Journal of Theoretical and Applied Information Technology
30th June 2022. Vol.100. No 12
© 2022 Little Lion Scientific

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

TVERSKY INDEXIVE CRAMER–SHOUP CRYPTOGRAPHY BASED DEEP STRUCTURED BELIEF NEURAL LEARNING FOR SECURED ROUTING IN MANET

Mrs.R.NAVAMANI[1], Dr.N.ELAMATHI[2]
[1]Ph.D Research Scholar (PT), Department of Computer Science, Periyar University, Salem, India
[2]Assistant Professor & Head, Department of Computer Science, Trinity College For Women, Namakkal, India
E-mail: [1]navamanikathir@gmail.com, [2] kavimathipriyan@gmail.com

ABSTRACT

A secure routing is a significant concern due to its self-organizing and cooperative nature, capable of independent process, rapid changing topologies, limited physical security and so on. With the routing being a critical aspect for MANETs, existing routing protocols are not sufficient for security constraints. In this paper, a novel routing algorithm called a Tversky Indexive Cramer–Shoup Cryptography based Deep Structured Belief Neural Learning (TICSC-DSBNL) technique is introduced with security and higher data confidentiality in MANET. The TICSC-DSBNL technique comprises one input layer, three hidden layers and one output layer. The number of mobile nodes is taken as input in the input layer and sends the mobile node to the hidden layer 1. For every mobile node in the hidden layer 1, the trust value is calculated to identify the node as normal node or malicious node using Tversky Similarity index. The index is used to find the similarity between mobile nodes for classifying the node as normal node or malicious node. After that, the normal nodes are given to the hidden layer 2. In that layer, a route path between the nodes gets established and selects the shortest route path. In third hidden layer, the Cramer–Shoup cryptosystem is applied for encryption and decryption to perform secure routing with higher confidentiality in MANET. Simulation is conducted in with different performance metrics such as packet delivery ratio, packet drop rate, and delay, throughput, and data confidentiality rate with respect to the number of data packets. The discussed results indicates that the proposed TICSC-DSBNL technique improves the performance of secure routing with higher delivery ratio, data confidentiality with lesser delay as well as packet drop than the state-of-the-art methods.

***Keywords**: MANET, Secure Routing, Deep Structured Belief Neural Learning, Tversky Similarity Index, Cramer–Shoup Cryptosystem.*

1. INTRODUCTION

A MANET is a dynamic and infrastructure-less networks includes a set of wireless nodes that linked with one another through the wireless connection. Due to the dynamic nature, security is a important concern in MANET since the network is vulnerable to several attacks during the communication. Therefore an efficient technique is required to improve the security as well as enhance the higher confidentiality.

A Cluster-based Key Management Scheme for Secured Multipath Routing (CKMSMPR) scheme was developed in [1] to enhance the secure data transmission using the Diffie-Hellman method of key exchange and elliptic curve cryptography. But the cryptography technique was more complex for improving security and data confidentiality.

An optimal Energy-Efficient Routing Protocol (EERP) with the signcryption (optimal EERP-signcryption) algorithm was developed in [2] for secure and reliable data transmission. The EERP was developed for clustering the mobile nodes. Then, the Modified Discrete Particle Swarm Optimization (MDPSO) was applied for CH selection. For enhanced the security of data transmission, a signcryption algorithm was introduced. The designed algorithm enhances overall efficiency and confidentiality but the multi-key encryption technique was not applied to achieve reliable security in the MANET.

A Multiplicative Diffie Hellman key exchange (MDKE) algorithm was introduced in [3] for enhancing the security. But the algorithm failed to concentrate on trust evaluation to further improve the MANE security. A trust-based secure and energy-aware (T-SEA) routing protocol was designed in [4] for detection of black/gray hole nodes. But the cryptographic technique was not applied to enhance the security.

An Evolutionary Self Self-Cooperative Trust (ESCT) technique was developed in [5] to prevent the different routing disruption attacks. The designed technique minimizes the delay but the packet loss rate was not minimized. An efficient Random Repeat Trust Computational method was designed in [6] for enhancing the security based on various trust evaluation. But the method failed to achieve higher delivery ratio.

A novel Privacy-Preserving History-Based (PPHB) routing method was introduced in [7] to increase the message delivery and minimize the drop. But the higher throughput was not achieved. A novel trust and fuzzy cluster-based dynamic secure routing algorithm were developed in [8] for enhancing the security. The algorithm increases the packet delivery and minimized the delay but it failed to perform the effective communication and coordination among the nodes.

A simple dual-key method was developed in [9] using fully homomorphic encryption for improving the privacy of data transmission. But the method failed to improve data confidentiality. A novel trust-based energy-aware routing (TEAR) method was introduced in [10] for providing the efficient security of data transmission. However, the performance of delay was not reduced.

