MSA-SFO-based Secure and Optimal Energy Routing Protocol for MANET

D.Naga Tej[1]
Research Scholar, JNTUK, Kakinada
Assistant Professor, Gayatri Vidya Parishad College of Engineering, Madhurawada, Visakhapatnam
Andhra Pradesh, India

K V Ramana[2]
Professor
JNTUK Kakinada
Kakinada
Andhra Pradesh, India

***Abstract*—Mobile Adhoc Network (MANET) is a fast deployable wireless mobile network with minimal infrastructure requirements. In these networks, autonomous nodes may function as routers. Due to the mobility of MANET nodes, the network's topology is dynamic. Recent scientific emphasis has been placed on MANET security. Few MANET attacks have been discussed in the existing literature. Wired networks provide more security choices than wireless networks. Most routing protocols fail in a MANET with a malicious node. This research focuses on S-DSR, a novel hybrid secure routing system that guarantees the delivery and performance of packets across network nodes. This protocol leverages neighbor trust information to choose the most secure route for file transfer. This protocol is used by OMNET++. It offers a higher delivery rate and lower delay than AODV, AOMDV, and other similar protocols. MANETs, or mobile ad-hoc networks, will be used in the future communication protocols of industrial wireless networks. These protocols will decentralise the connection of smart devices. Due to the unidimensional nature of digital data, it is impossible to apply encryption methods indirectly. These publications are digital. To strengthen the privacy of e-healthcare MANETs, a safe, lightweight keyframe extraction technique is required. The purpose of this project is to develop a secure protocol for MANET wireless networks. This study proposes the use of chaotic cryptography to enhance the security of MANET Wireless networks. Using Modified Self-Adaptive Sailfish Optimization (MSA-SFO), it is possible to construct vital maps in a chaotic setting. This method produces secure key pairs.**

Keywords*—MANET; sail fish optimization; energy; routing protocol

I. INTRODUCTION

One of the most often used kinds of independent wireless technology for communication with mobile nodes is called a MANET. Mobile ad hoc networks (MANETs) rely on mobile nodes to perform dual roles as end systems and routers for the network's packet transmissions [1]. Due to the fact that wireless communication is used, it is much simpler to reestablish the connection, and moreover, nodes might be designed to be mobile. Given the nature of the nodes, which is that they are movable, it is not required that a permanent network structure be used for communication. MANET, on the other hand, does not make use of base stations, which might be helpful in a number of different networking configurations. Due to the number of users using the MANET for diverse purposes, such as military and emergency operations, it is crucial that the platform be safeguarded from unwanted users. This is due to the fact that the network's popularity has made it hard for illegal users to connect to it.

There are several uses for mobile ad hoc networks (MANETs), such as between special events, communications in places where radio infrastructure does not exist, catastrophes, and military surgery. MANET's flexibility and dynamic topology make it vulnerable to a variety of attacks, including eavesdropping, routing, and the modification of applications. The quality of services has been surpassed by MANET's security problems (QoS). So, the best way to ensure MANET's security is to use intrusion tracking, which modifies the system to notice any other vulnerability. Anti-intrusion detection is vital to providing safeguards and serves as an additional layer of security against unauthorized entry. In the presence and absence of a selective packet dropping attack, this solution was put to the test against the best-known practices [1].

Ad hoc network (MANET) is a grouping of nodes that communicate without the intervention of a central administrator in an infrastructure-free environment. The nodes in these networks are more dependent on each other to perform basic network activities. Secure routing is difficult to establish because of the shortage of resources. A system must be in place to deter misbehavior and preserve the network's synergy in order to assure safe routing. At each node, a partly distributed dynamic model is used to enhance the overall network's security and privacy. During route creation, additional information about network misbehavior is provided across the nodes as a precautionary step to maintain safe routing. In the real world, a node may engage in many forms of misbehavior at various points in time. To cope with nodes that show different levels of misbehavior, it offers a dynamic decision-making method. The model's ability to cope with misbehaving nodes has been shown in a series of simulations [2].

Unlike traditional networks, mobile ad-hoc networks (MANETs) are self-contained and do not rely on centralized access. MANET's rapid and flexible networking style allows it to be used in a broad range of situations. However, the network's constantly shifting architecture and open communication channels provide security risks. Active-routing authentication (AAS) was suggested in this work using the properties of active routing protocols. In order to prove the

AAS's effectiveness against selective forwarding, fake routing, byzantine, and spoofing attacks, we used BAN logic to examine the potential of hostile nodes mixing in a MANET [3][4].

The research problem and contribution of this research is to design a brand-new heuristic algorithm known as MSA-SFO by enhancing the already existing SFO algorithm's capacity for self-adaptation. This study was done with the intention of preserving users' privacy inside MANETs. This speeds up the process of convergence and decrease the likelihood of being stuck in a local minimum.

