Journal of Theoretical and Applied Information Technology
15th October 2017. Vol.95. No 19

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SELF ORGANIZED SPECTRAL KEY AUTHENTICATION FOR SECURED TRANSMISSION IN MANET

[1] PROF. CHIDAMBAR INAMDAR, [2] DR. CHANDRASEKAR C, [3] DR. S. NITHYA REKHA

[1] Research Scholar , Bharathiar University, Coimbatore, India
[2] Professor, Periyar Univeristy, Salem, India.
[3] Asst.Professor, Department of Computer Science and Engg,
Qassim Private Colleges,Al-Qassim,Buraidah, Kingdom of Saudi Arabia.

E-mail: cinamdar@gmail.com

ABSTRACT

A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organized and temporary network topologies. MANET is a collection of wireless networks which consists of large number of mobile nodes. Nodes in MANETs are connected wirelessly without fixed infra structure. Due to the nodes mobility, the wide range of intrusion takes places in MANET. Therefore, security in data packet transmission between the mobile nodes plays major role in MANETs. In order to improve the secured transmission, Self Organized Spectral Key Authentication (SO-SKA) technique is introduced in MANET. Initially, the public and public key certificate of each mobile node in MANET is generated by the mobile node itself. Secondly, the trust values of the mobile nodes with their neighboring nodes are measured regarding the data packet forwarded and dropped to improve the security factor. Finally, Spectral clustering is applied to group the mobile nodes and certificate exchange Key authentication helps the mobile nodes to authenticate themselves with their neighboring mobile nodes to improve the data packet transmission. The simulation is carried out to analyze the performance of proposed SO-SKA technique with the parameters such as data packet delivery ratio, Average end to end delay and data packet security level.

Keywords: *Mobile Ad Hoc Networks, Self Organizing, Public Key, Public Key Certificate, Trust Value, Spectral Clustering, And Key Authentication.*

1. INTRODUCTION

MANET is a decentralized type of wireless network without considering the pre-existing infrastructure, such as routers in wired networks. Each node in the network performs routing by forwarding data to other nodes. During the transmission, the security is the major issues in MANET. Any attack in the network may disturb the overall communication and the entire network. Therefore, the objective of improving secured communication in MANET, the key authentication is used. It is also used to solve the problem of authenticating the keys of the nodes.

This is usually done after the keys have been shared between the two nodes over some secure channel. In our work, each node assigned as public key using self organizing key approach. This technique is used to allow the mobile nodes to generate their own public/private key pairs itself. This ensures the security for improving the network communication.

A report-based payment scheme (RACE) was introduced in [1] for multi-hop wirelesses networks to improve node cooperation, control packet transmission, and enforce fairness. However, trust system based on processing the payment reports failed to preserve a trust value for each node. Ad hoc on-demand multicast distance vector–secure adjacent position trust verification (AOMDV–SAPTV) technique was developed in [2] for providing higher packet delivery ratio and minimum delay. However, it has more time for key generation and security level of the data packet transmission was not improved at a required level.

Game theory was introduced in [3] using Optimized Link State Routing Protocol (OLSR) for security problem. However, the behavior of the mobile node was not evaluated based on the trust factor. A danger theory-based artificial immune algorithm called mobile dendritic cell algorithm (MDCA) was introduced in [4] to improve the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

security. However, the number of attacker in MANETs was not efficiently detected.

The secure framework for BeeAdHoc was developed in [5] based on fuzzy set theory and digital signature. However, the selfish node in the network was not detected. A high secure and efficient routing approach was introduced in [6] that control the properties of anonymity, security, authentication, non repudiation in ad hoc networks. However, trust of each node and their neighboring node was not performed.

An identity (ID) based protocol was designed in [7] that secures AODV and TCP hence it is used in dynamic and attack prone environments of mobile ad hoc networks. However, it failed to identify the trusted node in network. A secure group key management protocol with DH key agreement was introduced in [8] for data communication. But the data packet security level of the mobile node was not improved.

In [9], authentication and topology control TESLA scheme was introduced for mobile ad hoc network to improve the throughput. However, it failed to develop hop to hop connectivity and integrity. A Flooding Factor based Framework for Trust Management (F3TM) was introduced in [10] for secure data transmission in MANET. However, the key generation was not performed in self organized manner.

Secure Optimized Link State Routing mechanism [11] was designed to provide the secure data communication in MANET when certificates the authorized nodes. However, it failed to reduce the communication overhead in the network.
Cross-layer based distributed and cooperative Intrusion Detection System (IDS) with Dempster-Shafer (DS) evidence theory (CID) [12] was to provide direct trust values of unauthorized nodes in MANET. However, trust of each node was not measured efficiently.

Dynamic Multicast Height Balanced Group Key Agreement (DMHBGKA) technique [13] was developed to provide the security while communicating the nodes in MANET. But, the data transmission rate was low.

The issues are identified from above reviews such as lack of data packet security level, higher delay, lack of key authentication, more time for key generation and hop to hop connectivity. In order to overcome such kind of issues, Self Organized Spectral Key Authentication (SO-SKA) technique is introduced in MANET.

The contribution of the paper is summarized as follows,

- Self Organized Spectral Key Authentication (SO-SKA) technique is introduced to improve the security during the communication in MANET. At first, the Key Generation model includes the generation of public key and public key certificate of the each node in a self organizing manner. This helps to improve the mobile node that has to send data packets to other neighboring node with its public keys. The Issue and expiry time of public key are measured to identify the validity of the public key.
- Then the trust value of the each mobile node is performed in SO-SKA technique based on the data packet forwarded and dropped for neighboring node authentication. This is capable for selecting a node with maximum trust value among all pair of the nodes in MANET to perform transmission with minimum end to end delay.
- Finally, spectral key authentication is performed to improve the secured data packet transmission. In key authentication, the node which has higher trust values is grouped based on similarity pair of the mobile node. Then the key authentication is performed by exchange the certificate of the node with their one hop node. If the source node has the certificate of the destination node, the data packet is forwarded successfully to improve the packet delivery ratio.

