Modified Device Key Generation Algorithm and A* Algorithm to Optimize the Security Measures Based on Trust Value in Device-to-Device Communications

Gayathri VM (vmg188@gmail.com)
SRM Institute of Science and Technology
Supraja p
SRM Institute of Science and Technology
Razia Sulthana A
BITS: Birla Institute of Technology and Science
Mukunthan P
Sri Indu College of Engineering & Technology

Research Article

Keywords: Mobile Ad-hoc Networks, Quality of Service, Trust value, Agent node, MDKGA

Posted Date: May 27th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-502831/v1

Modified Device Key Generation Algorithm and A* algorithm to optimize the Security measures based on Trust value in Device-to-Device Communications

[1]Gayathri V M, [2,*]Supraja P, [3]Razia Sulthana A, [4]Mukunthan P

[1,2]Assistant Professor, Department of Information and Technology
SRM Institute of Science and Technology, Kattankulathur, Tamilnadu, INDIA.
[3]Assistant Professor, Department of Computer Science, BITS Pilani, Dubai Campus, UAE
[2]Professor, Electronics and Communication Engineering, Sri Indu College of Engineering and Technology, Hyderabad.
SRM Institute of Science and Technology, Kattankulathur, Tamilnadu, 603203, INDIA.
vmg188@gmail.com[1], p.supraja18@gmail.com[2], razia@dubai.bits-pilani.ac.in[3], mukunthance@email.com[4]

Corresponding Author: p.supraja18@gmail.com

Abstract:

Security plays a vital role in communication networks. Since the nodes are mobile in Mobile Ad-hoc Networks (MANET), they are vulnerable to different types of attacks. Because of its mobility nature any node can enter the network at any time based on the coverage of the network. No centralized mechanism is found to verify or authenticate the nodes that are arriving/leaving the network. An algorithm is proposed for secure communication between source and destination based on the QoS parameters is called Modified Device Key Generation Algorithm (MDKGA). This algorithm elects an agent node based on the QoS parameters. Agent node is responsible for secure key generation and distribution of keys among the nodes. The neighboring node selection is based on trust value which acts as a heuristic function to select the node using A* algorithm.Various performance metrics are also analyzed. Comparison study has been carried out between the protocols of MANET.

Keywords:

Mobile Ad-hoc Networks, Quality of Service, Trust value, Agent node, MDKGA

Introduction:

Mobile Ad-hoc Networks employs a major part in wireless communication. This acts as a base for Vehicular communication. Since there are many advantageous features with MANET, it lacks majorly on synchronization and security. Since the nodes are mobile, there is a high level of chance that attacker node joins the network and slows down or corrupt the entire communication. Due to the lack of centralized authority to track the in and out nodes of the network, the MANET is highly prone to the network attacks. It is mandatory to provide some authentication system to identify the characteristics of the node. Based on the characteristics the node will be identified as attacker node or not. In addition, encapsulating the data is much more required.

A Key based communication within the network and measuring metrics for analyzing the performance of the network are proposed. In key based communication, an algorithm is designed for generating and distributing the keys. QoS metrics such as delay factor, reliability ratio and energy utilization/efficiency are measured and analyzed for various simulation strategies. Different simulation scenarios are considered, compared and analyzed for efficient transmissions. The proposed MDKGA prevents the attacker nodes to join the network without compromising the performance of the network.

AODV, DSR protocols and NS2 simulator are used for the implementation. Trust value is calculated for each node in the network and based on the calculated trust values of the node, intruder nodes are identified. Trust value is calculated based on node's behavior over n number of simulations.

Background Work:

[1] A detailed study on various routing methods of MANET, various trust models, trust dynamics, various algorithms for predictions, the effects of trust dynamics and impact of trust model developed were discussed in detail. [2] A survey about the mobility models were described. Initially the authors discussed about synthetic mobility model, explained about mobile traces which were collected and analyzed, explained about performance degradation because of mobility issues and then finally explained about the open challenges and research area for the researchers to process.

[3] A scheme against chosen Cipher Text Attack (CCA) was proposed to enhance the security with less communication overhead to apply to massive scale MANETs and to increase performance metric with less cost overhead.

[4] A method which used Markov-chain model for analysis, evaluation of the OCSP-based model for certificates within the hybrid MANETs and the outcomes of absorbing Markov fashions are verified via the widespread simulations of the ADOPT and PS-ADOPT protocols in the OMNET++ simulator. [5] proposed Flooding Factor Framework for Trust Management (F3TM) in MANETs to be aware of attacker nodes based on the trust values calculated. Route Discovery Algorithm is to identify the efficient route from source to destination node. Experimental Grey Wolf algorithm is used for validation and authentication of network nodes. Four research areas of the Ad-hoc networks such as Mobile Ad-hoc networks, Mesh networks, Vehicular networks and [6] Sensor networks were discussed in detail and people centric direction towards the research in communications and computing is explained.

[7] proposed a protocol for both static and mobile network nodes which do the data delivery in an efficient manner with respect to the scalability of the nodes in the networks. That is, when the number of nodes in the networks increases the data delivery should not deviate from where it stands [8] proposed a novel technique, before initiating the data transfer between the nodes from source to destination the nodes which enters the network are validated and only if it is authenticated it can join in the network communication. This procedure carried out during Route Discovery phase.

[9] A protocol was proposed to identify the nodes which are unstable due to the signal fading interference from other alerts, or the intervention of intruder node. In MANET, the nodes are mobile and it can communicate with other nodes in the network Wi-Fi gadgets. For nodes that are not in the communication range transfer the packets through the router node. A MANET is characterized by way of its dynamic topological adjustments, confined conversation bandwidth, and restricted battery power of its nodes.

A unique certificate authorization distribution method to transfer data packets between source node and destination node based on the calculated trust value was proposed [10]. Initially the trust value is computed by the adjacent node and the if the trust value is below the threshold_value, the respective node's details will be distributed among other nodes in the network. The misbehaving nodes were removed from the network. A method was proposed where the keys of all the local nodes will be cached to reduce the communication overhead for the future communication [11].

[12] proposed a trust based public key encryption technique for secure communication. A Composite Trust-based Public Key Management (CTPKM) method was proposed to maximize

performance parameters of the network without compromising to give the protection to the network. Each and every node in the network calculates the trust value of its neighbor nodes whether to trust the nodes to transfer the data packets. The CTPKM minimizes the risk, increased reliability and less communication overhead. [13-15] proposed approaches to detect black hole nodes in the network. [16] proposed Modified AODV (AOMDV) protocol which uses Homomorphic encryption scheme to identify and eradicate the black hole nodes so that the it ensures to provide the reliable and secure data transmission in MANETs.

[17] designed an infinitely- repeated game and cooperation to detect malicious node without compromising the network performances. [18] proposed an approach to detect different types of security attacks and various optimization algorithms are discussed to optimize the routing process. [19] discussed about the effect of network parameters on Packet Delivery Ratio and Energy Consumption. [20] Image security for vehicle-based information in VANET.

[21] proposed a Hybrid Key Management Scheme for securing Multipath routing method for data transmission using Diffie-Hellman method and Elliptic Curve Cryptography. [22] discussed about various kinds of MANET attacks and compared the effects of attacks based on the evaluation parameters. In addition to this, the authors also giving an insight of the characteristics of MANET and performance evaluation with the help of performance metrics.

[23] proposed a novel approach for detecting DDOS attack based on bit rate, PDR and delay and also to classify the attacks either Beningn and Malicious traffic using Support Vector Machine (SVM). NS2 simulator is used for collecting the dataset and LIBSVM is used for analysis. [24] Simple dual-key encryption method based on fully homomorphic encryption and double decryption method on SDN controlled MANET. [25] A novel proactive routing strategy is proposed to secure the networks to avoid isolation attack by verifying the nodes in handshake method before the node starts with Multi Point Relay. [26] SDN controlled MANET using DISNEY Routing protocol for better performance of networks based on various performance metrics such as Packet Delivery Ratio, transmission delay, throughput and data transmission rate.