Paper organization is as follows:

The section outlines the format of this paper: The work that is connected to Optimal Energy Routing Protocol is shown in Section 2. This part also provides an explanation of the fundamental Routing Protocol for MANET techniques that were used throughout this research. The planned MSA-SFO-Modified Self Adaptive Sail Fish Optimization is described in Section 3, which reflects its current state. The analysis and discussion of the obtained data are presented in Section 4. Our results are summarised in Section 5, which also includes a discussion of the work that will be done in the future.

II. Related Work

Despite extensive deployment, the AOVDV routing scheme remains vulnerable to blackhole attacks. Lu and his team developed the SAODV protocol, a secure mechanism for routing networks, to overcome this problem. Due to the nature of a blackhole assault, which requires the cooperation of two nodes, it cannot be defended against using conventional protection measures. The BP-AODV protocol was created to solve this concern. It combines the features of the original AOVDV protocol with the BP-AODV to provide a secure and efficient routing system. A study of the BP-AODV protocol found that it can effectively repel a blackhole assault, regardless of whether it is launched by a forwarding node or a malicious actor. It also shows that BP-AODV may avoid a blackhole attack even if it happens throughout the whole routing procedure.

One of the most difficult and significant routing security concerns in VANETs and self-driving and connected cars is the detection of Black Hole attacks (ACVs). Cyber-physical paths may be hacked by malicious vehicles or nodes, converting a safe route into a less secure and dependable one. To avoid a neighboring node, malevolent nodes snatch data packets that may include emergency alerts and discard them instead [5]. When using MANETs, the nodes are on the move at all times. Macro-area networks (MANETs) have unique issues due to their inherent vulnerability to several types of security assaults and their inability to maintain secure operations while protecting their resources and providing safe routing among nodes. It is critical, therefore, to provide a reliable secure routing protocol to guard against anonymous attacks on nodes. Selfishness problems may now be studied, formulated, and solved using game theory. Malicious activity in networks is seldom detected using this technique. Instead, it focuses on the nodes' strategic and logical conduct. The dynamic Bayesian signaling game was utilized to examine the strategy profile of normal and malicious nodes in our research. In this game, specific tactics for each node were also disclosed. Combining player payoffs and tactics to achieve perfect Bayesian equilibrium (PBE) serves as a popular solution for signaling games dealing with partial knowledge. For both ordinary and malicious nodes, the use of PBE techniques is private information. In order to avoid being detected, legitimate nodes should cooperate with routing and keep their payoffs up-to-date, whereas malevolent nodes take calculated risks to avoid being detected. The reputation mechanism encourages improved collaboration between nodes by reducing the utility of malevolent nodes. [6] Bayes rule-based belief updating systems are used by regular nodes to continually assess their neighbors.

Since the beginning of the previous decade, MANET has been a major research focus. As the Internet-of-of-Things (IoT) expands into urban areas, this sort of networking paradigm is becoming more widely accepted as an essential component of the IoT's impending urban applications. Existing routing techniques in traditional MANETs cannot be used with IoT because of a considerable hurdle. The MANET-based application linked to the IoT platform may be exposed to security threats as a result of this routing mismatch. In order to enable real-time streaming applications, the mobile nodes in this study must communicate multimedia signals. Understanding the attacker's unexpected behavior is one of the most important aspects of safeguarding data. Attackers' sophistication is examined in the present research. To perform fatal assaults, they know one other's identities and collaborate, which is seldom represented in current security modeling data. This study utilizes the modeling capabilities of game theory to represent the multiple-collusion attacker situation. Modeling strategies of regular/malicious nodes as well as employing an optimization technique utilizing innovative auxiliary information to build the best strategies are some of its contributions. Malicious nodes may now be accurately predicted by each normal node, thanks to the new model's enhanced capacity to do exact computations. Game theory's baseline method is outperformed by the suggested mathematical model in MATLAB simulations [7].

Intelligent Transportation Systems may benefit from the use of Vehicular Ad-hoc Networks (VANET), which are a subset of Mobile Ad-hoc Networks (MANET) (ITS). Due to quick topological changes, high mobility, and frequent link disconnections, routing in these networks is a difficult issue. Because of this, establishing an effective routing system that meets the time constraints and minimizes the amount of overhead is a challenge. VANETs must also be capable of identifying malevolent vehicles. Using Unmanned Aerial Vehicles (UAVs) may be a useful tool in dealing with these constraints. UAVs in VANETs may be used to aid in the identification of potentially harmful vehicles by operating in ad hoc mode and collaborating with the vehicles. There are two unique modes of routing data in the VRU routing protocol: (1) sending packets of data between vehicles using UAVs, and (2) routing packets of data between UAVs. Using the NS-2.35 simulator on Linux Ubuntu 12.04, the performance of VRU routing components in an urban setting is evaluated. VANET MobiSim, a generator of mobility, and MobiSim, a UAV

motion generator, are both used in the generation of vehicle movements. Comparatively, the performance study shows that the VRU protocol may increase the delivery and detection rates by 16 and 7 per cent, respectively, over existing routing protocols. End-to-end latency and overhead are both reduced by 40% using the VRU protocol [8].

