Received: August 15, 2018

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

ID Based Multicast Secret-Key Management Scheme (SKMS) in MANETs

Medi Sandhya Rani[1]* **Redamalla Rekha[2]** **Kota Venkata Naga Sunitha[3]**

[1]*Bhoj Reddy Engineering College for Women, Jawaharlal Nehru Technological University, India*
[2]*University College of Engineering & Technology Mahatma Gandhi University, Nalgonda, Telangana, India*
[3] *BV Raju Institute of Technology, Jawaharlal Nehru Technological University, Hyderabad, Telangana, India*
* Corresponding author's Email: sandhya_medi@yahoo.com

Abstract: Mobile Ad-Hoc Network (MANET) is a self-configuring network of mobile nodes associated by wireless channel. The nodes are free to move arbitrarily anywhere in the network. Hence, lack of fixed infrastructure and host flexibility, providing secure communications is a big challenge. Because a temporary device recurrently joins or leaves a network, the authentication and security techniques should be equipped for the unorganised users. In cryptography it is ineffective if its key management is fragile. Key management is one of the vital aspects for security. Thus, the network's wireless topology may be disorganised and may adjust rapidly, the efficient-route is recognised using Multi-path AODV Routing-Protocol. The ID based SKMS (Secret Key Management Scheme) method is implemented in secured environment by using Rivest-Shamir Adleman (RSA) method and the Node ID based Secure Key Management Scheme (SKMS) mechanism for securing data packets from source to destination. The ID based is used to share secret key of an individual users. A multi-cast (AODV) group receiver or group-source-key pair is conserved and recognised by an ID. Each clustering group has its own exclusive identity number. "ID based Multicast SKMS using RSA" method increase in packet delivery ratio (6%) along with the decrease in drop (5%), delay (8%), and energy consumption (6%) in secured ad-hoc environment.

Keywords: Ad-hoc on-demand distance vector routing, Mobile ad-hoc network, Rivest-Shamir Adleman, Secure communication, Secret key management scheme.

1. Introduction

Key administration is the fundamental piece of any protected/secured communication. Most cryptosystems depend on some basic secure, robust, and productive key administration system. Secure system interchanges regularly include a key distribution method between communication parties, in which the key might be transmitted through unreliable channels [1]. The Group key establishment incorporates making and dispersing a typical secret for all the gathering individuals. However, key administration for a vast and dynamic gathering is a troublesome issue in light of adaptability and security [2]. The procedure encourages inter cluster communication by circulating private key shares to the node, which is performed by the concentrated key manager. By sealing the information utilizing private key share, inter group correspondence is refined [3]. A dynamic multicast height adjusted gathering key assertion (DMHBGKA) that permits a client in a multicast gathering to productively and progressively make the group key and safely convey multicast information from a multicast source to the next multicast source users in wireless ad hoc networks [4]. A dynamic multicast routing and routing optimization criteria have been described by comparing and analysing the advantages and disadvantages of several non-rearranged dynamic multicast algorithms [5].

Another node and gathering leader confirms each other commonly before joining the network. Thus, secure routing protocol permits both conveying parties and also intermediate nodes to authenticate different nodes keeps up message integrity [6]. The group leader is dependable to

create and disseminate ids and public private key combine to nodes. Open key cryptography (PKC) any of the two individuals from gathering can share a session key safely to communicate [7]. A multi-hop situation happens for correspondence in MANETs; where there might be at least one malicious node in the middle of source and goal. A routing protocol is said to be secure that identifies the inconvenient impacts of malicious nodes (in the way from source to goal) [8]. A group key-dispersion is from traditional plan, its secret shadows are not passed on from group controller, but rather from each sub-group focus node's private key signature, by getting together all these n secret shadows [9]. The secret keys are produced utilizing one-way function chain. In addition to secure key administration, the issue of versatility is additionally handled. A secret key administration technique brings about low overhead and delay and significantly builds the throughput [10].

To conquer this problem, "ID based Multicast SKMS using RSA" method is implemented for increasing the parameters such as, Through-put, Routing Overhead, Packet Delivery ratio, drop, delay and energy Consumption. In this work, the essential modification in AODV is used for the determination of accomplishing the performance in the secured-way and find well-organized routing-path using AODV-optimization to the favoured destination. The Rivest-Shamir Adleman (RSA) is used for security and to communicate with additional node in the secured-way. Thus, "ID based Multicast SKMS using RSA" method gives better results in packet delivery ratio, drop, and Delay energy consumption in secured-environment associated with End-2-End link reliable Multipath Routing (E2E-LRMR), (Optimal Key Management for Secure Data Transmission) OKMSDT.