A learning method is applied to identify the nodes which enters the network. This learning method is based on the individual nodes' performance in the network for n number of simulations. A secure transmission involves the concepts of symmetric key, public key and certificate-based scheme. To communicate via symmetric key, same key for both encryption and decryption are needed. Processing cost will be low but security level is also low. In case of public key cryptography, it needs two kinds of keys namely public key and private key. Figure 1 shows the General Certificate based communication. Certificate Issue Authority (CIA) is a Certificate issue authority/ Agency /node to issue keys to source S and destination D. Other nodes are intermediate nodes. In Certificate based scheme, a CIA will generate keys for encryption and decryption between source and destination. A CIA should be trusted resource or agency mainly used for key generation.

This work uses Modified Device Key Generation Algorithm (MDKGA) for efficient communication with reduced time cost. A Certificate Based Scheme where a central trusted agency provides key for source and destination is applied. Two separate keys are generated for source and destination nodes for encryption and decryption and also another set of keys will be generated for router and intermediate nodes. The vulnerable node is being identified by *n* number of trails runs over a particular time period *t*. A network is formed according to the RSSI distance. A vulnerable node is placed in the network and communication is recorded. Analysis is done on the communication report. Based on the analysis, the vulnerable node is identified. The analysis is done for each and every node in the network.

Protocols:

AODV and DSR protocols are used for implementation. Both the protocols are on-demand routing protocols. It means that only on demand the request from the source node will be sent from the source node to destination node. No pre-defined data about the neighboring nodes will be maintained in the routing table. Only on request the node sends the request message to the neighboring nodes. There are two phases which are common for all the on-demand protocols. They are Route Discovery phase and Route Maintenance phase. The route discovery phase is common for both the protocols. They differ in Route maintenance phase.

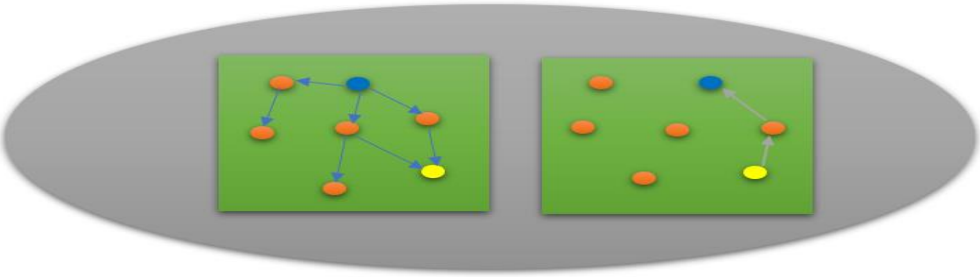


Fig. 1 Route Discovery Phase of AODV and DSR protocols

In the figure 1, the route discovery phase of the protocols is illustrated. Blue node is a source node, Yellow node is a destination node and orange nodes are intermediate nodes. In figure, the source node sends the Route_Request packet to its neighboring nodes to find the destination node with minimum hop distance. The neighboring nodes send the Route_Reqest packet received from the source node to their neighboring nodes. This process continues till the Route_Request message reaches the destination. The destination node will get more than one Route_Request message form its neighboring nodes. But the destination node selects the node with minimum hop distance. In figure, the destination node sends the Route_Reply message to the source node through the selected minimum hop path. This is called handshake process. Once the handshake process gets completed, the source node starts sending the data packet to the destination node. The above entire process is called Route Discovery phase.

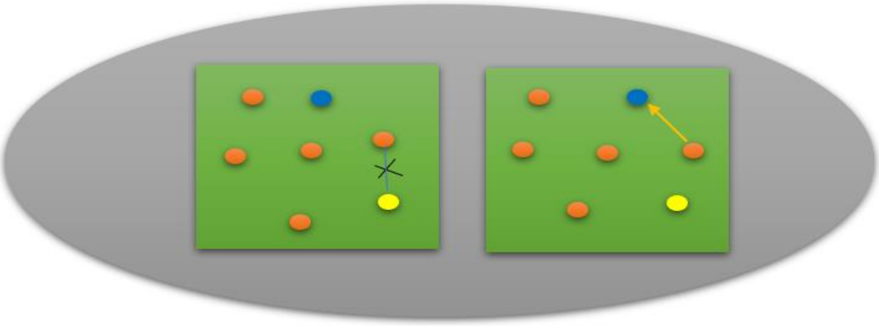


Fig. 2 Route Maintenance Phase of AODV

As stated earlier the route discovery phase of AODV differs from DSR. In Figure 2, illustration of Route maintenance phase is given. If the link failure between the nodes in the selected path occurs, then the intermediate node immediately sends Route_Err message to its predecessor neighbor node in the selected node. Once the error message reaches the source node, the source node again starts its Route Discovery phase to find the alternate path to the destination node with minimum hop distance.

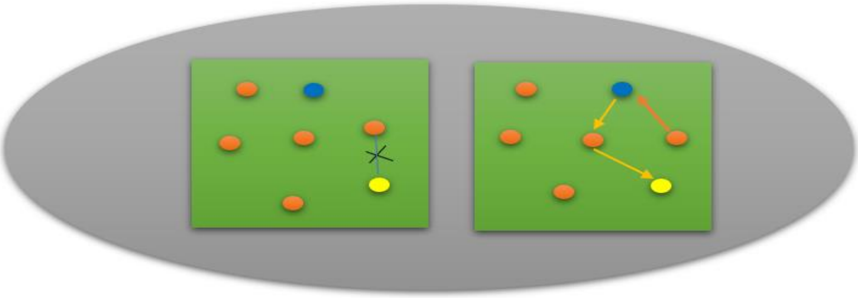


Fig. 3 Route Maintenance Phase of DSR

In Route Maintenance Phase of DSR, after Route Discovery Phase the routes to the destination node will be cached. Once the Route_Err message received by the source node through intermediate nodes it checks for alternate path to reach the destination with minimum hop distance without start over again from Route Discovery Phase or Construction Phase. The illustration of Route maintenance Phase of DSR is given in figure 3.

MDKGA

In this algorithm, the trust value of each node in the network is calculated. Once the trust value is calculated, the node with a highest trust value will be elected as Certificate Issuing Authority (CIA)/ node. The selected node acts as a router as well as a CIA according to request. The selection procedure of CIA node varies from one network to another. Initially, the CIA node will not be selected for the first round of simulation. Then after tenth round of simulation, CIA node is chosen based on the calculated average trust value of the nodes. The initial round of simulations for selecting the CIA node is also not a constant value. It takes some random value from 5-20 rounds. Trust node will be any intermediate node in the network. The information of trust node will be sent to all the nodes in the network. The details about the trust node will be added to the routing table. If the source node wants to send a data packet to its destination node it starts initiating to send the broadcast message to selected CIA node, Src_Key_Req message to the trust node. The trust node checks the type of message and sends Src_Key_Rep message.

Figures 4 (a) and (b) show the functionalities of MDKGM algorithm. In Figure 4 (a) blue node represents a CIA node. Before source node sends the broadcast message to its neighbors, it asks for key to encrypt the data packets from the CIA node which is used for transferring the packets securely. In Figure 4 (b), the destination node asks for key to decrypt the data packets.