Nodes in a mobile network self-organize into mobile ad hoc networks (MANETs), which develop a dynamic network architecture to link them. Before reaching its final node, data in a MANET must travel via a series of intermediate nodes. To keep malicious nodes from gaining access to this data, we need to have some kind of protection in place. Routing security has been addressed in a variety of ways in the literature, each of which addresses a distinct component of security [9].

Multipath routing, as compared to the conventional single-path routing, is often employed in wireless networks to increase their fault tolerance. The GAHC algorithm is a mix of the Hill-Climbing and Genetic Algorithms that takes into consideration all of the variables that influence route selection. In addition, an enhanced C-means algorithm was created to apply this method [10]. A computation is conducted based on the value of the nodes that fulfill the trust threshold for a certain route. The cluster heads then route their networks through other routes. The ideal route for their applications is then determined by analyzing these routes. MSA-SFO is a multi-path routing scheme with a maximum throughput of 0.85 bits per second and a 90 percent detection rate. Additionally, its packet delivery rate is 89 percent. To evaluate its performance, selective packet dropping was used [11].

Mobile ad hoc networks are well suited for emergency communications and rural locations lacking radio infrastructure. They may also be used for emergency communications. Nonetheless, owing to the network's changeable topologies, security is its most susceptible point. Due to the nature of the MANET's security challenges, it is advised that network managers monitor and identify possible attacks on a frequent basis, prior to them becoming severe. This may prevent them from influencing the performance of the system. The ability of a mobile node to forward packets is one of the most crucial aspects that might impact its performance [12]. This research intends to build a trust-based multi-path routing algorithm for usage in MANETs. The selected cluster heads based on the suggested method are next examined to find the appropriate application path. After calculating the trust levels of the nodes, the ideal path for the applications was determined. The cluster heads then route their networks using multi-hop routing. This approach calculates the ideal path based on several performance-affecting criteria.

Multiple Sub-Silo Order (MSA-SFO) is a multi-path routing technique that greatly outperforms previous algorithms. It may also lower network energy usage by around 80 percent. Due to its adaptability and portability, the mobile ad hoc network (MANET) is gaining popularity. Although security procedures have been implemented to secure the networks, they do not protect the communication channels. To provide total security, it is necessary to create both the communication and routing protocols. The implementation of security procedures developed for wireless and wired networks may be particularly costly on MANETs due to their restricted network resources. This research attempts to create a secure architecture that can guarantee total network security. SUPERMAN, a proposed security framework, was evaluated against three distinct security protocols: IPsec, SAODV, and SOLSR. The simulation results demonstrated that the SUPERMAN architecture is optimal for wireless communication security. Due to the nature of the mobile ad-hoc network, a significant portion of its nodes are susceptible to assault. These nodes offer access to the network by unauthorized persons and organizations. In order to preserve the network's functioning, network administrators must routinely monitor and identify possible risks. The study provides a safe approach for selecting neighbors that combines machine learning and conventional routing techniques. By combining these strategies, it may be feasible to construct safe and dependable routes to a target. By observing the behavior of the nodes at changing connection levels, this technique may be implemented [13].

Various measures, such as the packet delivery ratio and the throughput, are used while evaluating the performance of a suggested method. The research demonstrates via experimental analysis that the suggested technique can perform consistently. Due to the nature of mobile ad hoc networks, it is becoming more challenging to create and maintain end-to-end infrastructure in specific places. As a consequence, DTN networks are becoming increasingly prevalent in these regions. DTNs are appropriate for high-latency applications, but they should also be considered for maritime networks. Due to the characteristics of the maritime environment, DTN networks are also addressed while addressing security issues. In order to provide tactical signals, for instance, the article demonstrates how to employ a DTN to address perimeter security issues. This study suggests utilizing the discriminant analysis to enhance the security of DTN connections. NDN is a future Internet architecture that permits the efficient delivery of the material as opposed to the standard data carriers. With its diverse forwarding techniques, NDN-based wireless networks are able to maintain safe and dependable communication. The two primary kinds of packets that NDN networks send back and forth are INTEREST and DATA. This study examines the strategies and issues found during the implementation of NDN-based networks such as MANETs, VANETs, WSNs, and WMNs [14].

