International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 18 (2017) pp. 7823-7832
© Research India Publications. http://www.ripublication.com

Self Organized Gradient Boosting Key Authentication for Secured Data Communication in Mobile Ad-hoc Network

Mrs. S. Sangeetha
Research Scholar, Department Of Computer Science,
Erode Arts and Science College, Erode, Tamil Nadu, India.

Orcid Id: 0000-0002-5287-5795

Dr. S. Sathappan
Associate Professor, Department of Computer Science,
Erode Arts and Science College, Erode, Tamil Nadu, India.

Orcid Id: 0000-0003-2522-3318

Abstract

The key challenging tasks in Mobile Ad-hoc Networks (MANETs) are to present security during the transmission of data packets. The existing technique does not provide more security for improving the throughput rate. Reputation based Symmetric Key Authentication (RSKA) technique is designed for securely transmitting the data packets from source to destination nodes in MANETs with higher throughput rate. In this research work, Self Organized Gradient Boosting Key Authentication (SOGBKA) technique is proposed. The SOGBKA technique includes of three processes such as tree building, tree pruning and optimal node selection for performing secured data transmission in MANETs. The Self Organized Gradient Boosting Key Authentication (SOGBKA) technique initially constructs Gradient Boosting tree with help of mobile nodes in network and then generates self organized key for each mobile node. After that, the SOGBKA technique calculates trust values of mobile node based on the data packet forwarded and dropped rate. Then, SOGBKA technique performs tree pruning process in which the mobile node with lower trust value is eliminated in order to reduce the data loss rate during the data transmission and to improve the throughput rate. Finally, SOGBKA technique chooses the optimal node in network through self organized key authentication for transmitting the data packet with higher security. This in turn helps for SOGBKA technique to reduce the time taken for achieving secured data delivery in MANETs. The performance of SOGBKA technique is measured in terms of throughput, data loss rate and time for secured data delivery. The simulation result shows that the SOGBKA technique is able to improve the throughput rate and also reduces time taken for secured data delivery in MANETs when compared to the state-of-the-art works.

Keywords: Gradient Boosting tree, Mobile ad-hoc networks, mobile node, Public key, secured communication, trust value.

INTRODUCTION

A mobile ad-hoc network (MANETs) includes of collection of mobile nodes in mobility which are linked through wireless links in which any node can connect or leave the network at any time. All mobile nodes in the network are performed as a router and use routing mechanism to communicate with each other. Routing is a process of transmitting a data packet from one node to another node in network. Every mobile node in MANETs has to communicate with each other for broadcast the data. Different vulnerabilities are presented in MANETs such as wireless links, lack of centralized management, scalability, dynamic topology, cooperativeness, restricted resources and band-width constriction which affects the security of node. Hence, node security becomes an most important concerns in MANETs. Key Authentication is used for enhancing the security of communication. However, node authentication is more challenging task in MANETs.

LITERATURE SURVEY

Huansheng Ning [1] et al developed Aggregated-Proof based Hierarchical Authentication (APHA) scheme for improving security of data transmission with higher data confidentiality and data integrity. Kei Kobayashi [2] et al introduced Secure Communication method intended with aid of secret sharing scheme for achieving secure communication in MANETs. However, computational complexity of this scheme was more.

Sangeetha S and S Sathappan [3] proposed technique, Reputation based Symmetric Key Authentication (RSKA) technique was designed for securely transmitting the data packets from source to destination nodes in MANETs with higher throughput rate. However, security level of data transmission was not sufficient.

Ahmad Alomari [4] designed an authentication scheme to resolve the security and privacy issues between two communicating nodes in MANETs. This authentication

scheme improves the throughput in MANETs. But, the data loss rate was higher. Gorti VNKV Subba Rao, Garimella Uma [5] presented an Enhanced Homomorphic Encryption Scheme to improve the security of message transmission in MANETs. However, time utilized for secured data transmission was more.

Gautam M. Borkar, A. R. Mahajan [6] proposed an Ad hoc On-demand Multicast Distance- Vector–Secure Adjacent Position Trust Verification (AOMDV–SAPTV) to find out the optimal path for routing and improving the security in MANETs. However, avoiding different attacks was remained unsolved which affects the throughput rate and also increases the data loss rate. Ahmad Alomari [7] presented a new technique to improve the security between nodes and enhancing the authentication and confidentiality in MANETs. But, this does not provide more security for data delivery.

Rajinder Singh [8] et al developed Security based algorithmic approach to optimize the packet loss rate and to provide more security in MANETs. However, the throughput rate was poor. Tejashree Kokate, R.B.Joshi [9] designed a novel technique for securing communication in MANETs through performing authentication which resulting in increased throughput. But, secured data delivery rate was poor.

Abu Taha Zamani, Syed Zubair [10] designed Key Management Scheme for providing security services and reducing the complexity of key management in MANETs. Dega Ravi Kumar Yadav [11] presented a hybrid authentication protocol for MANETs that employs RSA algorithm for authentication between two nodes which resulting in improved communication security. But, the throughput rate was lower. In order overcome the above mentioned existing issues, a Self Organized Gradient Boosting Key Authentication (SOGBKA) technique is introduced.

