Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 44 No. 12
December 2023

Secure Data Communication in Wireless Sensor Networks Using Discriminative Weighted Emphasis boost Merkle–Hellman knapsack Certificate less Signcryption

D.Sudhakar[1]*,Dr. V. S. Meenakshi[2]

[1] Research Scholar, PG & Research Department of Computer Science, Chikkanna Govt. Arts College, Tirupur-2, India

2 Associate Professor, PG & Research Department of Computer Science, Chikkanna Govt. Arts College, Tirupur-2, India

Abstract: Wireless Sensor Networks (WSN) have been applied to a wider application for data gathering and data transmission by the number of sensor nodes. It has restricted battery power, resources, and computational power. Due to all these factors, WSN is susceptible to various attacks which are caused by a malicious node. Therefore a novel technique Discriminative Weighted Emphasis boost Merkle–Hellman knapsack Certificateless Signcryption (DWEBMKCS) is introduced for improving data communication safety in WSN. It consists of two major processes. First, for detecting the black hole and grey hole attacks, Otsuka-Ochiai Generalized Discriminative Weighted Emphasis boosting is employed. Next, Merkle–Hellman knapsack Certificateless Signcryption technique is used to achieve secure data transmission which includes three main processes namely time-synchronized Key-pair generation, signcryption, and unsigncryption. The performance of the DWEBMKCS is analyzed in terms of attack detection accuracy, data packet delivery, false positive and an end-to-end delay. An existing method such as Sequential Based Search and Light gradient boost (SLGBM), flexible, and lightweight encryption method called (FlexCrypt) are used to compare the proposed DWEBMKCS method. Thus the result shows higher attack detection accuracy, and fewer false positive rate by 94% and 6% for 500 nodes better performance than SLGBM, FlexCrypt., DA-LSTM. The data packet delivery is increased and the packet loss rate, end-to-end delay are minimized by 90%, 10%, and 23 ms for concerning the 250 number of sensor nodes when compared to the SLGBM, FlexCrypt, DALSTM.

Keywords: WSN, Secure data communication, Black hole and grey hole attack detection, Otsuka-Ochiai Generalized Discriminative Weighted Emphasis boosting, Merkle–Hellman knapsack Certificateless Signcryption

1. Introduction

WSN is a heterogeneous network and it includes huge circulated, tiny, low-powered devices called sensor nodes. It is used to sense the environmental conditions and transfer data to a remote base station. Security is a major issue since information is transmitted over the wireless channel where malicious attackers may get access to information. Data transmission is secured by numerous methods.

In 2020, Jiang et al. [1] introduced an integration of Sequential Based Search and Light gradient boost (LightGBM) classification algorithm called SLGBM to distinguish the different network attacks by selecting the characteristics of the sensor node. However, the designed algorithm was not efficient with higher security. The cryptographic technique was not employed for data communication. In 2021, Khashan et al. [2] secure connection established with an automated, flexible, and lightweight encryption method called (FlexCrypt) for WSN using symmetric keys. But, packet delivery ratio was not enhanced.

In 2021, Mathapati et al. [3] analyzed Multi-dimensional trust evaluation for secured communication with A new scheme. However, multiple attacks were not detected. In 2021, Gite et al. [4] were investigated Data patterns from each node to prevent the attacker with ML approach. In 2020, Ye et al. [5] performed efficient communication between the IoT devices by

detecting grey hole assault via fuzzy concept. But, it failed to reduce delay aware secure data transmission.

In 2021, Subasini et al. [6] identified the attack with hybrid DL method. But, the risk assessment and node mobility parameters were not estimated during the attack detection. In 2020, Shi et al. [7] detected malicious nodes in a novel secure routing protocol for WSNs. However, the routing scheme failed to consider transmission delay to make the secure routing model more realistic.

In 2021, Pang et al. [8] developed a fuzzy trust model as well as an artificial bee colony algorithm (ABC) by malicious node detection approach. The designed approach provided a high recognition rate as well as a low false-positive. But, the cryptography technique was not focused on improving system performance. In 2019, Luo et al. [9] determined wormhole attack detection by Credible Neighbour Discovery. However, the Neighbour Discovery algorithm failed to work well in the condition that the entire node with different communication ranges. In 2019, Agrawal et al. [10] used program integrity verification (PIV) protocol, a node capture attack via a cryptographic hash function. But, it failed to obtain higher detection accuracy. The main contribution of this research work by using DWEBMKCS are given as follows

- DWEBMKCS is mainly utilized for enhancing the security of data communication in WSN based on ensemble learning and cryptographic techniques.
- To identify the node attack with maximum accuracy, an Otsuka-Ochiai Generalized Discriminative Weighted Emphasis boosting technique is utilized. The novelty of Otsuka-Ochiai similarity is employed to categorize the attack node into a black hole or gray hole attack.
- The innovation of Weighted Emphasis boosting technique minimizes the quadratic error and accurately performs the classification. This helps to enhance attack detection accuracy and minimize the false positive rate.
- Secure data transmission is performed by using Merkle–Hellman knapsack Certificateless Signcryption technique with three main processes namely time-synchronized Key-pair generation, signcryption, and unsigncryption. If the signature is valid, the authorized node receives the data which helps to minimize delay and packet loss.
- Experimental evaluation is conducted by DWEBMKCS and existing techniques with dissimilar metrics.