The remaining paper is organized as follows. Section 2 describes the proposed Self Organized Spectral Key Authentication (SO-SKA) technique with neat diagram. In Section 3, Experimental settings are presented and the parametric matrices analysis is presented in section 4. Section 5 introduces a reviews related to the works. Section 6 provides the conclusion of the paper.

2. SELF ORGANIZED SPECTRAL KEY AUTHENTICATION FOR MANET SECURITY

Security is the major concern in order to provide preserve communication during the multi hop transmission between the mobile nodes. Hence, there is a need for designating a stable, reliable and secured transmission to ensure higher packet delivery ratio, minimum delay, and higher data packet security level. To overcome these problems occurred in MANET; A Self Organized

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Spectral Key Authentication (SO-SKA) technique is introduced.

2.1 System Model

In MANET, A Self Organized Spectral Key Authentication (SO-SKA) technique is introduced to improve the reliable and secure routing. Let us consider the design of MANET is constructed in a graph '$G(V,E)$' where 'V' denotes the number of mobile nodes $V \in MN_i = MN_1, MN_2, MN_3 \ldots MN_n$ and 'E' is the link between mobile nodes. A source node (SN) transmits a data packet based on route request (RREQ) and reply (RREP) to destination node (DN) through the intermediate node (IN). A one hops certificate chain from a public key 'PK_i' and their public key certificatesPK_C. With this system model the proposed Self Organized Spectral Key Authentication improves the data packet delivery ratio with reduced average end to end delay is designed.

2.2 Self Organized Spectral Key Authentication Technique

In MANET, a Security problem in term of authentication is carried out extensively to perform efficient transmission. Several efficient and secure Approaches have been designed to protect the network. However, they still lack the security during the transmission. Therefore, an efficient security mechanism called Self Organized Spectral Key Authentication (SO-SKA) is developed in MANET.

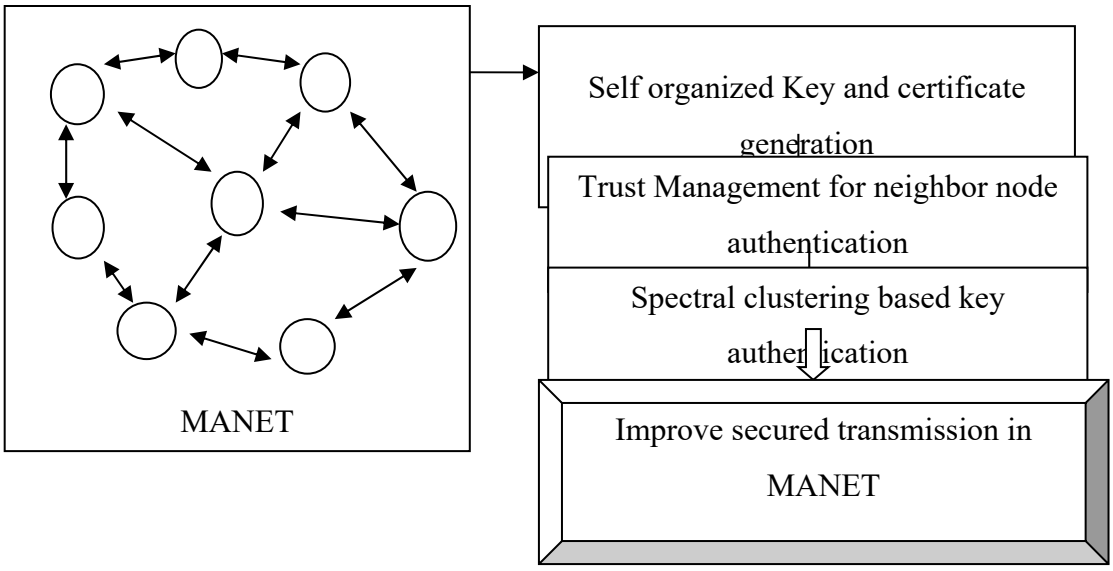

Figure 1 Flow Processing Diagram Of The Self Organized Spectral Key Authentication

Figure 1 clearly describes the Flow processing diagram of the Self organized spectral key authentication (SO-SKA) technique. The proposed SO-SKA technique includes three processing steps namely key generation, trust management and key authentication. In MANET, the mobile nodes are generates their own public key and certificates in a self organized manner. This shows the node identity to participate in network transmission. In second step, trust value of the node transmission is performed effectively. The brief description about the SO-SKA technique is presented in forth coming sections. is calculated for improving the level of authentication that one node about other neighboring node in network. These trust measurement is obtained based on the number of packet forwarded and number of packet dropped. In final step, the nodes are grouped using spectral clustering and perform the key authentication before the transmission. Once the certificate is verified, then the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2.2.1 Self organized key generation

The first step in the design of SO-SKA technique is the key generation process in a self organized manner. In key generation, the private or public key of the each mobile node and their neighboring node is generated. Self organizing key generation is the mobile node itself generates the public key and issuing certificates to neighboring nodes, holding these certificates in its certificate repository to store the subset of the repository for secured data transmission in MANET.