Snehal Javheri, Rahul Kulkarni [12] presented a DNA Based Cryptographic Technique for achieving secure data communication in MANETs. However, it takes more time. The time taken for secured data communication is reduced in proposed SOGBKA technique with application of self organized key authentication. Maha Abdelhaq [13] et al intended a Danger Theory-Based Artificial Immune Algorithm for secure routing and improving the network performance. However, secure data communication was remained unsolved. The secure data communication is attained in proposed SOGBKA technique through the generated self organized key.

Jan Papaj and Lubomir Dobos [14] developed a trust based relay node selection algorithm to afford the effectual communication among the mobile nodes and to choose the secured mobile node for transmitting the data packet in MANETs. This algorithm increases the delay time. But, data delivery ratio was poor. Sunil Deokule [15] et al developed a novel technique for achieving reliable communication in MANETs using topology control. However, communication security is remained unaddressed. This communication security is achieved in SOGBKA technique with help of self organized key generation.

Sukin Kang [16] et al presented a group key sharing scheme for attaining multicast security in mobile networks through key authentication under the decisional Diffie-Hellman (DDH) assumption. But, this scheme does not provide higher communication security. This drawback is solved in SOGBKA technique by application of gradient boosting and self organized key. Poonam Gera [17] et al presented the trust-based multi-path routing scheme to make sure secure discovery of multiple path between source and destination and enhancing the security of data delivery in MANETs.

Priyanka Takalkar, Aaradhana Deshmukh [18] designed trust based multi route routing protocol for improving the security of data communication in MANETs and ensuring security and undisrupted delivery of transmitted data. However, the throughput performance was not efficient. The higher throughput is achieved in SOGBKA technique by selecting the mobile node with higher trust value for data transmission.

Gautam M. Borkar, A. R. Mahajan [19] intended Ad hoc on-demand multicast distance vector–secure adjacent position trust verification (AOMDV–SAPTV) technique for achieving higher packet delivery ratio and reducing delay in MANETs. But, AOMDV–SAPTV technique takes more time for key generation which increases the time for achieving secured data delivery. The limitation is solved in SOGBKA technique with help of self organized key generation. By using generated key, the mobile nodes in MANETs validate themselves with neighbour node for securely transmitting the data. This helps for SOGBKA technique to reduce the time for secured data delivery.

Srinivas Aluvalaa [20] et al presented A novel technique for authenticating mobile node in MANETs. Saju P John and Philip Samuel [21] developed a self-organized key management technique using trusted certificate exchange for securing transmission of the packet in MANETs with lower loss rate. But, packet loss rate was more. This drawback is handled in SOGBKA technique through tree pruning process in which the mobile node with lower trust values in network are removed in order to enhance the security of data transmission. This assists for SOGBKA technique to minimize the packet loss rate.

METHODOLOGY

- In Mobile Ad-hoc Network to enhance the performance of communication security, a Self Organized Gradient Boosting Key Authentication (SOGBKA) technique is designed. The SOGBKA technique employed gradient boosting machine learning technique and self organized key for achieving secured data delivery.
- We intend to design and implement a self organized key is generated in SOGBKA technique to reduce the time for

secured data delivery and to improve the throughput rate in MANETs. The SOGBKA technique consist of three processes such as tree building, tree pruning and optimal node selection to improve the security of data transmission in MANETs with low data packet loss rate, the gradient boosting machine learning technique is used.

Self Organized Gradient Boosting Key Authentication technique

A MANETs is a self-organized wireless network in which the mobile nodes are interconnected with each other without any centralized authority. Each mobile node in MANETs is proficient to connect with other nodes within its transmission range and also based on other nodes to communicate with nodes outside its transmission range.

The self organizing and topology changing property of MANETs require security constraints to the mobile nodes in network during transmission of data for achieving higher throughput rate. Therefore, key authentication technique is necessitated for improving the security of data communication and reducing minimum packet loss rate in MANETs. Besides, achieving communication security is more difficult in MANETs due to problems of key exchange between the mobile nodes in network. In order to overcome such limitation, SOGBKA technique is designed.

The SOGBKA technique is used gradient boosting machine learning technique and self organized key for performing secured data delivery in MANETs. The regression and classification problems can be solved by designing the Gradient Boosting machine learning technique. Besides, the Gradient Boosting is generally used with decision trees (i.e. Classification and Regression Tree (CART)). Thus, the process of SOGBKA technique includes of three processes such as tree building, tree pruning and optimal node selection. The overall architecture diagram of SOGBKA technique is shown in below Figure 1.