The rest of the paper is organized as follows: Section 2, reports on related work. Section 3, presents a review on "ID based Multi-cast SKMS using RSA" Methodology in MANETs. Section 4, demonstrated the simulation parameters and Experimental results of the "ID based Multicast SKMS using RSA" and Section 5 designates the conclusion of this research work.

2. Related work

V. Bhuvaneswari, and M. Chandrasekaran [11] has proposed cluster head based gathering key-administration for malicious wireless networks utilizing trust-measurements. The gathering key produces the keys based on the nodes ability inside two hops. The execution isn't extensively better in larger networks. R. Bhuvaneswari and R. Ramachandran [12] has implemented Denial of Service (DoS) attack using invented nodes and key administration utilizing OLSR Protocol. Provide proper determination of highest common trust degree course and rotes the packets. Predetermined number of nodes are introduced in the systems.

In [13] K.K. Waraich, and B. Singh, AODV with presence and absence of false/malignant node is examined. AODV does not demonstrate routing overheads on data information, which is level directing convention and loop free. But it doesn't say preventing the attacks in the networks. P. Periyasamy, and E. Karthikeyan [14] has implemented End-to-end Link reliable energy efficient multipath routing (E2E-LREEMR) for MANETs. AOMDV are inclined to link failure and route disturbances because of the arrangement of numerous routes between any source and goal. Parameters contrasted are less and diverse situations of detecting zone. E2E-LREEMR protocol finds multiple link reliable path for data transmission in networks without any secured way.

M. Anupama and B. Sathyanarayana [15] designed an Optimal-Key-Management technique for Secure Data-transmission (OKMSDT) in MANETs. The authenticating and key distribution is used to monitor symmetric-key among gatherings. The signal strength dispersion the link-stability metric to a path rating metric appears capable in ad-hoc networks.

M. Sandhya Rani, R. Rekha, and K.V.N. Sunitha [16] presented a novel Scalable Group Key Management Protocol for MANETs. A member connects to the group or evicts from the group is crucial for multi-cast security. The broad-casting the data to the different nodes should be done further to diminish the number of messages send over the large-scale networks.

The above illustrated papers have some limitations yet to be performed well in ad-hoc networks such as key management, security, and network size. Thus, "ID based SKMS (Secret Key Management Scheme) performs effectively based on node ID key management by transmitting the data to two receivers at a time in the secured ad-hoc networks.

3. ID based multicast SKMS using RSA

The security is the major concern in any kind of wireless-networks. In this paper, ID based Multicast SKMS using RSA method is presented which will deliver the very high secured communication in sensor network via. Multicast. Also the network will

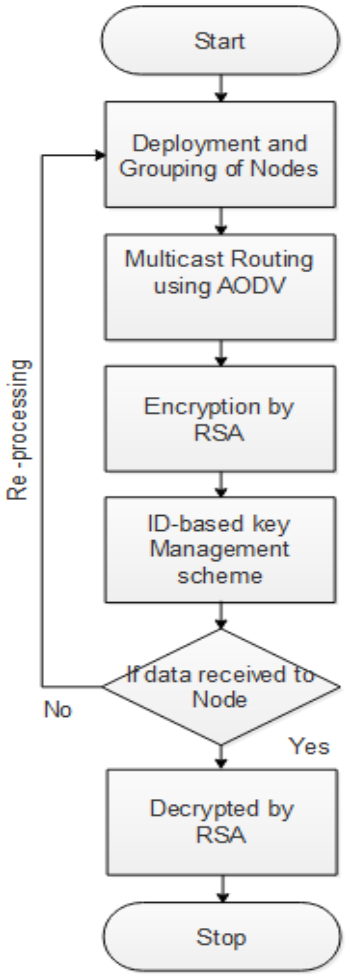

Figure.1 Block diagram of overall methodology

secure the information and afford efficient data to the destination.

This system involves of eight major steps:

1) Mobile node deployment
2) Grouping of ad-hoc network
3) cluster head selection based on node id
4) Multi-cast router estimation using AODV
5) Data received to cluster head
6) Encryption by RSA
7) ID based Secret-group-key management
8) Successfully receiving the data and decryption process.

The Overall block diagram of the "ID based Multicast SKMS using RSA" system through step by step process is shown in Fig.1

ID based secret key management (ID - SKMS) have four-phases such as operator identity i.e. ID and generating the corresponding private keys.

i) I = Initialization Phase – Users calculate long term public and private keys using RSA algorithm.

ii) R = Registration Phase – Each user sends its own identification number ID to the key registration centre to obtain the signature.

iii) V = Verification Phase – Multicast users communicate in the group by verifying their public keys.

iv) K = Key Exchange Phase - Source multicast-key (SMK) and receiver multicast-key (RMK) pair is distributed to all users.

