EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Reputation based Symmetric Key Authentication for Secure Data Transmission in Mobile Ad Hoc Networks

S. Sangeetha[1,*] and Dr. S. Sathappan[2]

[1]Research Scholar, Department of Computer Science, Erode Arts and Science College, Erode, Tamil Nadu 638112, India.
[2]Associate Professor, Department of Computer Science, Erode Arts and Science College, Erode, Tamil Nadu 638112, India.

Abstract

INTRODUCTION: MANETs were a group of nodes which connected each other to establish the network via wireless association to forward packets towards destinations.
OBJECTIVES: Reputation-based Symmetric Key Authentication (RSKA) technique is proposed to improve the security of data communication, which securely transmits data packets within MANET communication. Initially, a reputation counts-based node authentication algorithm is designed in RSKA technique by considering the reputation value of mobile nodes in networks.
METHODS: By using a reputation count-based node authentication algorithm, the RSKA technique performs the node authentication process before initiating route identification and selects cooperative nodes in MANETs for data transmission. Therefore, the RSKA of nodes results in improved security of data communication for enhancing throughput and reducing data loss rate. Besides, the RSKA technique uses symmetric key cryptography for secure data transmission in which a secret key is generated for the data to be transmitted by the corresponding mobile node along the route path of the source-destination pair. The destination node having the secret key can only decrypt the cypher text.
RESULTS: Thus, the RSKA technique improves the data confidentiality rate as well as minimizes the time to protect the data transmission in an efficient way. RSKA was calculated by various parameters, namely data loss rate, throughput and time to protect data delivery as well as data confidentiality rate. CONCLUSION: The simulation result of RSKA improves the data confidentiality rate for achieving secured data transmission as well as minimizes time to protect data delivery within MANETs compared with conventional methods.

Keywords: Reputation; Mobile nodes; Node authentication; Confidentiality; Symmetric key Cryptography; Secret key.

Received on 13 July 2022, accepted on 10 February 2023, published on 30 March 2023

doi: 10.4108/eetsis.v10i3.1940

1. Introduction

MANETs are a set of nodes that create the network for replacing data. The key challenging task in MANETs was used to offer protection for routing the data and checking malicious nodes over the network. Therefore, a node authentication technique is required to authenticate the node while connecting to the network. In addition, MANETs are more susceptible to security attacks, and therefore cryptographic schemes are exploited to ensure security and data confidentiality during transmission. However, existing cryptographic schemes does not afford more security and data confidentiality rate. Therefore, there is a need for a novel technique for node authentication to enhance the security of data transmission by a better data confidentiality rate.

2. Literature Survey

Kai He, Min-Rong Chen [1] et al. developed a Hierarchical Identity-Based Encryption (HIBE) scheme for achieving secure data transmission in MANETs. The HIBE scheme

*Corresponding author. Email: sangeethasaya8@gmail.com

ensures data confidentiality. However, the data loss rate was more. Huansheng Ning [2] et al. presented Aggregated-Proof based Hierarchical Authentication (APHA) to achieve data confidentiality as well as data integrity. But, the APHA scheme consumes more time to protect data.

Srinivas Aluvala [3] et al. developed a novel technique to provide node authentication and also to reduce the impact of attacks on nodes in MANETs. However, the performance issues of huge networks were not measured. Besides, data confidentiality remained unsolved. A. Suresh and K. Duraiswamy designed a mobility-based node's reputation for enhancing the effectiveness of network data transmission among various nodes. Though, the packet loss rate was higher.

Suja Rajeswari K, Arivazhagi A [5] introduced a novel method of belief and reputation management by combining dissimilar trust mechanisms for forecasting nodes precisely depending on cluster head and cluster member communication. Jan Papaj and Lubomir Dobos[6] developed a trust-based relay node selection for choosing the relay nodes with the aid of trust value and also providing the secure transportation of data in MANETs. However, this algorithm does not provide more security for data transmission. R. Menaka, V. Ranganathan [7] et al. presented a fuzzy-based model using trust and reputation to improve the routing performance of the network and to identify a secured method to perform data. However, DoS attacks were not measured, which reduces levels of security for achieving higher throughput.

Tejashree Kokate, R.B. Joshi [8] introduced a scalable and lightweight mechanism to solve the issues of authentication in multicast mobile ad hoc networks. However, hop-to-hop connectivity and integrity remained unsolved. Moazam Bidaki and Mohammad Masdari [9] designed a Trust-based clustering algorithm to identify malicious nodes by lesser communication as well as improve the routing process in MANETs. But the security level was poor.

J.Subash Chandra Bose[10] et al. developed an acknowledgment-Based Secure Authentication Method for MANETs multiple keys were employed for encryption as well as decryption along with a digital signature to enhance the protection of data. The network overhead caused by digital signature was not considered, which lacks throughput rate. Sangheetaa Sukumran et al [11] designed to improve the routing process with higher security in MANET.

Ahmad Alomari [12] et al. introduced a novel scheme to maintain mutual authentication as well as encrypt among nodes and to resolve protection as well as privacy problems among two nodes. Zehua Wang [13] et al. developed cooperative Opportunistic Routing in Mobile Ad hoc Networks (CORMAN) for detecting intermediate nodes for data transmission. The CORMAN enhances the packet delivery ratio as well as reduces delay within MANETs. But, the secured data communication has remained unsolved.

