Firstly, a one-way function is executed to generate the public and private keys for each sensor node in the WSN. Secondly, digital signature generation and encryption are both performed. The sender node, which handles the signature generation and data encryption, forwards the data to the aggregator node. Then, the receiver verifies the data by using the sender's public key during data decryption. Thus, data aggregation security can be guaranteed. Finally, the authorised node aggregates the data with much higher data confidentiality and privacy. Performance analysis is conducted by simulating the proposed LCS-SICADNN and conventional models. Results of comparison indicate that the LCS-SICADNN can improve data aggregation security with higher throughput and lesser delay, packet drop and overhead compared with the conventional methods.

Keywords: Wireless sensor network; secure data aggregation; Lamport one-time certificateless signcryption; shift-invariant connectionist artificial deep neural network

1 Introduction

Data aggregation is an efficient method of extending the lifetime of wireless sensor networks (WSNs) by preventing frequent data transmission. However, accuracy, confidentiality, delay and privacy preservation remain to be complex issues. Security has become a major concern in recent years because of insider and outsider attacks, but the identification and protection of information have also become increasingly complicated. Reference [1] proposed an asymmetric key encryption scheme by using elliptic curve cryptography to secure end-to-end data aggregation. Although this scheme reduced the computation overhead, the delivery ratio and transmission delay could not be improved. Reference [2] designed a continuous hybrid and energy-efficient secure data aggregation (CHESDA) algorithm for privacy-preserving data aggregation. Although the delay was minimised, the throughput could not be improved with a minimum overhead.

Reference [3] introduced a novel method for data aggregation security to detect good and bad sensor nodes, but the cryptographic technique was not adopted for enhancing the security of data aggregation. Reference [4] developed an identity-based aggregate signature method to secure big data aggregation, but the efficiency of the data aggregation design was not enhanced. Reference [5] developed the Fujisaki−Okamoto algorithm via the ID-based cryptographic method for secure data aggregation. Although the throughput was increased, the overhead was not minimised. Reference [6] designed a trust-weighted secure data aggregation algorithm to minimise packet drops, but data aggregation could not be performed with a minimum delay. Reference [7] introduced the heavy-weight security algorithm for securing data aggregation with a minimum overhead and a high throughput, but it failed to perform various types of attack detection in WSN. Reference [8] developed an authentication-based secure data aggregation technique to detect severe types of attacks, such as sinkhole and Sybil attacks, via cryptographic approaches. Although the delay was reduced, the packet delivery ratio could not be improved.

Reference [9] developed an efficient approach called the Hamming residue method to mitigate malicious attacks. The HRM increased the delivery ratio, but the overhead was not minimised. Reference [10] introduced a novel technique based on the clustering approach by using timestamps for attack prevention. Although the approach increased the packet delivery ratio, the delay could not be reduced. Reference [11] designed a program integrity verification (PIV) protocol to detect node capture attacks by using a cryptographic hash function. The PIV protocol minimised the computation overhead, but the security level could not be increased with a minimum packet drop due to the attacks. Reference [12] introduced a two-stage security mechanism to identify black hole and selective forwarding attacks. Although the packet drop was reduced, the overhead remained high.

Reference [13] developed a new data aggregation method of using the extreme learning machine technique to minimise redundant and invalid data, but the system failed to use the cryptographic technique for securing data aggregation. Reference [14] introduced the method called secure data aggregation based on principle component analysis (SDA-PCA) to increase confidentiality and integrity. The SDA-PCA decreased the pack delivery ratio, but the overhead could not be reduced.

Reference [15] proposed a lightweight structure-based data aggregation routing (LSDAR) protocol to protect data against malicious threats. Although the LSDAR protocol minimises the delay, multi-attack detection was not performed. Reference [16] developed a data aggregation protocol to reduce the communication overhead, but the method failed to protect data integrity and data privacy during data aggregation.

Reference [17] introduced a multi-functional secure data aggregation scheme by using the light-weight security method, but it failed to focus on data aggregation efficiency. Reference [18] developed an energy-efficient secure data aggregation technique to improve privacy preservation. The overhead was minimised, but confidentiality improvement could not be ensured.

Reference [19] introduced a secure and efficient verification scheme for data aggregation. End-to-end privacy and early detection of attacks were guaranteed, but multidimensional aggregation in WSNs could not be supported. [20] designed a secure data aggregation protocol to identify malicious nodes [21]. The throughput was increased, but performance could not be improved with respect to high delivery ratio [22].