The rest of the paper is categorized by the following sections. Section 2 briefly elaborates on the existing methods for attack detection in WSN. Section 3 describes the DWEBMKCS technique with a neat diagram. Section 4 describes the simulation settings. Section 5 presents performance evaluation and outcomes. Finally, the proposed technique is concluded in Section 6.

PROPOSED Algorithm 1: Otsuka-Ochiai Generalized Discriminative Weighted Emphasis boosting

Input: Number of sensor nodes$Sn_1, Sn_2, Sn_3, .. Sn_n$

Output: Increase the attack detection accuracy

Begin

Step 1: For each Sn

Step 2: Construct a set of weak learners $w_1, w_2, w_3, \dots . w_k$

Step 3: Initialize the classes c_1, c_2

Step 4: For each class c_i

Step 5: Initialize the mean value m_i

Step 6: Measure Otsuka-Ochiai coefficient 'φ'

Step 7: Classify the node into a black hole or gray hole attack

Step 8: end for

Step 9: Combine weak learners '

Step 10: For each 'w_i*'*

Step 11: Initialize weights 'β'

Step 12: Measure quadratic error 'ϑ'

Step 13: Update the weight

Step 14: Find a weak learner with minimum error

Step 15: End for

End

Otsuka-Ochiai Generalized Discriminative Weighted Emphasis boosting technique demonstrated in Algorithm 1 to boost accuracy. Initially, the 'k' number of weak learners is constructed. It analyzes the attack node characteristics using the Otsuka-Ochiai similarity measure. Based on the assessment, attack nodes are correctly classified and identified. Therefore, other normal nodes are revealed for efficient data

transmission. This helps to enhance the delivery and decreases packet loss.

PROPSOED Algorithm2:Merkle–Hellman knapsack Certificateless Signcryption based secure routing

Input: Number of data$d_1, d_2, d_{3,\ldots} d_m$
Output: Increase the security of routing
Begin
Step 1: For each data transmission 'd_i'
Step 2: For each sensor node 'Sn'
Step 3: Generates a Time synchronized Key-pair A and G
Step 4: End for
Step 5: End for
// Signcryption
Step 6: Encrypt the data using receiver public key'τ_c'
Step 7: Generate digital signature 'S' with sender private key
Step 8: Send to the receiver node
// Unsigncryption
Step 9: Generate digital signature S''
Step 10: If the signature ($S = S''$) is valid then
Step 11: Decrypt the data
Step 12: Obtain original data 'd'
Step 13: End if
Step 14: End for
End

Algorithm 2 given above describes the step-by-step processes of Merkle–Hellman knapsack Certificateless Signcryption-based secure routing in WSN. First, private as well as public keys are constructed in all sensor nodes through Time synchronized Key-pair generation. Followed by, generated key pairs employed to implement encryption and a digital signature and sent into the receiver. On the receiver side, the signature is again generated and verified. If the two signatures get matched, then the receiver decrypts the ciphertext and obtains the plaintext. Otherwise, the signature is not valid, the decryption is not performed. Thus the data transmission security is increased and helps to decrease packet loss.

4. Simulation Settings

DWEBMKCS technique, SLGBM [1], FlexCrypt [2], DALSTM [18] is implemented in the NS3 network simulator. 500 sensor nodes considered over a squared area of A^2 (1100 m * 1100 m) via experimental. To perform secure data transmission in WSN, the random waypoint is used as a mobility model. Black hole and gray hole attacks are established and detected by Ad hoc on-demand distance vector routing protocol (AODV) in WSN. 300 seconds have set simulation time and the sensor nodes' speed is varied from 0-20m/s. Table 1 shows various simulation parameters

Table 1 Simulation Parameters

Simulation Parameters	Values
Simulator	NS3
Network area	1100m * 1100m
Number of Sensor nodes	50,100,150,200,250,300,350,400,450,500
Mobility model	Random Waypoint model
Number of data packets	25,50,75,100,125,150,175,200,225,250
Speed of node	0 – 20 m/s
Simulation time	300s
Number of runs	10
Protocol	AODV

5. Results and Discussion

The simulation results of four DWEBMKCS techniques, SLGBM [1], FlexCrypt [2], DALSTM [18] are discussed with respect to performance metrics namely attack detection accuracy, packet delivery ratio, false-positive rate, packet loss rate, as well as an end to end delay. These metrics are described as given below.