3.1 Grouping/clustering of nodes

The clustering algorithm constrains the correspondence in a neighbourhood area and transmits the sending nodes (gateway-nodes). A gathering of nodes frame a cluster and the nearby collaborations between group individuals are controlled through a CH. Ak number of clusters are generated from the n number of ad-hoc nodes; the fitness-function is minimized by the algorithm. The fitness-function which is used in this clustering is squared error function and it is given in Eq. (1).

$$F = \sum_{j=1}^{k} \sum_{i=1}^{n} \left\| x_i - c_j \right\|^2 \quad (1)$$

Where, the centre of j^{th} cluster is represented asc_j, data point of i^{th}sample is denoted as x_i and the distance from the each ad-hoc nodes to the cluster centre is represent//ted by$\left\| x_i - c_j \right\|^2$.

There are four main steps performed in K-means clustering algorithm.

Step1: In the first place, the k groups are produced from the specially appointed nodes by taking the k number of centroids indiscriminately places.

Step 2: The Euclidean distance from each ad-hoc nodes to the centroid is figured for influencing the m to beginning groups. Consider every node is nearest to the centroid. The Euclidean distance from one node to another node is given in Eq. (2).

$$Eucildean\ distance = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \quad (2)$$

Where, the co-ordinates of x and y axis is represented as x_2, x_1 and y_2, y_1 respectively.

Step 3: The position of every node is checked and verified from the previous position and the each-cluster locations are again calculated in a network.

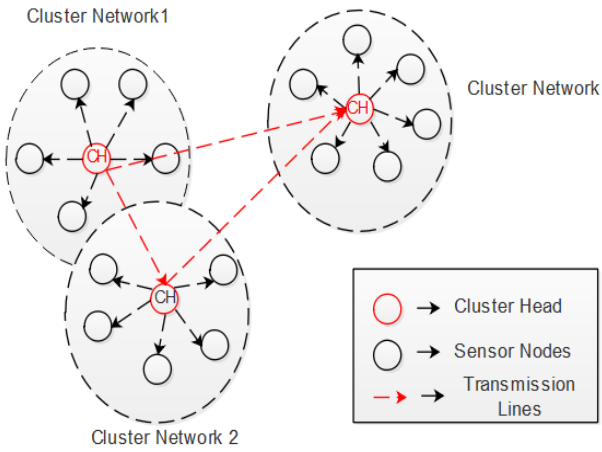

Figure.2 Basic clustering method of ad-hoc networks

Step 4: If the position of centroid becomes changed, then again go to step 2 for obtaining the effective clusters else the clustering process to end. Finally, the centroid which is selected from the K-means clustering as an CH for a cluster-groups. Fig. 2, explains basic Clustering.

3.2 AODV-routing protocol (Multicast routing)

The routing protocol is intended for use by mobile nodes in remote systems. The AODV is intended to diminish the spread of overhead and control activity. The AODV routing protocol deals with two functions such as Route-Discovery and Route-Maintenance by analysing multi-cast for data transmission. The finding of the fresh route is categorical by Route-Discovery function and the discovery of link-breaks and healing of an existing route is decided by Route-Maintenance function. The reactive protocol does not uphold permanent route table. AODV is rapidly able to examine the changes in network topology.

AODV routing protocol establishes uni-cast, broad-cast and multi-cast communications. The Route-discovery with AODV is virtuously On-demand and monitors a route-request (RREQ)/route-reply (RREP) discovery cycle. When a node requires a route to a destination, it broadcast a RREQ. The route-discovery with AODV is on-demand and happens when a node already has a recorded-route. The multi-cast algorithm uses the same RREQ/RREP messages. In AODV protocol each node occasionally sends HELLO messages to the neighbour node to know that there is any node-connectivity. Fig. 3, explains the block diagram data transfer of AODV routing-protocols.

3.3 RSA Algorithm

RSA cryptography is the popular cryptography system, which is used for security purpose in the wide range of networks. The security border should be raised in the RSA. The most difficult part of RSA cryptography is public and private key-generation. The Prime numbers p and q are created by employing the RSA cryptography. The modulus 'n' is subtracted by duplicating P and Q. The no. is exploited by both the general population such as private and public keys between the operators. The one user at the end sends Cipher text by encrypting with public key. Another end decryption takes place. ID based Key generation process such as encryption, decryption public key, private key, secret key, plain text and cipher text is explained in the following Eq. (3), (4), (5), (6), (7), and (8).

Key Generation	
Select $p, q \quad p, q \; both \; are \; prime \; , p \neq q$	
Calculate $n = pxq$	
Calculate $\emptyset(n) = (p-1) * (q-1)$	(3)
Select integer e	
$gcd(\emptyset\,(n), e) = 1; 1 < e < \emptyset\,(n)$	(4)
Calculated	
Public key $KU = \{e, n\}$	(5)
Private key $KR = \{d, n\}$	(6)
Secret Key User 1 and User 2	
Encryption	
Plain text $M < n$	
Cipher text $C = M^e \; (mod \; n)$	(7)
Decryption	
Cipher text C	
Plain text $M = C^d (mod \; n)$	(8)

The encryption operations in the RSA cryptosystem is exponentiation to the e^{th} power modulo n: in Eq. (9).

$$C = ENCRYPT\,(M) = m^e mod\; n \tag{9}$$

The input M is the message and C is the resulting cipher text. This construction makes it possible to encrypt a message of any length with only one exponentiation.

