ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2021.0379

SECURE AND ENERGY-AWARE ROUTING FOR RELIABLE DATA TRANSMISSION IN MOBILE AD HOC NETWORKS

P. Daniel Sundarraj[1] and K. Arulanandam[2]
[1]*Department of Computer Science, Thiruvalluvar University, India*
[2]*Department of Computer Science, Government Thirumagal Mills College, India*

Abstract

Mobile Ad-Hoc Network (MANET) is a generic technology utilized in various real-time applications. The MANET is a self-configuring and self-directed system that quickly deploys in a network. Data transfer is a big issue in MANET due to poor wireless medium and lack of data security and reliability. The prior system established a mobile ad hoc content distribution strategy. The ideal Cluster Head (CH) is chosen using the Teaching Learning Based Optimization (TLBO) approach. However, due to these features, it is more vulnerable to attacks. In addition, it impacts packet delivery and throughput. The proposed system designed a Secure and Energy Aware Routing (SEAR) mechanism to improve MANET data transmission reliability and security. Initially, nodes are clustered by distance. Then the Weight-based Artificial Fish Swarm Algorithm (WAFSA) is used to pick the optimum Cluster Head (CH). Mobility, remaining energy, and connectivity are considered objective functions for CH selection. Securing communication between these nodes will require proper cryptography. The security mechanism generates secret keys using Advanced Encryption Standard (AES) to encrypt or decode messages delivered between member nodes. This security approach enables secure communication between member nodes and CHs, uses the NS-2 analytical platform, and outperforms the existing system regarding average energy drop, network lifetime, and encryption time.

Keywords:

Cluster Head (CH), Advanced Encryption Standard (AES), Weight-based Artificial Fish Swarm Algorithm (WAFSA), Secret Keys

1. INTRODUCTION

Mobile Ad hoc Networks (MANETs) are short-term networks constructed for specific purposes and do not require pre-existing infrastructure [1]-[2]. A MANET most significant characteristics include autonomy and lack of infrastructure, changeable network topology, multihop routing, inadequate physical security, device heterogeneity, and variable capacity links with finite bandwidth [3]-[4].

Routing packets in these networks is a complicated issue due to the mobility of nodes and reliance on a small battery to stay active in the network. Therefore, multiple routing methods based on proactive, reactive, and hybrid protocols have been developed to manage one hop and multihops, self-organizing networks [5]-[7]. Even when there is no data to send, the proactive protocol stays active in the network and keeps route information available at all times. Moreover, in reactive protocols, power usage is low.

Clustering is one of the most effective ways to improve energy efficiency. CH selection is the process of selecting a node inside the cluster to serve as the cluster leader node. The CH is in charge of keeping track of information about its cluster. This information provides a list of cluster nodes as well as the path to each node [8]. The CH is responsible for communicating with all of the nodes in its cluster. However, CH must communicate with nodes in other clusters, which can be done directly, through the appropriate CH, or via gateways. Communication occurs in three stages. First, CH retrieves data sent by its participants, then compresses it, and lastly transfers it to the base station or another CH. A suitable CH can reduce energy consumption while increasing network lifetime [9]. Because clustering in the MANET is a non-deterministic polynomial-time-hard problem, many optimization methods can provide answers. Optimization techniques include the Genetic Algorithm (GA), Simulated Annealing (SA), Particle Swarm Optimization (PSO), and Artificial Bee Colony (ABS) systems.

Recently, the demand for solid security and resilience in wireless networks has risen [10]. MANETs play a crucial role in providing high security in trustworthy networks due to features such as open network boundaries, scattered networks, and quick and easy installation. To prevent data from being exposed by hackers, it must be securely delivered via a MANET. The cryptography algorithm must meet many security requirements, including confidentiality, integrity, authenticity, and availability (CIAA). Better mechanisms are necessary for this conducted study to attain increased energy efficiency and data security.

This study describes an energy-efficient clustering methodology for enhancing delivery ratio, minimizing end-to-end delay, and implementing more secure transmission. The WAFSA was used to choose CH. An encryption algorithm, such as the Advanced Encryption Standard (AES) technology, was utilized to improve security during data transmission in the MANET. Encryption algorithms encrypt data, which can improve overall efficiency and confidentiality. An authorized individual can view the data in the MANET using this security approach. Furthermore, this routing technique can be utilized to improve reliability while decreasing energy consumption.