Shengbo Yang [14] et al. presented Position-based Opportunistic Routing (POR) to address an issue related to data delivery in MANET. POR protocol achieves a higher packet delivery ratio as well as lessens the end-to-end delay within MANETs. Though, security and confidentiality of data delivery were not considered. B. Madhusudhanan[15] et al. introduced mobility-based key management to multicast protection within MANETs, which diminishes packet drop rate as well as enhances data confidentiality. However, routing overhead was higher.

Hamza Aldabbas[16] et al. designed the policy-based architecture to improve the privacy and data confidentiality in MANETs. Garimella Uma[17] et al. developed a novel technique using an enhanced homomorphic encryption scheme for achieving secure message transmission in MANETs. P. Sandhya[18] et al. performed a secure multipath routing to defend against the malicious attack to improve data confidentiality and reduce the overhead in MANET. But, data confidentiality was not sufficient.

Bello Musa Yakubu[19] et al. presented a novel method to attain data confidentiality and authentication by using an enhanced RSA cryptographic algorithm. However, the time taken to achieve secured data transmission was higher. Shuaishuai Tan [20] et al. introduced a trust-based routing model for choosing the path by maximum trust value between every potential path. This model increases the packet delivery ratio and lessens average latency. Though, data confidentiality remained unsolved. Jan Papaj and Lubomir Dobos [21] intended the assistance among trust as well as routing mechanism to choose reliable and secure nodes for data transmission.

Yin [22] et al. created the Modality Aware Graph Convolutional Network (MAGCN) module to improve link prediction performance, which integrates topological graph connectivity data and multi-modality entity properties into a single lower-dimensional feature space. To further transfer knowledge between subgraphs taken from the same knowledge graph, a Graph Knowledge Transfer Learning (GKLT) approach should be developed. An approach to create an access control knowledge network from user and resource attributes was developed by you, M [23] et al. On the basis of the created knowledge graph, a suggested online learning framework for access control decision-making was also built. To express high cardinality categorical user and resource attributes within the framework, topological features were extracted.

To handle the above existing problems, a Reputation-based Symmetric Key Authentication (RSKA) was introduced. RSKA was used for achieving secured data communication with a higher data confidentiality rate.

3. Methodology

The security of data communication, to improve a Reputation-based Symmetric Key Authentication (RSKA) technique is proposed that securely transmit data packets from source to destination nodes within MANET communication.

- To enhance the security of data communication as well as minimize data loss rate in MANETs, reputation values of mobile nodes are employed in the RSKA technique.

- To identify cooperative mobile nodes in a network, to improve the throughput of data transmission in MANETs, a reputation-based node authentication algorithm is designed in the RSKA technique.
- To enhance the confidentiality of data transmission with higher security and reduce the time for secured data delivery, Symmetric-key cryptography is applied in the RSKA technique.

3.1 Reputation-based Symmetric Key Authentication (RSKA) technique

The reputation-based Symmetric Key Authentication (RSKA) technique was developed to improve data transmission with a higher data confidentiality rate. The RSKA technique uses the reputation technique and symmetric key cryptographic mechanism for enhancing secured data within MANETs.

RSKA technique employs the reputation value of the mobile node to authenticate whether a node was supportive (i.e., normal) or compromised (i.e., malicious). Reputation value is measured by using the past behaviour of data packet forwarding of each node.

With the help of determined reputation value, the RSKA technique ensures routing has cooperative node by better reputation count value. Therefore, the RSKA technique mitigates the impact of malicious attacks node on data transmission, which in turn helps to improve throughput and reduce data loss rate.

Moreover, The RSKA technique uses a symmetric key cryptographic mechanism to further improve the security and confidentiality of data transmission in MANETs. The overall architecture diagram of the reputation-based Symmetric Key Authentication technique was described in Figure 3.1.

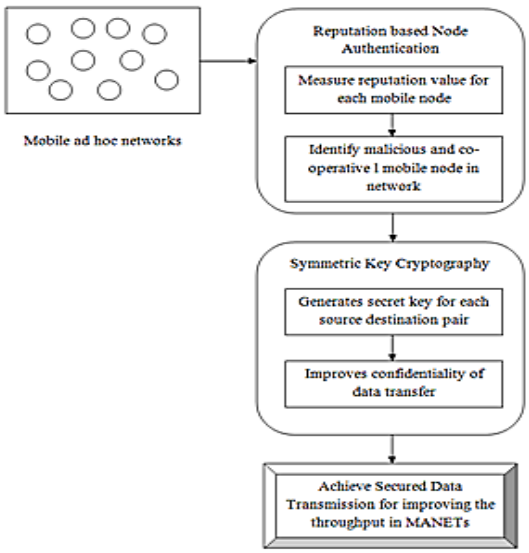

Figure 3.1 Architecture Diagram of Reputation based Symmetric Key Authentication technique for Secured Data Communication

As shown in Figure 3.1, the RSKA technique initially performs the node authentication process by measuring the reputation value of each mobile node. With the aid of computed reputation value, the RSKA technique finds the cooperative nodes and malicious nodes to enhance the security of data communication in MANETs.

Next, the RSKA technique employs only cooperative-mobile nodes for securely transmitting the data to reduce the data loss rate in MANETs. After identifying the cooperative-mobile nodes for data transmission, the RSKA technique used the Symmetric Key Cryptography mechanism to increase the confidentiality of data transfer by better security.

