SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V11I11P112

Volume 11 Issue 11, 133-145, November 2024

Original Article

A Novel Cryptographic Based Session Key Generation Algorithm Framework for Improving Security in Mobile Ad-Hoc Network

S. Muruganandam[1], S. Gnanavel[2], N. Duraimurugan[3], G. Balamurugan[4*]

[1]*Department of Computer Science and Business Systems, Panimalar Engineering College, Tamilnadu, India,*
[2,4]*Department of Computing Technologies, SRM Institute of Science and Technology, Faculty of Engineering and Technology, Kattankulathur Campus, Tamil Nadu, India*
[3]*Department of Computer Science and Engineering, Rajalakshmi Engineering College, Tamil Nadu, India.*

[4]*Corresponding Author : balamurg1@srmist.edu.in*

Received: 13 September 2024 Revised: 12 October 2024 Accepted: 11 November 2024 Published: 03 December 2024

Abstract *- Mobile Ad-Hoc Networks (MANETs) are characterized by their dynamic topologies and lack of centralized control, making them highly susceptible to security threats. In order to improve the security of the network, this paper presents a Novel Cryptographic-Based Session Key Generation Algorithm Framework (NCBSKGAF). This framework has two phases; the first phase is designed as an Elliptic Curve Cryptography-Based Session Key Protocol (ECCBSKP), and the second phase represents Node Reputation Value Based Malicious Node Analysis (NRVBMNA). This framework also incorporates a mutual authentication mechanism to prevent unauthorized access and mitigate common attacks such as man-in-the-middle and replay attacks. The Elliptic Curve Cryptography-Based Session Key Protocol (ECCBSKP) model produces the session keys, which are sent to the recipient node and encrypted in a data packet. The session key ensures that transmission is performed within a particular time and attains secure data transmission. The Node Reputation Value Based Malicious Node Analysis (NRVBMNA) and Shortest Path Identification methods are proposed to identify the suspicious nodes and select the optimum route for data communication. The simulation results show that the suggested framework provides the maximum efficiency in all simulation conditions; the proposed NCBSKGAF provides 95% security accuracy compared to recent algorithms.*

Keywords *- Mobile Ad-Hoc Network (MANET), Elliptic curve based cryptographic, Malicious node, Session key, Node authentication.*

1. Introduction

MANET is the most popular networking technology due to its advanced technologies. Many security issues have been raised, particularly unauthorised access to network services. It is essential to secure the details of packets, user identities, and other network components from attackers to secure the networks [1]. In application domains like defence forces, rescue activities, government sectors, research, and industry organisations, electronic fraud and eavesdropping are two significant threats to the administration. If the two users want to share secret information over the network, the messages should be encrypted using cryptographic solid methods [2].

The feasible identification of routing procedures and hash functions is a primary element in network privacy [3]. In MANET, the reliability of functional based distance vector routing is demonstrated by examining the active sequence distance vector protocol. This method recommends increasing the security for Denial of Service (DoS) attacks [4]. The improved acceptance idea is proposed in which the suspicious nodes are identified with the help of strategies such as Hop count and sequence number count of a node in the route. The sender and receiver transform the messages with the help of key encryption.

This method uses an additional hash function known as the manual essential function "S." After the target node obtains the encrypted information, it returns the ACPT message to the source node [5]. The encrypted information is forwarded to the recipient via intermediary routes that reach the target. The system is considered excellent if the ACT data packet is received within a specific time frame [6]. The algorithm proceeds to the next stage if the ACPT data packet is not received. The root nodes in a network are grouped, and ACPT messages are transmitted between them.

If any nodes fail to send an ACPT message, that root is identified as suspicious, and the sender receives a disclosure

for confirmation [7]. The sender node receives the report packets during verification, and subsequently, it moves those particular data to the desired location in an alternative path. After verifying the corresponding route nodes, the sender and destination reports are compared, and the node is flagged as malicious. But, they can still not predict the malicious nodes effectively [8].

The effective intrusion detection and prevention system is designed with the help of reactive and proactive protocols to detect and eliminate malicious nodes. In this case, a grouping of nodes is produced, and a master node of the clusters is elected to distribute packets across routers without interruptions. To improve the clustering accuracy and security of the network, a route value linked to the chosen master node method is proposed. But, this method utilises a long time and power to identify the malicious nodes by transmitting the secure key. A fuzzy-oriented application was suggested for enhancing system performance and cluster node security by determining nodes that hold a private key. A secure transmission scheme and real-time accurate clustering are proposed to enhance QoS in MANET [9]. As described in this paper, various parameters are used to compute a node's trust value to enhance the MANET's Quality of Service (QoS) [10].

2. Related Works

Authenticity-based scheduled distance-related routing and elliptic based on curve cryptography are suggested for implementing security in MANET. This model uses the unique time-based session key to perform packet transmission [11]. The encryption is performed using the elliptic shape method, and a hash function is used to protect the session key. The data source, node identity, packet size, and geographical information of network nodes are protected by this suggested method [1] primarily by utilizing hash algorithms, it ensures data security and validity. The AODV protocol is used in conjunction with this technique. Effective security in MANET is achieved by this suggested technique while consuming the minimum amount of resources possible [12]. An authentication technique was suggested to prevent the black hole attack in MANET [13].

A multi-factor Cuckoo search-enhancing technique is used to carry out the viable election of master nodes. This technique is used to find the optimum route for the delivery of data packets [14]. It is recommended that a credibility-value-based node segment method be used to eradicate DoS attacks in the network [15]. The elliptic curve encryption algorithm-based AODV protocol was adopted to present a reliable approach to determining packet-dropping cyber-attacks [16]. The Minimum Overhead Secure Hash Algorithm (SHA)-based protected key generation in MANET was recommended to improve the system's integrity [17]. The validity of the Secure Adaptable Key Validation Decision was suggested to provide a reliable routing framework for IoT-based wireless networks to reduce energy consumption and improve secure transmission [18]. The 5G MANET is recommended to incorporate innovative trust-aware detection and avoidance of intrusion techniques [19]. The dynamic key-based encryption method protects privacy in IoT-related wireless networks [20].

Using feature selection and classification techniques, the intrusion detection model was created based on the activity of the nodes in order to identify nodes that might be suspect. This strategy is used in wireless networks to resist routing attackers. To improve the security of MANET, proactive data protection is implemented by deploying cryptography-based encryption functions. MANET can deliver better-quality service by elevating the network's throughput, clustering accuracy, and worm node detection efficiency. The challenges associated with node clustering can be addressed by using a method of optimization that results in higher energy reduction. The game optimization algorithm was suggested to reduce energy consumption. The geometric feature-based Yolo algorithm was introduced to increase the clustering accuracy [21]. Various studies provide a unique method for improving the security of MANET, but some security issues still need to be addressed. Many threats are raised due to its infrastructure and the nature of the network. This paper develops a novel method using an efficient cryptographic algorithm, a node authentication function, session key generation, and node reputation-based malicious node identification to improve MANET's Quality of Service (QoS).