Attack detection accuracy: refers as the percentage of sensor nodes accurately identified as a normal or attack node over the total number of nodes. Therefore, the attack detection accuracy is calculated as follows,

$$ACC = \left[\frac{n_{CD}}{n}\right] * 100 \qquad (18)$$

From Eq. (18), ACC denotes an attack detection accuracy, number of sensor nodes has 'n', the number of sensor nodes correctly detected as normal or attack has n_{CD}. It estimated in percentage (%).

Table 2. Attack detection accuracy

Number of sensor nodes	Attack detection accuracy (%)			
	DWEBMKCS	SLGBM	FlexCrypt	DA-LSTM
50	94	88	90	92
100	91	87	89	90
150	94	86	88	89
200	92	85	90	91
250	93	84	87	88
300	94	87	88	89
350	92	85	89	90
400	96	86	90	91
450	95	84	88	89
500	94	85	87	88

Table 2 provides attack detection accuracy for the DWEBMKCS technique, SLGBM [1], FlexCrypt [2] and DALSTM [18]. The number of sensor nodes taken as input ranges from 50 to 500. Let us considers 50 sensor nodes for conducting the experiments in the first iteration. By applying the DWEBMKCS, 94 sensor nodes are correctly classified and the attack detection accuracy is 47% whereas the attack detection accuracy percentage of the existing [1] [2] and [18] are 88%, 90% and 92% respectively. Followed by, various performance results are observed for each method in Table 2. The observed results of the DWEBMKCS technique are compared with the results of existing methods. Comparisons outcomes of attack detection accuracy of DWEBMKCS are comparatively increased by 9% than both [1], [2] and 4% than [18].

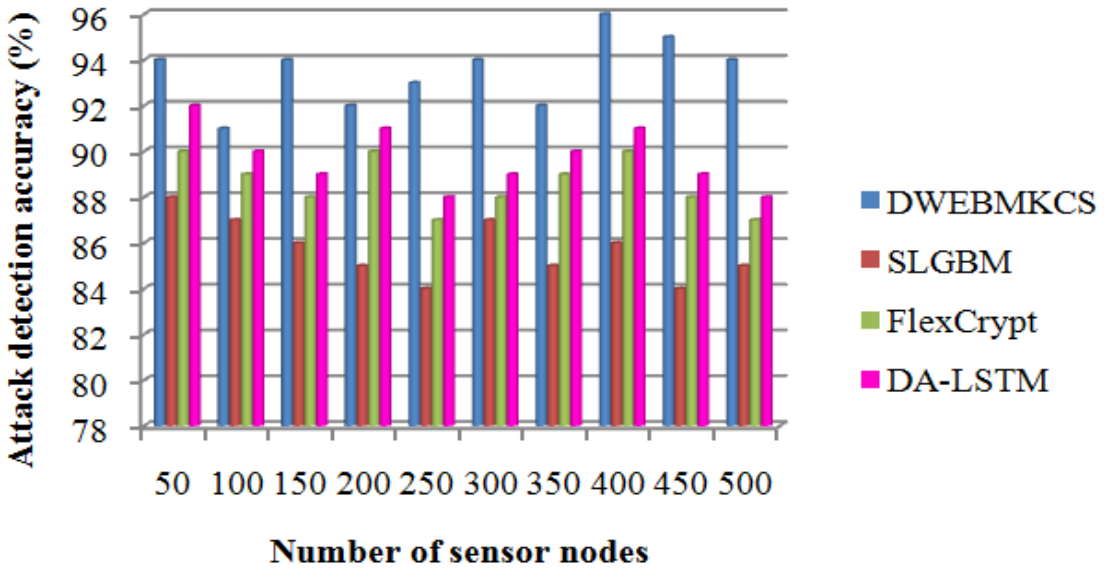

Figure 5 Comparison of attack detection accuracy

Fig. 5 illustrates attack detection accuracy. Four dissimilar colors namely blue, red as well as green, pink represented in Figure 5 by DWEBMKCS technique, SLGBM [1], FlexCrypt [2], DALSTM [18].Contrary to traditional schemes, the proposed DWEBMKCS provides superior performance. The proposed DWEBMKCS technique uses Otsuka-Ochiai Generalized Discriminative Weighted Emphasis boosting technique. The technique analyzes the gray hole and black hole node characteristics and classifies the nodes by constructing the Otsuka-Ochiai Generalized Discriminative classifier to improve the attack detection accuracy.

False-positive rate: It has measured the relation of sensor nodes incorrectly identified 'n_{ICD}' as a normal or attack node. The false positive rate is calculated in terms of percentage (%).

$$FP_{rate} = \left[\frac{n_{ICD}}{n}\right] * 100 \qquad (19)$$

From Eq. (19), FP_{rate} denotes false positive rate. 'n' refers the number of sensor nodes, n_{ICD}denotes the number of sensor nodes incorrectly identified as normal or attack node.