Let us consider the two mobile nodeMN_i' and 'MN_j and their public key is PK_i and PK_j respectively. Each mobile node generates its public key (PK) and the equivalent private key locally before connecting the network by the node itself. The self organized public-key certificates as combining the public keys and the equivalent node identities IDs. The certificate includes the node's identity/network address; certificate generation and validity time (i.e. instance ID). Therefore, the certificate of the of the mobile node MN is generated as follows,

$$PK_C \rightarrow MN_{ID}, PK_i, Des_{ID}, I_{ID} \quad (1)$$

From (1), PK_C is the public key certificate and MN_{ID} is the mobile node Id, PK_i denotes pubkic key of the node and destination ID (Des_{ID}), I_{ID} is the validity time. If the mobile node 'MN_i' considers that a public key 'PK_j' belongs to other mobile node 'MN_j', then the mobile node 'MN_i' allows a public key certificate in which 'PK_j ' is bound to 'MN_j' by the signature of 'MN_i. It is formulated as follows,

$$MN_i \rightarrow MN_j : \ PK_j \ \forall \ MN_j, (i, j \ \in 1,2, \dots, n) \quad (2)$$

Therefore, the Issued public key certificates to or from the node is stored in its certificate repository with a validity time. Hence the issue and expiry time of the certificate are measured as follows.

$$PK_C \rightarrow \ PK_i, Iss_T, Exp_T \quad (3)$$

From (3), the public key certificate (PK_C) issuing time (Iss_T) and expiry time (Exp_T) is measured in SO-SKA technique to avoid the mobile node pair being held by the network for longer period of time. When a public key certificate expires (PK_C) and the issuing mobile node believes that the certificate is still valid, and then the issuing mobile node issues an updated version of the similar certificate. The updated version consists of old public key certificate is formulated as given below.

$$UPK_C \rightarrow \ PK_i, UIss_T, UExp_T \quad (4)$$

From (4), U denotes a updated version of the public key certificate (UPK_C), Updated issue time ($UIss_T$)and expiry time ($UExp_T$) respectively. Therefore, the updated public key certificate is evaluated to perform efficient transmission. This also helps to send data packets with public key certificates based on the other mobile node's public keys. The self organized key and certificate generation algorithm is described as follows,

Input : Number of Mobile Nodes '$MN_i = MN_1, MN_2, \dots, MN_n$', Public Key '$PK_i$', public key certificate PK_C, public key issuing time 'Iss_T', public key expiry time 'Exp_T'
Output : public key and certificate generation
Step 1: Begin
Step 2: For each mobile node MN_i
Step 3: Generate public key (PK_i) by the node itself
Step 4: Measure public key certificate using (1)
Step 5: Measure the certificate Issue and expiry time for identifying the validity using (3)
Step 6: **if (**MN believes $PK_C$is valid) then
Step 7: Updates public key certificate
Step 8: else
Step 9: Invalid public key
Step 10: End if
Step 11: End for
Step 12: End

Figure 2 Self Organized Key And Certificate Generation

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Figure 2 describes the self organized key and certificate generation algorithm in SO-SKA technique. For each mobile node in MANET generates the public key itself. Then the public key certificate sent with each data packet based on the other mobile node's public keys. For each session, PK_c is updated in order to find their validity based on the issue time and expiry time. Therefore, the advantage of this system is that it reduces the delay of having a separate public key and certificate sent with each data packet.

2.2.2 Trust Management For Neighbor Node Authentication

Once the public key and public key certificate generation is completed, then the trust value of the each mobile node is measured for neighbor node authentication. The trust value between the nodes is measured based on the data packet forwarded and dropped. Let us consider the trust Factor $TF_{i,j}$, and the number of data packets $DP_i = DP_1, DP_2, DP_3 \ldots . DP_n$. The data packet forwarded is measured as follows,

$$DP_f = \sum_{i,j=1}^{n} \frac{DP_f(MN_j)}{DP_i\,(MN_i)} \quad (5)$$

From (5),DP_f represents the data packet forwarded rate , $DP_f(MN_j)$ is the number of data packet forwarded to neighboring node and $DP_i\,(MN_i)$ is the number of data packet issued from the mobile node MN_i. Similarly, the data packets dropped is measured as,

$$DP_D = \sum_{i,j=1}^{n} \frac{DP_D(MN_j)}{DP_i\,(MN_i)} \quad (6)$$

From (6),DP_D is the data packet dropped hence the difference between the data packet forward and data packet dropped is measured to attain the trust factor. Therefore, the trust factor is measured as follows,

$$TF = DP_f - DP_D \quad (7)$$

From (7),TF denotes a trut factor for any mobile nodes in network. With the help of the trust value, the node performs efficient transmission to the neighboring node thereby improving the security of the data transmission. The algorithmic process of Trust based neighbor node authentication is shown in figure 3.

Input : Mobile Nodes '$MN_i = MN_1, MN_2, \ldots, MN_n$', number of data packets$DP_i = DP_1, DP_2, DP_3 \ldots . DP_n$, Threshold '$'Th$'
Output : Reduced end to end delay
Step 1: Begin
Step 2: For each MN_i and neighboring node NN_i
Step 3: Measure data packet forwarded using (5)
Step 4: Measure data packet dropped using (6)
Step 5: Evaluate trust value using (7)
Step 6: If $(TF > Th)$ then
Step 7: Neighboring node is secured and exchange the key certificate to transfer the data packet
Step 8: else
Step 9: Neighboring node is not secured to transfer the data packet
Step 10: end if
Step 11: End for
Step 12: End

Figure 3 Trust Based Neighbor Node Authentication Algorithm

Figure 3 shows the algorithmic description of the Trust based neighbor node authentication for transferring the data packet in a secured manner. For each mobile node and their neighboring node, the trust value is calculated with respect to packet forwarded and dropped. If the trust value of the node is greater than the threshold value, the neighboring node is secured for capable for transmitting the data packet. Otherwise, it is not secured. Therefore, the SO-SKA technique effectively selects the neighboring node confidentiality to perform transmission with minimum delay.