The major contribution of the TICSC-DSBNL technique is summarized as given below,

- To improve the security of data routing in MANET, a TICSC-DSBNL technique is introduced based on Cramer–Shoup Cryptography based deep structured belief neural learning.
- A Tversky Similarity index is applied in the hidden layer of deep structured belief neural learning to identify the normal or malicious node based on the trust value in the hidden layer.
- To improve the secure data routing and minimize the packet drop, a novel Cramer–Shoup Cryptography is applied for key generation, encryption and decryption. Time based pseudo- randomness key generation is performed to generate the private and public key for each normal node in the network. The sender node encrypts the data packets and sends them to the receiver. The authorized receiver gets the original data through the decryption process. This process increases the security of data delivery and enhances confidentiality.
- The extensive simulation is carried out to measure the performance of the TICSC-DSBNL technique and other related approaches. The simulation result illustrates that our TICSC-DSBNL technique provides improved performance.

1.1 Organization of the paper

The structure of the article is organized as follows. Section 2 briefly describes the proposed methodology TICSC-DSBNL for secure routing in MANET. Section 3 provides information on the simulation settings. In section 4, the simulation outcomes and comparative analysis are presented using various performance metrics. In section 5, the related works of secure routing are discussed. Finally, section 6 concludes the paper.

Methodology

With the number of mobile nodes deployed in the MANET, a secure routing is a new paradigm of wireless communication due to its high dynamics. A MANET is an autonomous system of set of mobile routers and nodes which are connected by wireless links. Routing security is essential and it needed to improve the communication and protection of data from the attacks. Based on this motivation, the deep learning-based technique called TICSC-DSBNL technique is introduced in this paper.

The MANET is organized in a directed graph $g = (v, e)$, where 'v' represents a vertex i.e. mobile nodes $\{Mn_1, Mn_2, Mn_3, \dots . Mn_n\}$ distributed in a squared area $m * m$' and 'e' represents the link between the nodes within the communication range 'T_c'. The wireless network begins the source node 'Sn' and transmits data packets $p_1, p_2, p_3 \dots . . p_m$ to the destination node 'Dn' via the neighboring node 'Nn' in a secure manner. The source node finds the neighboring node which having maximum trust value.

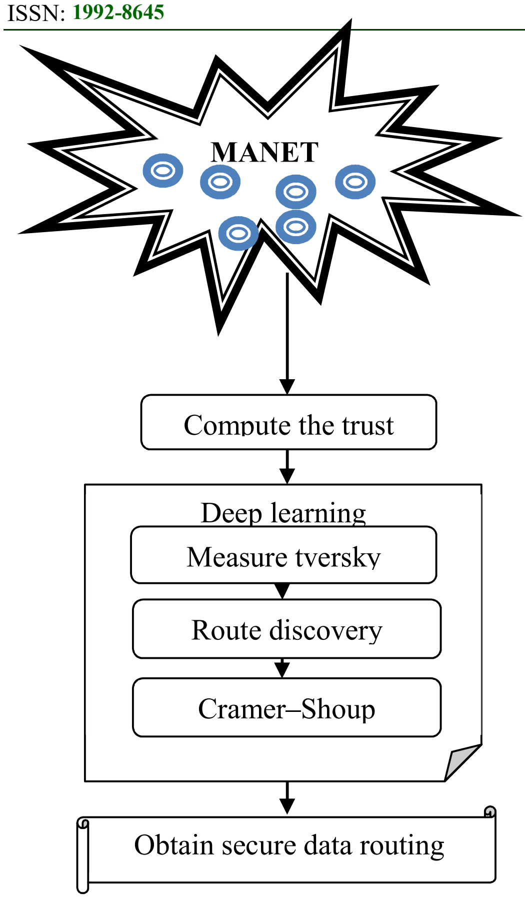

Figure 1 Architecture Diagram Of Proposed TICSC-DSBNL Technique

Figure 1 given above illustrates the architecture diagram of proposed TICSC-DSBNL technique. The TICSC-DSBNL technique uses the deep structured belief neural network to obtain the secure routing in MANET. As shown in figure 1, for each node in the network, the trust value is calculated. Then the Tversky similarity index is applied to find the normal or malicious node based on the trust value. With the selected normal node, the secured data transmission is performed using Cramer–Shoup cryptography.

The deep structured belief neural learning consists of only three layers such as one input layer, three hidden layers, and one output layer.

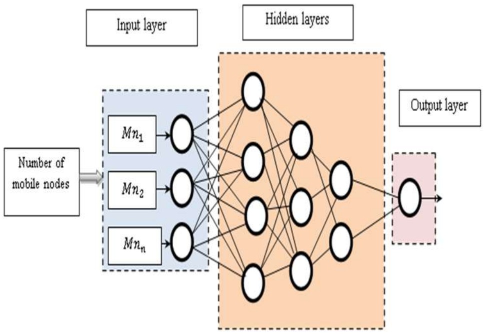

Figure 2 construction of the deep structured belief neural learning

Figure 2 given above illustrates the deep structured belief neural learning consists of the input layer, three hidden layers, and one output layer. The network consists of neurons like the nodes that are connected from one layer to another layer for constructing the whole network. Here the feed-forward network constructed to transfer the input from the previous layer into the consecutive layer hence the architecture also called as layer by layer method. The activity of the neuron at the input layer of the deep neural network is defined as follows,

$$Q(t) = d + \sum_{i=1}^{n} Mn_i(t) * k_1 \qquad (1)$$

Where, $Q(t)$ indicates the activity of the neuron, '$Mn_i(t)$' denotes an input i.e. number of mobile nodes '$Mn_1, Mn_2, Mn_3, \ldots . Mn_n$', '$k_1$' indicates a weight to strengthen the connections between the layers, 'd' denotes a bias and it simply stores the integer value is 1. Then the input is moved into the first hidden layer. In the first hidden layer, the node trust value is calculated to find the normal or malicious node. The trust values of the mobile nodes are measured as the ratio of a number of data packets correctly forwarded by the particular node to the ratio of a number of data packets forwarded. Therefore, the trust is calculated as given below,

$$T_{Mn} = \left[\frac{Number\ of\ packets\ correctly\ forwarded}{n}\right] \qquad (2)$$