Section 2 covers the existing MANET-related articles. Section 3 describes WAFSA as well as a secure encryption algorithm for mobile networks. The results and discussion are described in Section 4. Finally, Section 5 discusses the conclusion.

2. LITERATURE REVIEW

Robinson et al. [11] offer a particle swarm optimization-based bandwidth and connection availability prediction system for mobile ad hoc network multipath routing. The available bandwidth, link quality, and mobility factors are employed in this prediction phase to choose the node based on their fuzzy logic. The selected node will broadcast information to all nodes, and all details will be validated before transmission. In addition, the routes are redirected and twisted to identify a good link as an intermediary node. The developed approach significantly improves packet delivery ratio, path optimality, and end-to-end delay.

Pathak and Jain [12] created a reliable clustering technique that offers more network stability by avoiding CH modifications and lowering costs. When the cluster primary node leaves (or dies), the backup node takes over as the cluster primary node. Following that, the cluster head will re-select a new backup node to ensure that the network is always available. Furthermore, the priority of CH and a backup node is determined by the node degree and the remaining battery life. Therefore, the priority factor influences the selection of the cluster head and backup node. According to the testing results, the designed system outperforms energy usage and packet delivery ratio.

Popli et al. [13] developed a secure and efficient CH selection technique incorporating security into the clustering algorithm. In this method, distributed clusters are sustained using the k mean algorithm approach, and cluster heads are selected by considering multiple factors such as connectivity and residual energy. As a result, only non-malicious nodes participate in the selection of CHs and thus improving security. The experimental results suggest that the provided technique exceeds the conventional Lowest Identifier (LID) algorithm regarding energy conservation by balancing load distribution across various nodes by appropriately upgrading CHs.

Ahmad and Ismail [14] developed a user-selectable encryption approach that uses Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES), and the Diffie-Hellman Key Exchange (DHKE) protocol for key management to increase MANET security. The Network Simulator-2 (NS-2) is used to study the performance of the developed approach in terms of data transfer time and network throughput. The results demonstrate AES supremacy over alternative encryption schemes.

Sharma et al. [15] presented a new hybrid cryptography methodology for safe data transmission. The Ad Hoc On-Demand Vector Routing protocol maintains paths between nodes that intend to interact via routing messages. Thus, AODV provides loop-free pathways in the event of a link failure. SAODV is a trust-based secure routing technology for mobile ad-hoc networks and enhances security in MANET. The NS2 network simulation environment is used to implement the specified cryptographic routing method. The designed process produces a good packet delivery ratio, throughput, and energy.

3. PROPOSED METHODOLOGY

The proposed system created a Secure and Energy Aware Routing (SEAR) mechanism for enhancing MANET data transmission reliability while maintaining high security. The recommended work flow diagram is shown in Fig.1.

3.1 NETWORK MODEL

The network is depicted as a graph having nodes and edges as $G(v,e)$. A network made up of MTs coupled to BSs and a server. Optical wires connect the BS to the central server. The main server is in charge of retrieving and sending the necessary data to the BS. The amount of energy used per bit to send and receive data via LR with a particular bit rate remains constant.

3.2 CLUSTERING AND CLUSTER HEAD SELECTION

First, clustering is made based on distance. CH is the node having the most significant fitness value, and Cluster Members (CMs) are the remaining nodes in that cluster. The CH collects data from member nodes in its cluster and sends it to the BS. The chosen CH connects with all of the cluster member nodes, forming an association between them. In this proposed effort, AFSA was used to select the best CH for the MANET. The mobility, remaining energy, and degree of connectedness are considered objective functions in this proposed study for the CH selection.