III. Proposed MSA-SFO-Modified Self Adaptive Sail fish Optimization

The mobile networks serve as the terminal service in the wireless MANET, which allows for communication between the different wireless network devices. This communication has completely transformed the digital age. Because of its widespread use across a wide variety of sectors and employees, it is essential to provide a protected setting for the communication process at all times. The computing platform at the network's edge is often targeted in MANET, which is designed for wireless networks. This has the effect of reducing the platform's popularity in crucial services.

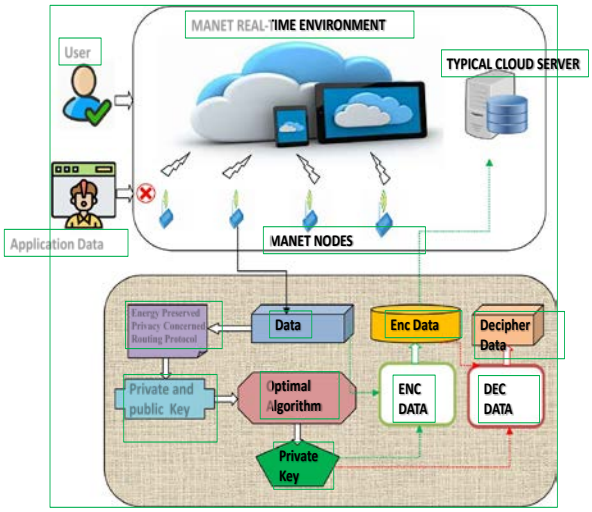

Fig. 1. Perspective on the Proposed MSA-SFO Architecture.

After the detailed analysis of the parallel and recent research outcomes, in this section of the work, the problem is formulated using the mathematical model.

In order for a network to have a long-life span, the cluster head must be replaced on a regular basis to ensure the security and the proposed architecture shown in Fig. 1.

At every moment, T(CH) signifies the cluster head determining function, which yields the cluster head instance g is a collection of groups. Any cluster has a total number of nodes known as N.

For the above lemma to hold, it must be shown (Eq. 1) that a cluster of nodes (Eq. 2) exists in the complete network, where the number of non-dead or active nodes is not zero.

$$\forall g \subset G \tag{1}$$

And,

$$\varnothing(g) \neq NULL \tag{2}$$

Also,

$$\forall n \subset N \tag{3}$$

Consequently, Eq. 4 and 5 so that the newly picked cluster head may avoid being comparable to the previous one.

$$\forall n(t) \subset N' \tag{4}$$

And,

$$N \notin N' \; and \; N' \notin N \tag{5}$$

If the R(k) represents the proportion of cluster heads in the N that are still available, then (Eq. 6) represents the percentage of cluster heads in the N that are still accessible.

$$1 - R(k)[\mathrm{k}.\mathrm{mod}\frac{1}{R(k)}] \tag{6}$$

As a result, we can write the cluster dead decision function as follows:

$$T(CH) = \frac{R(k)}{1 - R(k)[\mathrm{k}.\mathrm{mod}\frac{1}{R(k)}]} \tag{7}$$

The energy consumption is evenly distributed throughout the cluster's many components. In Eq. 5, the rationale for avoiding repeating clusters in subsequent eras is made evident.

The suggested algorithm for the control of energy consumption in clusters is presented in the following section:

Step (1). MSA-SFO serves as the foundation for the suggested approach. Before installing the cluster, the list of active nodes is compiled.

Step (2). After choosing it from the list of active nodes, the node's energy status is calculated. The node's status will be presented in the subsequent phase.

Step (3). For the time being, the cluster head will be chosen based on the weight function, which includes the amount of available energy and the number of non-repeating nodes. Cluster heads are referred to as CH.

Step (4). This data will be stored in the routing table RTab using the settings listed below in Step 4 of the installation process.

Step (5). After that the closest neighbour node will be determined, and the process will be repeated from steps 1 through 4.

Step (6). After deciding on a route, the data is sent. If the network topology changes, go back to step 1 to 5 and repeat the process.

It may have a larger delay than other algorithms, but it will be more secure and energy-conscious than others.

Further, based on the Proposed MSA-SFO algorithm, the obtained results are discussed in the next section of the work.

A Stepwise Procedure for the Protection of Privacy When Utilizing the Modified Self-Adaptive Sailfish Optimization (MSA-SFO) Algorithm

In order to provide a concise explanation of the technique for the suggested privacy preservation in the MANET environment, the following is provided:

1) Data collecting the first thing that has to be done in order to complete this procedure is to acquire the necessary data set from the MANET environment. Text messages are used to carry out communication amongst the various mobile devices that are part of a MANET. These mobile devices serve as the edge platform for the MANET. These text messages include vital information, and the privacy settings ensure that it will not be disclosed to unauthorized parties. The subsequent step is to compose the basic text. The text message is generated using the cluster's acquired data. The raw data contains a number of different characters and strings. To guarantee the appropriate formatting of the text message, each character is converted into a 16-digit number.