Symmetric Key Cryptography mechanism has symmetric key was created to the data transmitted by corresponding mobile node along the route path of source-destination pair. The generated symmetric key is shared only between the source-destination pair; therefore, attackers are unable to identify the key for disrupting the data communication in the route path. This, in turn, improves the throughput level as well as minimizes the time to protect data within MANETs in an efficient way.

3.2 Reputation Count based Node Authentication

In MANETs, node authentication is significant for increasing the security of data communication as well as reducing the data loss rate. By performing the node authentication process, the RSKA technique selects the cooperative nodes for securely transferring data toward the destination node.

Let's consider MANETs consisting of numerous mobile nodes $MN_i = MN_1, MN_2, MN_3, \ldots MN_n$. The reputation value of the nodes was measured on their past history of data packet transmission. Thus, RSKA estimates the reputation value of every node by considering the past history of data delivery of each mobile node. Therefore, the RSKA technique defines the reputation values since the mean differentiation among the successful data packet delivery as well as the data dropped to the entire amount of data transmitted.

The initial reputation value of all mobile nodes is initialized as 1. In the process of communication within the network, the reputation count value of mobile nodes may get an increment (+1) or decrement (-1) based on the packets being forwarded to the next corresponding node in the route path. The reputation count values of every mobile node are compared with a threshold reputation value which indicates each mobile node's cooperative behaviour in the network communication.

With the help of the measured count reputation value of all nodes, RSKA finds the number of cooperative and malicious nodes in the network for secure data communication. A cooperative node is a normal mobile node that efficiently transmits the data packets to the neighbouring node without more data loss.

The malicious node is a selfish node which failed in sending the data packets to the neighbour nodes and drops the all the data packets that received. The Reputation Count based Node Authentication process is shown from Figure 3.2.

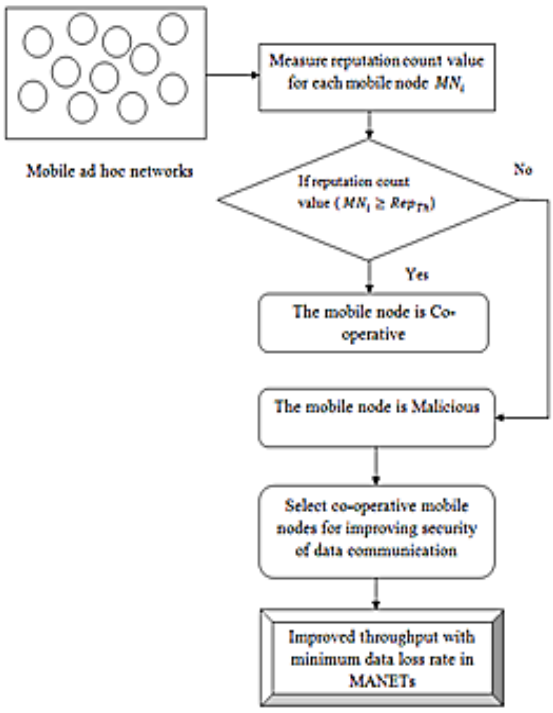

Figure 3.2 Process of node Authentication for Secured Data Communication Using Reputation Value

As shown in Figure 3.2, the RSKA technique improves throughput rate with minimum data loss by selecting the cooperative-mobile nodes to securely routing data from the source to the destination node using the reputation value of every node. The reputation value of a mobile node is computed with the aid of the following mathematical expression,

$$\mathrm{REP}_{\mathrm{MN_i}} = \frac{(\mathrm{DP_T} - \mathrm{DP_D})}{\mathrm{DP_N}} \qquad (3.1)$$

From (3.1), $\mathrm{DP_N}$ denotes the entire amount of data packets which mobile node was received over source node as well as $\mathrm{DP_T}$ indicates the number of data packets that the mobile node efficiently transmitted to the adjacent neighbouring node. Whereas $\mathrm{DP_D}$ indicates the number of data packets that the mobile node dropped. By using equation (1), the reputation count value for every node was calculated. The reputation value of the mobile node is either +1 or -1. In the process of communication over a network, the reputation count value of every mobile node gets incremented (+1) or decremented (-1) based on the past history of the packets being forwarded to the next corresponding neighbouring node in the route path. The following diagram shows the MANETs structure for achieving secure data communication.

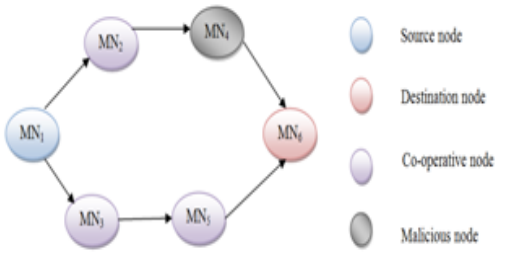

Figure 3.3 MANET's Structure for Achieving Secure Data Communication

From Figure 3.3, the source mobile node $\mathrm{MN_1}$ needs to transmit the data towards the destination node $\mathrm{MN_6}$. Here, the source node has two different route paths. For example, $\mathrm{MN_1 - MN_2 - MN_4 - MN_6}$ and $\mathrm{MN_1 - MN_3 - MN_5 - MN_6}$. Before performing the data transmission, all mobile nodes in MANETs compute their reputation value depending on the past history of data packets being forwarded to the next corresponding neighbouring node in the route path. The reputation value calculation for the above MANETs is shown in below Table 3.1.