Major Contribution

The current study proposes a novel method named the Lamport certificateless signcryption-based shift-invariant connectionist artificial deep neural networks (LCS-SICADNN) to overcome the issues obtained from the literature review. The contributing factors of LCS-SICADNN can be summarised as follows.

- The security of data aggregation in WSN is enhanced. In particular, the shift-invariant connectionist artificial deep neural network composed of neuron-like nodes located in different layers is utilised. The deep neural networks comprising neurons and connections are similar to the synapses of the human brain. The synapses, which are formed by neuronal junctions, transfer the signal (i.e, input) from one neuron to another.
- A novel Lamport one-time certificateless signcryption technique is applied with three different processes, namely, encryption, decryption and signature generation, to improve the confidentiality and privacy of the data transmission between the sender and receiver by avoiding unauthorised attacks. The Lamport one-time certificateless signcryption technique generates a pair of keys by using the one-way function to generate passwords (i.e., private and public keys). The encryption, signature generation and decryption altogether reduce the computation overhead at a minimum time. The sensed data packets are encrypted and sent along with the signature to the receiver. Then, the signature is verified at the aggregator node and validated. The decryption is implemented to obtain the original text, thus increasing the security of data delivery and minimising the packet drop.
- Extensive simulation is conducted to estimate the performance of the proposed LCS-SICADNN *vs.* those of the conventional methods. The simulation results indicate that the proposed technique outperforms the other methods in terms of data aggregation. Moreover, the experimental results verify that LCS-SICADNN performs better in securing data aggregation with lesser minimum computation overhead, packet drop rate and delay and higher packet delivery ratio and throughput compared with the existing methods.

2 Methodology

AWSN is a self-organising wireless network. It comprises low-cost sensor nodes that cooperatively perform data aggregation. If a node does not perform cooperatively, then it is called an attacker node. Attacker nodes often disrupt the functionality of a network. Therefore, an effective security method is needed to detect attacks during data aggregation. In this study, an algorithm called LCS-SICADNN is introduced for WSNs. The LCS-SICADNN integrates the Lamport one-time certificateless signcryption into the SICADNN to guarantee efficient data aggregation.

Fig. 1 illustrates the architecture of the proposed LCS-SICADNN for achieving data aggregation security. Shift-invariant connectionist artificial deep neural networks are used in the WSN. Firstly, a set of sensor nodes ($SD = \{sd1, sd2, \ldots, sdn\}$) is deployed in the network for sensing and collecting information from the environment. Then, the collected information is transmitted to the aggregator node A_d, which subsequently forwards this information to the base station. The aggregator node acts as a collector of the data ($d_1, d_2, .., d_m$) from the other sensor nodes. During the data transmission, a secure data transmission is established between the sender and receiver by means of a cryptographic technique.

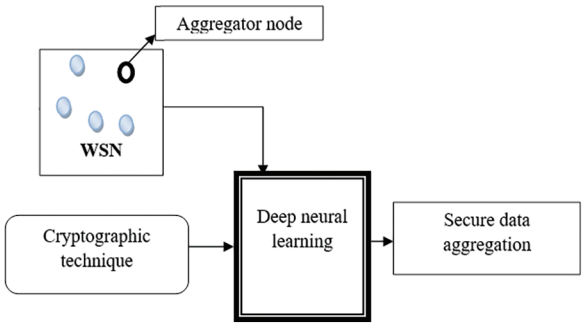

Figure 1: System architecture of the proposed LCS-SICADNN

Fig. 2 shows a schematic of SICADNN that includes neuron-like nodes positioned in different layers. The nodes constitute an entire network composed of simple and often consistent units. However, the structure of the connections and the units differ from one another in terms of design. The units represent neurons, whereas the connections denote the synapses of the human brain. The connections (synapses) are a neuronal junction and can transfer signals (i.e., inputs) from one unit (neuron) to another. Moreover, the network operates as a feedforward system in which information is transmitted from one layer to another in the forward direction.