2.2.3 Spectral clustering based key authentication

The final step of the SO-SKA technique is the spectral clustering based key authentication to transfer the data packet. Higher trusted nodes are grouped using spectral clustering. A spectral

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

clustering uses the spectrum of the similarity pair of the node for reducing the dimensionality. The node which has higher trust value is selected within the cluster it act as a cluster head. Nodes combined together permits monitoring work to continue more naturally, so as to improve the overall network security. The weighting matrix is performed based on the similarity pair of the mobile node which is based on the trust value. The weighting matrix between the two mobile nodes MN_i *and* MN_j is described as follows,

$$W_{ij} = F\left(\left\|MN_i, MN_j\right\|, \sigma\right) \quad (8)$$

From (8),W_{ij} represents the weighting matrix between the similarity function of two mobile nodes and σ is the scaling parameter which is used to determine the local structure of the connections between the nodes in Network. Each node has the different weighting factor namely trust value. The node which has higher trust value is a normal one and the security level is extremely high. Hence the diagonal matrix 'D_{ij}' is defined through the weight matrix,

$$D_{ij} = \sum_{i,j=1}^{n} W_{ij} \quad (9)$$

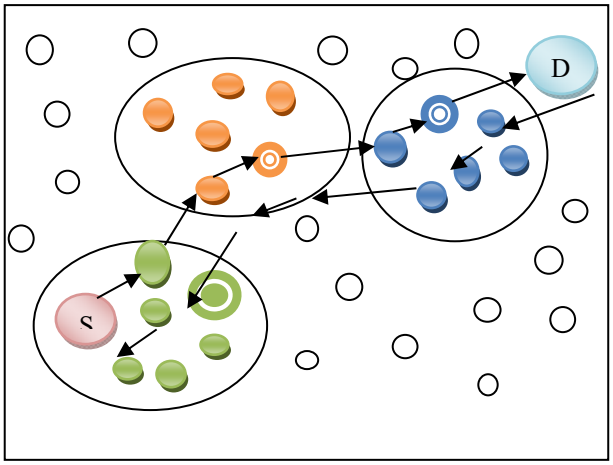

Figure 4 Spectral Clustering Based Key Authentication

Therefore, clustering of the mobile node is performed and the key authentication is performed to improve the secured data transmission from source nodes (SN) to destination node (DN). The clustered mobile nodes are shown in figure 4. Figure 4 shows the spectral clustering is described with different spectrum of colors. The condition of the spectral is not limited to a specific set of values but it can vary. Due to the varying nature of the mobile node, the key authentication is a major task to improve the security. Let us consider the Source node (SN), and the destination node (DN). Therefore, the authentication is performed by the each node exchange a certificate with one hop manner. Initially, a source node sends a route request to the one hop trusted node with their certificate.

$$SN \rightarrow A;\ \left\{RREQ, PK_{C;SN\rightarrow A}\right\} \quad (10)$$

From (10),A is the one hop node of source node. Once the one hop trusted nodes receives the request with public key certificates (PK_C) . Then one hop node searches the certificate of the source node signed by this node in its certificate repository and includes its route request packet before forwarding the route request packet to other one hop nodes. After receiving the RREQ from the one hop nodes, the DN has the whole certificate chain required to recover the source node's public key. The DN sends a reply packet to their one hop node.

$$DN \rightarrow A;\left\{RREP, PK_{C;DN\rightarrow A}\right\} \quad (11)$$

From (11), If the source node (SN) received the more than one route reply (RREP) for the similar route request, it selects the route which has the minimum number of certificates. The untrusted node is not receiving the route request. Therefore, the successful transmission result is obtained to improve the trust between certificate and signing more certificates for each others. If the source node received the public key certificates of the destination node, then the data packet is transmitted. Otherwise, the data packet is not transmitted. The authentication of the public-key certificate is performed by checking its validity time. This helps to improve the secured data packet transmission between source node and destination node in MANET. The algorithmic process of the Spectral clustering based key authentication algorithm is shown in figure 5.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Input : Source node 'SN', Mobile Nodes '$MN_i = MN_1, MN_2, \dots, MN_n$', PK_C, Destination node 'DN', Data Packets '$DP_i = DP_1, DP_2, \dots, DP_n$
Output: Improved packet delivery ratio and security level
Step 1: Begin
Step 2: For mobile nodes MN_i
Step 3: Group the mobile nodes using spectral clustering through the weighted matrix using (8)
Step 4: SN sends a request with public key certificates to one hop neighbor using (10)
Step 5 : DN sends reply packet to one hop neighbor using (11) for authentication
Step 6: If 'SN' has the certificates of 'DN' then
Step 7: Forwards the data packet 'DP_i'
Step 8: Else
Step 9: No data packet has to be forwarded
Step 10: End if
Step 11: End for
Step 12: End

Figure 5 Spectral Clustering Based Key Authentication Algorithm

Figure 5 shows the Spectral clustering based key authentication algorithm for improving the delivery ratio through corresponding neighboring nodes. The trusted nodes are grouped using spectral clustering. Then the authentication is performed to attain higher delivery ratio. If the SN has public key certificate of DN, then the data packets are forwarded to the neighboring nodes for achieving the data packet security level. There are no certificates obtained from the neighboring nodes, no data packets are forwarded. In this way, the mobile nodes send their data packets only to the neighboring nodes possessing certificates. This helps to improve the secured data packet transmission and improves the packet delivery ratio.