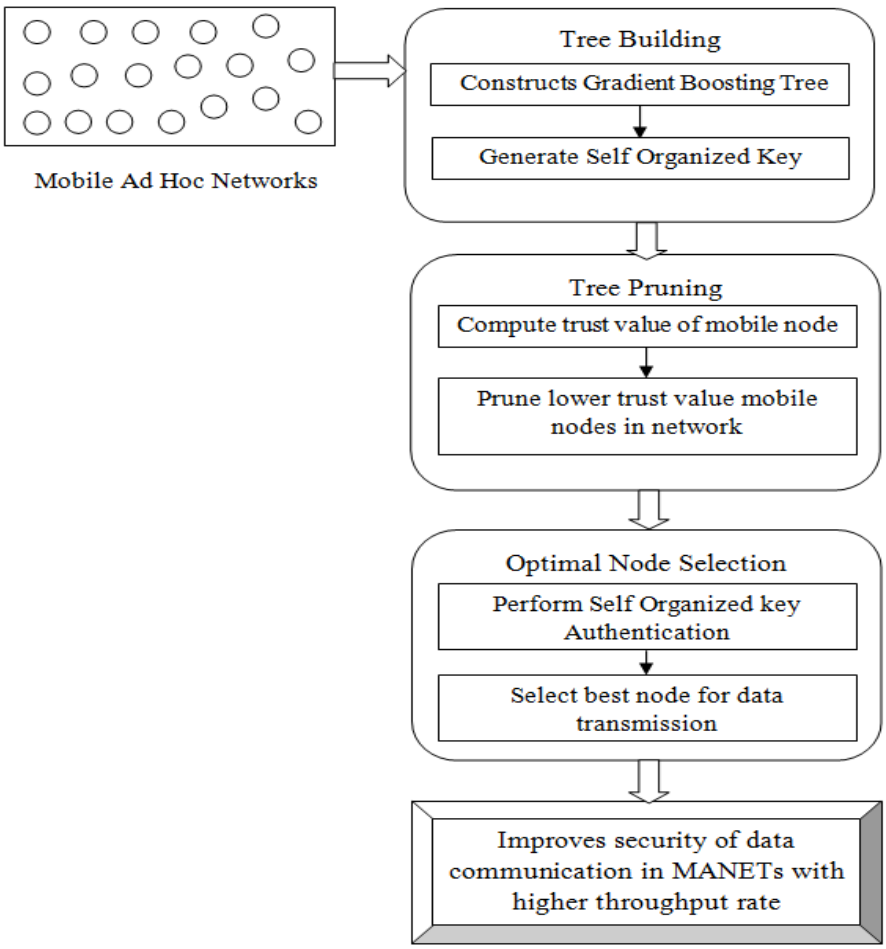

Figure 1: Architecture Diagram of Self Organized Gradient Boosting Key Authentication technique

The figure 1 shows that, SOGBKA technique consisting of three steps namely tree building, tree pruning, and optimal node selection for achieving higher communication security. In SOGBKA technique, initially tree building process is carried out in order to create gradient boosting tree and to generate the self organized key for each mobile nodes in network.

Then, SOGBKA technique estimates the trust value for every mobile node in MANETs with objective of optimizing the gradient boosting tree through pruning unsecure mobile nodes (i.e. the mobile nodes with lower trust value). Finally, SOGBKA technique performs optimal node selection process with help of generated self organized key of the mobile nodes in network. By using the formulated self organized key, SOGBKA technique authenticates mobile nodes in network in order to choose the optimal node for secured data delivery in MANETs. With aid of selected optimal node, then SOGBKA technique performs reliable data packet transmission. This in turn helps for SOGBKA technique to increase the throughput rate and to minimize packet loss rate in MANETs.

Tree Building

Let consider the MANETs comprises numerous mobile nodes which are represented as '$MN_i = MN_1, MN_2, MN_3, \ldots MN_n$'. Thus, SOGBKA technique constructs gradient boosting tree with mobile nodes in network. The following diagram shows the structure of gradient boosting tree in which t_p is a parent node and t_l, t_r denotes the left and right child of parent node respectively.

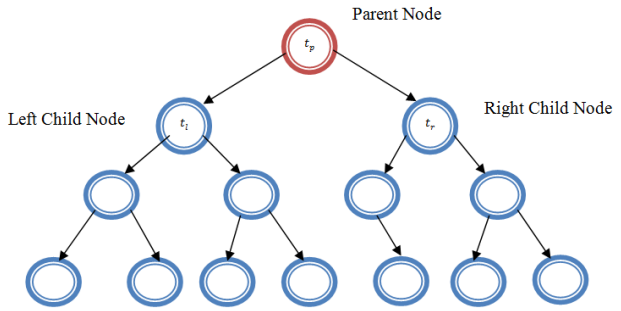

Figure 2: Structure of Gradient Boosting Tree

The figure 2 demonstrates that the gradient boosting tree structure. Thus, the tree model of gradient boosting is mathematically represented as,

$$F_{m+1}(x) = F_m(x) + h(x) \quad (1)$$

From the equation (1), $F_m(x)$ denotes the mobile nodes in network such as $MN_i = MN_1, MN_2, MN_3, \ldots MN_n$' whereas $h(x)$ indicates the trust value of mobile nodes. After building gradient boosting tree, the self organized key is formulated for securing the communication between the mobile nodes in MANETs. The private or public key is generated for each mobile node in network by the mobile node itself is called self organized key. During self organized key generation process, the mobile node itself creates the public key and provides its certificates to neighboring nodes in network. Then it saves these certificates in its certificate repository for achieving communication security in MANETs.