3. Proposed Methodology

3.1. Elliptic Curve Cryptography (ECC) Model for Secure Session Key Generation

It is a type of symmetric key. The cryptography method also called the encryption with two keys method, is used to encode data using the curve method, and the computed curve point, which is applied in the encoding process, is shared exclusively with legitimate nodes in a network. In this process, the key pair values (i.e., symmetric and asymmetric keys) shall be encoded using a different expression for a curve function. For instance, the parabola's curve equation is expressed as the value transferred as a symmetric key.

$$Y=KX^2 + ZX + C \quad (1)$$

Where K and Z are coefficient factors of the elliptical curve, and C is the constant value.

Concerning, for instance, a = 3, b = 5, and c = 6, for computing the point in a slope, it is used as a private key in the encryption. It is necessary to draw a line linking the origin (-2,4) and (0,8), with the value of C = 8.

We shall represent the slope function of that curve as.

$$SK = \frac{X2 - X1}{Y2 - Y1} \quad (2)$$

$$SK = \frac{0 - (-2)}{8 - 4}$$

Hence, the value of the Secret Key (SK) is 0.5. This value will be used as a secret key when transmitting data packets to the network to enhance secure communication in MANET.

3.2. Proposed System Architecture

The structure of the architecture design presented in Figure 1 first consists of initialising nodes and forming the network, then implementing the clustering algorithm to elect a Cluster Head (CH) node to monitor other nodes in MANET.

This suggested method can be separated into two stages. Phase 1 is called the Elliptic Curve Cryptography-Based Session Key Protocol (ECCBSKP).

In this part, a Node Authentication function is initialised to verify the originality of a node. Before the data transmission is initialised, every packet is encrypted using the MD5 algorithm at the source node.

After the data packet is encoded, the Elliptic Curve Cryptography (ECC) method is applied to generate the session key to send the information to the destination node. At the end of Phase 1, the proposed method ensures that the session key will be produced and is ready to be distributed to the destination with the data packets.

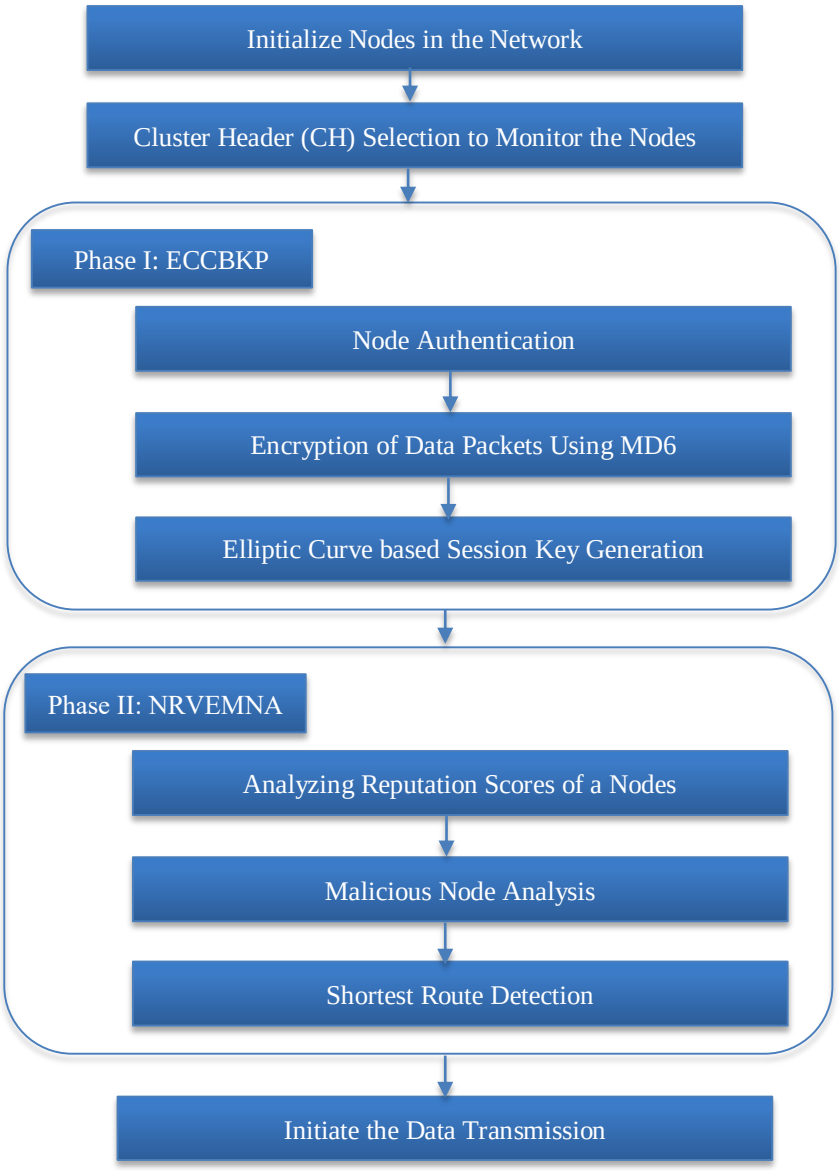

Fig. 1 Proposed system architecture

Phase II, called Node Reputation Value Based Malicious Node Analysis (NRVBMNA), will perform the reputation value analysis for all the nodes in the corresponding routes to the destination based on the neighbour node's suggestions. Various factors will be considered for computing the reputation value, such as energy consumption, distance between the nodes, and transmission speed. The merits of node reputation are included in detecting malicious nodes in networks. After executing all the above functions, the secure and shortest route is selected to initiate the data transmission process. The proposed approach develops the Quality of Service (QoS) in MANET.