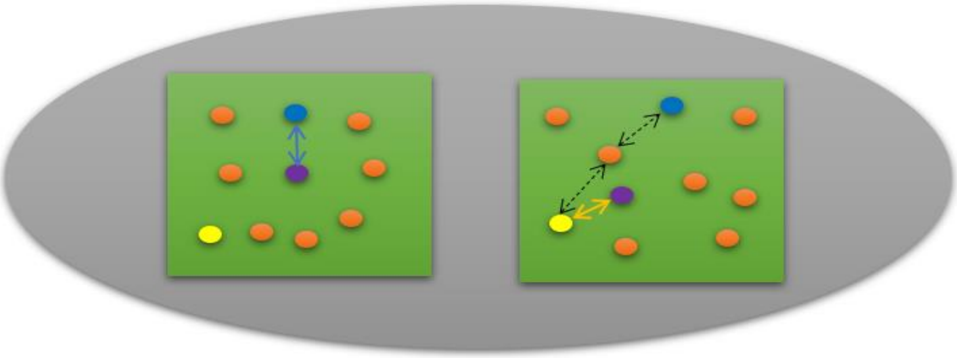


Fig. 4(a) and (b) Illustration of MDKGA

A Src_Key_Req message contains source_id, destination_id, #old_value #new_value and #trust_value. #new_value is a unique number or a text which is sent by the source node to the CIA node for identification. The #old_value is also a unique number which represents the previous key identification. For the initial request, always the value of #old_value will be null. The identification value of a node keeps changing for each and every communication. The updated trust value will be sent to the CIA node for each Src_Key_Req. The destination_ID will be saved in the trust node table for future confirmation. That is, when destination sends request for a key, it cross checks with the saved ID in the agent node. If it matches, then only the agent node generates the key and sends it to the destination node; else it simply ignores the message. If the CIA node receives a Src_Key_Req then it verifies the node based on the #trust_value. If the trust_value is above the threshold then the CIA node sends Src_Key_Rep message with source_id, destination_id, #new_value and ack='Verified'. If the trust_value is below the threshold then the CIA node reply with Req_Rej message with source_id, destination_id, #new_value and ack='rejected'.

The trust node acts as both router node and CIA node. Suppose if the trust node receives a Route_request message from its neighbor nodes, it just broadcast the message to its neighbors by updating its routing table. Or else, if it receives Src_Key_Req or Dest_Key_Req it acts as a CIA node. Based on the request the CIA node changes its characteristics and done accordingly. When destination node receives the route_request message from the source node, it sends Dest_Key_Req message to the CIA node. The Dest_Key_Req message contains source_id, destination_id, #old_value, #new_vaue and #trust_value. The #trust_value is required to identify whether the node which is requesting for key (encryption or decryption) is liable or not. If the trust_value is above the threshold then the CIA node sends Dest_Key_Rep message with source_id, destination_id, #new_value and ack='Verified'. If the trust_value is below the threshold then the CIA node reply with Req_Rej message with source_id, destination_id, #new_value and ack='rejected'. Once the handshake messages are over, the source node sends Src_Key_Req_enc message to the CIA node where the message contains source_id, destination_id, #new_value and #trust_value.

CIA node sends Src_Key_Rep_enc which contains the same content of Src_Key_Req_enc in addition to that it also contains the key for encryption and #random_new_value. This #random_new_value will be copied to #new_value field. If the same node seeking request from the CIA node it uses the random value generated by CIA for communication. The key is generated using RSA algorithm. Then, the source node starts to send the data packets to the destination node through the selected path. Here, public key cryptography method is used. That is, source and destination nodes will encrypt and decrypt using their own private keys respectively. The generated key varies for every new simulation. Node ID is used as a public key to access a particular node. If the request is for the first time to the CIA node, that is, before the handshake message, then Key_Reply message will not contain the key. It will have source_id/destination_id, #old_value and #new_value. This message is like an acknowledgement. For the next transmission onwards, it will send keys along with reply messages for encryption and decryption.

If the destination node receives data packet form the source node, it immediately sends Dest_Key_Request_dec message to CIA node. CIA node sends back Dest_Key_Reply_dec message which contains private key generated using RSA algorithm for decryption. This message also contains #random_new_value to copy into #new_value field of destination node router table for future identification.

If the source node completes handshake message with the destination node along the selected path identified after the discovery phase, it sends Src_Key_Req_enc message to the trust node. This key_reply message contains the #random_new_value similar to the old one along with the new value for the next request if it occurs. If the value matches then it generates the key and sends it. Once source receives the key it starts encrypting the data packets and sends to the neighboring nodes to reach the destination node. The same procedure is followed till all the packets reach the destination side.

Trust value for each node is calculated based on the average reliability and average energy efficiency from active participation of a node in the network and active participation of a node in a particular channel. They are defined as

$$\textit{Average Reliability of the node in the network } ARE_{Ni}=\frac{RE_i}{\bigcup_{j=1}^{r}\sum_{i=1}^{n}RE_i} \tag{1}$$

$$\textit{Average Residual Energy of the node in the network } AResEne_{Ni}=\frac{ResEne_i}{\bigcup_{j=1}^{r}\sum_{i=1}^{n}ResEne_i} \tag{2}$$

$$\textit{Trust value of the node in the network } TV_{Ni}=\frac{ARE_{Ni}+AResEne_{Ni}}{2} \tag{3}$$

In the above (1), *N* represents the current network and *i* is the corresponding node for which the trust value is calculated. *RE* is the reliability value of that particular node. (2) is used to calculate the average residual energy of the node in the network over ‘r’ number of rounds. ResEne is the residual energy of the node over ‘r’ number of rounds. (3) is used to calculate the trust value (TV_{Ni}) of the node in the network.

$$\textit{Reliability of the node in the channel } RC_i=\bigcup_{j=1}^{r}\frac{PR_i}{PS_i} \tag{4}$$

$$\textit{Residual Energy in the channel } ReC_i=\bigcup_{j=1}^{r}\frac{ResEne_i}{TE_i} \tag{5}$$

$$\textit{Trust value of the node in the channel } TV_{Nc}=\frac{RC_i+ReC_i}{2} \tag{6}$$

In the above (4), calculates the reliability of the node in the channel. It is defined as the ratio of number of packets received (PR_i) to the number of packets sent (PS_i) over the network. (5) is used to calculate the residual energy of the node in the channel over ‘r’ number of rounds. TE_i is the total energy was available at the initial stage. In (6), the trust value of a node is calculated by taking the ratio of its summation of reliability value and residual energy value over *r* number of rounds.

$$\textit{Effective Trust Value } ETV_i=TV_{Nc}+TV_{Ni} \tag{7}$$

In (7), the effective trust value (ETV) of a node ‘i’ in the network is calculated by taking the ratio of trust value of the node in the network to the trust value of the node in the channel. Agent node is elected based on the criteria satisfied by a node as specified in Table 1. The criteria that are given in the table is a dynamic one and the threshold value for fixing the criteria is calculated based on the history of the nodes’ trust value. There are only previous k Effective Trust Value of the node is maintained. If two or more nodes fall in the same category, then based upon the highest sequence value and number of times a node is selected as agent node in the previous network communication, the node will be elected as CIA node. Based on the trust value the neighbour node will be selected for the current node. The trust value acts as heuristic function to select the neighbor node and the optimized path from source to destination node using A* algorithm and the heuristic is based on trust value.

Table 1. Selection of CIA node based on Effective trust value ratio

At time t_0		**At time t_1**	
ETV (%)	**Decision**	**ETV (%)**	**Decision**
>=80	Most Promising CIA node	>=95	Promising CIA node
>=60 and <80	Can be taken as Promising CIA node	>=75 and <95	Can be taken as CIA node
>=50 and <60	Not allowed but it can be allowed in the network communication	>=6 5 and <75	Not allowed but it can be allowed in the network communication
<50	Not allowed and the entry about this node in the routing table of other nodes will be deleted	<65	Not allowed and the entry about this node in the routing table of other nodes will be deleted

In Table 1, the decision about the node is clearly tabulated. It is clearly seen that the threshold for taking the decision changes from time to time. At time t_0, if the effective trust value of a node is greater than 80, then the node which is having highest effective trust value can be elected as CIA/ Agent node. At time t_1, if the effective trust value of a node is greater than 95 then only the node will be elected as CIA/Agent node.

$$\textit{Average Effective Trust Value of a node } AETV_i = \frac{\sum_{j=1}^{n} ETV_j}{n} \qquad (8)$$

In (8), the Average Effective Trust Value (AETV) of a node i is calculated based on the previous n trust values of a node.

$$\textit{Average highest ETV of the network } AHETV_N = \frac{\sum_{i=1}^{n} HETV_i}{n} \qquad (9)$$

In (9), the Average Highest ETV (AHETV) of the network (N) is calculated based on Highest ETV of n rounds of simulation. HETV holds the previous 1n highest ETV of the network. AHETV is taken as the threshold value for accepting the node as CIA node. If the ETV of the node is greater than the AHETV will be considered as most promising node. Only after finding two effective trust values of each and every node, CIA node will be elected. Only after finding the 2nd ETV, the CIA node will be elected based on ETV. The intermediate values that are shown in the table 1, have considered as the relative value form the highest threshold value.