Let us assume the two mobile nodes MN_A and MN_B in network and their public key is $PubK_A$ and $PubK_B$ respectively. Every mobile node creates public key (PubK) and their corresponding private key locally before joining in network through the node itself. In self organized key generation, public-key certificates combine the public keys and the corresponding mobile node identities (IDs). The public-key certificate consists of the node's identity/network address, certificate generation and validity time (i.e. instance ID). Thus, the public key certificate $PubK_C$ of mobile node MN is mathematically represented as follow,

$$PubK_C \rightarrow MN_{ID}, PubK_i, DN_{ID}, I_{ID} \quad (2)$$

From the equation (2), MN_{ID} denotes the Id of mobile node in network and $PubK_i$ signifies public key of the node whereas DN_{ID} represents ID of destination node, I_{ID} indicates the validity time. If mobile node 'MN_A' believes that a public key '$PubK_B$' belongs to certain node 'MN_B', it provide a public key certificate to node MN_B where '$PubK_B$' is combined to 'MN_A' with aid of the signature of the mobile node MN_A which is mathematically formulated as,

$$MN_A \rightarrow MN_B : \ PubK_B \ \forall \ MN_B, (A, B \in 1,2, \ldots, n) \quad (3)$$

From the equation (3), the provided public key certificate is stored in certificate repository with a validity time. Therefore, the issue and expiry time of the public key certificate are determined using below formula,

$$PubK_C \rightarrow PubK_A, I_T, E_T \quad (4)$$

From the equation (4), the issuing time (I_T) and expiry time (E_T) of public key certificate ($PubK_C$) is estimated to evade the mobile node pair being performed via the network for longer period of time. When a public key certificate run outs ($PubK_C$) and the mobile node considers that the certificate is still valid, and afterward the issuing mobile node generates an updated version of the similar certificate which is mathematically expressed as,

$$UPubK_C \rightarrow PubK_A, UI_T, UE_T \quad (5)$$

From the equation (5), $UPubK_C$ indicates an updated version of the public key certificate whereas UI_T and UE_T represents the updated issue time and expiry time respectively. Hence, the updated certificate of public key is determined for reliable data packet transmission. This also assists to transmit data packets with public key certificates depends on other mobile node's public keys. The algorithmic process of self organized key is shown in below,

Input : Number of Mobile Nodes '$MN_i = MN_1, MN_2, \dots, MN_n$', Public Key '$PubK_i$', public key certificate $PubK_C$, public key issuing time 'I_T', public key expiry time 'E_T'

Output : public key and certificate generation

Step 1: Begin

Step 2: For each mobile node MN_i

Step 3: Create public key (PK_i) by the node itself

Step 4: Determine public key certificate using (2)

Step 5: Evaluate the certificate issue and expiry time for discovering the validity using (4)

Step 6: If (MN believes $PubK_C$ is legitimate) then

Step 7: Updates public key certificate

Step 8: else

Step 9: public key is invalid

Step 10: End if

Step 11: End for

Step 12: End

Figure 3: Self Organized Key Generation

The figure 3 explains that the process of self organized key and certificate generation algorithm in which each mobile node in MANETs formulates the public key by itself. After that, the public key certificate is broadcasted with data packet using the other mobile node's public keys. Subsequently, $PubK_c$ is updated for each session in order to evaluate their validity based on the issue time and expiry time. In SOGBKA technique, the generated self organized key helps the mobile nodes to authenticate themselves with the neighboring mobile nodes in the network. As a result, SOGBKA technique attains secured data communication in MANETs.

Tree Pruning

In SOGBKA technique, the tree pruning process is performed with help of trust value of mobile nodes in network for improving security of data transmission with lower data packet loss rate. The trust value is determined based on the normal communication service presented by mobile nodes in network. Thus, SOGBKA technique defines the trust value as the difference between the percentages of data packets forwarded and data packets dropped over the total number of data packets received by mobile nodes form the source node.

In trust value calculation, the data packets forwarded rate measures the percentages of data packets transmitted to the neighboring mobile node 'MN_j' to the total number of data packets received by mobile node 'MN_i'. From that, the data packets forwarded rate is formulated as,

$$\text{Data Packet Forwarded rate} = \frac{DPF(MN_j)}{N} \quad (6)$$

From the equation (6), the data packet forwarded rate of mobile node is measured. Here, $DPF(MN_j)$ indicates the number of data packets forwarded by mobile node 'MN_i' to neighbouring mobile node MN_j whereas the N represents the number of data packets obtained by mobile node 'MN_i'. In addition, the data packets dropped rate determines the percentages of number of packets dropped to the total number of data packets received by mobile node MN_i. Hence, the data packets dropped rate is mathematically expressed as below,

$$\text{Data Packet Dropped rate} = \frac{DPD(MN_j)}{N} \quad (7)$$

From the equation (7), the data packet dropped rate of mobile node is estimated. Here, $DPD(MN_j)$ point outs the number of data packets dropped by mobile node 'MN_i' to neighbouring mobile node MN_j whereas N denotes the number of data packets obtained by mobile node 'MN_i'. Thus, trust value of mobile node MN_i mathematically represented as,

$$\text{Trust Value}_{MN_i} = \text{Data Packet Forwarded rate} - \text{Data Packet Dropped rate} \quad (8)$$

From the equation (8), trust value is estimated for each mobile node in network. After calculating the trust value, gradient boosting concept is used to find out lower trust value mobile nodes in network in order to secure the data transmission.