Table 3. False positive rate

Number of sensor nodes	False positive rate (%)			
	DWEBM KCS	SLGBM	Flex Crypt	DA-LSTM
50	6	12	10	8
100	9	13	11	10
150	6	14	12	11
200	8	15	10	9
250	7	16	13	12
300	6	13	12	11
350	8	15	11	10
400	4	14	10	9
450	5	16	12	11
500	6	15	13	12

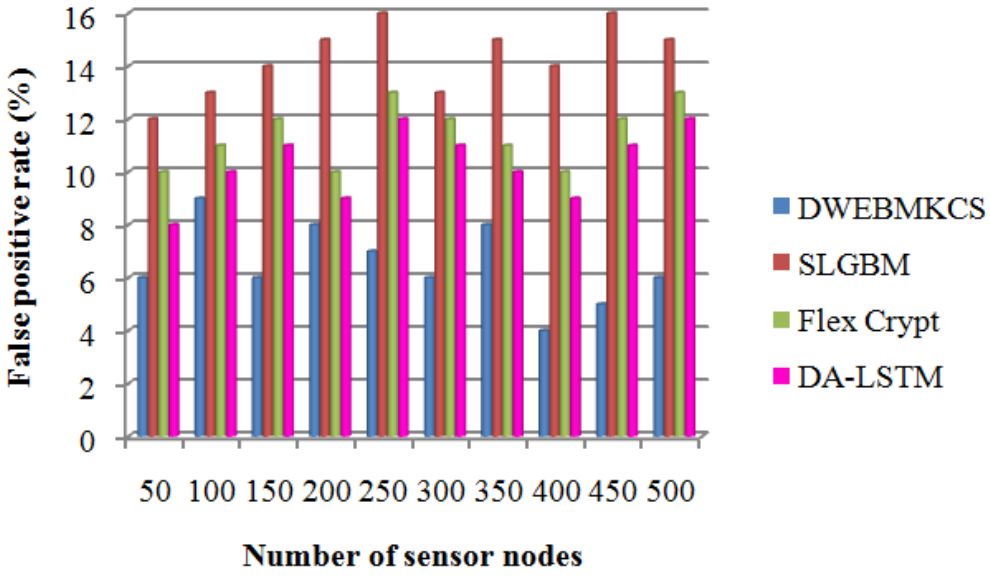

Figure 6 Comparison of False positive rate

Table 3 and Fig. 6 illustrate the performance analysis of the false-positive rate. A number of nodes have taken from 50 to 100. With the consideration of 50 sensor nodes, the false positive rate of DWEBMKCS was found to be 6%. However, the false positive rate of existing SLGBM [1], FlexCrypt [2], DALSTM [18] was found to be 12%, 10%, and 8%. Ten results are observed for each method in Table 3. The false positive rate of the DWEBMKCS is considerably minimized than the other three existing techniques SLGBM [1], FlexCrypt [2], DALSTM [18]. For investigating attack node characteristics, and finding attacks as well as other normal nodes, Otsuka-Ochiai Generalized Discriminative Weighted Emphasis boosting technique constructs weak learners. It aids in minimizing the quadratic error and increases the classification accuracy. False positive rate lessen up to 54%, 42% and 36% when compared to SLGBM [1], FlexCrypt [2], DALSTM [18] respectively.

Packet delivery ratio: It is estimated by the proportion of data packets effectively received on the sink node to the total data packets sent. The Packet delivery ratio is formulated as given below,

$$R_{PD} = \left[\frac{Numberofdata\ packets\ correctly\ received}{Numberofdata\ packets}\right] * 100 \quad (20)$$

Where, R_{PD} denotes a packet delivery ratio.

The packet delivery ratio is measured in terms of percentage (%).

Table 4. Comparison of packet delivery ratio

Number of data packets	Packet delivery ratio (%)			
	DWEBMKCS	**SLGBM**	**FlexCrypt**	**DA-LSTM**
25	92	80	84	88
50	92	84	88	90
75	91	85	87	89
100	93	86	89	91
125	92	85	87	90
150	91	84	86	87
175	90	83	85	86
200	89	84	86	87
225	91	86	88	89
250	90	84	86	88

Data packet delivery ratio reported in Table 4 with data packets as of 25 to 250. Dissimilar data packets utilized to obtain outcome. With DWEBMKCS technique, 92 data packets were profitably received on sink node and the delivery ratio R_{PD}is92%. Whereas, the delivery ratio of three existing methods SLGBM [1], FlexCrypt [2], DALSTM [18] are $80\%, 84\%$ and88%. The remaining runs are carried out to estimate DWEBMKCS technique performances. The observed results of delivery ratio increased up to 8% 5%, and 3% than conventional methods.