Table 3.1 Reptation Value Calculation

	MN_1	MN_2	MN_3	MN_4	MN_5	MN_6
DP_N	22	30	42	24	15	26
DP_T	18	25	38	0	12	21
DP_D	4	5	4	24	3	5
Reputation Value	0.63 (+1)	0.66 (+1)	0.79 (+1)	-1	0.6 (+1)	0.61 (+1)

As shown in Table 3.1, consider the mobile node $\mathrm{MN_2}$ that receives 30 packets from the source node in which it transmits 25 data packets for the corresponding neighbouring node and drops 5 packets due to some potential attacks. Therefore, the reputation value of the mobile node $\mathrm{MN_2}$ is 0.63 i.e. (+1). Similarly, using the above table values, the reputation value of every mobile node is evaluated.

During the mobile node communication process, the reputation count value of every mobile node gets incremented (+1) or decremented (-1) depending on the past history of packets forwarding to the next corresponding neighbouring in the route path. Finally, the reputation count value for every mobile node is compared with the threshold reputation value to detect the cooperative node for attaining secure data communication in MANETs. The algorithmic process of the reputation-based Node Authentication process was given as,

Algorithm 3.1 Reputation Count based Node Authentication Algorithm

```
// Reputation Count based Node Authentication Algorithm
Input: Mobile nodes 'MN_i = MN_1, MN_2, MN_3 ... MN_n',
Output: Improved throughput and reduced data loss rate
Step 1:Begin
Step 2:    For each mobile node MN_i
Step 3:        Compute reputation value using (1)
Step 4:        if REP_MNi > Rep_Th then
Step 5:            the mobile node is identified as co-
                   operative
Step 6:        else
Step 7:            the mobile node is identified as malicious
Step 8:    end if
Step 9:    End for
Step 10: End
```

Algorithm 3.1 explains that RSKA proficiently discovers cooperative nodes in the communication route path to increase the protection of data and reduce the data loss rate in MANETs. Initially, the reputation-based Node Authentication algorithm calculates the reputation value of every mobile node within the network and then compares it with the threshold reputation value for identifying the cooperative and malicious nodes. If the reputation value of the node was better than the threshold reputation value, then the node is identified as cooperative. Otherwise, that mobile node is identified as a malicious node.

After that, the RSKA technique chooses only the cooperative node in the network to enhance security and mitigate the impact of malicious nodes on data communication. This helps to improve the throughput and reduce the data loss rate within MANETs in a noteworthy way.

The reputation-based node authentication algorithm helps in choosing the secured route path for successful data delivery in MANETs with a reduced data loss rate. But, the reputation-based node authentication algorithm does not consider the confidentiality of data transfer in MANETs. Therefore, the RSKA technique employed Symmetric Key Cryptography to further enhance the security and the confidentiality of data transfer in MANETs which is detailed and explained in the next section.

3.3 Symmetric Key Cryptography

RSKA technique has Symmetric Key Cryptography employed with the objective of improving confidentiality of data transmission in MANETs. Symmetric-key cryptography employs to perform encryption and decryption. Symmetric-key cryptography has encryption and decryption are inverse of each other in which the sender, as well as the receiver of the message, allocate the single, regular key that was exploited for encrypting as well as decrypting the message.

Symmetric-key cryptography was termed secret-key cryptography. The most commonly used symmetric-key scheme was Data Encryption Standard (DES). The DES employs a 56-bit key as well as a block cypher that breaks messages within 64-bit blocks as well as encrypts them.

In order to encrypt and decrypt data, symmetric cryptography employs a single secret key. The party having this secret key can use it to encrypt and decrypt data. The symmetric-key encryption and decryption process is extremely, very fast and therefore reduces the amount of time to protect data within MANETs. The Symmetric-key cryptography for improving the confidentiality of data transmission is shown in Figure 3.4.

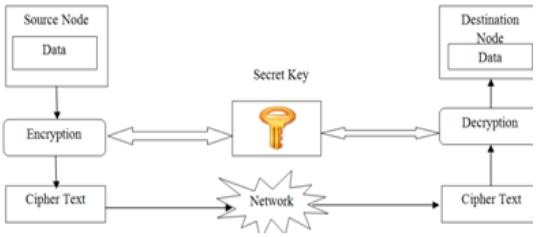

Figure 3.4 Process of Symmetric-key cryptography for Improving Confidentiality of Data Transmission in MANETs

From Figure 3.4, initially, the source node transmits the data transmitted over the network. Before the data transmission, the source node encrypts the data with the aid of secret key SK using a symmetric-key cryptography process which results in cypher text. The resultant cypher text is transmitted through the network to the corresponding destination node.

The destination node matches its secret key and then accomplishes the decryption process for obtaining the original data. The destination node has a secret key that can only decrypt the cypher text.

As a result, the RSKA technique enhances the confidentiality and security of data within MANETs. This aids in improving throughput and minimizing the time to protect data in an efficient way.