2) If a 16-character-long text message is deemed to be covered by the privacy policy. To convert it to a simple text, each letter is converted to a binary value of 16 bits. This number is subsequently converted into the text's length. After the plain text has been generated, the ideal key must be generated. This procedure is performed to enhance privacy protection. The key is then sent to the hybrid chaotic map that processes the text. Using the suggested approach, the fundamental parameters of the map are adjusted, and the optimum key is then generated.

3) The encryption of a data file occurs immediately after the generation of the key. This phase entails utilising the binary plain text as the encryption's foundation. The result of the encryption is stored on the cloud, and only the owner has access to it. The process of producing ciphertext is referred to as the binary extension-or operation.

4) The decoding procedure is executed to extract the file's data. The key and the binary representation of the encryption are then subjected to a kind of XOR to guarantee the integrity of the original data.

IV. Results and Discussions

The obtained results are highly satisfactory and are furnished in this section of the work.

The simulation results with 30 notes are formulated here (Table I).

TABLE I. Simulation with 30 Nodes

Node Seq	Number of times Identify Disclosed (#)			
	FSR	*AODV*	*AOMDV*	*Proposed MSA-SFO Algorithm*
1	15	5	5	0
2	17	9	5	0
3	17	9	4	0
4	13	10	4	0
5	14	8	5	3
6	13	8	5	3
7	12	7	3	1
8	11	5	3	2
9	12	6	4	2
10	13	9	4	3
11	18	10	5	2
12	16	7	4	1
13	18	6	3	0
14	10	7	5	1
15	13	5	4	3
16	15	8	5	0
17	15	10	4	3
18	16	10	4	3
19	13	7	5	1
20	12	8	3	3
21	19	8	4	0
22	13	8	4	2
23	11	8	5	1
24	10	8	4	0
25	20	6	5	2
26	10	8	5	2
27	14	8	3	0
28	20	5	3	2
29	15	8	5	0
30	16	8	4	1

The results are visualized graphically here (Fig. 2).

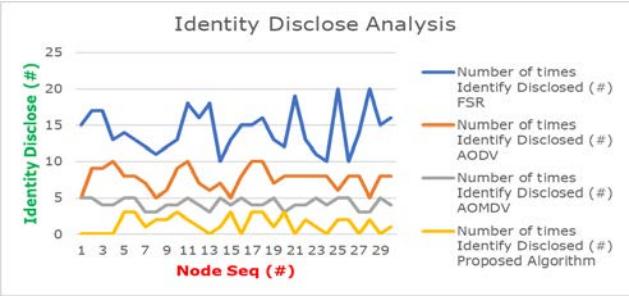

Fig. 2. Identify Disclose Analysis.

Further, in the next section of this work, the research conclusion is furnished.

The performance of the suggested MSA-SFO, as well as the performance of the comparison heuristic models is stated by the measurements. Tables II, III, IV, V, and VI exhibit the statistical performance of the suggested MSA-SFO as well as the comparing methodologies for different character lengths, including 20, 40, 60, 80, and 100 correspondingly. And the results are visualized graphically shown in Fig. 3, 4, 5, 6 and 7.

In comparison to the PSO, GWO, and SFO, the MSA-SFO framework has achieved the highest values. Additionally, it is 48 percent greater than the average performance. In terms of plot count, the proposed structure is likewise 90% better than the simple parameters. In addition, it has been 60 percent better than the GWO and 50 percent better than the WOA.

TABLE II. Statistical Analysis of with Key Generation with Length 20

Optimization Algorithm	PSO [15]	GWO [16]	WOA [17]	SFO [18]	Pamarthi [19]	Proposed MSA-SFO
Worst	0.0129	0.0136	0.0127	0.0127	0.0144	0.01512
Best	0.0497	0.0548	0.0457	0.053	0.0767	0.080535
Mean	0.0318	0.0342	0.0302	0.0335	0.0453	0.047565
SD	0.0112	0.0122	0.0101	0.012	0.0187	0.019635

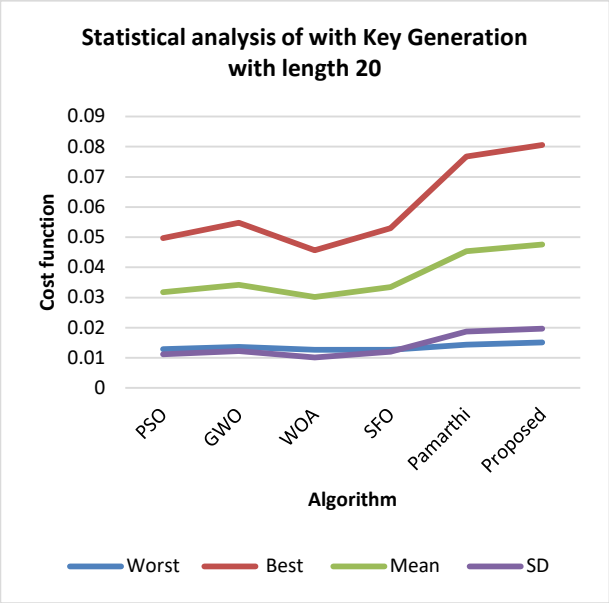

Fig. 3. Statistical Analysis of with Key Generation with Length 20.