3.3. Novel Cryptographic Based Session Key Generation Algorithm Framework (NCBSKGAF)

3.3.1. Algorithm 1: Cluster Head (CH) Node Identifying in MANET

Step 1: Initialization of every node in the network

```
function ClusterHeadSelection ():
for each node in the network:
    calculate Residual Energy (node)
    calculate Node Degree (node)
```

Step 2: Neighbour Information Exchange

```
for each node in network:
    exchange Information With Neighbors (node)
```

Step 3: Calculation of Node Weight

```
for each node in network:
    calculate Node Weight (node)
```

Step 4: Election of Cluster Heads

```
for each node in network:
    if decide To Become Cluster Head (node):
    announce Cluster Head Decision(node)
```

Step 5: Cluster Formation

```
for each non-cluster-head node in network:
    associate With Nearest Cluster Head (node)
```

Step 6: Periodic Update

```
Repeat every T seconds:
    for each node in network:
        if node is Cluster Head and
        energy Below Threshold (node):
        new Cluster Head=findBackupClusterHead(node)
    if new_ClusterHead is not None:
    announce_ClusterHeadDecision (new_ClusterHead)
    disassociate_WithPrevious_ClusterHead (node)
```

Step 7: End Process

3.3.2. Algorithm 2: Encryption of Data Packets Using MD5

Step 1: Initialize the function

```
function generateMD5Checksum(data):
    checksum = MD5(data)
    return checksum
```

Step 2: Include the MD5 checksum in the packet header or trailer

```
function sendPacketWithChecksum(data):
    checksum = generateMD5Checksum(data)
    packet = combine (data, checksum)
    send(packet)
```

Step 3: Extract data and checksum from the received packet

```
function receiveAndVerifyPacket(packet):
    received Data, received Checksum = split(packet)
```

Step 4: Calculate the MD5 checksum for the received data

```
calculate Checksum = generateMD5Checksum
                     (received Data)
```

Step 5: Compare the calculated checksum with the received checksum

```
if calculatedChecksum == received Checksum:
// Data integrity is verified; process the received data
process(received Data)
else:
// Data integrity check failed; discard the packet or
take appropriate action
discard(packet)
```

Step 6: End Process

3.3.3. Algorithm 3: ECC-Based Session Key Generation for Transmitting Data Packets between Source to Destination Node

Step 1: Key Pair Generation of Source and Destination nodes.

Initialization of Key Pair

Generate elliptic curve parameters (curve, base point, order, etc.)

```
// Public key of Source Node is indicted as pub(S)
// Private key of Source Node is indicted as priv(S)
// Public key of Target Node is indicted as pub(D)
// Private key of Target Node is indicted as priv(D)
```

Source Node: Generate private keys (priv(S)) and calculate public keys (pub(S)) = priv(S) * BasePoint

Destination Node: Generate private key (privD) and calculate public key (pubD) = priv(D) * BasePoint

Step 2: Perform Key Exchange between Source to Destination Node.

Source Node to Destination Node:

Source Node sends pub(S) to Destination Node

Destination Node to Source Node:

Destination Node sends pub(D) to Source Node

Step 3: Shared Secret Key Derivation.

Source Node:

SharedSecretKey (Source Node) = priv(S) * pub(D)

Destination Node:

SharedSecretKey (Destination Node) = priv(D) * pub(S)

Step 4: Session Key Generation.
Source Node (S):
Session Key(S) = Hash Function (Shared Secret (S))
Destination Node (D):
Session Key(D) = Hash Function (SharedSecret (D))

Step 5: Perform data transmission using the generated session key.

Step 6: End Process.

3.3.4. Algorithm 4: Malicious Node Detection in a MANET Using An ECC-Based Session Key

Step 1: Session Key Exchange and Monitoring.
Key Exchange (As per ECC-based session key generating techniques):
// Follow the ECC-oriented session key producing method
Monitor Session Key Usage:
while communication is ongoing:
if Source Node detects inconsistent session key usage by Destination Node:
// Flag NodeB as potentially malicious

Step 2: Behaviour Monitoring.
Monitor Communication Patterns between Source and Destination Node:
for each node in the network:
if node communication patterns deviate significantly from normal:
// Flag the node as potentially malicious
Monitor ECC Key Generation Behaviour:
for each node in the network:
if a node generates an abnormal number of ECC key pairs:
// Flag the node as potentially malicious

Step 3: Consistency Checks
Verify Consistency of Public Keys:
for each pair of communicating nodes (Source Node(S), Destination Node(D)):
if the received public key of Destination Node (D) does not match the expected public key:
// Flag Destination Node (D) as potentially malicious
Verify Consistency of Session Keys:
for each pair of communicating nodes *(Source Node(S), Destination Node(D)):*
if the session key usage between *Source Node(S), Destination Node(D)* is inconsistent:
// Flag Destination Node (D) as potentially malicious

Step 4: Reputation System.
Maintain a Reputation Score for Each Node:
for each node in the network:
periodically update the reputation score based on behaviour
Threshold-based Detection:
for each node in the network:
if the credibility score appears below a predefined threshold:
// Flag the node as potentially malicious

Step 5: Collaborative Detection.
Exchange Anomaly Information:
for each node in the network:
periodically exchange information about detected anomalies with neighbours
Consensus-based Detection:
for each node in the network:
if a consensus among neighbours is reached regarding a node's malicious behaviour:
// Flag the node as malicious

Step 6: Response Mechanisms.
If a node is flagged as potentially malicious:
- Initiate secure communication with the suspected node for verification
- Eliminate the node from the system if the suspicion is confirmed
- Share information about the malicious node with neighbouring nodes

Step 7: Eliminating the malicious node in the network

Step 8: End the process.

3.3.5. Algorithm 5: Calculating Reputation Scores in a MANET

Step 1: Initialization Reputation Score.
for each node in the network:
initialize Reputation Score[node] = InitialReputationValue initialize Trust Count[node] = 0

Step 2: Behaviour Monitoring of a Node.
Monitor Communication Patterns between Source and Destination Node:
for each communication event between Source Node(S) and Destination Node (D):
if the communication is successful and follows normal patterns:
Trust Count [Destination Node (D)] ++
else:
// Optionally decrease Trust Count or take other actions
Monitor Collaborative Behaviour of Source (S) and Destination Node(D):
for each collaborative task involving Source Node(S) and Destination Node (D):
if the collaboration is successful and meets expectations:
Trust Count [Destination Node (D)]++
else:
// Optionally decrease Trust Count or take other actions

Step 3: Update Reputation Score.
for each node in the network:
Reputation Score[node] = Trust Count[node] / Total Interactions

Step 4: Detection of Bonus/Malus points of a node.
for each node in the network:
if node exhibits exceptional behaviour:
Reputation Score[node] += Bonus Points
else if node exhibits suspicious or malicious behaviour:
Reputation Score[node] -= Malus Points

Step 5. Calculating Threshold-based detection of High and Low Reputation nodes in a network.
for each node in the network:
if Reputation Score[node] < Low Threshold:
// Optionally take actions, e.g., limit interactions or isolate the node
else if Reputation Score[node] > High Threshold:
// Optionally reward the node or increase its privileges

Step 6: End the process

3.3.6. Algorithm 6: Shortest Route Identification Using ECC-Based Session Key

Step 1: Discovery of Network Topology
Initialize the network topology by discovering neighbours and estimating link quality metrics.