Pseudocode for calculating the Highest threshold value:

//Storing the rounds of highest ETV of a node in the array

```
Begin
HETV[k], max=0, sum=0, AHETV, r
For i= 1 to k do //
 For j=1 to n do   //n is number of nodes in the network
   If ETV[j]>max
Max= ETV[i]
   End If
End For
HETV[j]=max
Sum=sum+HETV[j]
AHETV=sum/r
End For
```

//setting the criteria for the current node

```
Begin
J=0, h=0, k=0, l=0, max=0
For i= 1 to n do
        If ETV[i] >= AHETV
                Mp[j++]=ETV[i]
                Node[h++]=ETV[i]
        Else if ETV[i]<AHETV and ETV[i] >= AHETV-20
                P[k++]=ETV[i]
        Else if ETV[i]<AHETV-20 and ETV[i] >= AHETV-30
                D[l++]=ETV[i]
        Else
                Nodes that are fallen in these criteria gets deleted from the routing table of
other nodes in the network.
        Endif
End For
For m= 0 to j-1 do
        If(mp[m]>max)
                Max=mp[m]
        Endif
End For
CIA_ETV= max
CIA_node= node[m]
// update the details of CIA node in the routing table of other nodes in the network.
End
```

MDKGA Process Flow

The process flow of MDKGA is illustrated in the figure. The process starts with initiating the network topology and the communication between the nodes. Then the trust values of the node in the network and in the channel is calculated based on reliability and residual energy. The summation of the above two factor is taken as Effective Trust Value. The highest trust value of previous rounds of simulation to be identified and to be fixed with the threshold_value for the current round. The algorithm for MDKGA is given in the figure 5. The request and reply messages from source and destination nodes to the CIA node for encryption and decryption will be verified initially through the handshake message and dynamic unique ID will be generated for each request from the same node for different simulation instances.

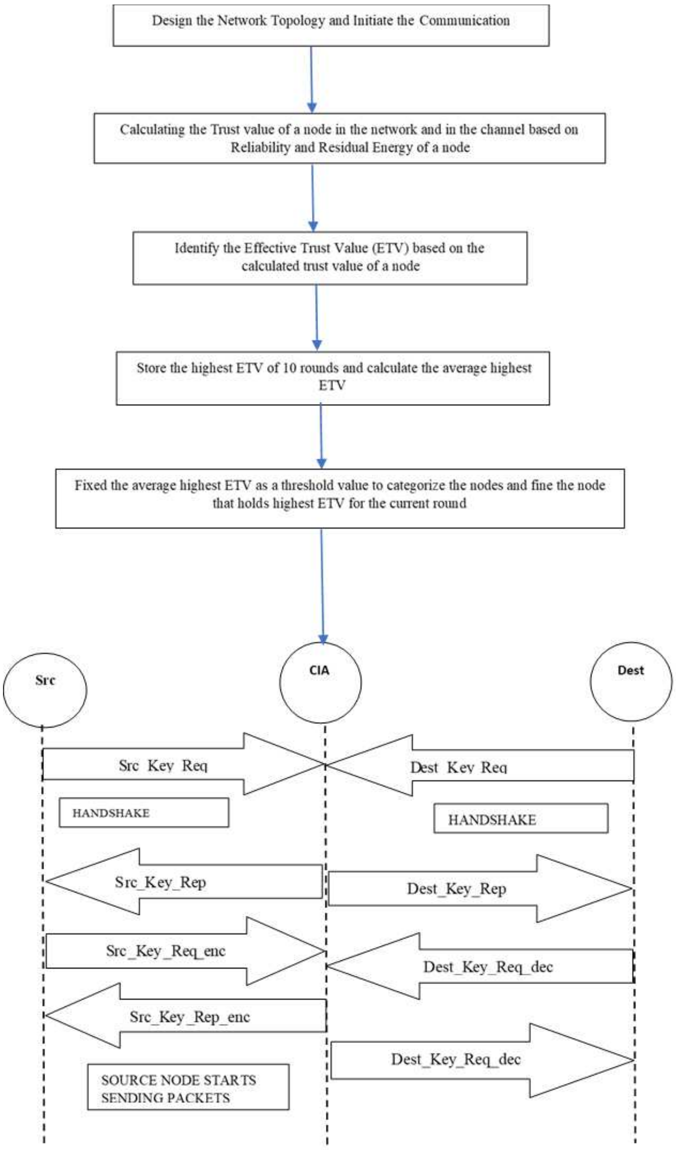

Design the Network Topology and Initiate the Communication
Calculating the Trust value of a node in the network and in the channel based on Reliability and Residual Energy of a node
Identify the Effective Trust Value (ETV) based on the calculated trust value of a node
Store the highest ETV of 10 rounds and calculate the average highest ETV
Fixed the average highest ETV as a threshold value to categorize the nodes and fine the node that holds highest ETV for the current round
Src
CIA
Dest
Src Key Req
Dest Key Req
HANDSHAKE
HANDSHAKE
Src_Key_Rep
Dest_Key_Rep
Src_Key_Req_enc
Dest_Key_Req_dec
Src_Key_Rep_enc
Dest_Key_Req_dec
SOURCE NODE STARTS SENDING PACKETS

Fig. 5 MDKGA Process Flow

MDKGAlgorithm

STEP 1: Define the network topology with n number of nodes and initiate the communication.

STEP 2: Calculate the average reliability of the node in the network.

STEP 3: Calculate the average residual energy of the node in the network.

STEP 4: Calculate the average trust value of the node in the network.

STEP 5: Calculate the average reliability of the node in the channel.

STEP 6: Calculate the average residual energy of the node in the channel.

STEP 7: Calculate the average trust value of the node in the channel.

STEP 8: Effective Trust Value of a node is the ratio of the total trust value of the node in the network to the total trust value of the node in the channel.

STEP 9: Repeat steps 2 to 8 for all the nodes in the network. CIA node selected after 10 rounds of simulation based on Average Highest trust value for previous rounds as threshold value.

STEP 10: Source node sends handshake message to the CIA node by sending Src_Key_Req.

STEP 11: CIA node sends acknowledgement by sending Src_Key_Rep message.

STEP 12: Start the discovery phase

STEP 13: Encryption will be done at source node based on key value given by CIA node using RSA algorithm by sending the message Src_Key_Req_enc.

STEP 14: Decryption at destination node will be based on key value generated by CIA node using RSA algorithm by sending Dest_Key_Rep_dec.

STEP 15: The source node starts sending packet data to destination node till the end of the data packet.

STEP 16: Run for n number of simulations and compare the performance measures based on results obtained from the simulations.

Performance measures

Performances of the network are calculated based on the following factors such as scalability, reliability, energy utilization, mobility etc. The output from the simulations will be analyzed and necessary changes are made if there are any drastic variations in the performances of the networking environment. The Average Reliability (AR_N) is defined as

$$AR_N = \frac{\sum_{i=1}^{k} re_{n_i}}{k} \qquad (10)$$

where *AR* is average reliability, *i* is a node and *k* is number of simulations.