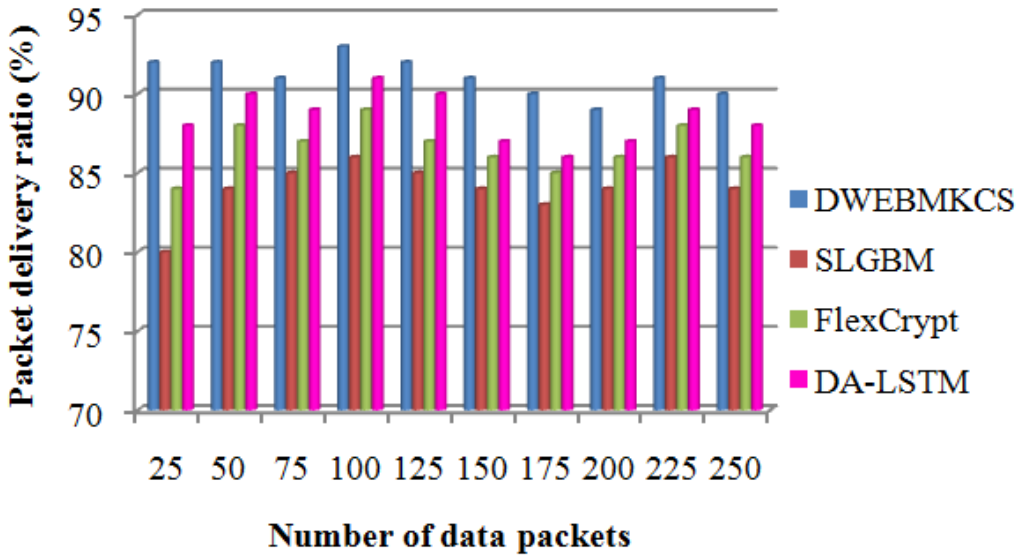

Figure 7. Comparison of packet delivery ratio

The packet delivery ratio is illustrated in Fig. 7. The Horizontal axis is taken as a number of data and the vertical axis is represented as packet ratio outcomes. Contrary to established approaches, $R_{PD}$of the DWEBMKCS technique is higher. Normal neighbouring nodes as of sources towards sink nodes are chosen by the DWEBMKCS technique. Transmitting data was secured via Merkle–Hellman knapsack Certificateless Signcryption with maximum data delivery.

Packet loss rate: It is calculated as the ratio between data packets lost and total data packets sent during information communication. It is calculated in percentage (%).

$$R_{PL} = \left[\frac{Numberofdata\ packets\ lost}{Numberofdata\ packets}\right] * 100 \qquad (21)$$

Where, packet loss rate has R_{PL}.

Table 5. Comparison of Packet loss rate

Number of data packets	Packet loss rate (%)			
	DWEB MKCS	**SLGBM**	**FlexCrypt**	**DA-LSTM**
25	8	20	16	12
50	8	16	12	10
75	9	14	13	11
100	7	14	11	9
125	8	15	13	10
150	9	16	14	13
175	10	17	15	14
200	11	16	14	13
225	9	14	12	11
250	10	16	14	12