Where, T_{Mn} represents a trust of the mobile nodes, 'n' symbolizes a number of data packets forwarded. Based on the trust value, the normal or malicious nodes are determined based on the Tversky index.

The Tversky correlative index is used to measure the similarity between the trust value of the mobile nodes and the trust value of the normal node. Therefore, the similarity index is measured as given below,

$$R = \frac{T_{Mn} \cap T_N}{p(T_{Mn} \Delta T_N) + q\,(T_{Mn} \cap T_N)} \tag{3}$$

From (4), 'R' denotes a similarity coefficient, T_{Mn} denotes a trust value of the mobile nodes, T_N denotes a trust value of the normal node, $T_{Mn} \cap T_N$ denotes a mutual dependence between the nodes trust value, $T_{Mn} \Delta T_N$ indicates a variance between the node trust value, from (3) p and q denotes parameters of the Tversky index $(u, v \geq 0)$. The coefficient provides the output ranges value between 0 or 1. If both the trust values are matched, then the node is said to a normal node. Otherwise, the mobile node is said to be malicious. Then the normal nodes are forwards to a hidden layer 2 for determining the route paths.

- **Route discovery**

After classifying the normal or malicious nodes, the route paths are established between the normal nodes for secure data transmission using two control messages namely route request $(\mathrm{req_r})$ and route reply $(\mathrm{rep_r})$.

$$Sn \overset{\mathrm{req_r}}{\Longrightarrow} \sum_{i=1}^{n}(Nn_i) \overset{\mathrm{req_r}}{\Longrightarrow} Dn \tag{4}$$

Where, Sn is the source node, $\mathrm{req_r}$ indicates a route request, Nn_i denotes a neighboring node, Dn is the destination node. Then the receiver node sent a reply to the source node through the intermediate neighboring nodes.

$$Sn \overset{\mathrm{rep_r}}{\Longleftarrow} \sum_{i=1}^{n}(Nn_i) \overset{\mathrm{rep_r}}{\Longleftarrow} Dn \tag{5}$$

Where, '$\mathrm{rep_r}$' denotes a reply message, Dn denotes a destination, Nn_i symbolizes neighboring nodes, Sn denotes a source node. Based on the control message distribution, multiple paths are established between source and destination. Among the multiple paths, the shortest path is selected for secure routing in MANET with minimum delay.

- **Cramer–Shoup system for secure routing in MANET.**

Finally, the secure data transmission between the nodes is performed using Cramer–Shoup cryptosystem in the third hidden layer. A Cramer–Shoup cryptography is an asymmetric key encryption algorithm and it efficient for protecting the data from the attack than the standard cryptographic techniques. The cryptography algorithm comprises three major processes namely key generation, encryption, and decryption.

- **Time-based pseudo- randomness key generation**

The proposed Cramer–Shoup system performs the key pair generation to perform encryption and decryption of data packets before the data transmission. The proposed cryptosystem performs the time-based pseudo- randomness key generation for each mobile node in the routing process. It is a time based key pair generation. It means that the generated private and public keys of mobile nodes are valid only for a particular time. Once the time is exhausted, keys are disabled and the algorithm creates a new key for the next session. This helps to avoid the attacks for hacking the keys during the data communication between the nodes.

Let us consider the cyclic group 'g'and randomly chose the two numbers $(a, b) \in g$ and the five pseudo-random values $(c, e, f, h, p) \in Z$ where Z denotes an integer value. Then the key generation is formulated as given below,

$$W = a^c\, b^e \tag{6}$$

$$B = a^f\, b^h \tag{7}$$

$$Y = a^p \tag{8}$$

From (6), (7), (8), the private key of the node is $K_r = (c, e, f, h, p)$ and the public key of the node is $K_b = (a, b, W, B, Y)$. The public keys are distributed and the private key of the node is kept secret. These generated key pair is valid only for a particular time.

- **Encryption**

After the key generation, the proposed technique performs encryption before the data transmission. Encryption is the process of converting the original data i.e. plaintext into ciphertext. The proposed cryptography is an asymmetric key algorithm it means that the public key used for encryption and the private key used for decryption. In other words, the different keys (i.e. related pair of keys) are used for encryption as well as decryption. This helps to improve the security of data packet transmission from source to destination and reduce packet loss.

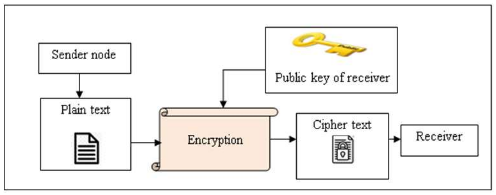

Figure 3 Block Diagram of Encryption

Figure 3 illustrates the block diagram of encryption to improve the secure data transmission from sender to receiver. The sender to node performs encryption with the receiver public key.