In the source node, the data is to be transmitted over the network is encrypted with secret key SK with the help of symmetric-key cryptography, which is mathematically represented as,

$$E = \text{encrypt}(\text{data}, \text{secret key}) \quad (3.2)$$

$$E = \text{cipher text} \quad (3.3)$$

From (3.3), the RSKA technique obtains the cypher text, which is sent to the appropriate destination node. The destination node decrypts the cypher text by using the same secret key SK, which is mathematically expressed as,

$$D = \text{decrypt}(\text{ciphertext}, \text{secret key}) \quad (3.4)$$

$$D = \text{orignial data} \quad (3.5)$$

From (3.4), the RSKA technique gets the original data transmitted from the source node by using a similar secret

key SK. The algorithmic process of symmetric key cryptography was explained as,

Algorithm 3.2 Symmetric Key Cryptography Algorithm for Enhancing Data Confidentiality

// Symmetric Key Cryptography Algorithm
Input: Mobile nodes '$MN_i = MN_1, MN_2, MN_3 \ldots MN_n$', Source Node SN_i, Destination Node $DN_i$and Secret Key SK_i, Data
Output: Improved Data Confidentiality with higher throughput rate and reduced time for secured data delivery
Step 1: Begin
Step 2: For each source and destination pair
Step 3: Generate secret key SK_i
Step 5: Before data transmission, source node accomplishes data encryption process and obtains cipher text using (2)
Step 6: This cipher text is send to corresponding destination node in network
Step 7: The destination node carry outs key matching process
Step 8: if key is matching then
Step 9: The destination node can decrypts the received cipher text using (4) and also gets original data
Step 10: else
Step 11: The transaction is declined
Step 12: End if
Step 13: End for
Step 14:End

As shown in Algorithm 3.2, the symmetric key cryptography algorithm initially creates the secret key for each source and destination pair. The source node encrypts the data to be sent to increase confidentiality and security of data transmission, as well as resultant cypher text, which is broadcasted. Destination node accomplishes key matching process.

If the secret key of both the source and destination node matches, then the destination node decrypts the received cypher text as well as acquires the original data. Otherwise, the transaction process is refused. Therefore, the RSKA technique improves confidentiality as well as the protection of data in MANETs which results in an improved throughput rate with minimum time

4. Experimental Settings

Reputation-based Symmetric Key Authentication (RSKA) was developed within the NS-2 simulator by network varies from 1500*1500 m in size.

RSKA technique takes 70 mobile nodes for performing simulation works and also employs DSDV protocol as a routing protocol. Simulations parameters used to perform experimental evolution are shown in Table 4.1.

Table 4.1 Simulation Parameters

Parameter	Value
Protocols	DSDV
Network range	1500 m * 1500 m
Simulation time	45 ms
Number of mobile nodes	10, 20, 30, 40, 50, 60, 70,80,90,100
Number of Data Packets	9, 18, 27, 36,45, 54, 63,72,81,90
Data Packets Size	15, 30, 45, 60,75, 90, 105,120,135,150
Network simulator	NS 2.34
Mobility speed	10 m/s
Mobility model	Random Way Point
Pause time	15 ms

The RSKA technique performs simulation many times to dissimilar node density with the rapidity of nodes. RSKA technique was tested by metrics such as security, throughput and time to protected data delivery, data confidentiality rate and data loss rate. The efficiency of the RSKA technique was compared to existing methods, namely the Hierarchical Identity-Based Encryption (HIBE) scheme [1] as well as Aggregated-Proof based Hierarchical Authentication (APHA).

5. Results and Discussion

To validate the efficiency of the reputation-based Symmetric Key Authentication (RSKA) technique, compared by Hierarchical Identity-Based Encryption (HIBE) scheme [1] and APHA. Simulation is conducted by various parameters, namely security, throughput and time to protected data delivery, data confidentiality rate and data loss rate. RSKA was estimated by various with the help of tables as well as graph values.

5.1 Measure of Throughput Rate

The throughput rate was defined as the total amount of data received over the sender, separated by the time taken by the receiver to get the preceding packet. It was evaluated by packets per second (PPS) as well as represented by,

$$\text{Throughput rate} = \frac{\text{Size}(DP_r)}{\text{Simulation time} * 1000} \qquad (5.1)$$

From (5.1), the throughput rate was calculated by the size of the data packet received in MANET. The throughput rate is better, and the method is very effective.

Table 5.1 Tabulation for the Throughput

Mobile Node Density	Throughput (pps)		
	HIBE Scheme	APHA scheme	RSKA technique
10	196	223	258
20	213	238	267
30	225	246	279
40	231	255	285
50	248	269	296
60	254	278	310
70	260	296	324
80	271	311	338
90	286	325	346
100	299	341	357

The comparative result analysis of throughput is based on various amounts of mobile nodes by three methods, as explained in Table 5.1. RSKA framework has various amounts of mobile nodes and data packets for performing the simulation process. 50 nodes were consumed to conduct simulation; the RSKA technique performs the 296 PPS throughput, whereas the HIBE Scheme [1] and APHA scheme [2] achieves 248 PPS and 269 PPS. Thus, the throughput rate by RSKA was better when compared with [1] and [2].

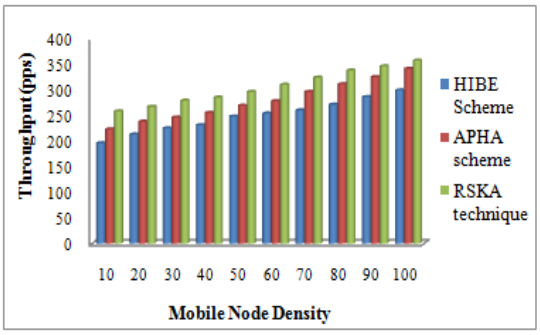

Figure 5.1 Measurement of Throughput Vs Mobile Node Density

Figure 5.1 shows the impact of throughput versus different mobile node densities. From Figure 4, RSKA achieves higher throughput compared with the existing HIBE Scheme [1] and APHA scheme [2]. In addition, by enhancing the number of mobile nodes for data transmission, throughput was improved. However, the throughput of the RSKA technique was better. This is due to the application of the RSKA algorithm, which efficiently detects the cooperative nodes in the communication route path to improve the security of data within MANETs. Therefore, the RSKA technique securely transmits the data packets to the destination node without more data loss. This aids in enhancing throughput in an efficient way. As a result, RSKA enhances throughput by 24 % compared with HIBE Scheme [1] and by 10 % when compared with the APHA scheme [2].