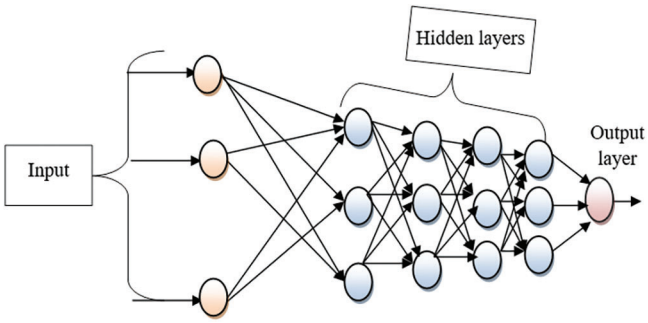

Figure 2: Schematic of SICADNN

An input node in the input layer interacts with a number of sensor nodes in the hidden layers where sensing and collection of information from the environment are both performed. Then, in the second hidden layer, the sensed information is securely transferred to the aggregator node. The activity of the neuron at the input layer of *k(t)* network is expressed with the number of sensor nodes and weight values as follows:

$$k(t) = \sum_{i=1}^{n} sd_i * \alpha_1, \tag{1}$$

where sd_i denotes a sensor node, and α_1 denotes a weight between the input layer and hidden layer.

In the second hidden layer, the sensed and collected data from each node are transmitted to the aggregator node by using the proposed Lamport one-time certificateless signcryption, a public key cryptography technique that can simultaneously perform encryption and digital signature generation. This proposed signcryption scheme is computationally efficient and can ensure security and confidentiality.

The Lamport one-time certificateless signcryption includes three major processes: key generation, signcryption and unsigncryption.

• Key generation

The base station generates private and public keys for each sensor node participating in the data aggregation. The advantage of using the Lamport one-time signature is that private and public keys are generated as passwords via a one-way function.

Assume a random set of positive integers to be used as passwords. The key generation process becomes useless once a period expires.

$$k_p = [R], \tag{2}$$

where k_p denotes a private key, and R is a random integer. After generating the private key, the public verification key is generated as follows:

$$k_{pb} = F[R], \tag{3}$$

where k_{pb} represents the public verification key, and F is a one-way function expressed as

$$F = [R] + 1 \; mod \; 16. \tag{4}$$

The public verification keys are distributed, whereas the private key is kept secret. However, this process becomes useless once the key generation period expires.

• Encryption and signature generation

The Lamport one-time signcryption can simultaneously perform digital signature generation and encryption. These two basic cryptographic processes can guarantee data confidentiality during transmission between the sender node and the aggregator node in the WSN.

Fig. 3 illustrates the block diagram of the encryption and signature generation for improving the confidentiality and privacy of the data transmission between the sender and receiver. The scheme can avoid unauthorised attacks, such as injection, compromised node, Sybil and block hole attacks.

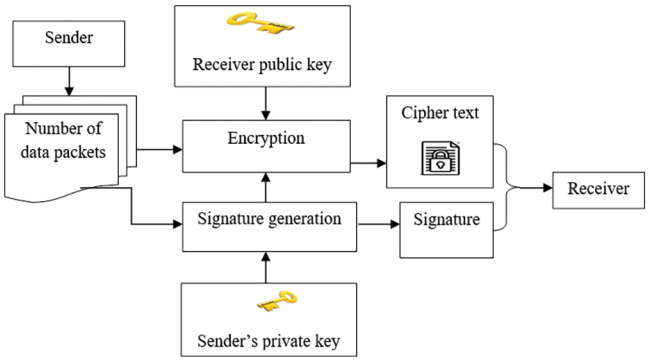

Figure 3: Block diagram of encryption and signature generation

A data injection attack is a malicious code introduced into the network. It obtains sensed information from the sensor node and transmits it to the attacker. A compromised node attack creates false data and injects these data into the WSN during data aggregation, and it also drops aggregated information.

A Sybil attack is a self-duplicating single sensor node that is found in many locations in the network. A black hole attack drops the data packets during the data packet transmission between sensor nodes. By introducing wormhole attacks, the attackers can record information at particular locations within the network and transmit them to other locations.

The sensed data ($d_1,\ d_2,\ ..,d_m$) are encrypted using the receiver's public key to generate the ciphertext as follows:

$$D \leftarrow E\ \left[k_{pb}, d\right], \tag{5}$$

where D is a ciphertext of data d, and E represents the encryption with the public key of the receiver (k_{pb}). Simultaneously, the digital signature is generated using the sender's private key.