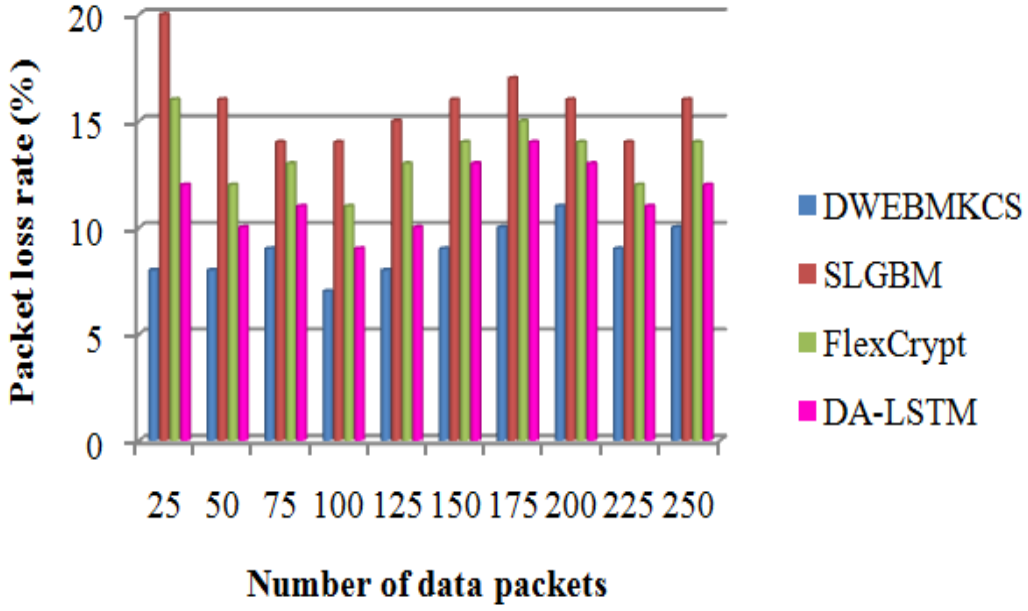

Figure 8. Comparison of Packet loss rate

Table 5 and Fig 8 illustrate the simulation results of packet loss rate. Performance results of R_{PL} using the DWEBMKCS technique is comparatively less. From the figure 8, the horizontal axis indicates number of data packets and vertical axis symbolizes packet loss rate. With the consideration of 25 data packets, the packet loss rate for secure transmission was found to be 8%. However, the data packet loss rate of existing SLGBM [1], and FlexCrypt [2], DALSTM [18] was found to be 20%, 16% and 12%. The observed results indicate that the DWEBMKCS reduces the packet loss rate. After obtaining the ten results, the overall packet loss rate of the DWEBMKCS is compared to the results of existing methods. This is due to identifying the attacker nodes and performing secure data transmission. The proposed DWEBMKCS technique finds the normal node before the data transmission. Since the attacker nodes drop the data packets after selecting the normal node, the Merkle–Hellman knapsack Certificateless Signcryption technique is applied to securely transmit the data packets. The average of ten results indicates that R_{PL} of the DWEBMKCS technique is relatively minimized by 43%, 33% and 22% when compared to existing SLGBM [1], FlexCrypt [2], DALSTM [18] respectively.

End-to-end delay: It has evaluated as difference between the actual arrival time and the observed data packets arrival time at the destination. The overall delay is measured as follows,

$$Delay = [T_{act}] - [T_{obs}] \qquad (22)$$

Where, T_{act} denotes an actual arrival time and 'T_{obs}' indicates an observed arrival time. The overall delay is estimated in terms of milliseconds (ms).

Table 6. End to end delay

Number of sensor nodes	delay (ms)			
	DWEBMKCS	**SLGBM**	**FlexCrypt**	**DA-LSTM**
25	8	14	12	10
50	10	15	13	12

75	11	17	14	13
100	13	18	15	14
125	15	20	17	16
150	17	22	20	18
175	20	24	22	21
200	21	25	23	22
225	22	26	24	23
250	23	28	25	24

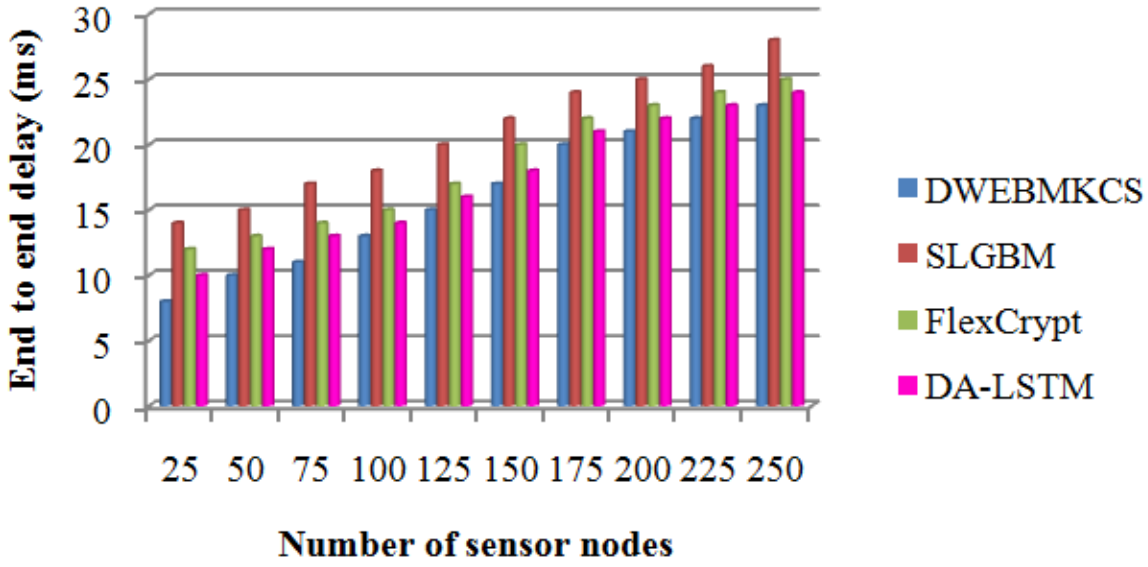

Figure 9. Comparison of end-to-end delay

Table 6 and Fig. 9 portrays End to end delay of data transmission in WSN. As shown in the table and graphical representation, the delays are shown in the increasing mode while increasing data transmission as of the source node. But comparatively, the delay of the DWEBMKCS technique is found to be minimized than the other three existing methods. By applying the DWEBMKCS technique, SLGBM [1], and FlexCrypt [2], DALSTM [18], the delay is measured as$8ms, 14\text{ms}, 12\ ms$ and 10ms respectively. Overall delay is identified by taking the average of ten comparison results. The observed results indicate that the delay is minimized by 25% when compared to [1], 15% when compared to [2], 9% when compared to [18] respectively.