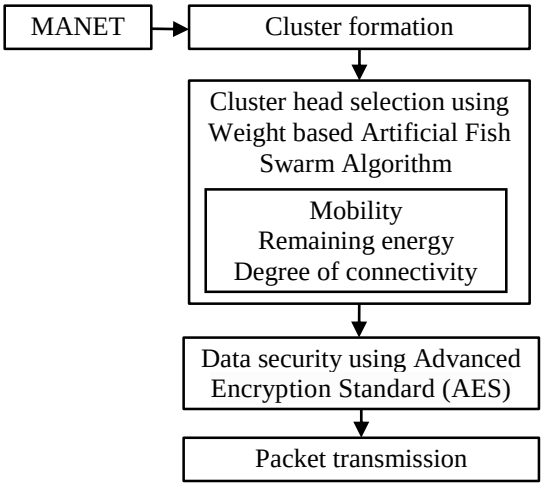


Fig.1. Flow diagram of the proposed work

3.2.1 Residual Energy (E_{RE}):

It is defined as the difference between initial energy (E_I) and consumed energy (E_C), which is calculated using Eq.(1).

$$E_{RE=} E_I - E_C \tag{1}$$

3.2.2 Degree of Connectivity:

The number of neighbors of node x (i.e., the number of linkages) is expressed by the degree of node x, denoted by $d(x)$. The node with the greatest number of neighbors is chosen as CH. A $d(x)=0$ node is isolated (no neighbors). The graph G degree is represented by

$$d(G) = \{d(x)\} \tag{2}$$

3.2.3 Mobility:

Relative mobility at node n_i concerning node n_j, $M_{n_i}^{Rel}\left(n_j\right)$ is computed as:

$$M_{n_i}^{Rel}\left(n_j\right) = 10\log_{10}\frac{Rx\,\mathrm{Pr}_{n_j\to n_i}^{new}}{Rx\,\mathrm{Pr}_{n_j\to n_i}^{old}} \tag{3}$$

where, $Rx\,\mathrm{Pr}_{n_j\to n_i}^{new}$ and $Rx\,\mathrm{Pr}_{n_j\to n_i}^{old}$ denote new and old retrieving powers of the HELLO packet from node n_j to node n_i.

The Eq.(4) computes the Weight of each node,

$$W = w_1 E_{RE} + w_2 d\left(G\right) + w_3 M_{n_i}^{Rel}\left(n_j\right) \tag{4}$$

$$w_1 + w_2 + w_3 = 1 \tag{5}$$

where, w_1, w_2, w_3 are the weighting factors

The weighted clustering method chooses a CH based on the weight value of every node.

4. WEIGHT-BASED ARTIFICIAL FISH SWARM ALGORITHM (WAFSA)

WAFSA is employed in this proposed work to pick the best Cluster Head (CH). Optimizing Cluster head selection reduces energy usage in a specific network as well as overall data transmission overheads. Artificial Fish (AF) is a fictitious organism resembling real fish. Fish usually shift to a location with higher food consistency by engaging in Prey, follow, swarm behavior, and leap activities. We employ these actions to undertake the problem analysis and explanation.

Nodes in the network $X=(x_1,x_2,...,x_n)$ are used as input, in which $x_i(i=1,2,...,n)$ is the number of nodes. The food concentration at the current node position can be represented as $Y=f(X)$, where X is the fitness function. The proposed work considers node weight value (W) as the fitness function. The Euclidean distance between two AFs, X_i, and X_j, can be written as in Eq.(6).

$$D_{i,j}=|X_i-X_j| \tag{6}$$

The crowd element δ ($0<\delta<1$) manages the crowding of AFs around a location, and the best position identified will be loaded into the column.

4.1 PREY BEHAVIOR

It is a natural biological activity of fish to find food. X_i represents the present position of node i, X_j represents a random state of its viewing range, Y represents the food concentration, and the objective function $Y=f(X)$. The following Eq.is used to calculate the position X_j:

$$X_j=X_i+Visual\times\text{rand}(0,1) \tag{7}$$

where, Y_j and Y_i determine the food concentration of X_i and X_j; if $Y_i<Y_j$ AF moves forward a step from its current position to X_j, which is done by:

$$X_i(t+1) = X_i(t) + \frac{X_j(t)-X_i(t)}{\left\|X_j(t)-X_i(t)\right\|} \times \text{step} \times \text{rand}(0,1) \tag{8}$$

The traditional AFSA algorithm is one of the best algorithms for determining the optimum global solution. However, in some circumstances, pure AFSA can take quite a long time to discover a satisfactory answer. Therefore, a new parameter called inertia Weight (ω) was added to the position update equation to address this issue. In addition, the Simulated Annealing Inertia Weight factor is introduced in the position updation stage in this work. The modified Eq.(9) is shown below.