Let z be a positive integer that can be converted by a string (i.e., (0, 1)). The signature is generated by

$$\varphi = \left[R_{ij\,z}\right], \tag{6}$$

where φ denotes a signature, R_{ij} is a position of the private key $(0 < i < r)$, r is a positive integer, and $j \in (0, 1)$. The generated signature, as well as the ciphertext, is sent to the receiver (i.e., aggregator).

• Unsigncryption

In the third hidden layer, the proposed technique performs the unsigncryption (i.e., signature verification and decryption) to obtain the original data.

Fig. 4 shows the block diagram of the unsigncryption at the receiver side. Firstly, signature verification is performed using the sender's public key to obtain the original data.

$$\varphi_b = F\ (\varphi), \tag{7}$$

$$F = [\varphi] + 1\ mod\ 16, \tag{8}$$

where φ_b is a signature generated at the receiver side, and F is a one-way function. Finally, the signature is verified as a means of obtaining the original data.

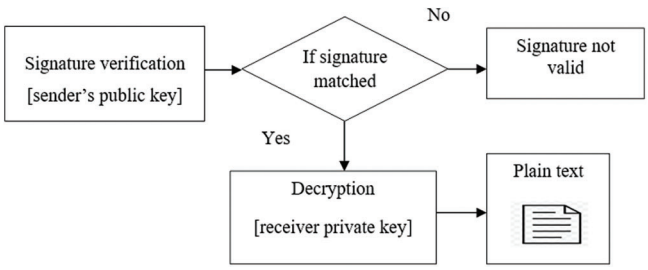

Figure 4: Unsigncryption

$$Y = \{\varphi = \varphi_b \quad ; signature\ is\ valid \varphi \neq \varphi_b \quad ; signature\ is\ not\ valid \tag{9}$$

When both signatures in Eq. (9) are matched, the aggregator node will decrypt the ciphertext; when an unmatched signature is considered invalid. This process increases the security of the data transmission between the sensor node and aggregator node. Finally, the authorised node decrypts the ciphertext to obtain the original data as follows:

$$d \leftarrow B\left[k_p, D\right], \tag{10}$$

where d denotes the original data, B is the decryption, k_p is the private key of the user and D is the ciphertext. As mentioned previously, the original data is subsequently obtained by the aggregator node. Finally, secured data aggregation is achieved with much higher data confidentiality at the output layer. The algorithmic process of the proposed technique is given in Algorithm 1.

Algorithm 1: Lamport Certificateless Signcryption-Based Shift-Invariant Connectionist Artificial Deep Neural Network

Input: Number of sensor nodes $SD = \{sd1, sd2, \ldots, sdn\}$, Number of data $d_1, d_2, d_3, \ldots .d_m$

Output: Increase the security of data aggregation

Begin

Number of sensor nodes $SD = \{sd1, sd2, \ldots, sdn\}$ **taken as input at the input layer**

For each sensor node *sd*

Sense and collect the data $d_1, d_2, d_3, \ldots .d_m$ // **hidden layer 1**

key generation // hidden layer 2

For each node *sd*

Base station generates private k_p and public key'k_{pb}'

End for

// Signcryption// hidden layer 3

Encrypt data using receivers public key $D \leftarrow E\left[k_{pb}, d\right]$

Generate digital signature '$\varphi = \left[R_{ij\,z}\right]$'

Send to aggregator node

// Unsigncryption// hidden layer 4

If ($\varphi = \varphi_b$) **then**

Signature is valid

Aggregator node decrypts the data using receiver private key $d \leftarrow B\left[k_p, D\right]$

Obtain original data '*d*'

else

The signature is not valid

End if

Obtain the security of data aggregation

End

Algorithm 1 presents the step-by-step process of securing data aggregation between the sensor node and aggregator node. The sensor nodes operate as the input of the deep neural network. These nodes start by collecting data from the environment in the first hidden layer. Then, the Lamport one-time signcryption is applied to generate the private and public keys for each registered user. Signature generation and encryption are subsequently performed using the sender's private key and the receiver's public key, and the encrypted data and signature are sent to the aggregator node. Finally, the unsigncryption is performed at the last hidden layer. A signature verification is initially performed using the sender's public key. If the signature is valid, then the data are decrypted using the receiver's private key. Finally, the authorised node aggregates the data with higher confidentiality and privacy.