3. **Discussion**

Security is vital for WSN. In research survey, some traditional encryption, decryption and other security protection technologies were utilized for guarantee the security of WSN. In addition, cryptography methods for WSN suffer from the disadvantages of low attack detection accuracy, and high false positive rate owing to the inadequate resources of sensor nodes. The battery power, resources, and computational power is very high and it decreases the network performance. It causes packet loss and delay for the number of nodes. Due to this it can affect the performance of the security of routing. To address the issue, DWEBMKCS is more effective than other baseline methods. Hence, the DWEBMKCS is compared and analyzed with existing SLGBM [1], FlexCrypt [2], and DALSTM [18]. This is according to the capability of

DWEBMKCS to obtain accurate results than the other traditional method. The experimental results reveal that the suggested DWEBMKCS achieves a better performance for secure transmission of the data in WSN.

4. Conclusion

In this paper, the DWEBMKCS technique is proposed for increasing the attack detection accuracy in WSN. First, the DWEBMKCS technique performs the black hole and grey hole attack detection using Otsuka-Ochiai Generalized Discriminative Weighted Emphasis boosting technique. The ensemble technique accurately analyzes the attack characteristics and identifies the normal node for data transmission. Next, to increase security and minimizing packet loss, the DWEBMKCS technique uses the Merkle–Hellman knapsack Certificateless Signcryption scheme. The simulation is conducted to estimate the performance of our DWEBMKCS technique with different performance metrics. The observed results and discussion revealed that the DWEBMKCS technique has considerably improved the attack detection accuracy, and delivery ratio and minimizes loss, and delay.

Table 7 list of notation and descriptions in Equation

Notation	Description
$Sn_1, Sn_2, Sn_3, \ldots Sn_n$	Number of sensor nodes
SN	Sink node
$d_1, d_2, .., d_m$	Data packets
$Nn_1, Nn_2, Nn_3, \ldots Nn_b$	Neighbouring nodes
$\{x_i, Z_i\}$	Training samples sets
x_i	Sensor node
Z_i	Ensemble classification outcomes
$G_1, G_2, G_3, \ldots . G_m$	Linear discriminant classifier
BA_{Sn}	Black hole node behaviour
dps	Data packets sent by previous node
dpd	Data packets dropped
GA_{Sn}	Gray hole attacks sensor nodes
spd	Selective number of packets dropped
φ	Otsuka-Ochiai Correlation coefficient
B_i	Node behaviours
m_j	Mean
Z	Output of ensemble classifier
$w_i(Sn)$	Linear combination of of weak learners output
β	Weight initialized
E	Quadratic error of class
Ω	Weighting factor
c_1, c_2	Classes
ϑ	Quadratic error

$r_1, r_2, r_3, \ldots . r_n$	Random sequence of positive integers
Q	Select the random integer
A	Public key
G	Private key
τ_c	Ciphertext of the data
ϑ_i	Binary string
a_i	Receiver's public key
S	Signature of data
G_s	Senders private key
d	Original data
B_r	Receiver public key
S''	New signature of data
$X_i = \{\}$	Empty set of index list
X_i	Set of index list
ACC	Attack detection accuracy
n	Number of sensor nodes
n_{CD}	Number of sensor nodes correctly detected as normal or attack
FP_{rate}	False positive rate
n_{ICD}	Number of sensor nodes incorrectly identified as normal or attack node
R_{PD}	Packet delivery ratio
R_{PL}	Packet loss rate
T_{act}	Actual arrival time
T_{obs}	Observed arrival time

Conflicts of interest

The authors declare no conflict of interest.

Author contributions

The paper conceptualization, methodology, software, validation, formal analysis, investigation, resources, data curation, writing—original draft preparation, writing—review and editing, visualization, have been done by 1st author. The supervision and project administration, have been done by 2nd author.

References

[1]S. Jiang, J. Zhao and X. Xu, "SLGBM: An Intrusion Detection Mechanism for Wireless Sensor Networks in Smart Environments", *IEEE Access*, Vol. 8, pp. 169548 – 169558, 2020

[2]O.A. Khashan, R. Ahmad and N. M. Khafajah, "An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks", *Ad Hoc Networks, Elsevier*, Vol. 115, pp. 1-14, 2021

[3]M. Mathapati, T. S. Kumaran, A. Muruganandham and M. Mathivanan, "Secure routing scheme with multi-dimensional trust evaluation for wireless sensor network", *Journal of Ambient Intelligence and Humanized Computing, Springer*, Vol. 12, pp. 6047–6055, 2021

[4]P. Gite, K.Chouhan, K. M. Krishna, C.K. Nayak, M. Soni and A. Shrivastava, "ML Based Intrusion Detection Scheme for various types of attacks in a WSN using C4.5 and CART classifiers", *Materials Today: Proceedings, Elsevier,* pp. 1-8, 2021.