The decryption operation to the d^{th} power modulo n: in Eq. (10).

$$M = DECRYPT\,(C) = c^d \; mod \;\; n \tag{10}$$

The input C is the cipher text and output M is the resulting plain text.

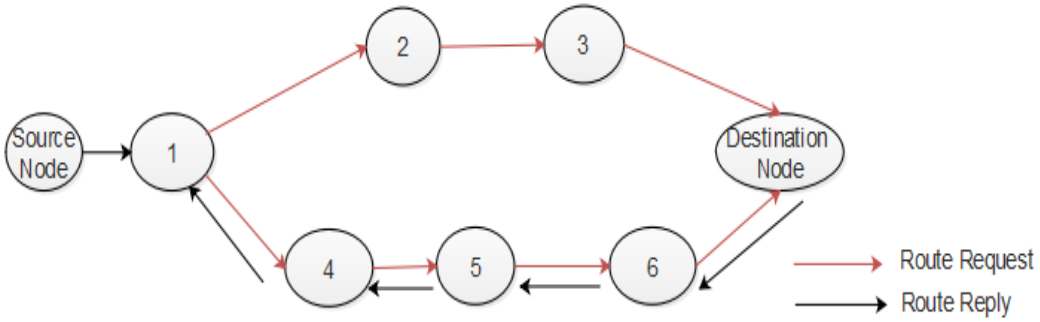

Figure.3 Data transfer of AODV routing protocols

3.4 ID based Secret Key Management Technique

A multi-cast group receiver or group-source-key pair is conserved and recognised by group ID. Each clustering group has its own exclusive identity number (For., One clustered group have 192.92.92.10 and another group have 192.92.92.11 respectively. The ad-hoc nodes with 192.92.92.10 (group ID) have different node ID such as 192.92.92.10.1, 192.92.92.10.2, 192.92.92.10.3.

Group key management plays a vital role in group communication. A common group key is required for individual users in the group for secure multicast communication. Group key has to be updated frequently, when a member joins and leaves in order to provide forward and backward secrecy. The ID-based key SKMS technique is explained as follows:

i. Each user is assigned with a unique identification number (ID). The individual user selects two prime numbers randomly by computing their private and public key pair.
ii. The server authenticates the user with its public key value and ID who needs to join the multicast group and also announces public key value, which is used for communication in the network.
iii. Each multicast group has a source multicast-key (SMK) and a receiver-multicast key (RMK) pair, which is actually proficient by security and authentication-server using group id and multicast user's ID.
iv. The encryption of message is done by multicast-group-sender (MGS) with SMK and that is decrypted by RMK. The MGS signs the message using its own-private-key to provide authentication.
v. SMK and RMK are encrypted with RSA encryption mechanism by authentication server and distributed to the group members. The group members except source decrypt RMK with their private keys.
vi. After decrypting RMK, cluster members in the multicast network can decrypt the secret message P from the received cipher text.

Fig. 4 explains Multi-cast ID based Key Encryption Mechanism. The run-time overview comprises many individuals such as private-key-generator, multicast-group-sender, multicast-group-receiver, security-authentication-server, and various nodes in the network. Two users are considered for security analysis. Secure channel is recognised between two users through private key generator. Network controller coordinate secure communication. The secure channel is recognised between two users finished private-key-generator.

4. Experimental results

The "ID based Multicast SKMS using RSA" method is implemented in NS2 simulation tool. The simulations parameters are shown in Table 1. The simulation starts and end time is denoted as 0.0001-50.0000 respectively by varying number of static nodes as 20, 40, 60, 80 and 100. The MAC Type is 802_11 with Omni Antenna model. The Proposed algorithm provides security to the messages, reduces the overhead in multicast routing and key management. Thus this scheme gives better performance compared with the existing methods. The Performance metrics are given below;