The gradient boosting tree splits the input space into J_m disjoint regions like $R_{1m}, R_{2m}, \dots R_{Jm}$ and then predicts a mobile node with lower trust value in each region. Here, J_m represent number of leaves in tree. Thus, output of gradient boosting tree $h_m(x)$ for input x (x indicates the mobile node with trust value) is mathematically formulated as follows,

$$h_m(x) = \sum_{j=1}^{J_m} b_{jm} I(x \in R_{jm}) \quad (9)$$

From the equation (9), b_{jm} denotes the predicted mobile nodes which consisting of lower trust value in tree. Thus, the number of unsecured mobile nodes in network is efficiently discovered. After that, the coefficients b_{jm} are multiplied by some value γ_m in order to remove the lower trust value mobile nodes in MANETs. Therefore, the tree model is updated as,

$$F_m(x) = F_{m-1}(x) + \gamma_m h_m(x) \quad (10)$$

$$\gamma_m = \arg\min_{\gamma} \sum_{i=1}^{n} L(y_i, F_{m-1}(x_i) + \gamma_m h_m(x_i)) \quad (11)$$

By using the equation (10) and (11), the mobile node consisting of lower trust value in network is eliminated in order to achieve higher secure data delivery in MANETs. Finally, the mobile nodes with higher trust value in each of the

tree regions (i.e. network) are identified using below mathematical formula,

$$F_m(x) = F_{m-1}(x) + \sum_{j=1}^{J_m} \gamma_{jm} I(x \in R_{jm}) \quad (12)$$

$$\gamma_{jm} = \arg\min_{\gamma} \sum_{x_i \in R_{jm}}^{n} L(y_i, F_{m-1}(x_i) + \gamma) \quad (13)$$

By using the equation (12) and (13), the trusted mobile nodes in MANETs are efficiently identified for carried outing the reliable packet transmission. This assists for proposed SOGBKA technique for minimizing packet loss rate and increasing the throughput in an effective manner.

Optimal Node Selection

After the trusted node identification process, self organized key authentication is carried out to select optimal node for data packet transmission. Let us consider the source node (SN), and the destination node (DN). Thus, the self organized key authentication is accomplished through the each node exchange a certificate with one hop manner. At first, a source node transmits a route request to the neighbour trusted node in network with their certificate using below mathematical expression,

$$SN \rightarrow X; \{RREQ, PubK_{C;SN \rightarrow X}\} \quad (14)$$

From the equation (14), X represents the neighbour node of source node. After receiving the route request with public key certificates ($PubK_C$), the neighbour node searches the certificate of the source node signed through this node in its certificate repository. Then, adds its route request packet before broadcasting the route request packet to other neighbour nodes in network. After obtaining RREQ from the neighbour nodes, DN has the entire certificate chain entailed to get the source node's public key. Therefore, DN transmits a reply packet (RREP) to their neighbouring node using following mathematical representation,

$$DN \rightarrow X; \{RREP, PubK_{C;DN \rightarrow X}\} \quad (15)$$

If SN gets the more than one RREP for the similar route request, it chooses the optimal route path as the path which has minimum number of certificates. If SN obtains the public key certificates of DN, then the data packet is broadcasted. Otherwise, the data packet is not transmitted. The verification of public-key certificate is accomplished through checking its validity time. This assists to enhance the security of data packet communication between the nodes in MANETs.

The Self Organized Gradient Boosting Key Authentication algorithm is shown below.

Input : Source node 'SN', Mobile Nodes '$MN_i = MN_1, MN_2, \ldots, MN_n$', PK_C, Destination node 'DN', Data Packets '$DP_i = DP_1, DP_2, \ldots, DP_n$

Output: Improved throughput and reduce the time for secured data delivery

Step 1: Begin

Step 2: For mobile nodes MN_i

Step 3: Construct gradient boosting tree with mobile nodes in network using (1)

Step 4: Generate self organized public key and certificate using (2)

Step 5: Calculate trust value of mobile node using (9)

Step 6: Optimize gradient boosting tree through pruning untrusted node using (10) and (11)

Step 7: Identify trusted mobile nodes in network using (12) and (13)

Step 8: SN broadcasts a RREQ with public key certificates to neighbor nodes in network using (14)

Step 10 : DN transmits a RREP to neighbouring node using (15) for authentication

Step 11: If 'SN' has the certificates of 'DN' then

Step 12: transmits the data packet 'DP_i'

Step 13: Else

Step 14: do not transmit the data packet 'DP_i'

Step 15: End if

Step 16: End for

Step 17: End

Figure 4: Self Organized Gradient Boosting Key Authentication For Secured Communication in MANETs

The figure 4 describes the process of Self Organized Gradient Boosting Key Authentication for performing the secured communication in MANETs. With the help of generated self organizing key (i.e. public key and their certificates) of each mobile node, an optimal route path is identified between the source node 'SN' and destination mobile node 'DN' for

securely transmitting the data in MANETs. The above algorithmic process helps for the mobile nodes to authenticate themselves with the neighboring mobile nodes in the network before they perform data packet transmission. As a result, SOGBKA technique establishes secured data communication in MANETs. This in turn assists to improves throughput rate and reduce the time for secured data delivery in a significant manner.

EXPERIMENTAL SETTINGS

The Self Organized Gradient Boosting Key Authentication (SOGBKA) technique is implemented in NS-2 simulator with the network range of 1500*1500 m size in order to analysis the effective of proposed method. The SOGBKA technique takes 100 mobile nodes for carry outing the simulation works. The simulations parameter utilized for performing experimental work is demonstrated in Table 1.