Step 2: Session Key Establishment in a network.
For each pair of neighbouring nodes (Source Node (S), Destination Node(D)):
Perform ECC-based session key exchange as per the session key generation algorithm.

Step 3: Detection of Shortest Route Identification.
Initialization:
Initialize the routing table and distance vectors for each node.
Dijkstra's Algorithm:
For each node in the network:
Initialize distance vector and predecessor information.Set the distance to itself as 0 and infinity for other nodes.
Repeat up to every node are included in the shortest path tree:
a. Select the node with the least distance that is not in the shortest path tree.
b. Update distances to neighbouring nodes considering link quality metrics.
c. Update predecessor information.

Step 4. Perform Secure Route Verification
For each identified route in a network:
Verify the security of the route using ECC-based session keys. Discard routes with compromised security.

Step 5: End the Process.

3.3.7. Algorithm 7: Inspection of Malicious Nodes in a MANET

Step 1: Perform Data Collection from all Cluster Head (CH) nodes in the network
Collect Reviews:
Collect reviews from CH in the MANET regarding Transmission Speed, Reputation Score, and utilisation of energies of nodes in the networks.

Step 2: Perform Review Analysis in a Network
Sentiment Analysis:
For each review:
Apply sentiment evaluation to identify an entire sentiment (positive, negative or neutral).
Source Reputation:
For each node providing reviews:
Check the reputation of the source node based on historical data or a eputation system.
Frequency Analysis:
For each reviewed entity:
Analyze the frequency of reviews from different nodes. Identify entities with a disproportionately high number of reviews from a single node or a group of nodes.

Step 3: Anomaly Detection in a network
Deviation from Norm:
Identify reviews that deviate significantly from the norm in terms of sentiment, source reputation, or frequency.
Collaborative Detection:
Exchange information about detected anomalies with neighboring nodes. Leverage consensus-based mechanisms to identify suspicious patterns collaboratively.

Step 4: Source Node Verification
Secure Identity:
Ensure that the source node's identity is secure and not easily forgeable.
ECC-based Verification:
Leverage ECC-based session keys or digital signatures to verify the authenticity of reviews.

Step 5: Response Mechanisms
For identified suspicious reviews:
- Flag the reviews for further investigation.
- Optionally, reduce the impact of suspicious reviews in decision-making processes.
- Consider isolating or limiting interactions with nodes providing suspicious reviews.

Step 6: End the Process

3.3.8. Algorithm Flow Model

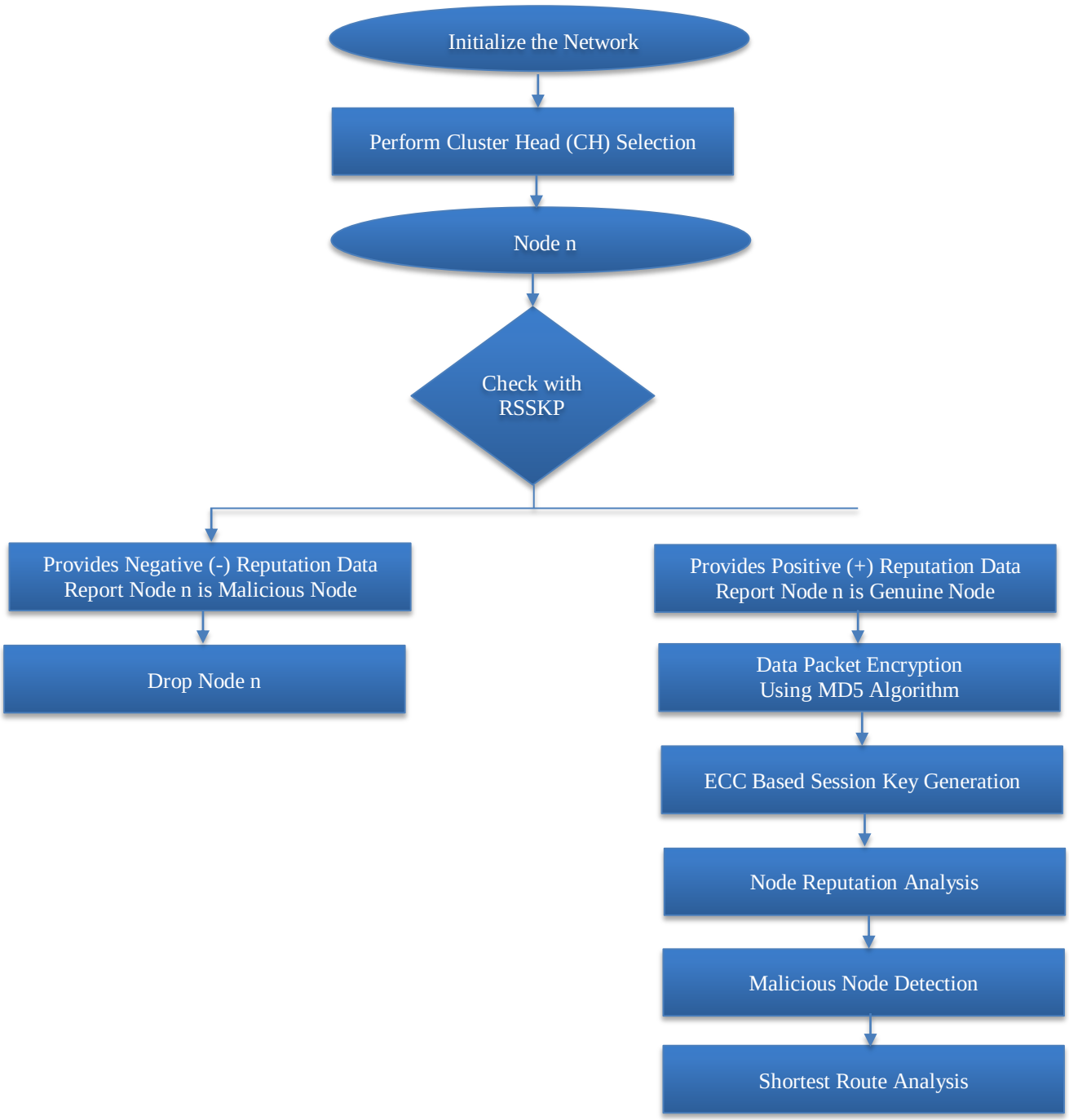

Fig. 2 Flow diagram of the proposed algorithm

4. Results and Discussion

The proposed method is adequately coded with Network Simulator (NS 3), and the performance is evaluated with multiple factors by different numbers of nodes in the network. This section examines the experimental outcomes that have been observed.