3 Simulation Settings

The proposed LCS-SICADNN and two existing methods, namely, the asymmetric key encryption scheme [1] and CHESDA [2], were simulated in the NS2 network simulator. Five hundred sensor nodes were deployed over a squared area of A^2 (1100 m * 1100 m) for the secure data aggregation. A random waypoint model was used as the mobility model for securing the data aggregation in the WSN. The *ad hoc* on-demand distance vector (AODV) routing protocol was used to detect the different types of attacks, namely, data injection, compromised node, replication [21] and wormhole attacks, in the simulation scenario [22]. The simulation time was set as 300 s, and the speed of the sensor nodes was varied between 0 and 20 m/s. The various simulation parameters are listed in Tab. 1.

Table 1: Simulation parameters

Simulation parameters	Values
Simulator	NS2
Network area	1100 m * 1100 m
Number of sensor nodes	50–500
Mobility model	Random waypoint model
Number of data packets	25–250
Speed of node	0–20 m/s
Simulation time	300 s
Number of runs	10
Protocol	AODV routing

4 Performance Analysis

The simulation results of the three different methods, namely, LCS-SICADNN, asymmetric key encryption scheme [1] and CHESDA [2], are analysed using a set of metrics (computation overhead, packet delivery ratio, packet drop rate, delay and throughput). These metrics can be described as follows:

$$CO = [E_t + D_t + A_t] \tag{11}$$

where CO is computation overhead, E_t is encryption time, D_t is decryption time and A_t is aggregation time. The computation overhead is measured in terms of seconds (sec).

Packet delivery ratio is measured as the ratio of the number of data packets correctly received at the aggregator node to the total number of data packets at different simulation times. The formula for calculating the packet delivery ratio is

$$PDR = \left[\frac{Number\ of\ data\ packets\ received}{Number\ of\ data\ packets}\right] * 100, \tag{12}$$

where PDR is the packet delivery ratio that is measured in terms of percentage (%).

Packet drop rate is defined as the ratio of the size of data packets dropped during the data aggregation. The packet drop rate is given by

$$R_{PD} = \left[\frac{data\ packets\ dropped\ (bytes)}{data\ packets\ size\ (bytes)}\right] * 100, \tag{13}$$

where R_{PD} is the packet drop rate that is measured in terms of percentage (%).

Transmission delay is measured as the difference between the actual arrival time of the data packets and the observed arrival time of the data packets at the aggregator node. The overall delay is formulated as

$$TD = [t_{act}] - [t_{obs}], \tag{14}$$

where TD is transmission delay, t_{act} is the actual arrival time and t_{obs} is the observed arrival time. The overall delay is measured in terms of seconds (sec).

Throughput is defined as the amount of data packets successfully delivered at an aggregator node in a given time. This metric is measured as

$$T = \left[\frac{Size\ of\ data\ packet\ received\ (bits)}{time\ (sec)}\right], \tag{15}$$

where T is measured in terms of bits per second (bps).

Fig. 5 shows the comparative analysis of the computation overhead metric for the aforementioned three methods. The proposed SDBCCML has a lower overhead than the asymmetric key encryption scheme [1] and CHESDA [2]. The difference can be attributed to the application of SICADNN for the encryption and decryption in the WSN. The computation overhead of the LCS-SICADNN is lower than those of the existing methods. In the simulation, the LCS-SICADNN consumed 0.3 s, whereas the asymmetric key encryption scheme [1] and CHESDA [2] obtained 0.6 s and 0.72 s, respectively. Then, the overall results of the LCS-SICADNN were compared with those of the existing methods. The computation overhead of the LCS-SICADNN could be minimised by 37% with respect to the asymmetric key encryption scheme [1] and by 44% with respect to CHESDA [2].