Let us consider the given input message ‘m ‘$\in g$ and select the random value ‘r’

$$\left.\begin{array}{c} v_1 = a^r, v_2 = b^r, \\ t = Y^r m \\ \varphi = W^r\, B^{r\delta} \\ \delta = H(v_1, v_2, e) \end{array}\right\} \quad (9)$$

Where, H denotes a one-way hash function, a, b, W, B, Y denotes a public key of the receiver. Then the ciphertext (T) of the given message ‘m’ is given below,

$$T = (v_1, v_2, t, \varphi) \quad (10)$$

Then the ciphertext of the data is sent to the receiver node.

➢ Decryption

Finally, the proposed technique performs the decryption at the receiver end to obtain the plaintext using the receiver's private key.

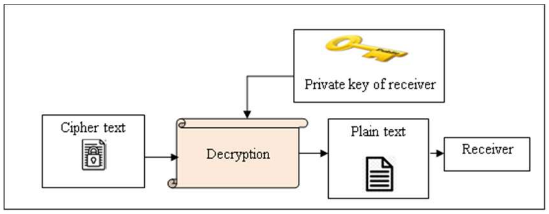

Figure 4 Block Diagram of Decryption

Figure 4 illustrates the block diagram of the decryption to obtain the original text with higher security. Before the decryption, the receiver calculated as follows,

$$\beta = H(v_1, v_2, t) \quad (11)$$

Then the algorithm verifies that = ${v_1}^c, {v_2}^e\, ({v_1}^f, {v_2}^h)^\beta$. If it is satisfied, then the receiver decrypts the data otherwise it is rejected. The decryption is performed as given below,

$$m = \frac{t}{{v_1}^p} \quad (12)$$

Where, m denotes a plaintext, t denotes a ciphertext, ‘p’ denotes a private key of receiver. In this way, secure communication between sender and receiver is obtained. The algorithmic process of the proposed technique is described as given below,

Algorithm 1: Tversky Indexive Cramer–Shoup Cryptography based deep structured belief neural learning

```
Input: Number of mobile nodes $Mn_1, Mn_2, Mn_3, \ldots . Mn_n$, data packets $p_1, p_2, p_3 \ldots . . p_m$
Output: Increase secure routing
Begin
    Collect the number of mobile nodes ‘$Mn_1, Mn_2, Mn_3, \ldots . Mn_n$ at input layer
// hidden layer 1 (node classification)
    for each ‘$Mn_i$’
        Calculate trust value ‘$T_{Mn}$’
        Measure the similarity ‘$R$’
        If $(R = 1)$ then
            Node is said to be a normal
        Else
            Node is said to be a malicious
        End if
    End for
// hidden layer 2 (route discovery)
    For each normal node
        Establishes the route paths based on $\mathrm{req_r}$ and route reply $\mathrm{rep_r}$
    End for
// hidden layer 3 (secure routing)
Time based pseudo- randomness key generation
    For each mobile node ‘$Mn_i$’
        The base station generates a pair of keys $(K_b, K_r)$
    End for
// Encryption
    For each data packet ‘$p_i$’
        Encrypt the data $T = (v_1, v_2, t, \varphi)$ using receiver public key ‘$K_b$’
        Source node sends the ciphertext to the receiver node
    End for
// Decryption
    For each ciphertext
        If ( $\varphi = v_1{}^c, v_2{}^e\,(v_1{}^f, v_2{}^h)^\beta$ ) then
            The receiver performs decryption and obtains the original data '$m$'
        Else if
            Decryption is rejected
        End if
    End for
End
```

Algorithm 1 given above illustrates the step by step process of Tversky Indexive Cramer–Shoup Cryptography based deep structured belief neural learning for secure routing in MANET. In the input layer, the numbers of nodes are taken as input. In the first hidden layer, the trust value of each mobile node is measured. In that layer, the similarities between the nodes are measured for finding the normal or malicious node. With the normal nodes, the route paths are established in the second hidden layer. In the third hidden layer, the Cramer–Shoup Cryptography is applied to perform the secure data communication between sender and receiver. Finally, the secure data transmission is performed at the output layer. This helps to improve the delivery ratio and minimizes the packet drop.

3. SIMULATION SETUP

In this section, the simulation of the TICSC-DSBNL technique and existing methods namely CKMSMPR [1], Optimal EERP-Signcryption [2] are implemented using the NS2.34 network simulator. In order to perform the simulation, 500 mobile nodes are randomly deployed in a squared area ($1100\,m * 1100\,m$) in MANET. A Random Waypoint model is used as a mobility model for secured routing. The mobile nodes are moved with a speed of 0 to 20m/sec. The simulation time is set as 300 sec. The Dynamic Source Routing (DSR) protocol is implemented for secure routing in MANET. The simulation parameters with the values are listed in Table 1.