Table 1: Simulations Parameter

Parameter	Value
Protocols	DSDV
Network range	1500 m * 1500 m
Simulation time	45 s
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
Mobility speed	10 m/s
Mobility model	Random Way Point
Pause time	15 s
Number of runs	10

The efficiency of SOGBKA technique is tested with parameters such as security, throughput and time for secured data delivery, data confidentiality rate and data loss rate. The effectiveness of SOGBKA technique is compared against with existing methods such as Aggregated-Proof based Hierarchical Authentication (APHA) scheme [1], Secure Communication method [2] and Reputation based Symmetric Key Authentication (RSKA) technique [3].

RESULTS AND DISCUSSION

In order to validate the efficiency of the proposed Self Organized Gradient Boosting Key Authentication (SOGBKA) technique, the comparison is made with existing methods such as Aggregated-Proof based Hierarchical Authentication (APHA) scheme [1], Secure Communication method [2] and Reputation based Symmetric Key Authentication (RSKA) technique [3]. The simulation is conducted on the factors such as security, throughput and time for secured data delivery, and data loss rate. The performance of SOGBKA technique is estimated along with the following metrics with aid of tables and graph values.

Measurement of Throughput Rate

Throughput is defined as the rate at which the data packet received at the destination node at specified amount of time. The throughput is measured in terms of packets per second (pps) and expressed as,

$$\text{Throughput} = \frac{\text{Packets received at the destination}}{\text{Time}} * 100 \quad (16)$$

Throughput rate of SOGBKA technique is measured is shown in equation (16). While the throughput is higher, the method is said to be more efficient.

Table 2: Tabulation for Throughput

Mobile Node Density	Throughput (pps)			
	APHA Scheme	Secure Communication Method	RSKA Technique	SOGBKA Technique
10	250	260	349	390
20	262	266	355	401
30	276	271	366	419
40	285	278	377	426
50	299	285	385	432
60	318	293	398	441
70	326	299	403	455
80	332	305	417	466
90	345	312	426	475
100	351	325	430	482

Table 2 illustrates the tabulation results for throughput using four methods. While considering the 70 mobile nodes for data packet transmission, the proposed SOGBKA technique attains the 455 bps throughput rate whereas the APHA scheme [1], Secure Communication Method [2] and RSKA technique [3] attains 326 pps, 299 pps, 403 pps respectively. Therefore, throughput rate using proposed SOGBKA technique is higher while compared to other existing methods.

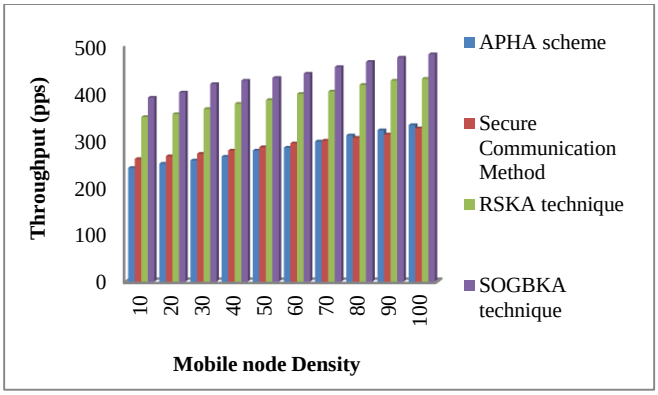

Figure 5: Measurement of Throughput rate

The figure 5 demonstrates the performance of throughput versus diverse mobile node density using four methods. As revealed in Figure 3, proposed SOGBKA technique affords better throughput when compared to existing APHA scheme [1], Secure Communication Method [2] and RSKA technique [3]. In addition, while increasing the number of mobile nodes for data transmission, throughput is also gets increased using all the three methods. But comparatively throughput using proposed SOGBKA technique is higher. This is because of application of self organized gradient boosting key authentication algorithm in proposed SOGBKA technique. By using this algorithmic process, SOGBKA technique authenticates every mobile node in network before transmitting the data using public key and their certificate. This helps for SOGBKA technique to choose the optimal node for secure data transmission which resulting in enhanced throughput rate in an efficient manner.

Therefore, proposed SOGBKA technique increases the throughput rate by 45% when compared to APHA scheme [1] and 52 % when compared to Secure Communication Method [2] and 12 % when compared to RSKA technique respectively.

Measurement of Data Loss Rate

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

$$\text{Data Loss Rate} = \sum_{i=1}^{n}[\text{Size}\,(DP_{send}) - \text{Size}\,(DP_{received})] \quad (17)$$

Data loss rate is lower, the method is said to be more efficient is shown in equation (17).

Table 3: Tabulation for Data Loss Rate

Data Packets Size (KB)	Data Loss Rate (KB)			
	APHA Scheme	Secure Communication Method	RSKA Technique	SOGBKA Technique
15	2	1.50	0.99	0.91
30	5	4	2	1
45	7	5	4	3
60	14	10	9	5
75	10	8	6	4
90	17	15	13	9
105	22	19	17	13
120	25	22	20	16
135	29	25	22	18
150	30	28	23	20

Table 3 presents the tabulation results for data loss rate using four methods with respect to different number of data packet size in the range of 15-150 KB. While considering the 120 KB size of data packet for transmission, the proposed SOGBKA technique acquires the 16 KB data loss rate whereas the APHA scheme [1] and Secure Communication Method [2] and RSKA technique[3] acquires 25 KB, 22 KB, 20 KB respectively.