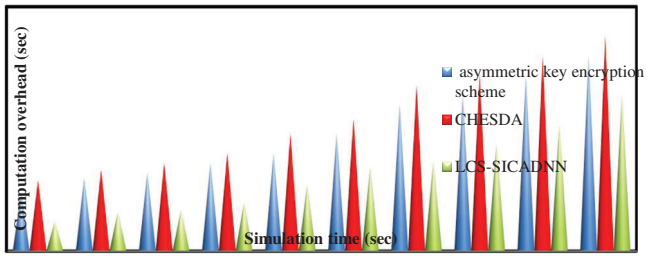

Figure 5: Performance results of the computation overhead metric

Fig. 6 shows the comparative analysis of the packet delivery ratio metric at different simulation times. The proposed LCS-SICADNN and the conventional methods (asymmetric key encryption scheme [1] and CHESDA [2]) were implemented in the same experimental setting. Meanwhile, the simulation was conducted by considering 100 data packets to be sent from the sender node, and the time was set as 10 s. For the LCS-SICADNN, 93 data packets were successfully delivered to the aggregator node, and the delivery ratio was 93%. By contrast, the delivery ratio of the asymmetric key encryption scheme [1] and CHESDA [2] were 88% and 84%, respectively. Subsequently, various delivery ratios were considered by setting different simulation times. The average of ten results showed that the packet delivery ratio of the

proposed LCS-SICADNN was increased by 8% and 11% with respect to the state-of-the-art asymmetric key encryption scheme [1] and CHESDA [2], respectively.

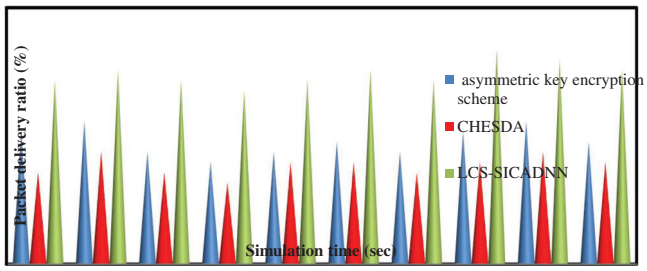

Figure 6: Performance results of the packet delivery ratio metric

Fig. 7 shows the comparative analysis of the packet drop rate metric for the three aforementioned methods during data aggregation in the WSN at different simulation times. The packet drop rate of the proposed LCS-SICADNN was lower than the existing aggregation techniques. The simulation was implemented with 100 bytes of data, and the time was set as 10 s.

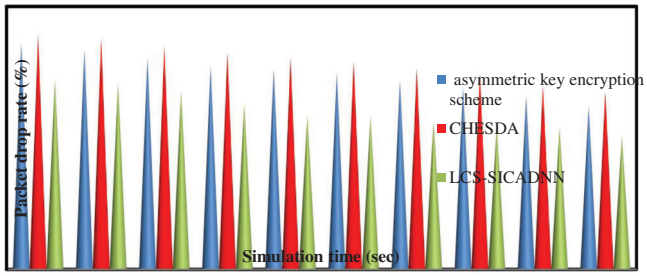

Figure 7: Performance results of the packet drop rate metric

The comparative analysis in Fig. 8 indicates that 50.8 bytes of data could be dropped by the proposed LCS-SICADNN, whereas 60.5 and 62.3 bytes of data can be dropped with the asymmetric key encryption scheme [1] and CHESDA [2], respectively. Moreover, the average of ten results showed that the packet drop rate of the LCS-SICADNN could be minimised by 19% and 23% with respect to the asymmetric key encryption scheme [1] and CHESDA [2], respectively. The transmission delay was also simulated with different data packet sizes in the range of 100−1000 bytes. The simulation results indicate that the transmission delay of the LCS-SICADNN was lower than those of the conventional methods. This finding was proven by the sampling calculation, in which 100 bytes of data were considered for the transmission delay. The transmission delay was 0.8 ms in the LCS-SICADNN, whereas the values were 1.5 *ms* in the asymmetric key encryption scheme [1] and 1.7 ms in CHESDA [2]. The transmission delay metric was also analysed with different data packet sizes for the three methods. The average of ten results showed that the LCS-SICADNN was minimised by 40% and 45% of the conventional asymmetric key encryption scheme [1] and CHESDA [2], respectively.