Table 1. Specifications of modeling

Parameters	Values
Simulator	NS3
Simulation Range	1000 Meters
Quantity of nodes	200
Movement Range	100 Meters

The parameters taken for the performance analysis of various methods are detailed in Table 1, where they have been evaluated using various metrics and discussed in this section.

4.1. Node Clustering Reliability

The clustering reliability of any algorithm is estimated in relation to the number of consistent nodes created by the techniques for the total number of nodes in the networks.

$$Node\ Clustering\ Reliability\ = \frac{No.of\ Consistent\ Nodes}{Total\ No.of\ Nodes\ in\ the\ Network} \quad (3)$$

Table 2 provides a detailed presentation of the analysis conducted on several methods to estimate the accuracy of clustering. However, the suggested NCBSKGAF method has provided higher clustering accuracy than previous techniques. The recommended algorithm has generated 85%, 93%, and 96% of classifying reliability in the presence of 50-node, 100-node, and 200-node in the system, which is higher than the DNACA, NRAI, ECC-AODV-ACO, and SA-SFO algorithms.

Table 2. Evaluation of clustering reliability

Evaluation of Clustering Reliability			
	50 Nodes	100 Nodes	200 Nodes
DNACA	67	72	76
NRAI	71	74	81
ECC-AODV-ACO	73	76	82
SA-SFO	75	81	84
NCBSKGAF	83	91	96

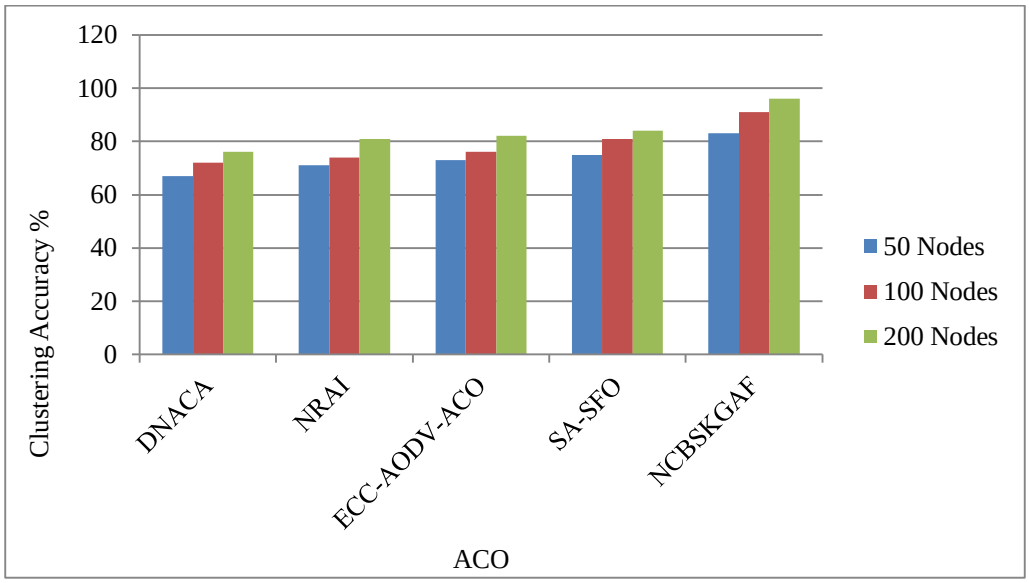

Fig. 3 Analysis of clustering reliability

By modifying the network nodes, the efficiency of clustering the nodes is examined and shown in Figure 3. The recommended method has initiated greater efficiency than the DNACA, NRAI, ECC-AODV-ACO, and SA-SFO algorithms.

4.2. Security Analysis

The integrity review of the approach is calculated in relation to the number of risks identified and the total number of risks produced. It has been evaluated and has the following equation:

$$Security\ Analysis = \frac{No.Of\ Risks\ Identified}{Total\ No.Of\ Risks\ Produced} \quad (4)$$

Table 3 presents the security attainment of various methods by evaluation. It shows that the proposed method produces greater security improvements than other methods. The proposed NCBSKGAF attained security enhancement in the proportion of 86%, 92%, and 97% of privacy enforcement in the presence of 50-node, 100-node, and 200 -node of testing scenarios, which is greater than DNACA, NRAI, ECC-AODV-ACO, and SA-SFO algorithms.

Table 3. Evaluation of security performances

Evaluation on Security			
	50 Nodes	100 Nodes	200 Nodes
DNACA	66	67	72
NRAI	68	72	75
ECC-AODV-ACO	72	73	76
SA-SFO	74	76	84
NCBSKGAF	85	91	95