Table 1 Simulation Parameters Settings

Simulation parameters	Values
Network Simulator	NS2.34
Simulation area	1100 m * 1100 m
Number of mobile nodes	50,100,150,200,250,300,350,400,450,500
Number of data packets	25,50,75,100,125,150,175,200,225,250
Mobility model	Random Waypoint model
Nodes speed	0 – 20 m/s
Simulation time	300sec
Routing Protocol	DSR
Number of runs	10

4. RESULTS AND DISCUSSION

Performance analysis of the TICSC-DSBNL technique and the conventional routing methods namely CKMSMPR [1], Optimal EERP-Signcryption [2] are discussed with different metrics such as packet delivery ratio, packet drop rate, delay, throughput, and data confidentiality rate. The parameters are described as given below,

Packet delivery ratio: It is defined as the number of data packets that are successfully delivered at the destination to the total number of (i.e. no. of) data packets. The packet delivery ratio is mathematically formulated as given below,

$$Ratio_{PD} = \left[\frac{No.of\ packe\ \ received}{No.of\ packets}\right] * 100 \qquad (13)$$

Where, $Ratio_{PD}$ symbolizes the packet delivery ratio is measured in the unit of percentage (%).

Packet drop rate: It is measured as the ratio of number of data packets dropped during the transmission from the total number of data packets. The formula for calculating the packet drop rate is given below,

$$Rate_{PD} = \left[\frac{No.of\ packet\ dropped}{No.of\ packets}\right] * 100 \qquad (14)$$

Where $Rate_{PD}$ represents the packet drop rate and it is measured in terms of percentage (%).

End to end delay: It is defined as the difference between the actual arrival time of the packet and the expected arrival time of the data packets. The overall end to end delay is expressed as given below,

$$D_{ETE} = [T_{actual}] - [T_{ex}] \qquad (15)$$

Where, 'D_{ETE}' represents the end to end delay, T_{ex} indicates an expected arrival time and 'T_{actual}' indicates the actual arrival time. The overall delay is measured in terms of milliseconds (ms).

Throughput: It is measured as the amount of data packets received at the destination at a particular time. The throughput is measured as follows,

$$T_{put} = \left(\frac{size\ of\ packets\ received(bits)}{time\ (sec)}\right) \qquad (16)$$

Where, 'T_{put}' represents the throughput and it is measured in terms of bits per second (bps).

Confidentiality rate: It is the security parameter and it measured as the ratio of the number of data packets only accessed by the authorized receiver. The formula is expressed as given below,

$$DCR = \left(\frac{p_{AN}}{No.of\ packets}\right) * 100 \qquad (17)$$

Where DCR denotes a data confidentiality rate, p_{AN} denotes the number of data packets received by the authorized receiver. The confidentiality rate is measured in terms of percentage (%).

Table 2 Comparison Of Packet Delivery Ratio And Packet Drop Rate

No. of data packets	Packet delivery ratio (%)			Packet drop rate (%)		
	TICSC-DSBNL	CKMSMPR	Optimal EERP-	TICSC-DSBNL	CKMSMPR	Optimal EERP-
25	96	88	84	4	12	16
50	96	86	84	4	14	16
75	97	89	87	3	11	13
100	94	87	84	6	13	16
125	95	88	85	5	12	15
150	96	89	86	4	11	14
175	94	88	87	6	12	13
200	93	87	85	7	13	15
225	95	89	87	5	11	13
250	96	87	86	4	13	14

Table 1 describes the simulation results of the packet delivery ratio and packet drop rate using three different methods namely TICSC-DSBNL technique and the conventional routing methods namely CKMSMPR [1], Optimal EERP-Signcryption [2]. The numbers of data packets are taken as input to calculate the packet delivery ratio as well as packet drop rate. For each method, ten runs are carried out with a different number of data packets. The observed results demonstrate that the TICSC-DSBNL technique increases the packet delivery ratio and minimizes the packet drop. Let us consider the 25 data packets transmitted from the source node. By applying the TICSC-DSBNL technique, 24 data packets are successfully delivered and 1 data packet gets dropped. The packet delivery ratio of the TICSC-DSBNL technique is 96% and the drop rate is 4%. Whereas, the packet delivery ratio of CKMSMPR [1] is 88% and the drop rate is 12% and the packet delivery ratio and drop rate of Optimal EERP-Signcryption [2] is 84%, and 16% using [2]. The ten different runs are carried out for each method. The overall observed results of the TICSC-DSBNL technique are compared to existing results. Similarly, various runs are carried out with different counts of data packets. The average of ten results indicates that the packet delivery ratio of the TICSC-DSBNL technique is considerably increased by 8% when compared to [1] and 11% when compared to [2] respectively. In addition, the average results of packet drop rate of TICSC-DSBNL technique is considerably reduced by 61% and 67% when compared to existing CKMSMPR [1] and Optimal EERP-Signcryption [2] respectively.