3 EXPERIMENTAL SETTING

An efficient Self Organized Spectral Key Authentication (SO-SKA) technique is implemented in NS2.34 network simulator. Totally 500 nodes are deployed within the network range of 1500 m*1500 m size. The Destination-Sequenced Distance Vector (DSDV) routing protocol is used to analyze the performance of the proposed SO-SKA technique. The nodes' mean speed varies from 0 to 35 m/s. The node mobility uses the random waypoint model. The simulation parameter is shown in following table 1.

Table 1 Simulation Parameters

Simulation parameter	Value
Simulator	NS2 .34
Protocol	DSDV
Number of nodes	50,100,150,200,250,300,350,400,450,500
Simulation time	2000sec
Mobility model	Random Way Point
Nodes speed	0-35m/s
Network area	1500m * 1500m
Data packets	9,18,27,36,45,54,63,72,81,90
Number of runs	10

4. RESULT ANALYSIS

Result analysis of SO-SKA technique is performed and compared with two existing methods namely Report-based pAyment sChemE (RACE) [1] and Ad hoc On-demand Multicast Distance and Vector–Secure Adjacent Position Trust Verification (AOMDV–SAPTV) [2]. In order to evaluate the performance of SO-SKA technique, a network consisting of 500 nodes within the area and uses Random Waypoint Model as the mobility model. The various

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

simulation parameters such as packet delivery ratio, average end to end delay and data packet security level with the help of tables and graphs.

4.1 Impact of data packet deliver ratio

Data packet delivery ratio is defined as the number of data packets delivered at the destination to the number of data packet being sent from source node. The data packet delivery ratio is measured as follows.

$$DPDR = \frac{DP_r}{DP_s} * 100 \quad (12)$$

From (12),$DPDR$ represents the Data Packet Delivery Ratio and it is measured in terms of percentage (%). Higher delivery ratio, the method is said to be more efficient.

Table 2 Tabulation For Data Packet Deliver Ratio

Data Packets Sent	Data packet Delivery Ratio (%)		
	SO-SKA	RACE	AOMDV–SAPTV
9	92.25	54.28	66.85
18	95.57	58.04	72.36
27	97.38	64.16	75.20
36	91.20	53.04	68.58
45	93.36	56.17	70.12
54	94.21	63.04	73.65
63	96.02	64.11	78.20
72	97.26	68.36	80.12
81	97.89	72.32	82.64
90	98.23	78.47	85.10

Table 2 describes the performance analysis of data packet delivery ratio based on the number of data packets being sent from source node to destination. Delivery ratio gets increased while increasing the number of data packets in all the methods. But comparatively, the SO-SKA technique achieves higher delivery ratio when compared to existing RACE [1] and AOMDV–SAPTV [2].

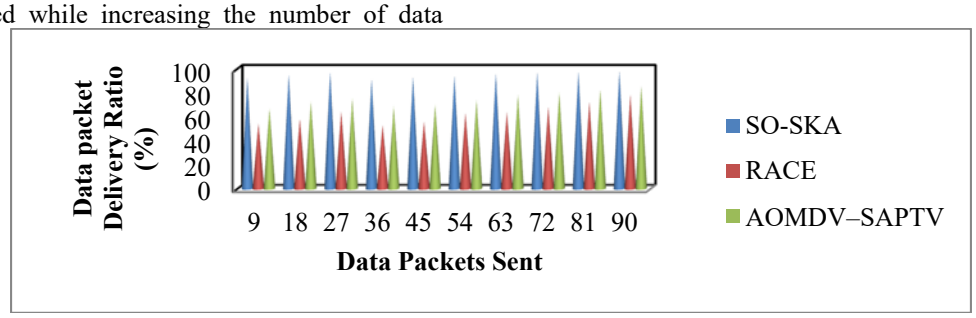

Figure 6 Measure Of Data Packet Delivery Ratio

Figure 6 illustrates the data packet delivery ratio performance analysis with respect to number of data packets being sent are varied from 9 to 90. As shown in figure, while increasing the number of packets, the packet delivery ratio gets increased in all the methods. But it is not linear due to data packet loss. The proposed SO-SKA technique improves data packet delivery ratio than the existing methods [1] [2]. This is because; the SO-SKA technique uses Spectral clustering based key authentication. In SO-SKA technique, the node public key is generated and issues the certificates by self organizing manner. Then the trust value of the each node is calculated based on the number of packet forwarded and dropped in order to perform the neighbor node authentication. This helps to improve the data packet delivery ratio. Moreover, the Spectral clustering based key authentication is performed according to the public key certificate exchange. If the SN has the public key certificate of DN, then the data packets are forwarded to the neighboring nodes. Followed by, the SN sends their data packets only to the neighboring nodes possessing certificates. Therefore, the data packet delivery is considerably increased by 53%

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and 27% when compared to existing RACE [1] and AOMDV–SAPTV [2] respectively.

4.2 Impact of Average end to end delay

Average end to end delay is defined as the Average time taken by a data packet to arrive in the destination with respect to time for data packet forwarding (i.e. sending). It is measured in terms of milliseconds (ms).

$$AEED = Arrival\ time\ (DP) - Forwarding\ time\ (DP) \quad (13)$$

From (13),$AEED$ is the Average end to end delay with respect to number of packet being sent. Less end to end delay more efficient the method is said to be.