$$\omega = \omega_{min}+(\omega_{max}-\omega_{min})\times\lambda^{(k-1)} \tag{9}$$

where, λ=0.95; ω-Inertia weight; ω_{max}-maximum weight value; ω_{min}-minimum weight value and k-constant

Therefore, Eq.(8) is modified as:

$$X_i(t+1)=X_i(t)+\frac{X_j(t)-X_i(t)}{\left\|X_j(t)-X_i(t)\right\|}\times\text{step}\times\omega\times\text{rand}(0,1) \tag{10}$$

$$X_i(t+1)=X_i(t)+\frac{X_j(t)-X_i(t)}{\left\|X_j(t)-X_i(t)\right\|}\times\text{step}\times\omega_{min}+(\omega_{max}-\omega_{min}) \times\lambda^{(k-1)}\times\text{rand}(0,1) \tag{11}$$

If $Y_i>Y_j$, a state X_j is chosen randomly and confirmed whether food consistency fulfills the required criteria. After try_number times, node i is not satisfied with the on state, the concerned AF performs leap behavior.

4.2 SWARM BEHAVIOR

To maintain swarm characteristics, AFs seek to migrate to the center position in each iteration. The Eq.(12) can be used to calculate the center position:

$$X_c = \frac{1}{N}\sum_1 X_i \tag{12}$$

where, X_c denotes arithmetic average of all nodes. N represents the size of the population. n_f shows the number of nodes in the viewing range of X_c. If $n_f/N<\delta$ and $Y_c>Y_i$, then node i moves forward a step to the companion center by:

$$X_i(t+1)=X_i(t)+\frac{X_C-X_i(t)}{\left\|X_C-X_i(t)\right\|}\times\text{step}\times(\omega_{min}+(\omega_{max}-\omega_{min}) \times\lambda^{(k-1)}\times\text{rand}(0,1)) \tag{13}$$

Otherwise, AF performs prey behavior.

4.3 FOLLOW BEHAVIOR

When a single or many fishes discover food while the AF is moving, the neighboring fishes will follow and quickly arrive at the place. Assume node i current position is X_i, and position X_j is its neighbor in its viewing range. Here n_f denotes the number of AF swarms in the visible area of X_c; if $Y_i<Y_j$ and $n_f/n<\delta$, node i moves forward a step to the neighbor X_j.

$$X_i(t+1)=X_i(t)+\frac{X_j(t)-X_i(t)}{\left\|X_j(t)-X_i(t)\right\|}\times\text{step}\times(\omega_{min}+(\omega_{max}-\omega_{min}) \times\lambda^{(k-1)}\times\text{rand}(0,1)) \tag{14}$$

If there are no neighbors around X_j, then node i performs the prey behavior.

4.4 LEAP BEHAVIOR

The usual search process for food or companions over huge distances can successfully restrict local optimum. Node i execute this behavior and modifies the parameter to leap out of the present position. To avoid the local extreme values, it selects a state in the picture and goes towards it. Therefore,

$$X_i(t+1)=X_i(t)+Visual\times(\omega_{min}+(\omega_{max}-\omega_{min})\times\lambda^{(k-1)}\times\text{rand}(0,1)) \tag{14}$$

Algorithm 1: WAFSOA

Input: Number of nodes in the network

Output: Cluster Head (CH)

Step 1: Establish nodes in network $X=(x_1,x_2,...,x_n)$, where $x_i(i=1,2,...,n)$

Step 2: Set up the parameters of artificial fish and a maximum number of iterations.

Step 3: Choose the optimal value based on the fitness function and save the same.

Step 4: Choose an optimal value of each node and save.

Step 5: Establish prey, swarm, follow, and leap behaviors.

Step 6: The saved value is upgraded by the best individual optimum.

Step 7: If the stopping criteria are fulfilled, outputs the optimal node (CH) result;

Step 8: Else, return to step 2

5. DATA SECURITY USING ADVANCED ENCRYPTION STANDARD (AES) TECHNIQUE

The security approach introduced the AES technique to create secret keys that can encrypt or decode messages delivered between member nodes and CH. In cluster-based MANETs, this security paradigm enables safe communication between member nodes and cluster chiefs. The AES approach provides both security and speed. Moreover, the implementation of both hardware and software is even faster. Encrypts 128-bit data blocks in 10, 12, or 14 rounds, depending on the key size.