The scalability factor (SC_N) is defined as

$$SC_N = \frac{\sum_{j=1}^{k}\sum_{i=1}^{n} sc_i}{k} \tag{11}$$

where *SC* is scalability, *i* is a node, *k* is number of simulations and *n* is number of nodes in each simulation.

$$EU_N = \frac{\sum_{j=1}^{k}\sum_{i=1}^{n} eu_i}{k} \tag{12}$$

where *EU* is Energy Utilization, *i* is a node, *k* is number of simulations and *n* is number of nodes in each simulation.

The Average Trust value (AT_N) is defined as

$$AT_N = \frac{\sum_{i=1}^{k} ETV_i}{k} \tag{13}$$

where *AT* is Average Trust Value, *ETV* is Effective trust value of a network and *K* is number of simulations.

Equations (10) to (13) are used to calculate the performance factors of the network based on *k* number of simulations. In (10), average reliability of a network is calculated. The reliability values of all nodes in a network are added for *n* number of simulations. The average value is the ratio of total reliability of a network to the number of simulations. In (11), average scalability of a network is calculated. The scalability value of a node is calculated based on packet delivery ratio and by varying number of nodes in the network for each simulation. The scalability values of all nodes in a network are added for *n* number of simulations. The average value is the ratio of total scalability of a network to the number of simulations. In (12), average energy utilization of a network is calculated. For n number of nodes over k number of simulations the Energy Utilization value is calculated. In (13), average Effective Trust Value of a network is calculated. The Effective Trust Values of all nodes in a network are added for *n* number of simulations. The average value is the ratio of total Effective Trust Value of a network to the number of simulations. The values obtained from the calculations are compared with/without using DKGM.

Results

NS2 simulator is used for the implementation of MDKGA. The simulator instance of the environment that is being created is shown in Table 2. The protocol used for the implementation is AODV and DSR. The maximum simulation time is 600 sec. From the results, the reliability, scalability, energy utilization and effective trust value are calculated and then compared with the corresponding improvised algorithm implemented using the protocols AODV and DSR. Comparison between the protocols is also done based on these performance parameters.

Table 2 Simulation instances for implementation

Simulator Instances	
Parameters	**Default Values**
Topology	Dynamic
Number of nodes	5-150
Transmission range	120m
MAC Protocol	802.11
Network Protocol	AODV, DSR & CHGRP
Packet Size	512 Byte
Packet Interval	120 packet/sec
Bandwidth	7Mbps
Simulation Time	Maximum up-to 600sec

Table 3 Reliability value of AODV and DSR for 5 rounds

Node ID	**Reliability (AODV)**				
	Round1	**Round2**	**Round3**	**Round4**	**Round5**
1	80	45	67	66	75
2	53	89	90	83	78
3	87	79	80	91	75
4	34	23	56	45	39
5	77	81	57	62	84
6	76	71	83	85	79
7	63	58	49	71	33
8	91	89	92	88	95
9	73	78	80	74	70
Node ID	**Reliability (DSR)**				
	Round1	**Round2**	**Round3**	**Round4**	**Round5**
1	84	50	69	70	79
2	57	92	95	88	83
3	90	81	88	96	78
4	42	39	68	50	45
5	82	89	70	75	89
6	77	78	85	91	83
7	72	63	56	82	34
8	96	92	97	89	98
9	78	83	88	79	72

Table 4 Average Reliability of a node in the network using AODV and DSR

Node ID	Average Reliability of the node in the network (AODV)	Average Reliability of the node in the network (DSR)
1	0.104	0.102
2	0.123	0.121
3	0.129	0.126
4	0.062	0.071
5	0.113	0.118
6	0.123	0.120
7	0.086	0.089
8	0.142	0.137
9	0.117	0.116

Table 3 shows the reliability value (Packet Delivery Ratio) using AODV and DSR for 5 rounds. Here the PDR is taken for 9 nodes. From the Reliability value measured in the table, the average reliability value of the node in the network is calculated in table 4.

Table 5 Energy utilization of nodes using AODV and DSR for 5 rounds

Node ID	Energy Utilization (J) (AODV)				
	Round1	Round2	Round3	Round4	Round5
1	56	56	54	50	49
2	68	65	45	63	53
3	34	45	43	32	47
4	78	79	67	59	64
5	44	49	51	45	34
6	42	40	39	39	38
7	52	53	57	59	63
8	23	29	22	28	22
9	47	43	41	45	43
Node ID	**Energy Utilization (J) (DSR)**				
	Round1	**Round2**	**Round3**	**Round4**	**Round5**
1	50	48	49	50	42
2	67	63	34	56	49
3	30	43	40	26	32
4	65	70	61	48	59
5	38	41	43	40	32
6	36	31	33	35	27
7	43	49	54	51	60
8	17	19	18	20	22
9	44	41	35	37	38

Table 6 Residual Energy of nodes using AODV and DSR for 5 rounds

Node ID	Residual Energy (J) (AODV)				
	Round1	Round2	Round3	Round4	Round5
1	44	44	46	50	51

2	32	35	55	37	47
3	66	55	57	68	53
4	22	21	33	41	36
5	56	51	49	55	66
6	58	60	61	61	62
7	48	47	43	41	37
8	77	71	78	72	78
9	53	57	59	55	57

Node ID	**Residual Energy (J) (DSR)**				
	Round1	**Round2**	**Round3**	**Round4**	**Round5**
1	44	44	46	50	51
2	32	35	55	37	47
3	66	55	57	68	53
4	22	21	33	41	36
5	56	51	49	55	66
6	58	60	61	61	62
7	48	47	43	41	37
8	77	71	78	72	78
9	53	57	59	55	57

Table 7 Average Residual Energy of the nodes in the network using AODV and DSR

Node ID	**Average Residual Energy of the node to the network (AODV)**	**Average Residual Energy of the node to the network (DSR)**
1	0.100	0.100
2	0.088	0.088
3	0.128	0.126
4	0.065	0.075
5	0.118	0.117
6	0.129	0.129
7	0.092	0.093
8	0.160	0.155
9	0.100	0.117

Table 8 Trust Values of the nodes in the network using AODV and DSR

Node ID	**Trust value of the node to the network (TV_{Ni}) AODV**	**Trust value of the node to the network (TV_{Ni}) DSR**
1	0.102	0.101
2	0.105	0.104
3	0.128	0.126
4	0.063	0.073
5	0.116	0.117
6	0.126	0.125
7	0.089	0.091
8	0.151	0.146
9	0.119	0.116

Table 5 shows the energy utilization value of 9 nodes for 5 rounds. From the energy utilization value, the residual energy is calculated in table 6. Initially, the maximum energy for each node is kept as 100J. Using the calculated residual energy, the Average residual energy of the node in the network is calculated in table 7. In table 8, the trust value of the node to the network is calculated. Though it shows very little difference for 9 nodes and 5 rounds. For different combination of nodes and rounds, these values may vary.

Table 9 Average Reliability of the nodes in the channel using AODV and DSR

Node ID	Average Reliability of the node in the channel (AODV)	Average Reliability of the node in the channel(DSR)
1	66.6	70.4
2	78.6	83
3	82.4	86.6
4	39.4	48.8
5	72.2	81
6	78.8	82.8
7	54.8	61.4
8	91	94.4
9	75	80

Table 10 Average Residual Energy of the nodes in the channel using AODV and DSR

Node ID	Average Residual Energy of the node in the channel (AODV)	Average Residual Energy of the node in the channel (DSR)
1	47	52.2
2	41.2	46.2
3	59.8	65.8
4	30.6	39.4
5	55.4	61.2
6	60.4	67.6
7	43.2	48.6
8	75.2	80.8
9	56.2	61

Table 11 Trust Value of the nodes in the channel using AODV and DSR

Node ID	Trust Value of the node in the channel (AODV)	Trust Value of the node in the channel (DSR)
1	56.8	61.3
2	59.9	64.6
3	71.1	76.2
4	35	44.1
5	63.8	71.1
6	69.6	75.2
7	49	55

8	83.1	87.6
9	65.6	70.5

Table 9 shows the average PDR value of 9 nodes for 5 rounds. In table 10, average Energy utilization values of 9 nodes in 5 rounds are calculated. From the above two values, Trust value of the nodes in the channel are calculated and shown in table 11.