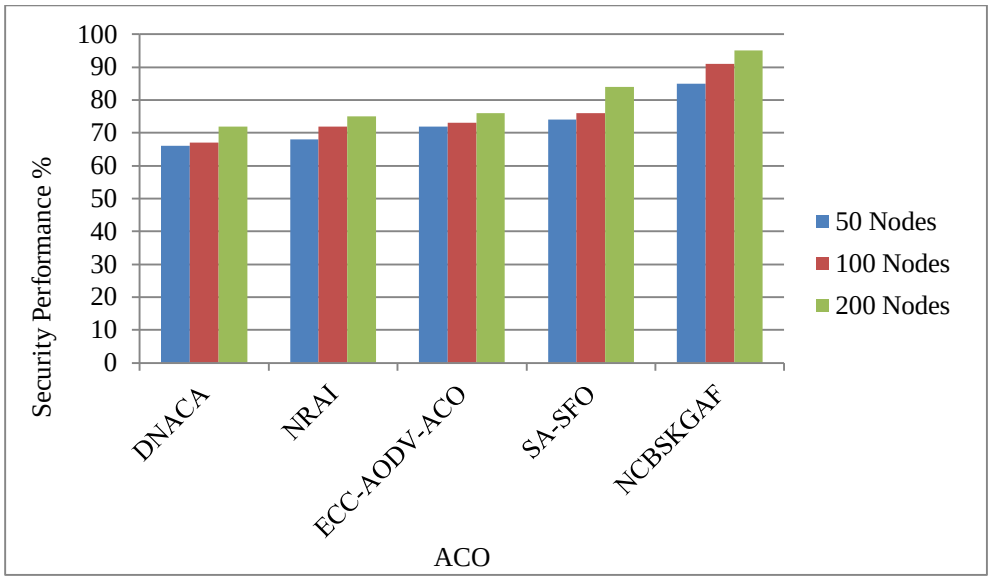

Fig. 4 Enhancement in security

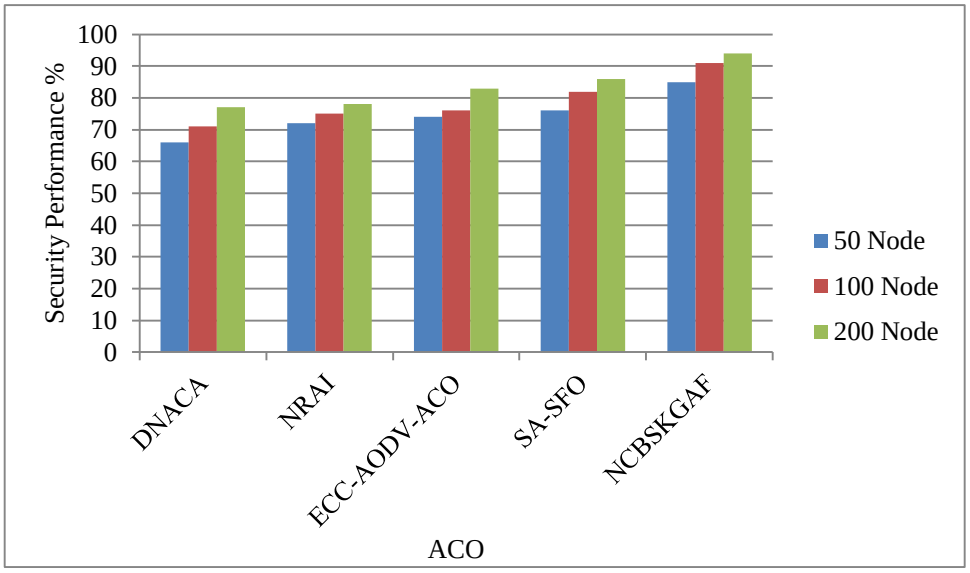

Fig. 5 Throughput analysis

The security enhancements produced by several methods are compared in Figure 4. The suggested algorithm produces greater security improvements than other methods considered.

4.3. Throughput Analysis

The throughput achievement of any method is computed by the number of data packets delivered at a particular time. It has been examined using the below equation:

$$Throughput = \frac{Total\ No.Of\ \ Data\ Packets\ Transmitted}{Time} \quad (5)$$

The estimated throughput ratios obtained by different techniques are presented in Table 4. It displays that the proposed algorithm delivers maximum throughput efficiency when compared to existing approaches. The suggested method has generated a data transfer rate of 86%, 92%, and 97% in the 50-node, 100-node, and 200-node simulation scenarios, respectively, compared to various techniques.

Table 4. Assessment of throughput attainment

Evaluation of Throughput Analysis			
	50 Node	100 Node	200 Node
DNACA	66	71	77
NRAI	72	75	78
ECC-AODV-ACO	74	76	83
SA-SFO	76	82	86
NCBSKGAF	85	91	94

The throughput efficiency obtained with the execution of various algorithms is identified and presented in Figure 6. The suggested technique performed better than various techniques with respect to throughput performance.

4.4. Suspicious Node Identification Reliability

The degree of reliability in identifying suspicious nodes in the network is computed in relation to the total quantity of nodes present in the network and the number of nodes observed accurately. It is calculated by using the formula below:

$$Suspicious\ Node\ Detection\ Reliability = \frac{No\ of\ Nodes\ Presence\ in\ the\ Network}{No\ of\ Nodes\ identified\ sucessfully} \quad (6)$$

Table 5. Assessment of suspicious node identification analysis

Assessment of Suspicious Node Identification Efficiency			
	50 Node	100 Node	200 Node
DNACA	62	68	73
NRAI	65	73	76
ECC-AODV-ACO	72	76	78
SA-SFO	74	78	82
NCBSKGAF	85	91	96

The effectiveness of different methods for identifying suspicious nodes in the networks is identified and shown in Table 5: The suggested NCBSKGAF method has produced a maximum prediction rate in suspicious node identification capacity compared to different methods. The recommended model generates suspicious node detection efficiency in proportion to 86%, 92%, and 97% in the 50-node, 100-node, and 200-node simulation cases compared to DNACA, NRAI, ECC-AODV-ACO, and SA-SFO algorithms. The efficiency of suspicious node identification is reviewed and presented in Figure 6. The recommended algorithm raised suspicious node detection reliability with various algorithms.

4.5. Power Utilization Analysis

The amount of power consumed by a method is evaluated based on how many transmissions are made and how many joules the node uses.

$$Power\ utilisation\ Efficiency = \frac{The\ amount\ of\ power\ in\ joules\ allocate\ by\ the\ Node}{Total\ No.Transmission\ completed} \quad (7)$$

Table 6. Power utilisation analysis

Power utilisation Analysis in Joules			
	50 Node	100 Node	200 Node
DNACA	67	76	86
NRAI	64	74	85
ECC-AODV-ACO	66	72	76
SA-SFO	53	63	71
NCBSKGAF	47	54	57

The energy consumption generated by various methods with different numbers of nodes is identified and presented in Table 6. The proposed method utilizes much less power for a particular number of communications in all testing scenarios. The suggested NCBSKGAF method shows power utilization in the proportion of 47%, 54% and 57% in the 50 - node, 100 - node and 200 - node simulation testing cases than existing DNACA, NRAI, ECC-AODV-ACO, SA-SFO algorithms.