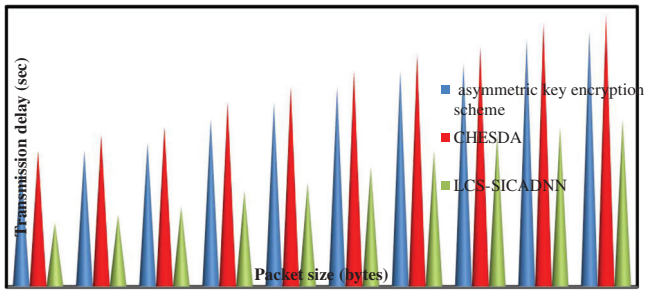

Figure 8: Performance results of the transmission delay metric

Fig. 9 shows the comparative analysis of the throughput metric during data aggregation. The horizontal axis represents the size of data packets in the network, whereas the vertical axis represents the number of packets successfully delivered by bits per second. The throughput was increased using the LCS-SICADNN. Consider 100 byts of data packets sent from the source node. By applying the LCS-SICADNN, 65 bits of the data packets can be transmitted in 1 s. By contrast, the throughputs of the asymmetric key encryption scheme [1] and CHESDA [2] were 50 and 45bps. The superior performance of the LCS-SICADNN can be attributed to the Lamport one-time certificateless signcryption, which minimises the packet drop caused by data injection, compromised node, Sybil and block hole attacks; hence, successful data delivery is achieved.

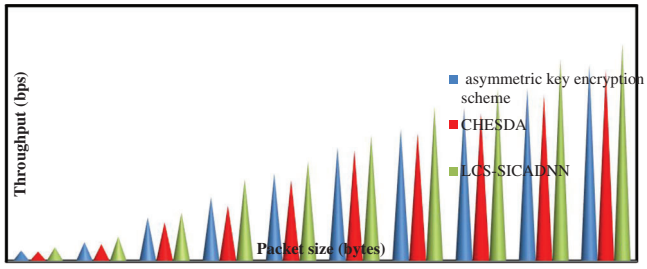

Figure 9: Performance results of the throughput metric

5 Conclusion

The LCS-SICADNN, a novel data security technique, is proposed in this study to secure the data aggregation in the WSN. The proposed technique utilises SICADNN to achieve higher data delivery with a minimum delay. In the LCS-SICADNN, different layers, namely, an input layer, four hidden layers and an output layer, are considered. Initially, the number of sensor nodes is transmitted to the input layer as the input. Then, the sensor node performs sensing and collecting information from the environment, and the sensed information is transferred to the aggregator node. The Lamport one-time certificateless signcryption technique adopted in this study entails three processes: key generation, signcryption, and unsigncryption. First, in the key generation process, a public key and a private key are created for each sensor node. Then, the Lamport one-time signcryption performs digital signature generation and encryption to convert the data into plaintext and transfers it to the aggregator node. Finally, on the receiver side, the signature is verified using the sender's public key during decryption. If the signature is valid, then the aggregator node attains the original data, thus enhancing the data transmission security. The performance of the proposed LCS-SICADNN is simulated and compared with those conventional aggregation methods by using different metrics. The observed results indicate that the proposed

LCS-SICADNN outperforms the existing methods as proven by the higher data delivery ratio, lesser computation delay and lesser computation overhead.

Funding Statement: This paper is a collaboration with the Faculty of Computing and Informatics, Universiti Malaysia Sabah, 88400 Kota Kinabalu, Sabah, Malaysia. The authors would like to thank Professor/Dr. Yong-Jin Park (IEEE Life Member), Former Director of IEEE Region 10, for his expertise, valuable comments and suggestions in helping improve the quality of the study.

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

References

[1] X. Qi, X. Liu, J. Yu and Q. Zhang, "A privacy data aggregation scheme for wireless sensor networks," *Procedia Computer Science*, vol. 174, pp. 578–583, 2020.

[2] R. Hajian and S. H. Erfani, "CHESDA: Continuous hybrid and energy-efficient secure data aggregation for WSN," *Journal of Supercomputing*, Springer, vol. 77, no. 5, pp. 5045–5075, 2021.

[3] A. Yessembayev, D. Sarkar and F. Sikder, "Detection of good and bad sensor nodes in the presence of malicious attacks and its application to data aggregation," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 3, pp. 549–563, 2018.

[4] L. Shen, J. Ma, X. Liu, F. Wei and M. Miao, "A secure and efficient id-based aggregate signature scheme for wireless sensor networks," *IEEE Internet of Things Journal*, vol. 4, no. 2, pp. 546–554, 2017.

[5] K. N. Raja and M. M. Beno, "Secure data aggregation in wireless sensor network-fujisaki okamoto (fo) authentication scheme against sybil attack," *Journal of Medical Systems*, Springer, vol. 41, no. 7, pp. 1–6, 2017.