Table 12 Effective Trust value of the nodes using AODV and DSR

Node ID	Effective Trust Value of the node (AODV)	Effective Trust Value of the node (DSR)
1	56.90	61.40
2	60.01	64.70
3	71.23	76.33
4	35.06	44.17
5	63.92	71.22
6	69.73	75.32
7	49.09	55.09
8	83.25	87.75
9	65.72	70.62

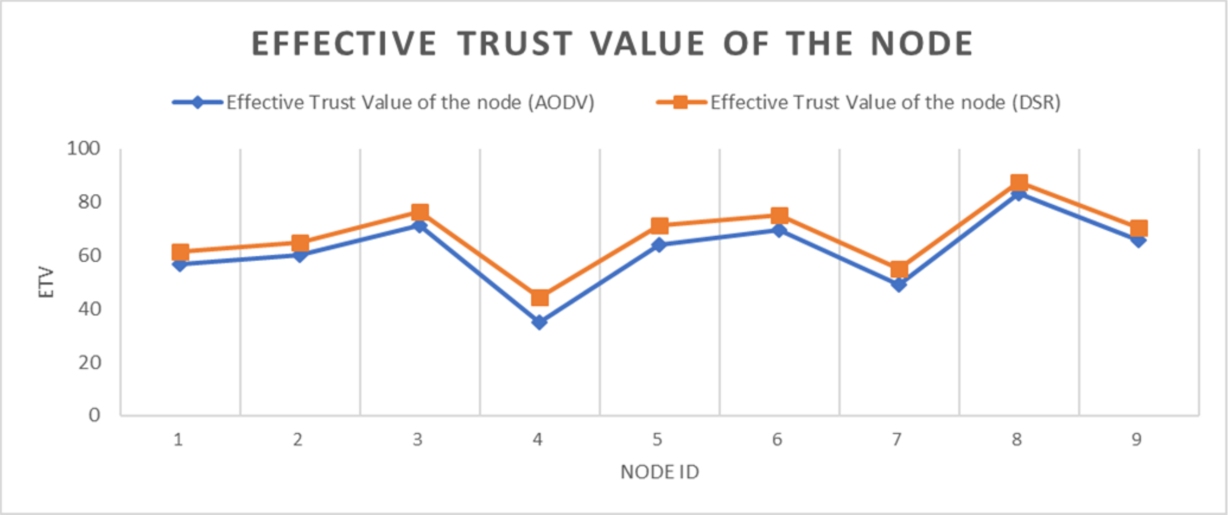


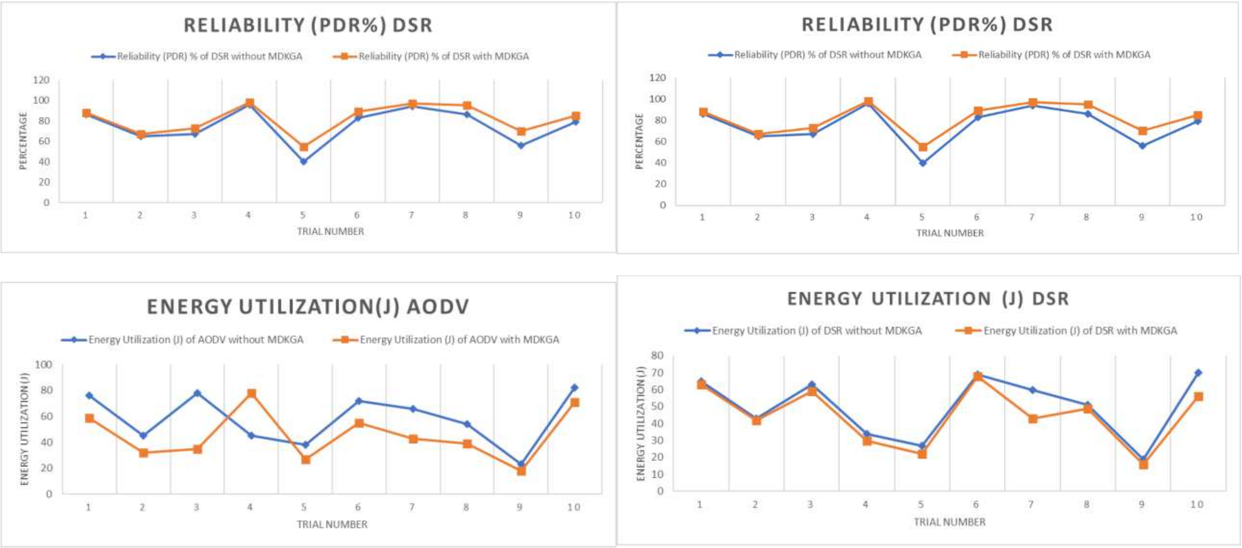
Fig. 6 Effective Trust value of the nodes using AODV and DSR

Table 12 and Figure 6 represent the Effective Trust Values of the nodes using the protocols AODV and DSR. From Table 12, it is clearly understood that Effective Trust values of the nodes using DSR are having higher values than AODV.

Table 13 Comparisons of reliability (%) and Energy Utilization with and without using DKGM using AODV and DSR

Without MDKGA					With MDKGA reliability				
Trial Number	Reliability (PDR) %		Energy Utilization (J)		Trial Number	Reliability (PDR) %		Energy Utilization (J)	
	AODV	DSR	AODV	DSR		AODV	DSR	AODV	DSR
1	80	86	76	65	1	85	88	59	63
2	56	65	45	43	2	58	67	32	42
3	58	67	78	63	3	69	73	35	59
4	94	96	45	34	4	97	98	78	30
5	32	40	38	27	5	50	55	27	22
6	78	83	72	69	6	83	89	55	68
7	90	94	66	60	7	94	97	43	43
8	81	86	54	51	8	92	95	39	49
9	45	56	23	19	9	61	70	18	16
10	75	79	82	70	10	83	85	71	56

Figure 7 Comparisons of reliability (%) and Energy Utilization with and without using DKGM using AODV and DSR



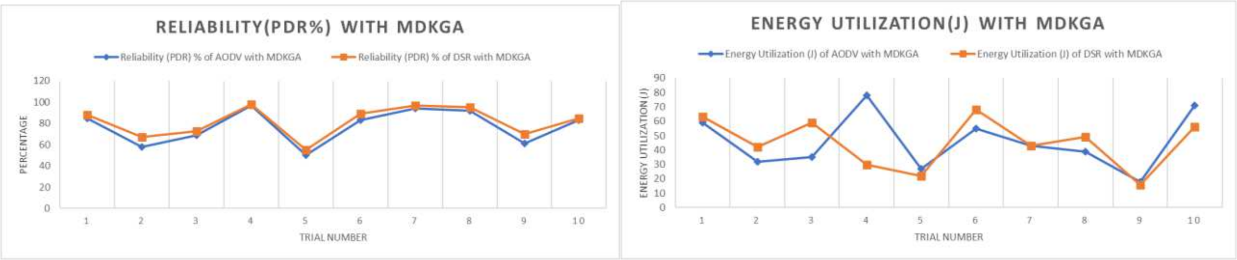
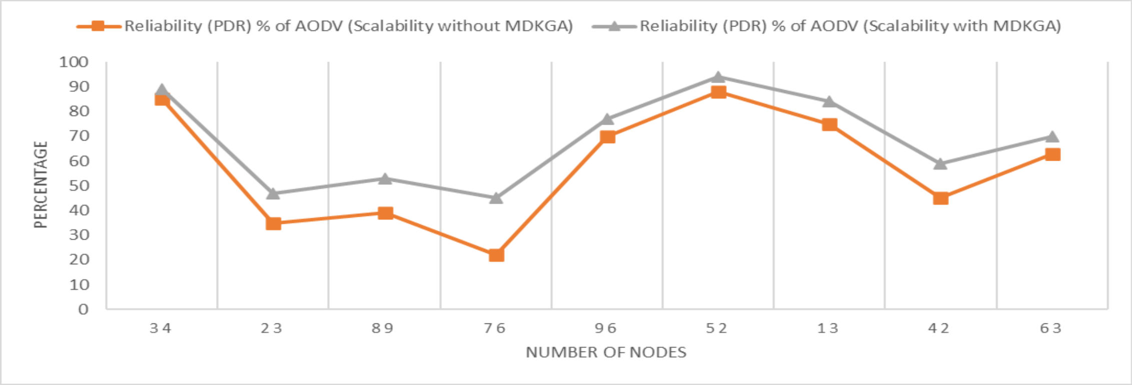