5.2 Measure of Time for Secured Data Delivery

In the RSKA technique, time to secure data delivery computes the amount of time consumed to achieve data transmission with a higher data confidentiality rate in MANET. The time for secured data delivery was calculated by milliseconds and formulated as,

$$\text{Time for Secured Data Delivery} = \sum_{i=1}^{n} DP * \text{Time}(DP_i) \quad (5.2)$$

From (5.2), time for secured data delivery denotes the product of the number of data packets transmitted and time consumed for delivering data packets. While the time taken for secured data delivery was lesser, the method is very efficient.

Table 5.2 Tabulation for Time for Secured Data Delivery

Number of Data Packets	Time for Secured Data Delivery (ms)		
	HIBE Scheme	APHA scheme	RSKA technique
9	0.681	0.654	0.610
18	0.693	0.679	0.628
27	0.711	0.693	0.637
36	0.728	0.710	0.645
45	0.739	0.731	0.651
54	0.767	0.756	0.669
63	0.786	0.772	0.678
72	0.803	0.795	0.686
81	0.822	0.812	0.695
90	0.840	0.825	0.709

Table 5.2 explains the time for secured data delivery on various amounts of data packets. 36 data packets are consumed for experimental, RSKA takes 0.645 ms time to achieve secured data delivery throughput, whereas the HIBE Scheme [1] and APHA scheme [2] acquires 0.728 ms and 0.710 ms, respectively. Therefore, the time taken for secured data delivery by RSKA was lesser compared with existing [1], [2].

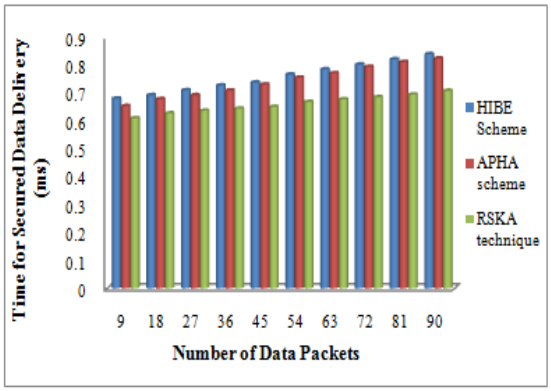

Figure 5.2 Measurement of Time for Secured Data Delivery Vs Number of Data Packets

Figure 5.2 demonstrates the impact of time taken for secured data delivery versus the various amount of data packets. From Figure 5.2, RSKA performs better time for secured data delivery compared with HIBE Scheme [1] and APHA scheme [2]. With the enhancing amount of data packets, the time taken for secured data delivery is improved. However, the time taken for secured data delivery by RSKA was lesser. This is because of symmetric key cryptography for secured data transmission in MANETs. The symmetric key cryptography algorithm generates a secret key for the data to be transmitted for the route path of the source-destination pair and, therefore, securely transmits the data packets to the destination node in lesser time. This aids in minimizing the time taken for secured data delivery in an efficient way. Thus, the proposed RSKA reduces the time for secured data delivery by 13 % compared with HIBE Scheme [1] and 11 % compared with the APHA scheme [2].

5.3 Measure of Data Loss Rate

The data loss rate is defined as differentiation among the size of data packets sent in size $(DP_{send})'$ as well as the size of data packets received size $(DP_{received})'$. It is evaluated by Kilo Byte (KB) and mathematically formulated as,

$$\text{Data Loss Rate} = \sum_{i=1}^{n}[\text{Size}\,(DP_{send}) - \text{Size}\,(DP_{received})] \quad (5.3)$$

From (5.3), the data loss rate is measured. While the data loss rate was lesser, the method is very efficient.

Table 5.3 Tabulation for Data Loss Rate

Data Packets Size (KB)	Data Loss Rate (KB)		
	HIBE Scheme	APHA scheme	RSKA technique
15	8	6	3
30	13	10	7
45	17	15	11
60	24	20	16
75	21	17	15
90	29	26	21
105	31	29	25
120	35	33	29
135	41	36	31
150	46	40	36

Table 5.3 illustrates the result analysis of time for data loss rate by various data packets size. 75 KB data size is taken for the transmission process, and the proposed RSKA technique attains a 15 KB data loss rate, whereas the HIBE Scheme [1] and APHA scheme [2] attains 21 KB and 17 KB. Thus, the data loss rate of RSKA was lesser when compared with [1], [2].