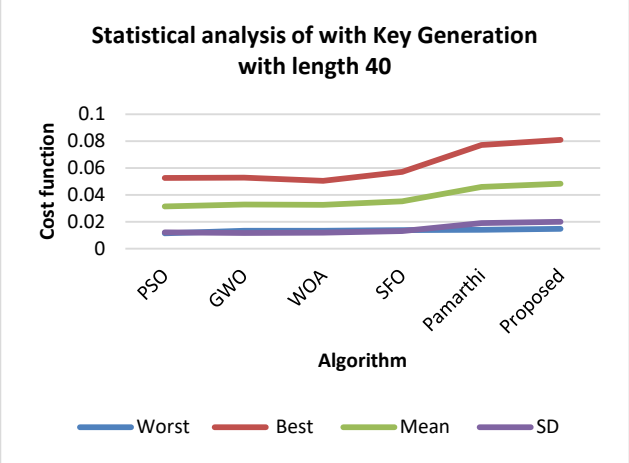

Fig. 4. Statistical Analysis of with Key Generation with Length 40.

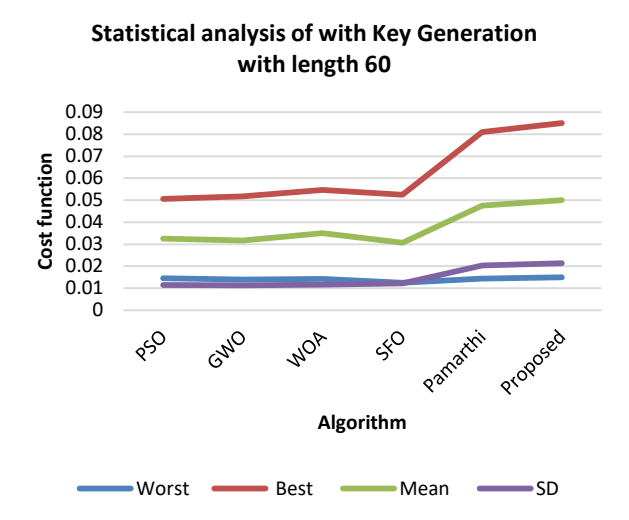

Fig. 5. Statistical Analysis of with Key Generation with Length 60.

TABLE III. STATISTICAL ANALYSIS OF WITH KEY GENERATION WITH LENGTH 40

Optimization Algorithm	PSO	GWO	WOA	SFO	Pamarthi	Proposed MSA-SFO
Worst	0.0116	0.0134	0.0135	0.0138	0.0141	0.014805
Best	0.0526	0.0529	0.0505	0.0573	0.0771	0.080955
Mean	0.0316	0.0329	0.0328	0.0353	0.046	0.0483
SD	0.0123	0.0118	0.0119	0.0133	0.0192	0.02016

TABLE IV. STATISTICAL ANALYSIS OF WITH KEY GENERATION WITH LENGTH 60

Optimization Algorithm	PSO	GWO	WOA	SFO	Pamarthi	Proposed MSA-SFO
Worst	0.0145	0.0139	0.0142	0.0125	0.0143	0.015015
Best	0.0506	0.0517	0.0546	0.0525	0.081	0.08505
Mean	0.0326	0.0317	0.035	0.0307	0.0476	0.04998
SD	0.0114	0.0113	0.0116	0.0122	0.0203	0.021315

TABLE V. STATISTICAL ANALYSIS OF WITH KEY GENERATION WITH LENGTH 80

Optimization Algorithm	PSO	GWO	WOA	SFO	Pamarthi	Proposed MSA-SFO
Worst	0.0143	0.0146	0.0133	0.0129	0.0138	0.01449
Best	0.0496	0.0526	0.0531	0.0443	0.079	0.08295
Mean	0.0324	0.034	0.0337	0.0285	0.046	0.0483
SD	0.011	0.012	0.0118	0.0093	0.0196	0.02058