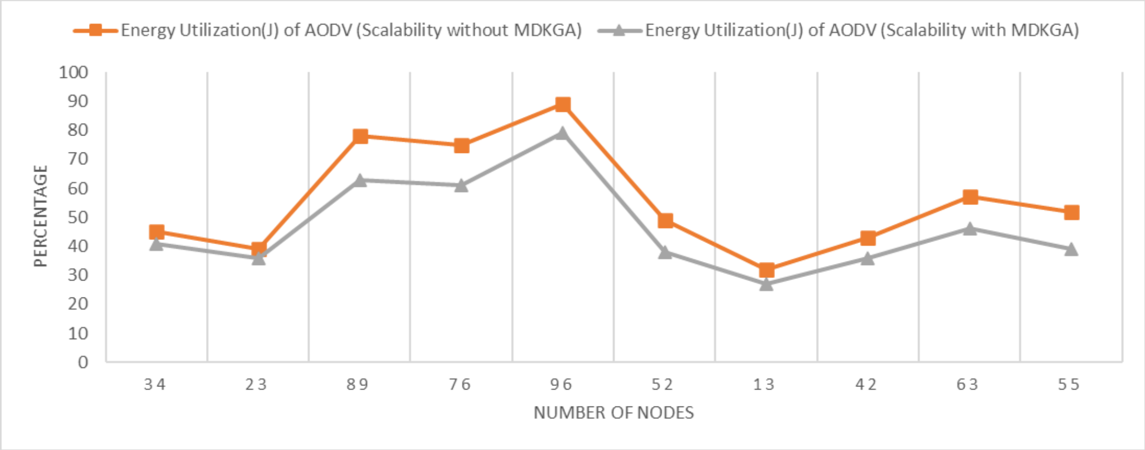
Fig. 7 Comparisons of reliability (%) and Energy Utilization with and without using DKGM using AODV and DSR

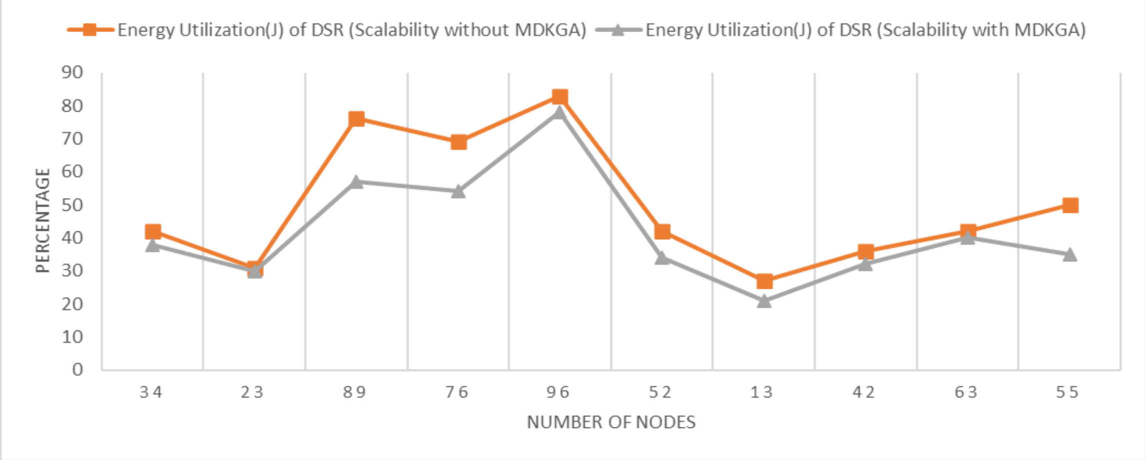
From Table 13 and Figure 7, it is inferred that without using MDGKA, the performance parameters such as PDR and Energy Utilization re showing poor values. The performance metrics of DSR shows better values than AODV. When using MDKGA, both AODV and DSR work better. There is an increasing value for both the performance metrics PDR and Energy Utilization.

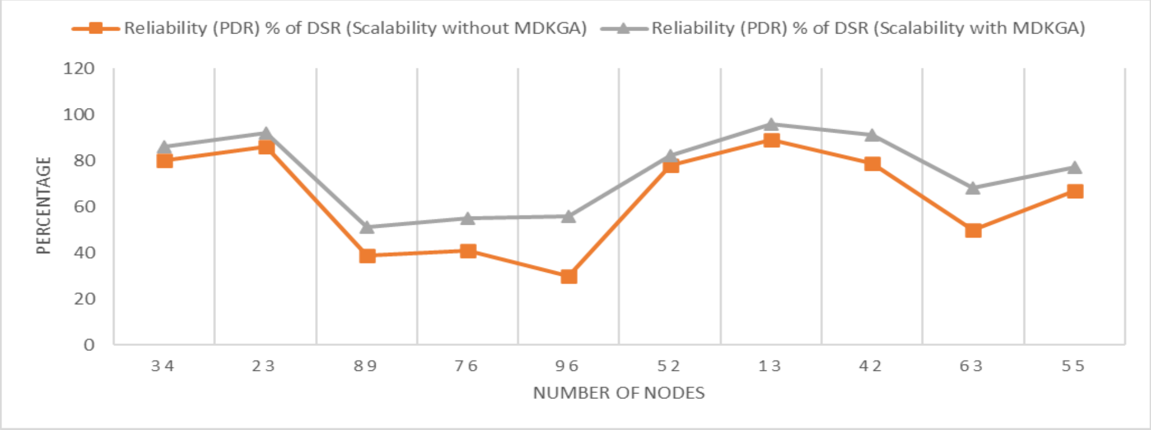
Table 14 Reliability (%) and Energy Utilization based on scalability with and without using DKGM using AODV and DSR

Scalability Without MDKGA					**Scalability With MDKGA**				
Number of nodes	**Reliability (PDR) %**		**Energy Utilization (J)**		**Number of nodes**	**Reliability (PDR) %**		**Energy Utilization (J)**	
	AODV	**DSR**	**AODV**	**DSR**		**AODV**	**DSR**	**AODV**	**DSR**
34	78	80	45	42	34	83	86	41	38
23	85	86	39	31	23	89	92	36	30
89	35	39	78	76	89	47	51	63	57
76	39	41	75	69	76	53	55	61	54
96	22	30	89	83	96	45	56	79	78
52	70	78	49	42	89	77	82	38	34
13	88	89	32	27	13	94	96	27	21
42	75	79	43	36	42	84	91	36	32
63	45	50	57	42	63	59	68	46	40
55	63	67	52	50	55	70	77	39	35


Reliability (PDR) % of AODV (Scalability without MDKGA)
Reliability (PDR) % of AODV (Scalability with MDKGA)
PERCENTAGE
100
90
80
70
60
50
40
30
20
10
0
34
23
89
76
96
52
13
42
63
NUMBER OF NODES