5.1 AES ENCRYPTION

This AES encryption has ten rounds of encryption and converts information into an unreadable form known as ciphertext. Sub-bytes, shift-rows, mix column, and add round key are the four processing processes in each round. The Fig.2 depicts the AES encryption method, which is detailed further below.

5.1.1 Algorithm Steps:

These steps used to encrypt a 128-bit block

Step 1: The group of round keys from the cipher key.

Step 2: Establish a state array and insert the initial round key to the starting state array.

Step 3: Carry out round = 1 to 9: Run Usual Round.

Step 4: Run Final Round.

Step 5: Corresponding ciphertext output of Final Round Step

5.1.2 Usual Round:

It includes the following.

Step 1: Sub Bytes

Step 2: Shift Rows

Step 3: Mix Columns

Step 4: Add Round Key, using *K*(round)

5.1.3 Final Round:

It involves the following.

Step 1: Sub Bytes

Step 2: Shift Rows

Step 3: Add Round Key, using K(10)

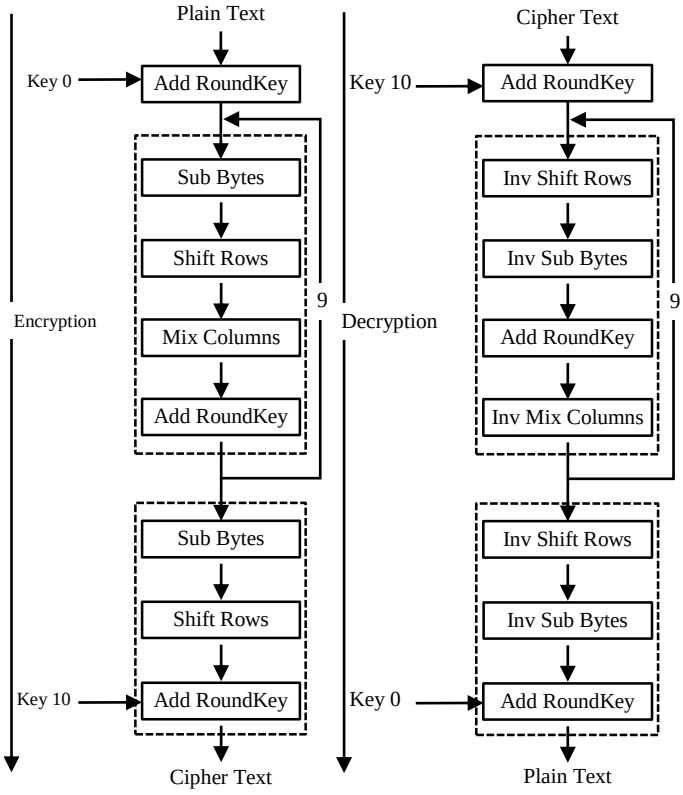
5.2 ENCRYPTION

The data is encrypted and sent to CH by the cluster members. The encryption procedure is outlined in the following phases.

- ***Sub Bytes***: The encryption site employs the first transformation, Sub Bytes as two hexadecimal digits.
- ***Shift Rows***: It is a transformation used in encryption.
- ***Mix Columns***: This transformation changes each state column into a new column.
- ***Insert a Round Key***: One column at a time, Add Round Key progresses as a matrix addition process, adding a keyword to every stage column matrix.
- ***XO*** is the final phase in the process. Also, the Mix columns step is skipped in the final round of encryption.

5.3 DECRYPTION

The CH decrypts encrypted data received from a target node using its key and the source node ID. Thus, CH s can immediately communicate with each other. Inverse functions like a) Inverse shift rows, b) Inverse replace bytes, c) Add round key, and d) Inverse mix columns are used to reverse AES encryption. The AES encryption and decryption approach is shown in Fig.2.



(a) Encryption (b) Decryption

Fig.2. AES Encryption and Decryption

The XO step is the final stage. Also, the Inverse mix columns phase is not used in the final round of decryption. The packets are then decoded and delivered to the base station through an efficient path. The described approach allows intra-cluster communication between communicating nodes to be authenticated.

6. EXPERIMENTAL RESULTS

The complete simulation is run on the NS-2 simulator. The Table.1 highlights the various parameters employed in both

simulations. The parameter values are chosen to allow results obtained to be generalized to real-life situations.