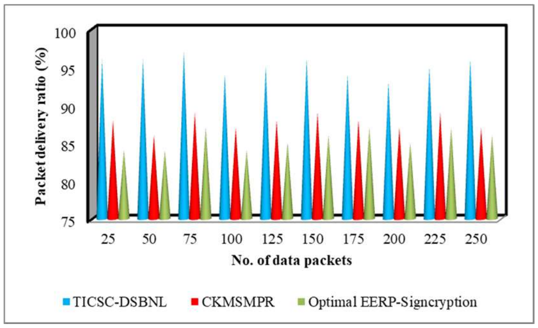

Figure 5 Performance Analysis Of Packet Delivery Ratio

Figure 5 depicts the performance results of packet delivery ratio with respect to a number of data taken in the range from 25 to 250. As revealed in the above graph, the number of data is taken on the horizontal axis and the different results of packet delivery ratio are obtained at the vertical axis. The graphical results illustrate that the proposed TICSC-DSBNL technique achieves a higher delivery ratio than the conventional methods namely CKMSMPR [1], Optimal EERP-Signcryption [2]. This improvement is achieved by classifying the normal node or malicious node using the Tversky Similarity index. The Similarity Index is measured between the mobile nodes and classified as a normal node or malicious node based on the trust value. After that, the secure data transmission is performed using Cramer–Shoup cryptosystem is applied to improve the data delivery between sender and receiver.

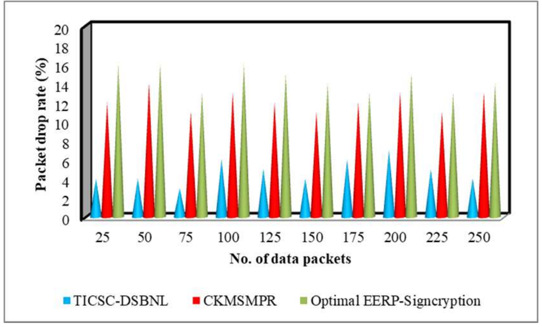

Figure 6 Performance Analysis Of Packet Drop Rate

The comparative results analysis of the packet drop rate of three routing techniques with respect to the number of data packets is shown in figure 6. The graphical results inferred that the packet drop rate of the TICSC-DSBNL technique is minimized than the conventional routing techniques. This is because of selecting the normal node for data transmission. Besides, the Cramer–Shoup cryptosystem encrypts the data packets before the transmission. The authorized receiver gets the original data and it minimizes the packet drop.

Table 3 performance analysis of end to end delay

No. of data packets	End to end delay (ms)		
	TICSC-DSBNL	CKMSMPR	Optimal EERP-Signcryption
25	7	11	13
50	8	12	14
75	9	14	16
100	10	15	17
125	11	16	18
150	13	18	20
175	14	20	21
200	15	21	23
225	17	22	24
250	19	24	26

Table 3 reports the performance results of end to end delay versus a number of data packets taken in the ranges from 25 to 250. The observed simulation results illustrate that the number of data packets is directionally proportional to the delay. In other words, while increasing the number of data packets, the delay gets increased. But comparatively the TICSC-DSBNL technique consumes lesser delay of data delivery. Let us consider the '25 data packets taken as input, the TICSC-DSBNL technique consumes '7ms' of delay. Similarly, the delay of the other two existing methods namely CKMSMPR [1] and Optimal EERP-Signcryption [2] consumes '11ms' and '13ms' of delay to deliver the data packets. There are ten different results are obtained for each method. The overall results indicate that the TICSC-DSBNL technique minimizes the end to end delay by 30% and 37% when compared to existing methods.

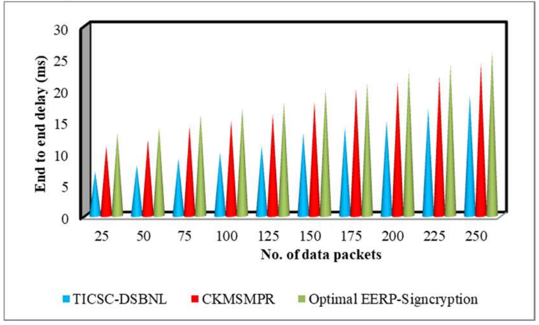

Figure 7 Performance Analysis Of End To End Delay

Figure 7 given above illustrates the end to end delay of data transmission from source to destination. From the figure, it is noted that the end to end delay is directly proportional to the number of data packets. But the TICSC-DSBNL technique reduces the delay than the other two conventional routing techniques. The reason behind the reduced end to end delay was due to the incorporation of shortest route path discovery from source to destination. By distributing the two control message via the normal mobile nodes, the multiple route paths are established. The data packets are transmitted along the shortest route path resulting it minimizes the delay.

Table 4 Comparison Of Throughput

Data packet size (KB)	Throughput (bps)		
	TICSC-DSBNL	CKMSMPR	Optimal EERP-Signcryption
15	225	205	190
30	330	320	300
45	400	360	340
60	485	455	430
75	560	533	500
90	690	600	580
105	795	723	708
120	915	850	825
135	1080	980	955
150	1310	1240	1180

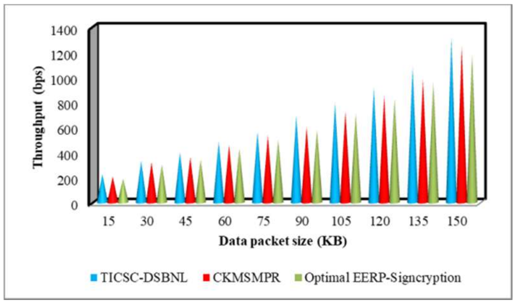

Figure 8 Performance Analysis Of Throughput

Table 4 and Figure 8 depict the impact of throughput with respect to the size of data packets taken in the ranges from 15KB to 150KB. From the figure, it is illustrative that the throughput is in the increasing trend while increasing the size of the data packets. Besides, for experimentation, the 10 iterations are used and hence a fair comparison is said to be performed for all three routing methods. The graphical results demonstrate that the throughput is found to be increased using the TICSC-DSBNL technique when compared to [1] and [2]. This significant improvement is achieved by selecting the shortest route path from source to destination.