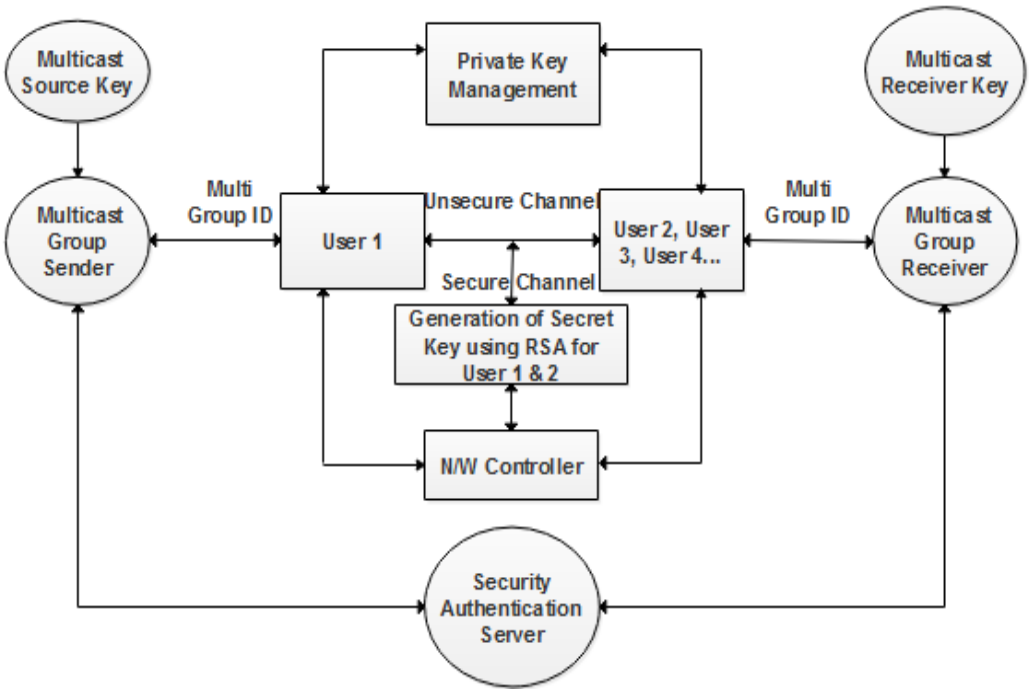

Figure.4 Block diagram of multicast ID-based key encryption mechanism

Table 1. Simulation Parameters

Multicast Routing	AODV
Security algorithm	RSA
Key Management	ID-SKMS
Simulator used	NS2
Simulation start time	0.0000000001
Simulation End time	50.000000000
Number of mobile nodes	20, 40, 60, 80 and 100
Antenna Model	Omni Antenna
Minimum speed	28 ms
Network Interface types	Wireless
MAC Type	MAC/802_11
Initial Transmit Power	0.660
Initial Receive Power	0.395

4.1 Packet delivery ratio (PDR)

Based on a total amount of packets established in a ratio by a total number of destination packet sent by the source node, which is given in Eq. (11)

$$DelRatio = \frac{(no.\ of\ packets\ send - packets\ lost)}{no.of\ packets\ send} \times 100 \quad (11)$$

4.2 Energy consumption

The huge number of nodes is equivalent to the huge amount of received energy consumption. A node drops a specific amount of energy for every packet transmission and received, which is given in Eq. (12)

$$Energy = \frac{amount\ of\ energy\ for\ every\ packets}{total\ simulation\ time} \quad (12)$$

4.3 Delay

Difference between Sending time of packets and receiving time of packets is known as delay, which is given in Eq. (13).

$$Delay = Time\ spend\ on\ Hop1 + time\ spend\ on\ Hop2 + \cdots . . + time\ spend\ on\ Hop\ n \quad (13)$$

4.4 Packet drop/Packet loss

Total amount of packets sent and packet established is known as the packet drop/packet loss, which is given in Eq. (14).

$$Drop = \frac{(Total\ no.of\ packets\ send - Packet\ received)}{Total\ number\ of\ simulation} \quad (14)$$

Table 2 shows the delay by changing different nodes such as 20, 40, 60, 80, and 100 of fixed Nodes. Hence, ID-SKMS Methodology shows better results than those of E2E-LRMR [14] and OKMSDT [15].

The Evaluation of Nodes vs. delay between ID-SKMS and existing method is plotted in Fig. 5 the delay value is decreased in ID-SKMS method, when compared with the E2E-LRMR [14] and OKMSDT [15] method with different 20, 40, 60 80 and 100 Nodes.

Table 2. Delay by varying number of nodes

QoS	Delay				
Nodes	**20**	**40**	**60**	**80**	**10**
E2E-LRMR [14]	1.986463	3.152960	3.713986	4.964285	3.964285
OKMSDT [15]	1.656479	3.106972	3.532987	4.324796	4.523796
ID-SKMS	0.179187	1.359974	1.801087	3.084184	1.683421