Table.1. System parameters for simulation

Parameters	Values
Area	$1000\times1000m^2$
Number of nodes	250
$E_{Rx/S}$	$0.3\times S_T$ J
$E_{Tx/S}$	$0.5\times S_T$ J

6.1 AVERAGE ENERGY DROP

The average energy loss among nodes indicates the overall energy efficiency of the routing procedure. It can be seen that the non-cooperative technique has the most significant average energy drop values, suggesting that it is inefficient.

In terms of average energy drop, the proposed method outperforms the existing k-means and TLBO techniques. The number of nodes is plotted on the x-axis, and the average energy loss is plotted on the y-axis. WAFSA technique decreases the energy costs involved during the data receiving process by using fitness values to pick the best nodes as CHs during a particular round, resulting in a considerable overall reduction in energy consumption. Based on the experimental results, it is possible to conclude that the proposed system obtains the lowest energy drop compared to k-means and TLBO techniques.

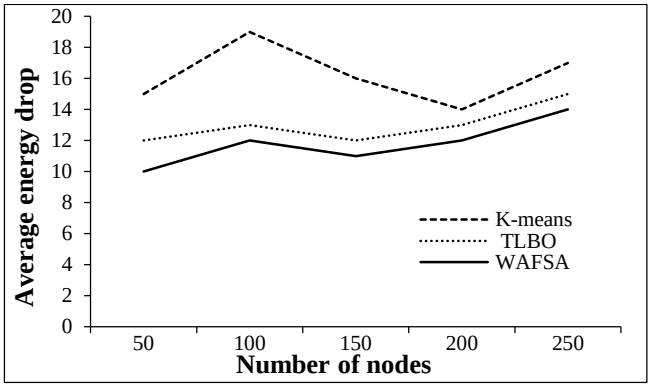


Fig.3. Average energy drop

6.2 NETWORK LIFETIME

The network lifetime of novel WAFSA and conventional k-means and TLBO algorithms is depicted in Fig.4. The number of nodes is plotted along the x-axis, and the number of rounds is taken along the y-axis. Here, power utilization is low as the optimal node is chosen for the receiving process, prolonged network lifetime. The simulation results suggest that the proposed system has a higher lifespan than the existing k-means and TLBO.

6.3 ENCRYPTION TIME

The proposed AES is compared to prior Rivest–Shamir–Adleman (RSA) standards regarding encryption time. The system performance varies in milliseconds (ms) according to the size of the key. The Fig.5 depicts the system performance using two alternative ways. Their associated time is taken (ms) for both encryption outcomes, based on which the AES and RSA algorithm performance is measured.

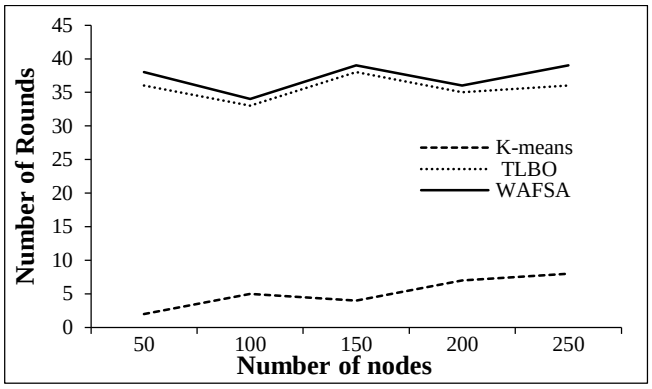


Fig.4. Network lifetime

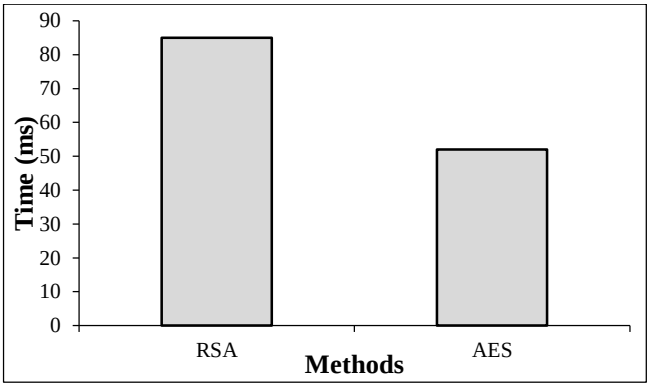


Fig.5. Encryption time

7. CONCLUSION

The proposed system developed a SEAR approach to improve secure data transmission in the MANET. First, the WAFSA was used to pick the ideal CH based on mobility, remaining energy, and degree of interconnectivity to enhance energy efficiency. The AES method is then used to secure packet transmission. It assures the data availability and dependability, as well as its readability from beginning to end. For the analysis, the proposed approach is implemented on the NS-2 platform. Thus, this novel approach has low energy consumption and a high network lifespan. In the future, the technique efficiency can be increased by combining bio-inspired algorithms.