Thus, data loss rate using proposed SOGBKA technique is lower while compared to other existing methods.

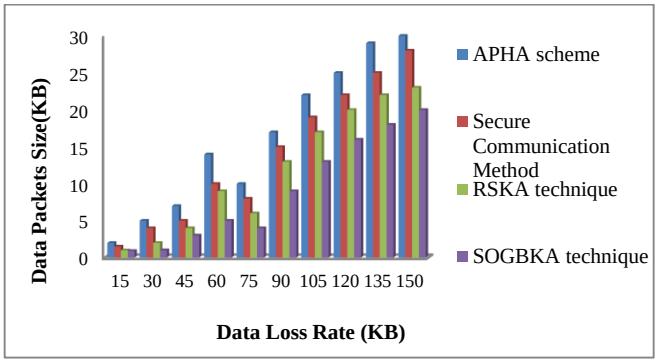

Figure 6: Measurement of Data Loss Rate

The figure 6 depicts that the performance of data loss rate versus different number of data packet size using four methods. Data loss rate using proposed SOGBKA technique is lower due to the process of tree pruning in SOGBKA technique. During the tree pruning process, the trust value is evaluated for mobile nodes in network. With help of determined trust value, then SOGBKA technique efficiently removes the mobile node with lower trust value with objective of enhancing the data security in MANETs. This in turn supports for minimizing the data loss rate in an effective manner.

As a result, proposed SOGBKA technique reduces the data loss rate by 51% when compared to APHA scheme [1] and 41 % when compared to Secure Communication Method [2] and 27 % when compared to RSKA technique respectively.

Measurement of Time for Secured Data Delivery

Time for secured data delivery determines the amount of time taken for achieving secured data transmission with minimum data loss rate in MANETs. The time for secured data delivery is measured in terms of milliseconds (ms) and mathematically represented as,

$$\text{Time for Secured Data Delivery} = \sum_{i=1}^{n} DP * \text{Time}(DP_i) \quad (18)$$

By using equation (18), time for secured data delivery is the product of number of data packets sent and the time taken to deliver the data packets in the network. While the time taken for secured data delivery is lower, the method is said to be more efficient.

Table 4: Tabulation for Time for Secured Data Delivery

Number of Data Packets	Time for Secured Data Delivery (ms)			
	APHA Scheme	Secure Communication Method	RSKA Technique	SOGBKA Technique
9	0.654	0.602	0.512	0.475
18	0.679	0.623	0.532	0.482
27	0.688	0.638	0.541	0.490
36	0.698	0.645	0.556	0.499
45	0.705	0.656	0.566	0.512
54	0.716	0.671	0.579	0.521
63	0.732	0.683	0.582	0.535
72	0.755	0.695	0.599	0.542
81	0.768	0.704	0.618	0.550
90	0.789	0.711	0.627	0.563

While considering the 45 data packet for transmission, the proposed SOGBKA technique takes the 0.512 ms time whereas the APHA scheme [1] and Secure Communication Method [2] and RSKA technique[3] acquires 0.705 ms , 0.656 ms, 0.566 ms respectively. As a result, the secured data delivery using proposed SOGBKA technique is lower while compared to other existing methods.

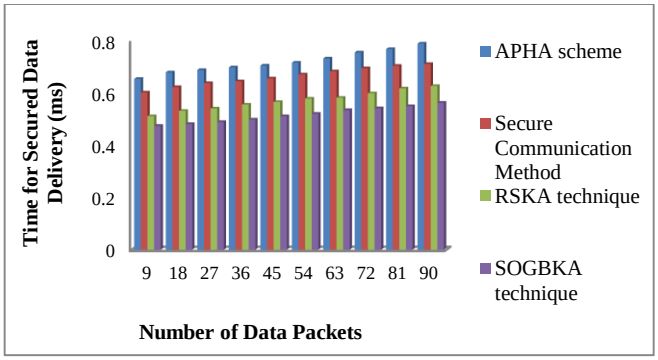

Figure 7: Measurement of Time for Secured Data Delivery

The secured data delivery using proposed SOGBKA technique is lower because of application of self organized gradient boosting key authentication algorithm where each mobile node in MANETs creates the public key and certificate by the mobile node itself shown in figure 7. This helps for SOGBKA technique to choose a most favorable route path between the source node and destination mobile node for securely transmitting the data in MANETs through node authentication. This in turn helps for minimizing the time for performing the secured data delivery in an effectual manner.

Thus, proposed SOGBKA technique reduces the time taken for achieving secured data delivery by 28% when compared to APHA scheme [1], 22 % when compared to Secure Communication Method [2] and 10 % when compared to RSKA [3] technique respectively.

CONCLUSION

An efficient Self Organized Gradient Boosting Key Authentication (SOGBKA) technique is developed for improving the security of data communication in MANETs with higher throughput. The SOGBKA technique comprises three processes such as tree building, tree pruning and optimal node selection for securely transmitting the data transmission in MANETs. At first, the SOGBKA technique creates Gradient Boosting tree with assist of mobile nodes in network and then makes self organized key for each mobile node. Subsequently, the SOGBKA technique computes trust values of mobile node using the data packet forwarded and dropped rate. Next, SOGBKA technique accomplishes tree pruning process where the mobile node with lower trust value is removed for significantly minimizing the data loss rate during the data transmission. At last, SOGBKA technique selects the optimal node in network for securely transmitting the data packet through self organized key authentication. This in turn increases the throughput of SOGBKA technique with minimum time for achieving secured data delivery in MANETs. The performance of SOGBKA technique is tested with the metrics such as data loss rate, throughput and time for secured data delivery. With the simulations performed for SOGBKA technique, it is observed that the throughput rate is

provided more accurate results as compared to state-of-the-art works. The simulation results reveal that SOGBKA technique affords better performance with an improvement of throughput rate and reduction in time for secured data delivery the when compared to the state-of-the-art works.