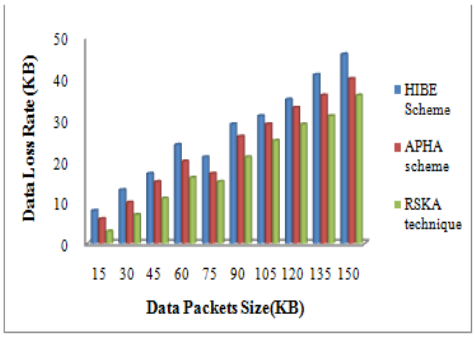

Figure 5.3 Measurement of Data Loss Rate Vs Difference Data Packets Size

Figure 5.3 explains the data loss rate versus various amounts of data packet size. From Figure 5.3, RSKA performs a higher data loss rate when compared with the existing HIBE Scheme [1] as well as the APHA scheme [2]. As the enhancing amount of data packets size, the data loss rate is improved s. However, the data loss rate of RSKA was lesser. Due to the application of reputation count-based node authentication within RSKA. RSKA select only the cooperative node in the network for data. This aids in improving the data loss rate in an effective manner. Thus, the RSKA technique minimizes the data loss rate by 32 % compared with HIBE Scheme [1] and 21 % compared with the APHA scheme [2].

5.4 Measure of Data Confidentiality Rate

In the RSKA technique, data confidentiality is achieved to protect data communication by symmetric key cryptography.

Therefore, it was referred by the capability of a scheme to safeguard data transferred as well as accessed by authorized destination nodes in MANETs. The confidentiality rate was calculated by percentages (%). The data confidentiality rate is higher, and the method is very efficient.

Table 5.4 Tabulation for Data Confidentiality Rate

Mobile Node Density	Data Confidentiality Rate (%)		
	HIBE Scheme	APHA scheme	RSKA technique
10	65.12	71.65	83.26
20	68.17	73.19	84.88
30	69.25	75.18	86.13
40	72.46	76.92	87.19
50	74.37	78.23	90.82
60	75.90	79.95	91.58
70	78.33	81.26	93.44
80	79.12	83.12	94.91
90	81.36	84.91	96.31
100	83.65	88.11	97.45

Table 5.4 illustrates the result analysis of data confidentiality achieved during secure data communication with respect to different mobile node densities using three methods. While 30 mobile nodes are taken for performing simulation, the proposed RSKA technique achieves 86 % data confidentiality rate, whereas the HIBE Scheme [1] and APHA scheme [2] attains 69 % and 75 %. Therefore, the data confidentiality rate of RSKA was improved with [1], [2].

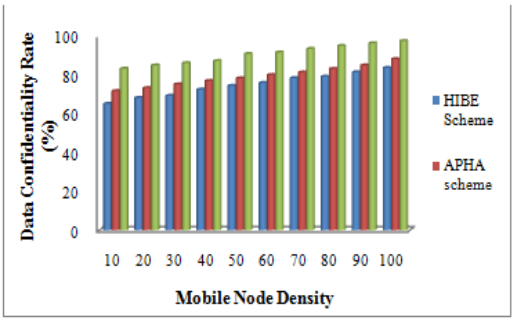

Figure 5.4 Measurements of Data Confidentiality Rate Vs Mobile Node Density

Figure 5.4 describes the data confidentiality rate versus various amounts of data density. From Figure 5.4, RSKA has a higher data confidentiality rate compared with the existing HIBE Scheme [1] and APHA scheme [2]. Also, by enhancing the number of mobile nodes, the data confidentiality rate is improved. However, the data confidentiality rate of RSKA was increased. Due to the utilization of symmetric key cryptography used in the RSKA technique for secured data transmission.

Table 5.5 Key generation and encryption cost comparison

Techniques	Key Generation cost		Encryption cost	
	Timings (ms)	Energy (mj)	Timings (ms)	Energy (mj)
Proposed	201.17	154.21	9604	101.5
QASEC [24]	257.49	199.23	102.1	119.3
ECC [25]	738.27	226.65	151.4	134.2

In Table 5.5, the cost associated with key generation and encryption for various schemes is shown. Proposed approach is compared with QASEC and ECC existing approaches. Both these operations consumes a significant amount of time and energy during keys generation and encryption. As a result, proposed model performs much better in terms of timing and energy consumption.

By using this algorithmic process, the source node encrypts the data with the help of a secret key which results in cypher text. The resultant cypher text is sent through the network to the consequent node. The destination node has a secret key that can only decrypt the cypher text. Therefore, the RSKA technique enhances the data confidentiality rate in a significant manner. Hence, the proposed RSKA technique improves the data confidentiality rate by 21 % and 14% with [1] and [2].

6. Conclusion

Reputation-based Symmetric Key Authentication (RSKA) technique is designed to securely transfer the data to destination nodes with an improved data confidentiality rate. At first, the RSKA technique developed a reputation count-based node authentication node algorithm for authenticating a node before the route identification process.

Then, the RSKA technique chooses only cooperative, mobile nodes for secured data communication which in turn mitigates the impact of attacks during transmission. Therefore, the RSKA technique improves the throughput and also lessens the data loss rate. Finally, the RSKA technique employs symmetric key cryptography to enhance the data confidentiality rate in lesser time.

The efficiency of the RSKA technique is tested by various parameters. Simulation of RSKA technique is performed by data confidentiality rate has accurate to achieve higher throughput. Simulation of RSKA has a higher performance of data confidentiality rate as well as a reduction in time for secured data delivery compared with conventional methods.

Declarations

Funding: There is no funding provided to prepare the manuscript.
Conflict of Interest: The process of writing and the content of the article does not give grounds for raising the issue of a conflict of interest.

Data availability statement: If all data, models, and code generated or used during the study appear in the submitted article and no data needs to be specifically requested.

References

[1] He K, Chen M-R, Mao Y, Zhang X and Zhan Y. Efficient Hierarchical Identity-Based Encryption for Mobile Ad Hoc Networks, Mobile Information Systems, Hindawi Publishing Corporation, 2014, 10(4), 407-425.