Table 3 Tabulation For Average End To End Delay

Data Packets Sent	Average end to end delay (ms)		
	SO-SKA	RACE	AOMDV–SAPTV
9	78	83	94
18	83	86	104
27	91	92	112
36	102	106	120
45	112	123	129
54	114	134	140
63	116	140	146
72	120	146	150
81	126	148	159
90	130	150	167

Table 3 describes the average end to end delay analysis with respect to number of data packets being sent. As a result, end to end delay of proposed SO-SKA technique is compared with existing RACE [1] and AOMDV–SAPTV [2]. The proposed method considerably reduces the average end to end delay during the transmission than the other existing methods

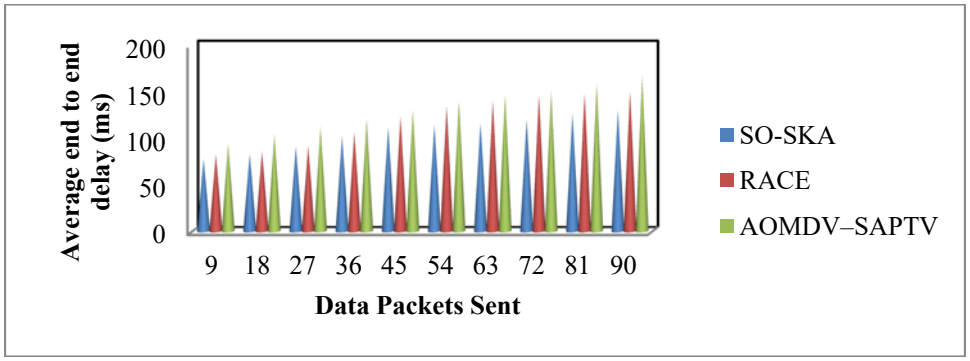

Figure 7 Measure Of Average End To End Delay

Figure 7 shows the average end to end delay with respect to number of packets is used for experimental purposes is varied from 9 to 90. the existing methods [1] [2]. This is because; the key generation is performed and each mobile node has public key and public key certificate. This helps to improve the transmission with minimum delay. Moreover, the key authentication process is carried out using spectral clustering. The trust management is used for neighbor node authentication. The trust The simulation result shows that the proposed SO-SKA technique considerably reduced the Average end to end delay than value of the node and their neighbor's nodes are measured to perform data transmission. The network which has high trusted nodes is selected to reduce the delay. Then the SN sends a data packet to the destination to avoid the packet drop and improves the packet delivery with minimum delay. As a result, Average end to end delay is significantly reduced by 10% and 19% when

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

compared to existing RACE [1] and AOMDV–SAPTV [2] respectively.

4.3 Impact of Data packet security Level

Data packet security level is measured based on the difference between the number of data packets being sent and number of data packets are not received (i.e. data packet loss) by the neighboring node. It is measured in terms of packets per second (pps).

$$DPS = DP_s - DP_{NR} \quad (14)$$

From (14), DPS denotes Data Packet Security and DP_s represents data packet sent whereas DP_{NR} is the number of data packet not received by the neighboring node.

Table 4 Tabulation For Data Packet Security Level

Data Packets Sent	Data packet security level (pps)		
	SO-SKA	RACE	AOMDV–SAPTV
9	8	5	6
18	15	9	11
27	23	15	17
36	33	24	25
45	42	32	34
54	51	40	42
63	60	48	50
72	68	56	58
81	77	64	67
90	83	72	74

As listed in table 4, data packet security level is measured with respect to number of data packets. Let us consider, data packets sent is 9 and the number of data packet not received is 1 using SO-SKA technique. Therefore, 8 packets are successfully received per second by the neighboring node. This helps to improve security level during the data packet transmission. The Data packet security level of the proposed SO-SKA technique is reduced than the existing RACE [1] and AOMDV–SAPTV [2] respectively.

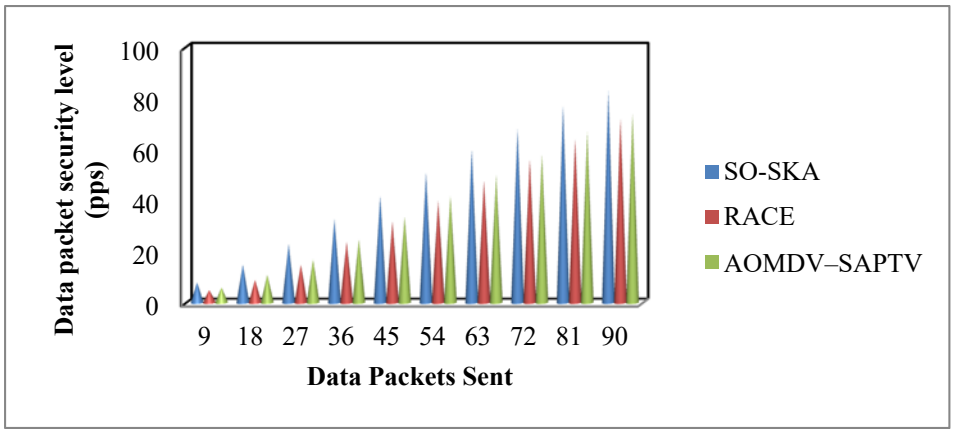

Figure 8 Measure Of Data Packet Security Level

Figure 8 shows the simulation analysis of Data packet security level with respect to number of data packets being sent from source node. Among the several data packets being transmitted, an amount of data packets are correctly received by the neighboring node is higher using SO-SKA technique. This improvement is achieved using self organized spectral key authentication method to perform public key certificate exchange to their neighboring node for

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

performing effective communication. In SO-SKA technique, the trust value is measured for all the mobile nodes in MANET. The node which higher trusts value is selected for grouping using spectral clustering. This helps to improve the Data packet security level. Moreover, SO-SKA technique performs authentication for all the nodes for managing the data packets to perform efficient data packet forwarding. Therefore, this helps to find a node by exchanging the certificate for improving the security during the data packet transmission. As a result, Data packet security level is significantly improved by 34% and 25% compared to existing RACE [1] and AOMDV–SAPTV [2] respectively.