REFERENCES

[1] Huansheng Ning, Hong Liu and Laurence T. Yang, "Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Things", IEEE Transactions on Parallel and Distributed Systems, Vol. 26, No. 3, pages 657 – 667, March 2015

[2] Kei Kobayashi, Yosuke Totani, Keisuke Utsu, Hiroshi Ishii, "Achieving secure communication over MANET using secret sharing schemes", The Journal of Supercomputing, Springer, Volume 72, Issue 3, Pages 1215–1225, March 2016

[3] Sangeetha S and S Sathappan [3], "Reputation based Symmetric Key Authentication for Secure Data Transmission in Mobile Ad Hoc Networks", International Journal of Electrical and Computer Engineering (IJECE), applied

[4] Ahmad Alomari, "Mutual Authentication and Updating the Authentication Key in MANETS", Wireless Personal Communications, Springer, Volume 81, Issue 3, Pages 1031–1043, April 2015

[5] Gorti VNKV Subba Rao, Garimella Uma, "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, Volume 13, Issue 9, Pages 21-33, 2013

[6] Gautam M. Borkar, A. R. Mahajan, "A secures and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks", Wireless Networks, Springer, Pages 1–18, 2016

[7] Ahmad Alomari, "Security Authentication of AODV Protocols in MANETs", Network and System Security, Springer, Pages 621-627, 2013

[8] Rajinder Singh, Parvinder Singh and Manoj Duhan, "An effective implementation of security based algorithmic approach in mobile adhoc networks", Springer, Human-centric Computing and Information Sciences, Volume 4, Issue 7, Pages 1-14, December 2014

[9] Tejashree Kokate, R.B.Joshi, "Authentication in Mobile Ad Hoc Network for Secure Communication", International Journal of Science and Research (IJSR), Volume 4 Issue 6, June 2015, Pages 327-331

[10] Abu Taha Zamani, Syed Zubair, "Key Management Scheme in Mobile Ad Hoc Networks", International Journal of Emerging Research in Management &Technology, Volume 3, Issue 4, Pages 157-165, 2014

[11] Dega Ravi Kumar Yadav, K. Nikitha Reddy, N. Vamshi Krishna, "Authenticated Mutual Communication between two Nodes in MANETs", International Journal of Computer Science and Information Technologies, Volume 4, Issue 2, Pages 331- 333, 2013

[12] Snehal Javheri, Rahul Kulkarni, "Secure Data Communication Using DNA based Cryptography in Mobile Adhoc Network", International Journal of Science and Research (IJSR), Volume 3 Issue 9, Pages 1504-1508, September 2014

[13] Maha Abdelhaq, Raed Alsaqour, Shawkat Abdelhaq, "Securing Mobile Ad Hoc Networks Using Danger Theory-Based Artificial Immune Algorithm", Plos One, Volume 10, Issue 5, Pages 1-16, 2016

[14] Jan Papaj and Lubomir Dobos, "Cooperation between Trust and Routing Mechanisms for Relay Node Selection in Hybrid MANET-DTN", Hindawi Publishing Corporation, Mobile Information Systems, Volume 2016, Article ID 7353691, Pages 1-18, 2016

[15] Sunil Deokule, Nivedita Malvadkar, Rupali Nimbalkar, "Reliable Communication Using Topology Control in Mobile Ad-hoc Network", International Journal of Computer Science and Information Technologies, Volume 5, Issue 2, Pages 991-993, 2014

[16] Sukin Kang, Cheongmin Ji, and Manpyo Hong, "Secure Collaborative Key Management for Dynamic Groups in Mobile Networks", Journal of Applied Mathematics, Hindawi Publishing Corporation ,Volume 2014, Article ID 601625, Pages 1-10, 2014

[17] Poonam Gera, Kumkum Garg, and Manoj Misra, "Trust-based Multi-Path Routing for Enhancing Data Security in MANETs", International Journal of Network Security, Volume16, Issue 2, Pages 102-111, 2014

[18] Priyanka Takalkar, Aaradhana Deshmukh, "Trust Based Secure Data Communication in MANET", International Journal of Emerging Technology and Advanced Engineering", Volume 4, Issue 12, Pages 542-546, December 2014

[19] Gautam M. Borkar, A. R. Mahajan, "A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks", Wireless Networks, Springer, Pages 1–18, May 2016

[20] Srinivas Aluvalaa, K. Raja Sekhara and Deepika Vodnala, "A novel technique for node authentication in mobile ad hoc networks", Perspectives in Science, Elsevier, Volume 8, Pages 680-682, 2016

[21] Saju P John and Philip Samuel, "Self-organized key management with trusted certificate exchange in MANET", Ain Shams Engineering Journal, Volume 6, Issue 1, Pages 161–170, March 2015.