[2] Ning H, Liu H and Yang LT. Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Things, IEEE Transactions on Parallel and Distributed Systems, March 2015, 26(3), 657 – 667.

[3] Aluvala S, Sekhar KR, Vodnala D. A novel technique for node authentication in mobile ad hoc networks, Perspectives in Science, Elsevier, September 2016, 8, 680–682.

[4] Suresh A and Duraiswamy K. Security for Reactive Routing Protocol with Node Reputation Scheme, Journal of Advanced MANET Research in Computer Engineering, 2011, 5(2), 115-121.

[5] Rajeswari KS, Arivazhagi A. Trust and Reputation Management Based Cluster Head Selection in Mobile Ad-Hoc Networks, International Journal of Technology and Engineering System (IJTES), 2015, 7(1), 54-58.

[6] Papaj J and Dobos L. Cooperation between Trust and Routing Mechanisms for Relay Node Selection in Hybrid MANET-DTN, Hindawi Publishing Corporation, Mobile Information Systems, Article ID 7353691, 2016, 2016, 1-18.

[7] [7]Menaka R, Ranganathan V and Sowmya B. Improving Performance through Reputation Based Routing Protocol for MANET, Wireless Personal Communications, Springer, 2016, 1–16.

[8] [8]Kokate T and Joshi RB. Authentication in Mobile Ad Hoc Network for Secure Communication, International Journal of Science and Research (IJSR), June 2015, 4(6), 327-331.

[9] Bidaki M and Masdari M. Reputation-Based Clustering Algorithms in Mobile Ad Hoc Networks, International Journal of Advanced Science and Technology, May 2013, 54:1-12.

[10] Bose JSC, Devi UA, Prasanalaxmi M, Malathi K, Vinodhini KP, Saranya S. Acknowledgment-Based Secure Authentication Method for MANET, International Journal of Innovative Research in Computer and Communication Engineering, March 2014, 2(Special Issue 1), 1895-1900.

[11] Sukumran S, Jaganathan V, Korath A (June 2012) Reputation based Dynamic Source Routing Protocol for MANET, International Journal of Computer Applications (0975 – 888), 47(4), 42-46.

[12] Alomari A. Mutual Authentication and Updating the Authentication Key in MANETS, Wireless Personal Communications, Springer, April 2015, 81(3), 1031–1043.

[13] Wang Z, Chen Y, Li C. CORMAN: A Novel Cooperative Opportunistic Routing Scheme in Mobile Ad Hoc Networks, IEEE Journal on Selected Areas in Communications, February 2012, 30(2), 289 – 296.

[14] Yang S, Yeo CK and Lee BS. Toward Reliable Data Delivery for Highly Dynamic Mobile Ad Hoc Networks, IEEE Transactions on Mobile Computing, January 2012, 11(1), 111 – 124.

[15] Madhusudhanan B, Chitra S and Rajan C. Mobility Based Key Management Technique for Multicast Security in Mobile Ad Hoc Networks, Hindawi Publishing Corporation, The Scientific World Journal, 2015, Article ID 801632, 2015: 1-10.

[16] Aldabbas H, Alwada'n T, Janicke H, Al-Bayatti A. Data Confidentiality in Mobile Ad hoc Networks, International Journal of Wireless & Mobile Networks (IJWMN) February 2012, 4(1), 225-236.

[17] Gorti VNKV, Rao S, Uma G. An Efficient Secure Message Transmission in Mobile Ad Hoc Networks using Enhanced Homomorphic Encryption Scheme, Global Journal of Computer Science and Technology Network, Web & Security, 2013, 13(9), 21-33.

[18] Sandhya P and Dhas JPM, Secure Multipath Routing for Data Confidentiality in Mobile Ad Hoc Networks", Research Journal of Applied Sciences, Engineering and Technology, 2013, 6(13), 2415-2422.

[19] Yakubu BM, Chajera P, Dr. Garko AB. Advanced Secure Method for Data Transmission in MANET Using RSA Algorithm, International Journal of Advanced Technology in Engineering and Science, 2015, 3(1), 176-185.

[20] Tan S, Li X, Dong Q. Trust based routing mechanism for securing OSLR-based MANET, Ad Hoc Networks, Elsevier, July 2015, 30, 84–98.

[21] Papaj J and Dobos L. Cooperation between Trust and Routing Mechanisms for Relay Node Selection in Hybrid MANET-DTN, Hindawi Publishing Corporation, Mobile Information Systems, 2016, Article ID 7353691, 1-18.

[22] Yin, J., Tang, M., Cao, J., You, M., Wang, H., & Alazab, M. (2022). Knowledge-driven cybersecurity intelligence: software vulnerability co-exploitation behaviour discovery. IEEE Transactions on Industrial Informatics.

[23] You, M., Yin, J., Wang, H., Cao, J., Wang, K., Miao, Y., & Bertino, E. (2022). A knowledge graph empowered online learning framework for access control decision-making. World Wide Web, 1-22.

[24] Usman, M., Jan, M. A., He, X., & Nanda, P. (2020). QASEC: A secured data communication scheme for mobile Ad-hoc networks. Future Generation Computer Systems, 109, 604-610.

[25] Gharib, M., Moradlou, Z., Doostari, M. A., & Movaghar, A. (2017). Fully distributed ECC-based key management for mobile ad hoc networks. Computer Networks, 113, 269-283.