Therefore, the performance analysis of the Self Organized Spectral Key Authentication (SO-SKA) technique is introduced to improve the security in data transmission with minimum end to end delay.

5. RELATED WORKS

A fast and secure routing was performed in [14] for providing the security using security algorithm. However, the key authentication based secured routing was not solved in order to enhance the security. The proposed SO-SKA technique performs spectral key authentication to achieve higher security level.

A trusted routing protocol also called TDS-AODV protocol was designed in [15] along with the trust values of its neighbor nodes. However, it failed to evaluate the certificate exchange in order to improve the security. The SO-SKA technique performs the key authentication by certificate exchange for achieving higher security.

An Effective Trusted Knowledge Algorithm (ETKA) was designed in [16] for secure data transmission. However, it failed to use secret keys for archiving higher security of communication. The SO-SKA technique measure the trust value of the node based on data packet forwarded and dropped and it have the public key of the node for improving the higher security level.

A self-organized key management technique coupled with trusted certificate exchange was introduced in [17] for mobile ad hoc networks. However, secured transmission of the packet was not improved. The proposed SO-SKA technique considerably improves the performance of the data packet delivery ratio with high secured manner.

A gateway authentication scheme was introduced in [18] for secure data transmission in MANE but it takes more delay. The SO-SKA technique significantly improves the packet delivery ratio with minimum average end to end delay.

A novel technique was introduced in [19] for node authentication in mobile ad hoc networks. However, the packet delivery ratio and delay analysis was not performed. The SO-SKA technique improves the performance analysis of delivery ratio and reduced average end to end delay.

Data delivery technique with respect to neighbor nodes' information was presented in [20] to achieve stable communication in MANET. But it failed to discover the DN for improving the communication in MANET. The proposed SO-SKA technique improves the data packet delivery ratio between source and destination node.

A unified trust management approach was introduced in [21] for improving the security of MANETs using Bayesian inference and Dempster-Shafer theory. However it increased the average end-to-end delay. The SO-SKA technique effectively improves security and reduces the average end to end delay.

In [22], a new routing scheme was developed based on trust between the nodes using clustering approach in MANETs. But it failed to analysis the node behaviors such as related mobility, and data packet forwarding for measuring the rust value. The SO-SKA technique significantly measures the data packet forwarding rate in order to measure the trust value.

A trust based model was designed in [23] for measuring the trust level of nodes and to perform secured routing in MANETs. However, the key management scheme was not used to achieve higher security. The SO-SKA technique uses the self organized key management approach for achieving higher security during data packet transmission.

6. CONCLUSION

An efficient Self Organized Spectral Key Authentication (SO-SKA) technique is introduced in MANET for secured data packet transmission in

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MANET. The main aim of proposed SO-SKA technique is to increase the secured data transmission in MANET. The proposed SO-SKA technique includes three processing steps for achieving the higher data packet security level. Initially, node public key and certificates are generated for each mobile node in a self organized approach. Authenticated is an on demand process which identifies intrusion action performed by untrusted mobile nodes in the network. This problem is difficult to solve in literature evaluation. Therefore, SO-SKA technique provides security services like such as authentication and message reliability. Proposed SO-SKA needs the support of trusted mobile node certificates for combining the ad-hoc network. The certificate holds the IP address of the node, public key, time when the certificate terminated. Proposed SO-SKA technique considers all nodes that include new certificates from the trusted node and public key of the network. This in turns the security of the network is improved using proposed SO-SKA technique.

After that, the trust factor of the each mobile node and their neighboring node is evaluated to obtain the higher security. It is referred as a measure of subjective certainty. In MANET, trust is analyzed as a level of certainty with the actions of nodes for providing higher security and enhances efficiency of the network. Node trust value is estimated by neighbor's cooperative opinion. The trust factor is measured based on the number of packet forwarded to neighboring node and packet dropped. This in turns proposed SO-SKA technique reduces the data communication cost during data transmission. Finally, the spectral key authentication is performed using spectral clustering with one hop public key certificate exchange for improving the data packet delivery ratio. Proposed SO-SKA technique effectively determines the node behaviors for calculating the trust value. It achieves higher security while transmitting the data packets with the aid of self-organized key management in MANET. Therefore, the nodes are effectively transfers from source node to destination for attaining effective secure communication. The main benefits of proposed SO-SKA technique improves the reliability of the network while secure transmission. Proposed technique also applies trust management system in a MANET for the evaluating different metrics like trusting accuracy; malicious node detection is done effectively. The performance result shows that the SO-SKA technique improves the data packet security level and packet delivery ratio with minimum average end to end delay than the state-of-art methods. Several authentication and key management scheme was presented in the literature evaluation for providing security aspects in MANET. However, they not improve the trust value of the nearby nodes in the network. The key authentication based secured routing was designed to provide the security in the network. However, security level was not sufficient. Therefore, proposed SO-SKA technique uses spectral key authentication to obtain the higher security level. In addition, certificate exchange scheme was developed in MANET. However, security was not improved. Therefore, SO-SKA technique performs the key authentication by certificate exchange for achieving higher security. However, during the transmission, communication overhead may be occurred when transmitting more number of data packets in the network. This leads to degrade the performance of the network. SO-SKA minimizes the computational cost for providing the security in MANETs while the security depends on the hardness of spectral key management issues. However, secure authentication rate is not at required level and also energy efficiency of the network is not considered.