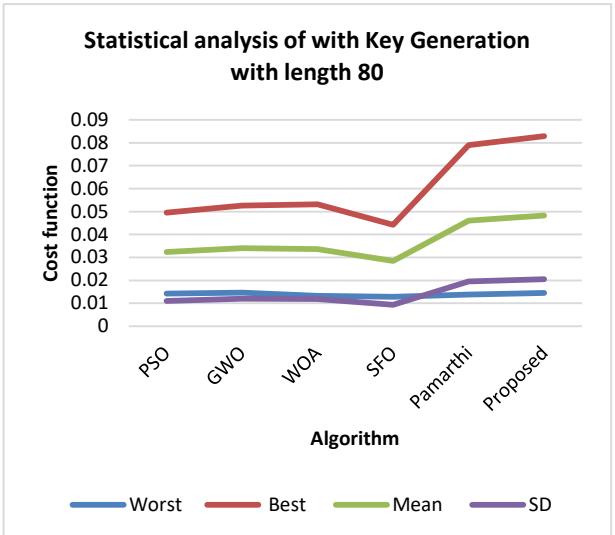

Fig. 6. Statistical Analysis of with Key Generation with Length 80.

TABLE VI. STATISTICAL ANALYSIS OF WITH KEY GENERATION WITH LENGTH 20

Optimization Algorithm	PSO	GWO	WOA	SFO	Pamarthi	Proposed MSA-SFO
Worst	0.0129	0.0136	0.0121	0.0121	0.0148	0.01554
Best	0.047	0.0526	0.053	0.0533	0.0794	0.08337
Mean	0.0296	0.0326	0.0338	0.0325	0.0466	0.04893
SD	0.0103	0.0122	0.013	0.0128	0.0196	0.02058

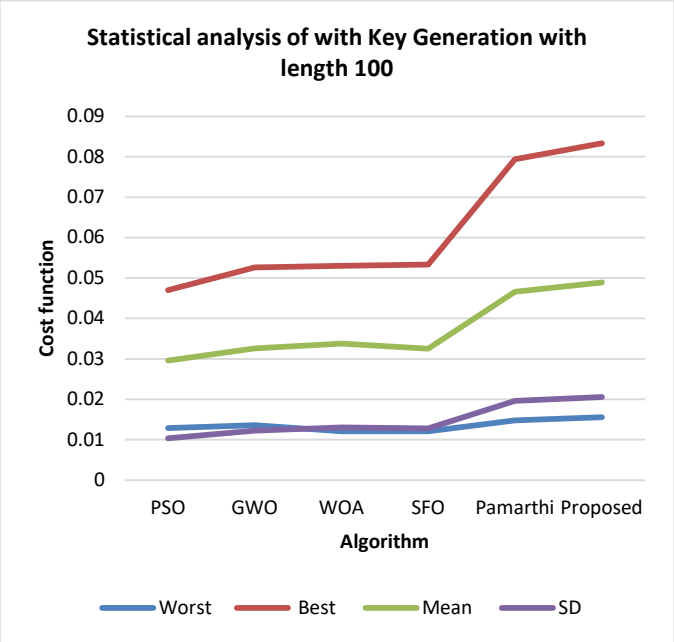

Fig. 7. Statistical Analysis of with Key Generation with Length 20.

V. CONCLUSION

MSA-SFO (Modified Self Adaptive Sail Fish Optimization) is a cluster-based routing method designed to increase the energy efficiency of current MANET routing algorithms. This research focuses on examining the different denial criteria of current algorithms. he researches compared the proposed system's performance to that of the current systems. Then, a performance study was conducted on the various systems, including the DSDV, DLSR, and FSR. It was discovered that the suggested strategy is more consistent and energy-efficient. The suggested algorithm, which has a 50 percent improvement in power awareness, serves as the foundation for a new algorithm designed to enhance the energy efficiency of current algorithms. In addition, a privacy preservation model was created to improve the security of MANET Wireless networks. The development of the suggested method has been significantly enhanced by the incorporation of the multi-state adaptive scheduling optimization approach (SFO). Utilizing this method, optimum key pairs were generated for the chaotic map. Messages were then encrypted and decrypted using the suggested technique. The development of the suggested method has been substantially enhanced by the use of the multi-state adaptive scheduling optimization approach (SFO). Utilizing this method, optimum key pairs were generated for the chaotic map. It has also increased the degree to which text messages may be secured from prying eyes. To verify that the suggested algorithm can safeguard the privacy of sensitive data, the investigators altered the length of the text messages. The suggested method has acquired the highest performance values, which are much greater than those of the PSO, GWO, and SFO. It is also much superior than the maximum character count for text messages, which is 100. In terms of performance, the suggested method has enhanced its values by around 90 percent. According to the results, the suggested algorithm MSA-SFO provides more security for MANET Wireless networks than alternative models. It also provides a high degree of security. Implementation of the suggested technique on a large number of nodes will increase the scope of this investigation.

REFERENCES

[1] N. Veeraiah et al., "Trust Aware Secure Energy Efficient Hybrid Protocol for MANET," in IEEE Access, vol. 9, pp. 120996-121005, 2021.