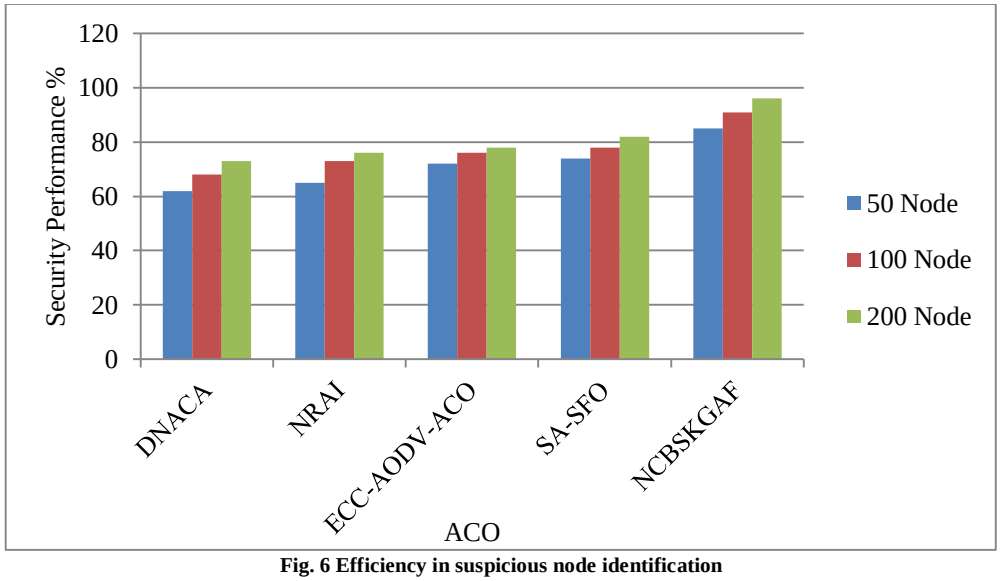

Fig. 6 Efficiency in suspicious node identification

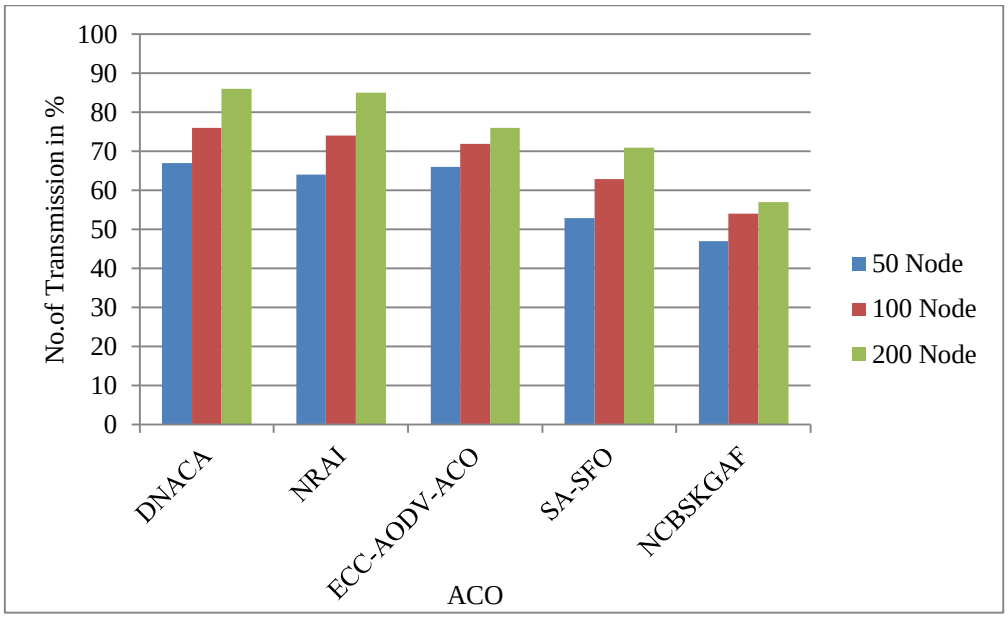

Fig. 7 Analysis of energy consumption

The productivity of the proposed technique was evaluated for power utilization for packet transmission. Based on the analysis, it has been determined that the suggested NCBSKGAF method has consumed less power than existing methods.

4.6. Efficiency Analysis of Various Specifications

The efficiency of existing algorithms in various measures is identified and presented in Table 7. The estimated power utilisation of the suggested algorithm is 57 joules in a 200-node network, which is comparatively less than existing algorithms. The minimum power consumption is particularly attained as a result of reliability in clustering. The clustering reliability of the suggested algorithm is 96%, which is significantly greater than existing methods. ECC-AODV-ACO and SA-SFO gain the following position for classification reliability with a reliability rate of 82% and 84%, respectively. The greater network dimension and suspicious node identification are the main reasons for the higher classification accuracy. Data transmission and suspicious node identification reliability depend on the number of suspicious nodes present in the network. Due to suspicious nodes, which result in high packet delays or disable transmissions by utilizing higher power for delivering suspicious data chunks, The deficiency of a stable protection plan in the DNACA and NRAI algorithms affects minimum bandwidth and suspicious node identification reliability. The suggested algorithm has created more efficiency in all attributes than existing methods.

Table 7. Efficiency analysis of various methods

Efficiency Analysis of Various Methods					
	Suspicious Node Identifying Accuracy %	**Throughput attainment %**	**Security attainment %**	**Average Energy Utilization in Joules**	**Clustering Quality %**
DNACA	73	77	72	86	76
NRAI	76	78	75	85	81
ECC-AODV-ACO	78	83	76	76	82
SA-SFO	82	86	84	71	84
NCBSKGAF	96	94	95	57	96

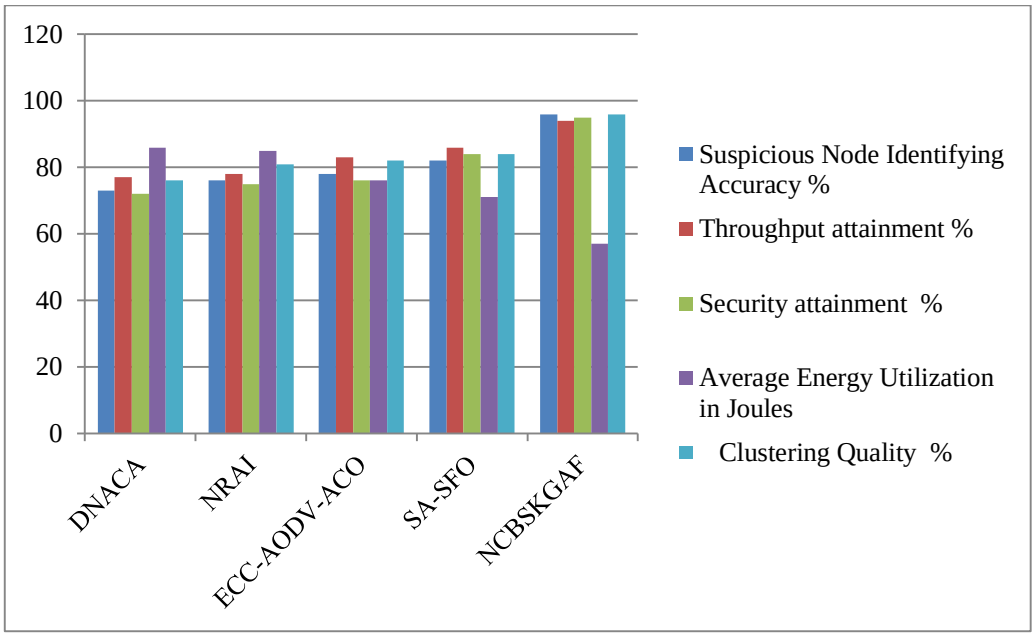

Fig. 8 Efficiency analysis of various methods

The efficiency analysis of various algorithms in various measurements is displayed in Figure 8. The suggested algorithm has created greater efficiency in all the features compared to existing methods.