REFERENCES:

[1] Mohamed M.E.A. Mahmoud and Xuemin (Sherman) Shen, "A Secure Payment Scheme with Low Communication and Processing Overhead for Multihop Wireless Networks", IEEE Transactions on Parallel and Distributed Systems, Volume 24, Issue 2, February 2013, Pages 209-224

[2] 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

[3] Hicham Amraoui, Ahmed Habbani, Abdelmajid Hajami and Essaid Bilal, "Security-Based Mechanism for Proactive Routing Schema Using Game Theory Model", Mobile Information Systems, Hindawi Publishing Corporation, Volume 2016, October 2016, Pages 1-7

[4] Maha Abdelhaq, Raed Alsaqour and Shawkat Abdelhaq, "Securing Mobile Ad Hoc Networks Using Danger Theory-Based Artificial Immune Algorithm" PLoS ONE, Volume 10, Issue 5, 2015, Pages 1-16

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[5] Marjan Kuchaki Rafsanjani, Hamideh Fatemidokht, "FBeeAdHoc: A secure routing protocol for BeeAdHoc based on fuzzy logic in MANETs", AEU-International Journal of Electronics and Communications, Elsevier, Volume 69, Issue 11, Pages 1613-1621, 2015

[6] Wei-Chen Wu and Horng-Twu Liaw, "A Study on High Secure and Efficient MANET Routing Scheme", Hindawi Publishing Corporation, Journal of Sensors, Volume 2015, February 2015, 2015, Pages 1-10

[7] Waleed S. Alnumay and Uttam Ghos, "Secure Routing and Data Transmission in Mobile Ad Hoc Networks", International Journal of Computer Networks & Communications (IJCNC) Volume 6, Issue 1, Pages 111-127, January 2014

[8] Sukin Kang, Cheongmin Ji, andManpyo Hong, "Secure Collaborative Key Management for Dynamic Groups in Mobile Networks", Hindawi Publishing Corporation, Journal of Applied Mathematics, Volume 2014, August 2014, Pages 1-11.

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

[10] Malik N. Ahmed, Abdul Hanan Abdullah, Hassan Chizari, Omprakash Kaiwartya, "F3TM: Flooding Factor based Trust Management Framework for secure data transmission in MANETs", Journal of King Saud University –Computer and Information Sciences, Elsevier, Pages 1-12, 2016

[11] Alaa Abdullah Majhool and Nor Effendy Othman, "Certificate Mechanism Improvement For Securing Optimized Link State Routing Protocol In Mobile Ad Hoc Networks", Journal of Theoretical and Applied Information Technology, Volume 92, Issue 1, Pages 98-108, 2016

[12] Y.Sharmasth Vali, T.R.Rangaswamy, "An Efficient Cross-Layer Based Intrusion Detection System for Mobile Ad Hoc Networks", Journal of Theoretical and Applied Information Technology, Volume 95, Issue 1, Pages 47-58, 2017

[13] G.Narayana, M.Akkalakshmi , A.Damodaram, "Dynamic Multicast Tree Maintenance Protocol For Secure Group Communication In MANET", Journal of Theoretical and Applied Information Technology, Volume 95, Issue 11, Pages 2383- 2392, 2017

[14] Priyanka Takalkar, Aaradhana Deshmukh, "Trust Based Secure Data Transmission Model in MANET", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 11, Pages 95-98, November 2013

[15] Renjian Feng, Shenyun Che, XiaoWang, and Ning Yu, "A Credible Routing Based on a Novel Trust Mechanism in Ad Hoc Networks", Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, Volume 2013, March 2013, Pages 1-13

[16] C. Atheeq and M. Munir Ahamed Rabbani, "Secure Data Transmission in Integrated Internet MANETs Based on Effective Trusted Knowledge Algorithm", Indian Journal of Science and Technology, Volume 9, Issue 47, December 2016, Pages 1-7

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

[18] Amit Kumar Gupta , Naveen Kumar Gupta, Rakesh Kumar, "An efficient secure gateway selections and authentication scheme in MANET", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 2, February 2014, Pages 11-18

[19] 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, 2016, Pages 680—682

[20] Shigeru Kashihara, Takuma Hayashi, Yuzo Taenaka, Takeshi Okuda, and Suguru Yamaguchi," Data Delivery Method Based on Neighbor Nodes' Information in a Mobile Ad Hoc Network", Hindawi Publishing Corporation, The Scientific World Journal, Volume 2014, February 2014, Pages 1-12

[21] Zhexiong Wei, Helen Tang, F. Richard Yu, Maoyu Wang, Peter Mason, "Security Enhancements for Mobile Ad Hoc Networks with Trust Management Using Uncertain Reasoning", IEEE Transactions on Vehicular Technology, Volume 63, Issue 9, 2014, Pages 4647 – 4658

[22] Keyvan RahimiZadeh and Peyman Kabiri, "Trust-based routing method using a mobility-based clustering approach in mobile ad hoc networks", Security and Communication Networks, Willey Publications, Volume7, Issue11, November2014, Pages 1746–1763

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[23] Suyash Bhardwaj, Swati Aggarwal and Shikha Goel, "A Novel Technique of Securing Mobile Ad hoc Networks using Shared Trust Model", International Journal of Information and Computation Technology, Volume 3, Issue 9, Pages 909-916, 2013