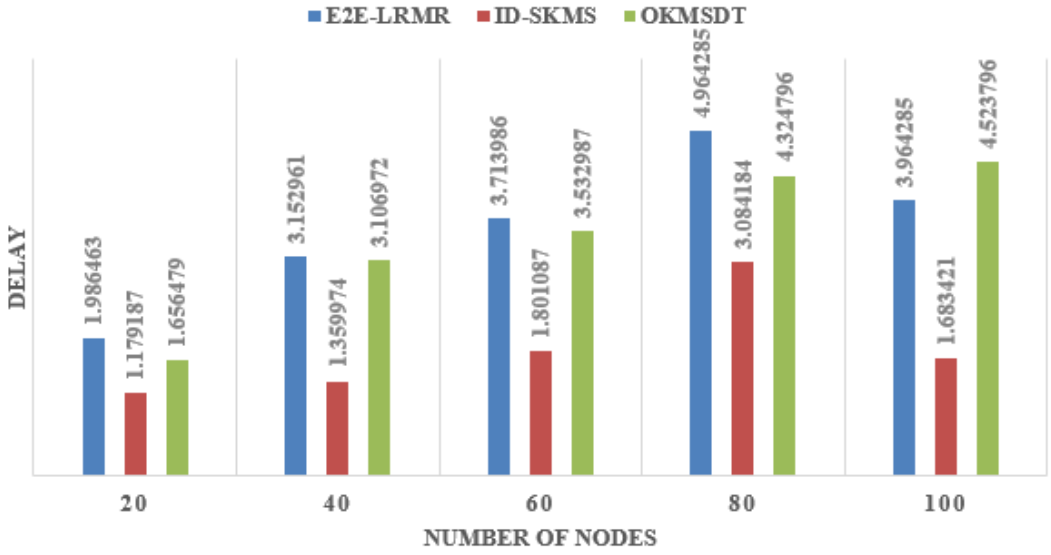

Figure.5 Node vs. delay

Table 3. Packet Delivery Ratio by varying number of nodes

QoS	Packet Delivery Ratio				
Nodes	**20**	**40**	**60**	**80**	**100**
E2E-LRMR [14]	450.400	147.050	135.550	157.735	70.0600
OKMSDT [15]	632.7300	107.0500	235.357	216.37560	100.6700
ID-SKMS	782.750	289.950	265.357	237.387	197.750

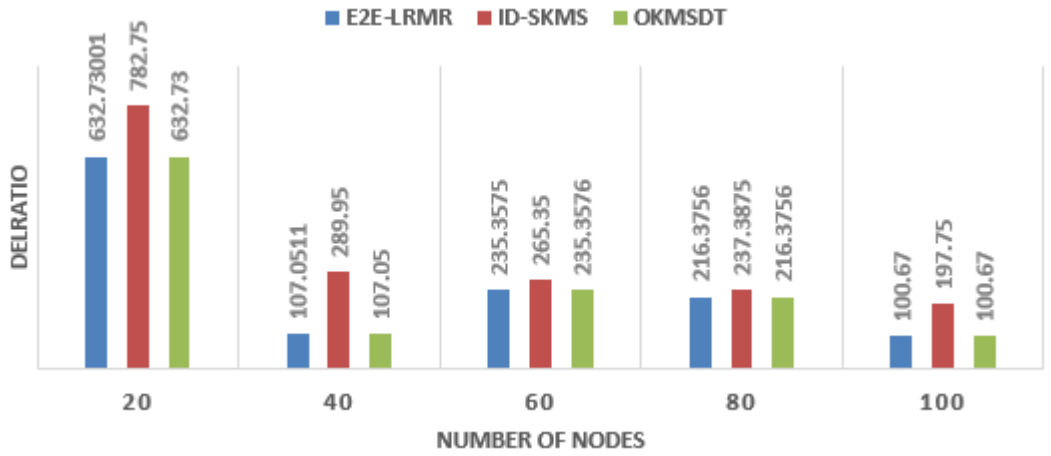

Figure.6 Node vs. Packet Delivery Ratio

The Assessment of Nodes vs. Packet Delivery Ratio between ID-SKMS and existing methods is plotted in Fig. 6. The Delivery Ratio value is increased in ID-SKMS method, when compared with the E2E-LRMR [14] and OKMSDT [15] method with different 20, 40, 60 80 and 100 Nodes. Table 3, shows the corresponding data values. Hence, ID-SKMS Methodology shows better results than those of E2E-LRMR and OKMSDT.