5. Conclusion and Future Enhancement

This article discusses the novel Cryptographic Based Session Key Generation Algorithm Framework (NCBSKGAF) for improving security in MANET. This proposed framework first implements cluster head selection based on node features. Additionally, it was recommended that data packets be encrypted using the MD5 technique to enable privacy when delivering packets over a network.For secure communication of data between nodes in the MANET, the Elliptic Curve Cryptography (ECC)-based session authentication system is used. An automated node detection method integrated with session keys was developed to discover and eliminate the suspected nodes in the MANET. In addition, node trust values are computed to confirm that every node in the network is authentic.

In order to maintain and enhance the security of data interaction, a feasible path identification algorithm is subsequently executed by applying an ECC-based session key and a suspected node analysis. The proposed framework increases the efficiency of suspected node discovery, cluster stability, and productivity. In mobile ad hoc networks, the recommended algorithm design increases the network's overall Quality of Service (QoS).

In future enhancements, a region-based node identification model will be introduced to identify suspected nodes' locations. The advanced supervised machine learning algorithm is developed to detect the malicious nodes more accurately, and the node location is taken as one of the node quality features to compute the reliability of a node in the network. The network capacity will be improved by adding more than 200 nodes; the system will also be enhanced to support a sizeable wireless network with better security performances.

References

[1] K. Sakthidasan Sankaran, and Seng-Phil Hong, “Trust Aware Secured Data Transmission Based Routing Strategy Using Optimal Ch Selection in Mobile Ad-Hoc Network,” *Mobile Networks and Applications*, pp. 1-13, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] V. Krishnakumar, and R. Asokan, “Block Chain Based Trusted Distributed Routing Scheme Using Optimized Dropout Ensemble Extreme Learning Neural Network in MANET,” *Peer-to-Peer Networking and Applications*, vol. 16, pp. 2696-2713, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] Meena Rao et al., “A Secure Routing Protocol Using Hybrid Deep Regression Based Trust Evaluation and Clustering for Mobile Ad-Hoc Network,” *Peer-to-Peer Networking and Applications*, vol. 16, pp. 2794-2810, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] Gajendra Kumar Ahirwar, Ratish Agarwal, and Anjana Pandey, "An Extensive Review on QoS Enhancement in MANET Using Meta-Heuristic Algorithms," *Wireless Personal Communications*, vol. 131, pp. 1089-1114, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] Dipak W. Wajgi, and Jitendra V. Tembhurne, "Localization in Wireless Sensor Networks and Wireless Multimedia Sensor Networks Using Clustering Techniques," *Multimedia Tools and Applications*, vol. 83, pp. 6829-6879, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] M. Venkata Krishna Reddy, P.V.S. Srinivas, and M. Chandra Mohan, "Energy Efficient Routing with Secure and Adaptive Trust Threshold Approach in Mobile Ad Hoc Networks," *The Journal of Supercomputing*, vol. 79, pp. 13519-13544, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] Rakesh Kumar, Bhisham Sharma, and Senthil Athithan, "TBMR: Trust Based Multi-Hop Routing for Secure Communication in Flying Ad-Hoc Networks," *Wireless Networks*, pp. 1-17, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Zafar Sherin, and M.K. Soni, "Secure Routing in MANET through Crypt-Biometric Technique," *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014, Advances in Intelligent Systems and Computing*, vol. 328, pp. 713-720, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[9] N. Sridevi, and V. Nagarajan, "A Curve Based Cryptography for Wireless Security in MANET," *Cluster Computing*, vol. 22 pp. 4017-4025, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[10] Priyanka Pandey, and Raghuraj Singh, "QoS Based Modified Route Discovery in MANET for Multimedia Applications," *Multimedia Tools and Applications*, vol. 82, pp. 29671-29688, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] Vivek Mankotia, Ramesh Kumar Sunkaria, and Shashi Gurung, "DT-AODV: A Dynamic Threshold Protocol against Black-Hole Attack in MANET," *Sādhanā*, vol. 48, no. 4, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] Subrata Joardar et al., "Mitigating DoS Attack in MANETs Considering Node Reputation with AI," *Journal of Network and Systems Management*, vol. 31, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] S. Kanthimathi, and P. Jhansi Rani, "An Efficient Packet Dropping Attack Detection Mechanism in Wireless Ad-Hoc Networks Using ECC Based AODV-ACO Protocol," *Wireless Networks*, vol. 30, pp. 4851-4863, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] Srividya Ramisetty, and K.P. Vyshali Rao, "Light Weight Hash Function Using Secured Key Distribution Technique for MANET," *International Journal of Information* Technology, vol. 14, pp. 3099-3108, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] Uma Meena, and Promila Sharma, "Secret Dynamic Key Authentication and Decision Trust Secure Routing Framework for Internet of Things Based WSN," *Wireless Personal Communications*, vol. 125, pp. 1753-1781, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Saleh A. Alghamdi, "Novel Trust-Aware Intrusion Detection and Prevention System for 5G MANET–Cloud," *International Journal of Information Security*, vol. 21, pp. 469-488, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[17] Satyanarayana Pamarthi, and R. Narmadha, "Adaptive Key Management-Based Cryptographic Algorithm for Privacy Preservation in Wireless Mobile Adhoc Networks for IoT Applications," *Wireless Personal Communications*, vol. 124, pp. 349-376, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[18] Mahendra Prasad, Sachin Tripathi, and Keshav Dahal, "An Enhanced Detection System against Routing Attacks in Mobile Ad-Hoc Network," *Wireless Networks*, vol. 28, pp. 1411-1428, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[19] Sunil Kumar, "Security Enhancement in Mobile Ad-Hoc Network Using Novel Data Integrity Based Hash Protection Process," *Wireless Personal Communications*, vol. 123, pp. 1059-1083, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[20] D. Anuradha et al., "Energy Aware Seagull Optimization-Based Unequal Clustering Technique in WSN Communication," *Intelligent Automation & Soft Computing*, vol. 32, no. 3, pp. 1325-1341, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[21] R. Saravanan, A. Swaminathan, and S. Balaji, "An Intelligent Shell Game Optimization Based Energy Consumption Analytics Model for Smart Metering Data," *Scientific and Technical Journal of Information Technologies*, vol. 23, no. 2, pp. 374-381, 2023. [CrossRef] [Google Scholar] [Publisher Link]