Let us consider $10KB$ sizes of data packets and 225 bits of the data packets are successfully delivered at the destination. Whereas 205bits and 190bits of the data packets are delivered per one second at the destination end using CKMSMPR [1], Optimal EERP-Signcryption [2]. The different results are observed for each method. The average of ten results indicates that the TICSC-DSBNL technique increases the throughput by 8% and 14% when compared to existing routing methods.

Table 5 Comparison Of Data Confidentiality Rate

No. of data packets	Data confidentiality rate (%)		
	TICSC-DSBNL	CKMSMPR	Optimal EERP-Signcryption
25	92	84	80
50	94	84	82
75	96	88	85
100	93	86	83
125	94	86	84
150	95	88	86
175	93	87	85
200	92	86	84
225	94	87	86
250	95	86	85

Table 5 describes the simulation results of the data confidentiality rate versus the number of a number of data packets in the counts from 25 to 250. The reported results indicate that the TICSC-DSBNL achieves a higher data confidentiality rate than the other two existing methods. For example, 25 data packets are considered for simulation. By applying the TICSC-DSBNL technique, 23 data are correctly accessed by the authorized receiver and the confidentiality rate of the proposed TICSC-DSBNL technique is 92% whereas the confidentiality rate of existing CKMSMPR [1], Optimal EERP-Signcryption [2] is 84%, and 80% respectively. For each method, ten different runs are performed and results are compared. The comparison of ten results shows that the data confidentiality is increased by 9% and 12% using the TICSC-DSBNL technique than the existing methods.

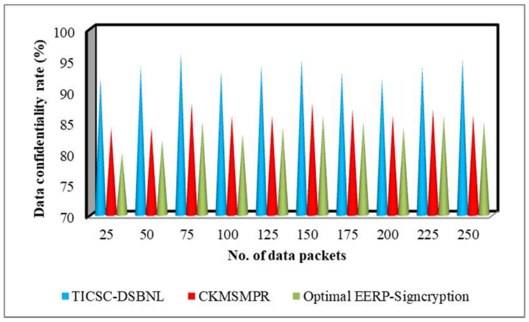

Figure 9 performance analysis of data confidentiality rate

Figure 9 exhibits the performance analysis of the data confidentiality rate of different methods. The graphical plot noticed that the proposed TICSC-DSBNL achieved a higher data confidentiality rate during transmission in MANET.

The reason for this significant improvement is to apply the Cramer–Shoup system in the deep neural network. The cryptography performs the Time based pseudo- randomness key generation for each node in the network. The time based key generation avoids unauthorized access. This helps to protect the data packets and improve the confidentiality rate.

4. RELATED WORKS

A Bayesian approach and Dempster Shafer Theory was developed in [11] for creating the Secure Routing Path based on trust. The designed approach increases the throughput but higher confidentiality was not achieved. A QoS-Aware Secured End-to-End data Communication (QASEC) technique was introduced in [12] to identify the normal or malicious node for authentication. But, the technique method failed to improve the performance of the packet delivery ratio.

Bird swarm-whale optimization algorithm was introduced in [13] for optimal-secure multi-path routing with minimum delay. The designed algorithm failed to increase the network's system performance. Various security routing protocols was presented in [14] based on a machine learning technique to improve the delivery ratio and minimize the delay. A QoS based secure routing was performed in [15] for improving the communication efficiency. But the routing model failed to analyze the performance of packet loss. A trust enhanced cluster-based multipath routing (TECM) algorithm was designed in [16] to minimize the security problems.

A disruption tolerant secure opportunistic routing technique was introduced in [17] to ensure reliable and secured communication. The technique increases the delivery ratio and throughput but the delay was not minimized. An efficient trust model and distributed clustering framework were introduced in [18] for enhancing security. But it failed to implement the cryptographic-based schemes to secure the clustering process.

A trust-based secure QoS routing method was introduced in [19] based on the trust estimation. The method minimized the routing overhead but the packet loss was not minimized. An energy-aware and social trust inspired multi-dimensional trust management approach was developed in [20]. But it failed to identify the node behavior such as malicious and legitimate nodes for achieving higher security.

.

5. CONCLUSION

To guarantee secure data routing in MANET, the TICSC-DSBNL technique is proposed for improving the data delivery with higher data confidentiality. The proposed TICSC-DSBNL technique uses multiple layers for identifying the normal or malicious node and secure data transmission. For each node in the network, the trust value is measured using the Tversky Similarity index. The node which has higher trust is selected as a normal node. Otherwise, the node is said to be malicious. Followed by, the route paths between source and destination are established to find the shortest path. Finally, the Cramer–Shoup cryptosystem is applied for secure routing and avoid the unauthorized node to access the data with higher confidentiality in MANET. Simulation is performed to estimate the performance of the TICSC-DSBNL technique over the two conventional routing methods and different performance metrics such as packet delivery ratio, packet drop rate, delay, throughput, and data confidentiality rate. The numerical validated results demonstrate that the TICSC-DSBNL technique achieves improved performance in terms of higher data confidentiality, packet delivery with lesser delay and drop than the conventional routing techniques.