Table 4. Energy consumption by varying number of nodes

QoS	Energy consumption				
Nodes	**20**	**40**	**60**	**80**	**100**
E2E-LRMR [14]	24.753734	22.941715	22.616316	22.727089	23.76053
OKMSDT [15]	24.241127	22.431217	22.217316	22.176739	22.56789
ID-SKMS	24.062211	22.011249	21.725402	21.974539	22.23823

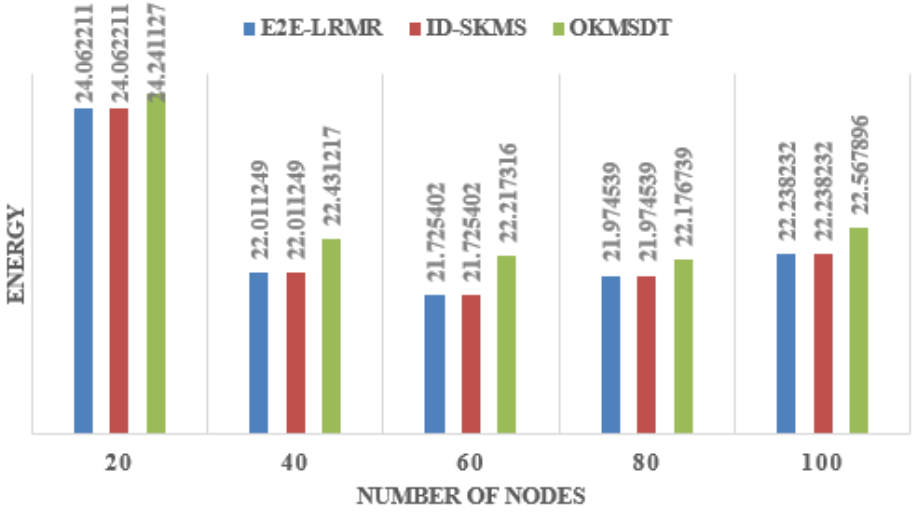

Figure.7 Node vs. energy

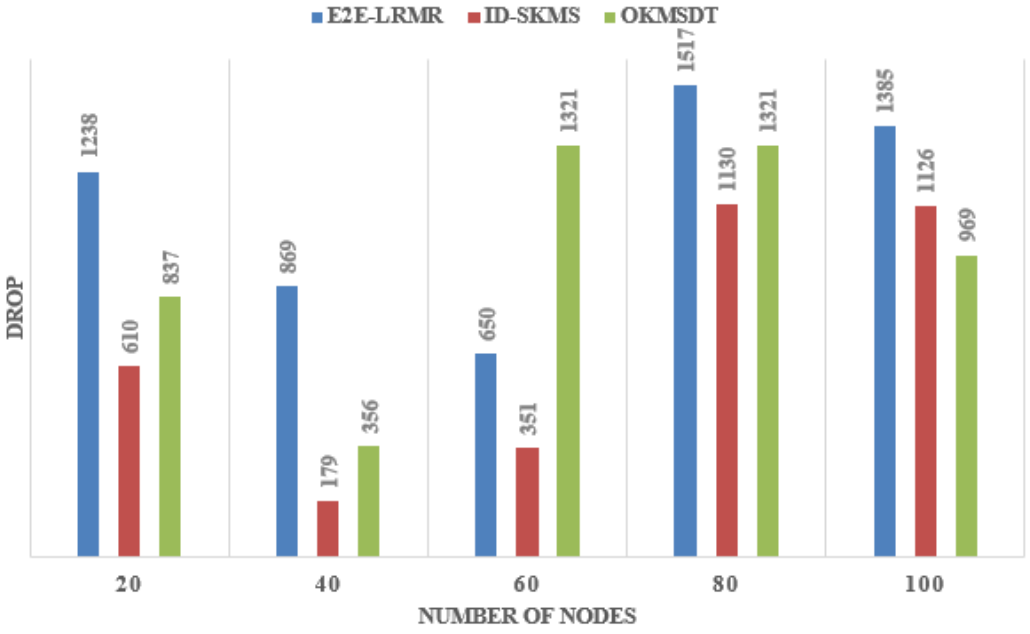

Figure.8 Node vs. Drop

Table 4, shows the Energy of variable number of nodes such as 20, 40, 60, 80, and 100 of fixed Nodes. Hence, ID-SKMS Methodology shows better results than those of E2E-LRMR [14] and OKMSDT [15].

The Comparison of Nodes vs. Energy between ID-SKMS and existing methods is plotted in Fig. 7. The Energy value is decreased in ID-SKMS method, when associated with the E2E-LRMR and OKMSDT method with different 20, 40, 60 80 and 100 Nodes.

Table 5 shows the Drop of variable different nodes such as 20, 40, 60, 80, and 100 of fixed Nodes. Hence, ID-SKMS Methodology shows better results than that of E2E-LRMR [14] and OKMSDT [15].

The Comparison of Nodes vs. Drop between ID-SKMS and existing method is plotted in Fig. 8. The Drop is decreased in ID-SKMS method, when compared with the E2E-LRMR and OKMSDT method with different 20, 40, 60 80 and 100 Nodes.