[2] A. Anand, H. Aggarwal and R. Rani, "Partially distributed dynamic model for secure and reliable routing in mobile ad hoc networks," in Journal of Communications and Networks, vol. 18, no. 6, pp. 938-947, Dec. 2016.

[3] M V Narayana, Rishi Sayal, H.S. Saini, Aparna Manikonda “Timestamp Based Certified Routing For Authorization And Authentication In Mobile Ad Hoc Network” Journal of Advanced Research in Dynamical and Control Systems, Volume-10, Issue-10, Page no.351-358, October-2018 -ISSN: 1943-023X.

[4] A. M. El-Semary and H. Diab, "BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map," in IEEE Access, vol. 7, pp. 95197-95211, 2019.

[5] Z. Hassan, A. Mehmood, C. Maple, M. A. Khan and A. Aldegheishem, "Intelligent Detection of Black Hole Attacks for Secure Communication in Autonomous and Connected Vehicles," in IEEE Access, vol. 8, pp. 199618-199628, 2020.

[6] M V Narayana, G Narsimha, SSVN Sarma, “Genetic - ZHLS Routing Protocol for Fault Tolerence and Load Balancing” Journal of Theoretical and Applied Information Technology, ISSN: 1992-8645 and E-ISSN: 1817-3195, 10th January 2016. Vol.83. No.1, pp. 72 – 80.

[7] B. U. I. Khan, F. Anwar, R. F. Olanrewaju, M. L. B. M. Kiah and R. N. Mir, "Game Theory Analysis and Modeling of Sophisticated Multi-Collusion Attack in MANETs," in IEEE Access, vol. 9, pp. 61778-61792, 2021.

[8] H. Fatemidokht, M. K. Rafsanjani, B. B. Gupta and C. -H. Hsu, "Efficient and Secure Routing Protocol Based on Artificial Intelligence Algorithms With UAV-Assisted for Vehicular Ad Hoc Networks in Intelligent Transportation Systems," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 7, pp. 4757-4769, July 2021.

[9] M V Narayana, Aparnarajesh Atmakuri “A-ZHLS: Adaptive ZHLS Routing Protocol for Heterogeneous Mobile Adhoc Networks” International Journal of Engineering & Technology, Volume 7 Issue 3(2018), PP.1626- 1630-ISSN: 2227-524X.

[10] U. Srilakshmi, S. A. Alghamdi, V. A. Vuyyuru, N. Veeraiah and Y. Alotaibi, "A Secure Optimization Routing Algorithm for Mobile Ad Hoc Networks," in IEEE Access, vol. 10, pp. 14260-14269, 2022.

[11] D. Hurley-Smith, J. Wetherall and A. Adekunle, "SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks," in IEEE Transactions on Mobile Computing, vol. 16, no. 10, pp. 2927-2940, 1 Oct. 2017.

[12] M V Narayana, G Narsimha, SSVN Sarma, “Secure- ZHLS: Secure Zone Based Hierarchical Link State Routing Protocol using Digital Signature”, International Journal of Applied Engineering Research, ISSN 0973-4562 Volume 10, Number 9 (2015) pp. 22927-22940..

[13] D. Falcão, R. Salles and P. Maranhão, "Performance evaluation of disruption tolerant networks on warships' tactical messages for secure transmissions," in Journal of Communications and Networks, vol. 23, no. 6, pp. 473-487, Dec. 2021.

[14] A. Tariq, R. A. Rehman and B. Kim, "Forwarding Strategies in NDN-Based Wireless Networks: A Survey," in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 68-95, Firstquarter 2020.

[15] Challa, S., Wazid, M., Das, A. K., Kumar, N., Reddy, A. G., Yoon, E. J., & Yoo, K. Y. (2017). Secure signature-based authenticated key establishment scheme for future IoT applications. IEEE Access, 5, 3028–3043.

[16] Gomes, G. F., da Cunha, S. S., Jr., & Ancelotti, A. C., Jr. (2019). A sunflower optimization (SFO) algorithm applied to damage identification on laminated composite plates. Engineering with Computers, 35, 619–626.

[17] Shadravan, S., Naji, H. R., & Bardsiri, V. K. (2019). The sailfish optimizer: A novel nature-inspired metaheuristic algorithm for solving constrained engineering optimization problems. Engineering Applications of Artificial Intelligence, 80, 20–34.

[18] Pedersen, M. E. H., & Chipperfield, A. J. (2010). Simplifying particle swarm optimization. Applied Soft Computing, 10(2), 618–628.

[19] Pamarthi, Satyanarayana, and R. Narmadha. "Adaptive Key Management-Based Cryptographic Algorithm for Privacy Preservation in Wireless Mobile Adhoc Networks for IoT Applications." Wireless Personal Communications 124.1 (2022): 349-376.