[6] P. Padmaja and G. V. Marutheswar, "Energy efficient data aggregation in wireless sensor networks," *Materials Today: Proceedings*, Elsevier, vol. 5, no. 1, pp. 388–396, 2018.

[7] A. Saravanaselvan and B. Paramasivan, "Design and implementation of an efficient attack resilient computation algorithm in WSN nodes," *Cluster Computing*, Springer, vol. 22, pp. 3301–3311, 2019.

[8] A. Razaque and S. S. Rizvi, "Secure data aggregation using access control and authentication for wireless sensor networks," *Computers & Security*, Elsevier, vol. 70, no. 4, pp. 532–545, 2017.

[9] M. Alotaibi, "Security to wireless sensor networks against malicious attacks using hamming residue method," *EURASIP Journal on Wireless Communications and Networking*, Springer, vol. 8, no. 1, pp. 1–7, 2019.

[10] S. G. H. Rose and T. Jayasree, "Detection of jamming attack using timestamp for WSN," *Ad Hoc Networks*, Elsevier, vol. 91, pp. 1–12, 2019.

[11] S. Agrawal, M. L. Das and J. Lopez, "Detection of node capture attack in wireless sensor networks," *IEEE Systems Journal*, vol. 13, no. 1, pp. 238–247, 2019.

[12] D. C. Mehetre, S. E. Roslin and S. J. Wagh, "Detection and prevention of black hole and selective forwarding attack in clustered WSN with active trust," *Cluster Computing*, Springer, vol. 22, no. S1, pp. 1313–1328, 2019.

[13] I. Ullah and H. Y. Youn, "Efficient data aggregation with node clustering and extreme learning machine for WSN," *Journal of Supercomputing*, Springer, vol. 76, no. 12, pp. 10009–10035, 2020.

[14] M. V. Babu, J. A. Alzubi, R. Sekaran, R. Patan, M. Ramachandran *et al.,* "An improved IDAF-FIT clustering based ASLPP-RR routing with secure data aggregation in wireless sensor network," *Mobile Networks and Applications*, Springer, vol. 26, no. 2, pp. 1–9, 2020.

[15] K. Haseeb, N. Islam, T. Saba, A. Rehman and Z. Mehmood, "LSDAR: A light-weight structure based data aggregation routing protocol with secure internet of things integrated next-generation sensor networks," *Sustainable Cities and Society*, Elsevier, vol. 54, no. 2, pp. 1–9, 2020.

[16] J. Wang and Y. Chen, "Research and improvement of wireless sensor network secure data aggregation protocol based on smart," *International Journal of Wireless Information Networks*, Springer, vol. 25, no. 3, pp. 232–240, 2018.

[17] P. Zhang, J. Wang, K. Guo, F. Wu and G. Min, "Multi-Functional secure data aggregation schemes for WSNs," *Ad Hoc Networks*, Elsevier, vol. 69, no. 2, pp. 86–99, 2018.

[18] W. Fang, X. Z. Wen, J. Xu and J. Z. Zhu, "CSDA: A novel cluster-based secure data aggregation scheme for WSNs," *Cluster Computing*, Springer, vol. 22, pp. 5233–5244, 2019.

[19] O. R. M. Boudia, S. M. Senouci and M. Feham, "Secure and efficient verification for data aggregation in wireless sensor networks," *International Journal of Network Management*, vol. 28, no. 1, pp. 1–17, 2018.

[20] S. Gomathi and C. G. Krishnan, "Malicious node detection in wireless sensor networks using an efficient secure data aggregation protocol," *Wireless Personal Communications*, Springer, vol. 113, no. 4, pp. 1775–1790, 2020.

[21] L. Krishnasamy, R. Dhanaraj, D. G. Gopal, T. R. Gadekallu, M. K. Aboudaif *et al.,* "A heuristic angular clustering framework for secured statistical data aggregation in sensor networks," *Sensors*, vol. 20, no. 17, pp. 4937, 2020.

[22] I. S. Comşa, S. Zhang, M. E. Aydin, P. Kuonen, Y. Lu *et al.,* "Towards 5g: A reinforcement learning-based scheduling solution for data traffic management," *IEEE Transactions on Network and Service Management*, vol. 15, no. 4, pp. 1661–1675, 2018.