REFERENCES

[1] N.S. Farheen and A. Jain, "Improved Routing in MANET with Optimized Multi Path Routing Fine Tuned with Hybrid Modeling", *Journal of King Saud University-Computer and Information Sciences*, Vol. 83, No. 1, pp. 1-23, 2020.

[2] V.V. Kumar and S. Ramamoorthy, "Secure Adhoc On-Demand Multipath Distance Vector Routing in MANET", *Proceedings of International Conference on Computing and Communication Systems*, pp. 49-63, 2018.

[3] Josh Kumar and Ayyaswamy Kathirvel, "Analysis and Ideas for Improved Routing in MANET", *International Journal of*

Interactive Mobile Technologies, Vol. 13, No. 4, pp. 164-177, 2019.

[4] N. Kousik and P. Johri, "Improved Energy Efficient Wireless Sensor Networks Using Multicast Particle Swarm Optimization", *Proceedings of International Conference on Wireless Networks and Communication*, pp. 1-7, 2020.

[5] A.S. Nandhini and P. Vivekanandan, "Survey on Energy Efficient Routing Protocols in MANET", *International Journal of Advances in Engineering and Technology*, Vol. 6, No. 1, pp. 370-386, 2013.

[6] T. Karthikeyan and K. Praghash, "Improved Authentication in Secured Multicast Wireless Sensor Network (MWSN) using Opposition Frog Leaping Algorithm to Resist Man-in-Middle Attack", *Wireless Personal Communications*, Vol. 113, pp. 1-17, 2021.

[7] S.H.H. Nazhad and M. Conti, "An Efficient Routing Protocol for the QoS Support of Large-Scale MANETs", *International Journal of Communication Systems*, Vol. 31. No. 1, pp. 3384-3392, 2018.

[8] K. Shankar and M. Elhoseny, "Trust Based Cluster Head Election of Secure Message Transmission in MANET using Multi Secure Protocol with TDES", *Journal of Universal Computer Science*, Vol. 25, pp. 1221-1229, 2019.

[9] S. Pathak and S. Jain, "Comparative Study of Clustering Algorithms for MANETs", *Journal of Statistics and Management Systems*, Vol. 22, No. 4, pp. 653-664, 2019.

[10] V.V, Sarbhukan and L. Ragha, "Establishing Secure Routing Path using Trust to Enhance Security in MANET", *Wireless Personal Communications*, Vol. 110, pp. 245-255, 2020.

[11] Y.H. Robinson and E.G. Julie, "PSOBLAP: Particle Swarm Optimization-based Bandwidth and Link Availability Prediction Algorithm for Multipath Routing in Mobile Ad Hoc Networks", *Wireless Personal Communications*, Vol. 106, No. 4, pp. 2261-2289, 2019.

[12] S. Pathak and S. Jain, "An Optimized Stable Clustering Algorithm for Mobile Ad Hoc Networks", *EURASIP Journal on Wireless Communications and Networking*, Vol. 2017, No. 1, pp.1-11, 2017.

[13] R. Popli, K. Garg and S. Batra, "SECHAM: Secure and Efficient Cluster Head Selection Algorithm for MANET", *Proceedings of International Conference on Computing for Sustainable Global Development*, pp. 1776-1779, 2016.

[14] A. Ahmad and S. Ismail, "User Selective Encryption Method for Securing MANETs", *International Journal of Electrical and Computer Engineering*, Vol. 8, No. 5, pp. 3103-3111, 2018.

[15] A. Sharma and U. Singh, "Secure Data Transmission on MANET by Hybrid Cryptography Technique", *Proceedings of International Conference on Computer, Communication and Control*, pp. 1-6, 2015.