[5]Q. Ye, Y. Wang, M. Xi and Y. Tang, "Recognition of grey hole attacks in wireless sensornetworks using fuzzy logic in IoT", *Transaction on Emerging*

Telecommunication Technology, Wiley, Vol. 31, No. 12, pp. 1-16, 2020

[6]C. A. Subasini, S. P. Karuppiah, Adlin Sheeba and S. Padmakala, "Developing an attack detection framework for wirelesssensor network-based healthcare applications using hybridconvolutional neural network", *Transaction on Emerging Telecommunication Technology, Wiley,* Vol. 32, No. 11, pp. 1-17, 2021

[7]Q.Shi, L. Qin, Y. Ding, B. Xie, J. Zheng, and L. Song, "Information-Aware Secure Routing in WirelessSensor Networks", *Sensors*, Vol.20, No. 1, pp. 1-21, 2020

[8]B. Pang, Z. Teng, H. Sun, C. Du, M. Li and W. Zhu, "A Malicious Node Detection Strategy Based on Fuzzy Trust Model and the ABC Algorithm in Wireless Sensor Network", *IEEE Wireless Communications Letters,* Vol. 10, No. 8, pp. 1613 – 1617, 2021

[9]X. Luo, Y. Chen, M. Li, Q. Luo, K. Xue, S. Liu and L. Chen, "CREDND: A Novel Secure Neighbor Discovery Algorithm for Wormhole Attack", *IEEE Access*, Vol. 7, pp.18194 – 18205, 2019

[10]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

[11]S. Ali, A Humaria, M S. Ramzan, I. Khan, S. MSaqlain, A. Ghani, J. Zakia and B. A. Alzahrani, "An efficient cryptographic techniqueusing modified Diffie–Hellman inwireless sensor network", *International Journal of Distributed Sensor Networks*, Vol. 16, No. 6, pp. 1-24, 2020

[12] M. Alotaibi, "Security to wireless sensor networks against malicious attacks using Hamming residue method", *EURASIP Journal on Wireless Communications and Networking*, Vol. 2019, pp. 1-7, 2019

[13] C. Cao, Y. Tang, D. Huang, W. Gan, and C. Zhang, "IIBE: An Improved Identity-Based Encryption Algorithm forWSN Security", *Security and Communication Networks, Hindawi,* Vol. 2021, pp. 1-8, 2021

[14]G. Mehmood, M. S. Khan, A. Waheed, M. Zareei, M. Fayaz, T. Sadad, N.Kama,and A. Azm, "An Efficient and Secure Session Key Management Scheme inWireless Sensor Network", *Complexity, Hindawi*, Vol. 2021, pp.1-10, 2021

[15]T. A. Alghamdi, "Convolutional technique for enhancing security in wireless sensor networks against malicious nodes", *Human-centric Computing and Information Sciences, Springer*, Vol. 9, pp. 1-10, 2019

[16]H. A. Babaeer and S. A. Al-Ahmadi, "Efficient and Secure Data Transmission and Sinkhole Detection in a Multi-Clustering Wireless Sensor Network Based on Homomorphic Encryption and Watermarking", *IEEE Access*, Vol. 8, pp.92098 – 92109, 2020

[17]Y. Xie, X. Li, S. Zhang and Y. Li, "iCLAS: An Improved Certificateless Aggregate Signature Scheme for Healthcare Wireless Sensor Networks", *IEEE Access*, Vol. 7, pp.15170 – 15182, 2019

[18] C. S. Reddy and G. Narsimha, "Secure Optimized Routing and Data Transmission in Wireless Sensor Networks with Elliptic Curve Cryptography", *International Journal of Intelligent Engineering Systems*, Vol.15, No.4, pp. 1-13, 2022

[19] G. Halidoddi and R.Pandu, "Secured Data Transmission Using Multi-Objective Trust Based Bat Optimization Algorithm and Enhanced Homomorphic Cryptosystem for WSN", *International Journal of Intelligent Engineering Systems,* Vol.15, No.1, 2022, pp. 1-11, 2021

[20] R. A. Kumar and R. Kannan, "Region Based Secured Data Transmission Protocol for Wireless Sensor Network", *International Journal of Computer Networks and Applications (IJCNA),* Vol.9, No.5, 2022, pp. 1-12, 2022

[21] L. Zhou, M. Kang and W. Chen, "Lightweight Security Transmission in Wireless Sensor Networks through Information Hiding and Data Flipping", Sensors, MDPI, Vol.22, No.3, pp. 1-16, 2022