REFERENCES

[1] Valanto Alappatt, P.M.Joe Prathap, "Hybrid cryptographic algorithm based key management scheme in MANET", Elsevier, 2020, Pages 1-9

[2] Elbasher Elmahdi, Seong-Moo Yoo, Kumar Sharshembiev, "Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks", Journal of Information Security and Applications, Elsevier, Volume 51 (2020) 102425

[3] T. Manjula, B. Anand, "A secured multiplicative Diffie Hellman key exchange routing approach for mobile ad hoc network", Journal of Ambient Intelligence and Humanized Computing, Springer, 2019, Pages 1-11

[4] Deepika Kukreja , Deepak Kumar Sharma, "T-SEA: trust-based secure and energy aware routing protocol for mobile ad hoc networks",

International Journal of Information Technology, Springer, 2019, Pages 1-15

[5] Ruo Jun Cai, Xue Jun Li, Peter Han Joo Chong, "An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs", IEEE Transactions on Mobile Computing, Volume 18, Issue 1, 2019, Pages 42 – 55

[6] V. Nivedita , N. Nandhagopal, "Improving QoS and efficient multi-hop and relay based communication frame work against attacker in MANET", Journal of Ambient Intelligence and Humanized Computing, Springer, 2020, Pages 1-11

[7] Samaneh Rashidibajgan, Robin Doss, "Privacy-preserving history-based routing in Opportunistic Networks", Computers & Security, Elsevier, Volume 84, 2019, Pages 244-255

[8] K. P. Rama Prabha , N. Jeyanthi, "A Trust and Fuzzy Cluster Based Dynamic Secure Routing Algorithm for Mobile Ad Hoc Networks", Wireless Personal Communications, Springer, Volume 98, 2018, Pages 2959-2974

[9] Suneel Miriyala ,M. Satya Sairam, "Improving privacy in SDN based MANET using hybrid encryption and decryption algorithm", Microprocessors and Microsystems, Elsevier, 2020, Pages 1-7

[10] R. Tino Merlin , R. Ravi, "Novel Trust Based Energy Aware Routing Mechanism for Mitigation of Black Hole Attacks in MANET", Wireless Personal Communications, Springer, Volume 104, 2019, Pages 1599-1636,

[11] Vaishali V. Sarbhukan , Lata Ragha, "Establishing Secure Routing Path Using Trust to Enhance Security in MANET", Wireless Personal Communications, Springer, Volume 110, 2020, Pages 245-255

[12] Muhammad Usman, Mian Ahmad Jan, Xiangjian He, Priyadarsi Nanda, "QASEC: A secured data communication scheme for mobile Ad-hoc networks", Future Generation Computer Systems, Elsevier, Volume 109, 2020, Pages 604-610

[13] Neenavath Veeraiah ,B. T. Krishna, "An approach for optimal-secure multi-path routing and intrusion detection in MANET", Evolutionary Intelligence, Springer, 2020, Pages 1-15

[14] Nedumaran Arappali , Ganesh Babu Rajendran, "MANET security routing protocols based on a machine learning technique (Raspberry PIs)", Journal of Ambient Intelligence and Humanized Computing, Springer, 2020, Pages 1-15

[15] Jaikumar Vinayagam, CH. Balaswamy, K. Soundararajan, "Certain Investigation on MANET Security with Routing and Blackhole Attacks Detection", Procedia Computer Science, Elsevier, Volume 165, 2019, Pages 196-208

[16] Vallala Sowmya Devi , Nagaratna P Hegde, "Multipath Security Aware Routing Protocol for MANET Based on Trust Enhanced Cluster Mechanism for Lossless Multimedia Data Transfer", Wireless Personal Communications, Springer, Volume 100, 2018, Pages 923–940

[17] K. Pushpalatha, M.Karthikeyan, "A generalized framework for disruption tolerant secure opportunistic routing during emergency situations using MANETs", Cluster Computing, Springer, Volume 22, 2019, Pages 9905-9913

[18] Ali Mansouri, Mohamed Salim Bouhlel, "Trust in Ad Hoc Networks: A New Model Based on Clustering Algorithm", International Journal of Network Security, Volume 21, Issue 3, 2019, Pages 483-493

[19] Muhammad Salman Pathan, Nafei Zhu, Jingsha He, Zulfiqar Ali Zardari, Muhammad Qasim Memon, and Muhammad Iftikhar Hussain, "An Efficient Trust-Based Scheme for Secure and Quality of Service Routing in MANETs", Future Internet, Volume 10, Issue 2, 2018, Pages 1-16

[20] Panel Antesar M.Shabut, M. Shamim Kaiser, Keshav P.Dahal, Wenbing Chen, A multidimensional trust evaluation model for MANETs", Journal of Network and Computer Applications, Elsevier, Volume 123, 2018, Pages 32-41