Table.5 Drop by varying number of nodes

QoS	Drop				
Nodes	**20**	**40**	**60**	**80**	**100**
E2E-LRMR [14]	1238	869	650	1517	1385
OKMSDT [15]	837	356	1321	1321	969
ID-SKMS	610	176	351	1130	1126

5. Conclusion

"ID based Multicast SKMS using RSA" method used for multicasting the data packets in the network by using AODV routing-protocol. It provides efficient key management based on node id and RSA method. Along with the security, this scheme delivers efficient results in transporting data-packets from source to destination. From obtained results, we undertake that the presented method has stretched the best-routing and better Through-put, Routing-Overhead, Packet-Delivery-ratio, drop, delay and energy-consumption among existing methods such as E2E-LRMR and OKMSDT with varying number of nodes. Hence, Delay decreases 8% in ID-SKMS than E2E-LRMR and OKMSDT methodology. DelRatio increases 6% in ID-SKMS than E2E-LRMR and OKMSDT methodology. Drop decreases 5% in ID-SKMS than E2E-LRMR and OKMSDT methodology. Energy decreases 6% in ID-SKMS than E2E-LRMR and OKMSDT methodology.

As a Future Scope, hybrid key management techniques can be used for improving security in the Mobile ad-hoc network by varying network topology and rate.

References

[1] A.T. Zamani and S. Zubair, "Secure and efficient key management scheme in MANETs", *IOSR Journal of Computer Engineering*, Vol.16, No.2, pp.146-158, 2014.

[2] N.V.B. Jayaram and R. Balasubramanian, "Efficient Group Key Management Protocol forRegion Based MANETs", *International Journal of Engineering and Technology*, Vol.3, No.1, pp.68, 2011.

[3] V. Rajamanickam and D. Veerappan, "Inter cluster communication and rekeying technique for multicast security in mobile ad hoc networks", *IET Information Security*, Vol.8, No.4, pp.234-239, 2014.

[4] H.Y. Lin and T.C. Chiang, "Efficient key agreements in dynamic multicast height balanced tree for secure multicast communications in Ad Hoc networks", *EURASIP Journal on Wireless Communications and Networking*, pp.382701, 2011.

[5] Y.F. Dai, N.F. Li, and Z. Guo, "Comparison and analysis of several non-rearranged dynamic multicast routing algorithms", In: *Proc. of International Conf. on Intelligent Information, Control, and Communication Technology for Agricultural Engineering*, Vol.8762, pp.87620E, 2013.

[6] K.K. Chauhan and A.K.S Sanger, "Securing mobile Ad hoc networks: key management and routing", *arXiv preprint arXiv:*1205.2432, 2012

[7] V. Sravani and M.S.B. Rao, "An Efficient Mechanism for Securing Mobile Ad Hoc Networks Using Public Key Cryptography (PKC)", *IJMETMR*, Vol.2, No.12, pp.1675-1683, 2015.

[8] C.M. Gulzar, K.V. Subba, and R. Kashyap, "Securing Mobile Ad hoc Networks: Key Management and Routing", *International Journal of Core Engineering & Management*, Vol.2, No.1, 2015.

[9] X. Hai-tao, "A Cluster-Based Key Management Scheme for MANET", In: *Proc. of the 3rd International Conf. on Intelligent Systems and Applications*, 2011.

[10] R. Vennila and V. Duraisamy, "Multi-level group key management technique for multicast security in Manet", *J. Theor. Appl. Inform. Tech.*, Vol.49, No.2, pp.472-80, 2013.

[11] V. Bhuvaneswari and M. Chandrasekaran, "Cluster head based Group Key Management for Malicious Wireless Networks using Trust Metrics", *Journal of Theoretical and Applied Information Technology*, Vol.68, No.1, pp.1-9, 2014.

[12] R. Bhuvaneswari and R. Ramachandran, "OLSR Protocol Denial of Service Attack Solution Using Fictitious Nodes and Key Management", *International Journal of Engineering and Technology*, Vol.9 No.3, pp.2068-2075, 2017.

[13] K.K. Waraich and B. Singh, "Performance Analysis of AODV Routing Protocol with and without Malicious Attack in Mobile Adhoc Networks", *International Journal of Advanced Science and Technology*, Vol.82, pp.63-70, 2013

[14] P. Periyasamy and E. Karthikeyan, "End-to-End Link Reliable Energy Efficient Multipath Routing for Mobile Ad Hoc Networks", *Wireless Personal Communications*, Vol.92, No.3, pp.825-841, 2017.
[15] M. Anupama and B. Sathyanarayana, "An Optimal Key Management Technique for Secure Data Transmission in MANET", *Journal of Theoretical& Applied Information Technology*, Vol.95, No.16, pp.3783-3795, 2017.
[16] M. Sandhya Rani, R. Rekha, and K.V.N. Sunitha, "Simulation of A Novel Scalable Group Key Management Protocol for Mobile Adhoc Networks", *International Journal of Computer Science and Engineering*, Vol.8, No.3, pp.70-75, 2016.