Energy Utilization(J) of AODV (Scalability without MDKGA)
Energy Utilization(J) of AODV (Scalability with MDKGA)
PERCENTAGE
100
90
80
70
60
50
40
30
20
10
0
34
23
89
76
96
52
13
42
63
55
NUMBER OF NODES


Energy Utilization(J) of DSR (Scalability without MDKGA)
Energy Utilization(J) of DSR (Scalability with MDKGA)
PERCENTAGE
90
80
70
60
50
40
30
20
10
0
34
23
89
76
96
52
13
42
63
55
NUMBER OF NODES


Reliability (PDR) % of DSR (Scalability without MDKGA)
Reliability (PDR) % of DSR (Scalability with MDKGA)
PERCENTAGE
120
100
80
60
40
20
0
34
23
89
76
96
52
13
42
63
55
NUMBER OF NODES

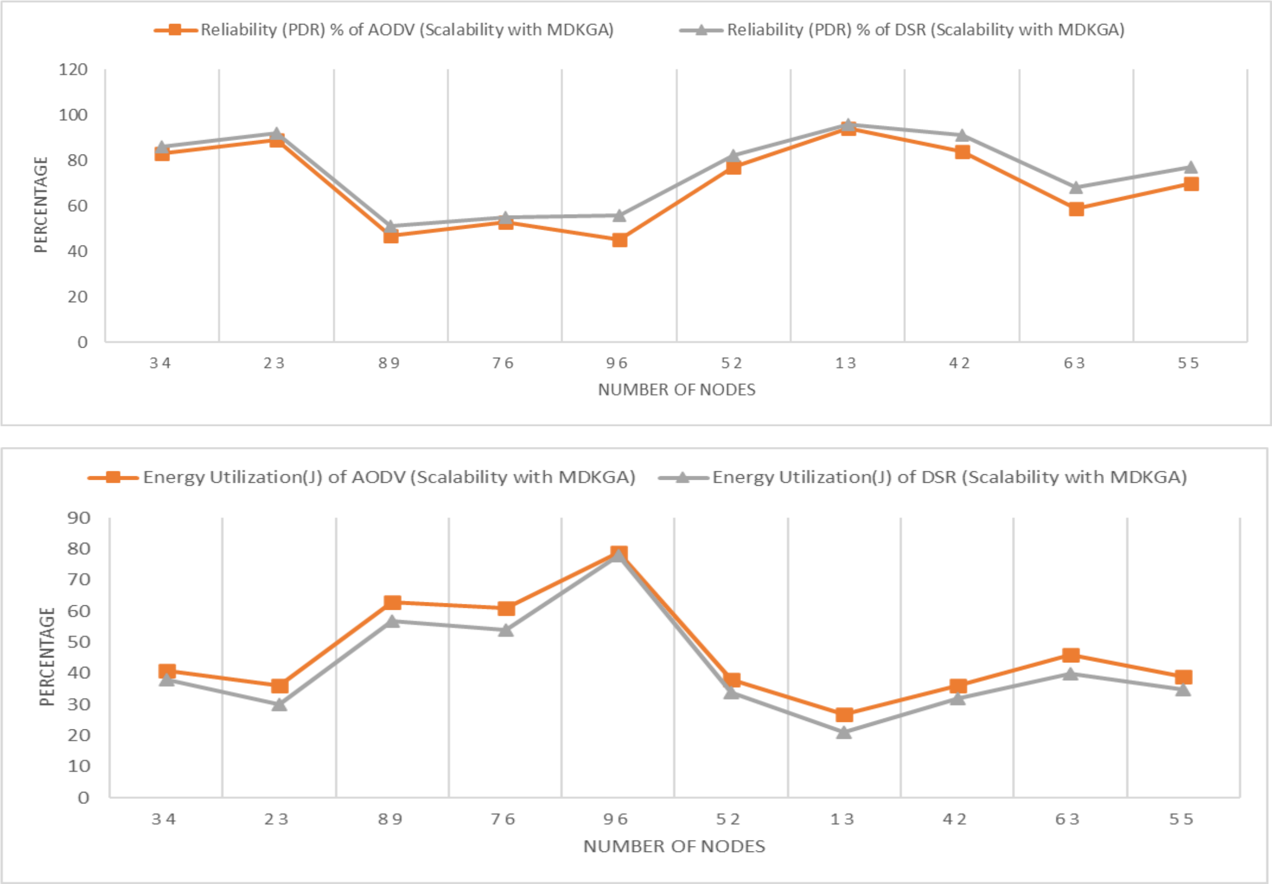


Figure 8 Reliability (%) and Energy Utilization based on scalability with and without using DKGM using AODV and DSR

From Table 14 and Figure 8, it is inferred that without using MDGKA, when the number of nodes in the network increases there is a drastic decrease in the % PDR value and Energy Utilization. Only 10 random simulation environments by varying the number of nodes in the network are considered. Including MDGKA, the performance gives good percentage of PDR and Energy Utilization.

Conclusion and Future Work

The main application of MANET is Vehicular Ad-hoc Network (VANET). Though it is a rapidly growing field of research, still it lags in major issues such as scalability, reliability, mobility, security etc. In this work, a key generation algorithm called MDKGA is proposed which selects the CIA node from the network based on the highest ETV. Source and destination nodes communicate with the CIA node before the source node starts transmitting the data packets. The public key cryptography method is used for encryption method. RSA key generation algorithm for generating private key is used. This method has invoked end-to-end encryption since it is not advisable to share keys via intermediate nodes because of node's mobility. Performance evaluations were done and compared with various simulation experiments. AODV and DSR Protocols are used for implementation. Comparisons between both the protocols have been done after incorporating the proposed algorithm on them. The comparisons have done based on PDR, Scalability, Energy Utilization and Trust value. In future work, in addition to the above performance factors, we can include delay time based on synchronization between the nodes during the communication and mobility. For the analysis part, we can train and test the dataset obtained from the simulation using Machine Learning techniques.

Compliance with Ethical Standards

Data Availability: Available

Animal Research (Ethics): Not Applicable

Consent to Participate (Ethics): Not Applicable

Consent to Publish (Ethics): Not Applicable

Plant Reproducibility: Not Applicable

Clinical Trials Registration: Not Applicable

Author Contribution: Experiment: Gayathri V M, Supraja P, Razia Sulthana A, Mukuntha P;

Write up: Gayathri V M, Supraja P; **Validation of Results:** Razia Sulthana A, Gayathri V M;

Supervisor: Gayathri V M**.**

Conflict of Interest: We have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding: Self Finance

References:

[1] BanothRajkumar and G.NarsimhaDr., "Trust Based Certificate Revocation for Secure Routing in MANET", Procedia Computer Science, Volume 92, 2016, Pages 431-441.

[2] Jin-HeeCho et.al, "Trust threshold based public key management in mobile ad hoc networks", Ad Hoc Networks, Volume 44, 1 July 2016, Pages 58-75.

[3] MarcoConti et.al, "From MANET to people-centric networking: Milestones and open research challenges", Computer Communications, Volume 71, 1 November 2015, Pages 1-21.

[4] Kannan Govindan, Prasant Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey", IEEE Communications Surveys & Tutorials, Volume 14, Issue 2, May 2011, Pages 279 – 298.

[5] Suvadip Batabyal, Parama Bhaumik, "Mobility Models, Traces and Impact of Mobility on Opportunistic Routing Algorithms: A Survey", IEEE Communications Surveys & Tutorials, Volume 17, Issue 3, April 2015, Pages 1679 – 1707.

[6] YangYang et al, "Broadcast encryption based non-interactive key distribution in MANETs", Journal of Computer and System Sciences, Volume 80, Issue 3, May 2014, Pages 533-545.

[7] MohammadMasdari et.al, "Markov chain-based evaluation of the certificate status validations in hybrid MANETs", Journal of Network and Computer Applications, Volume 80, February 2017, Pages 79-89.

[8] Malik N.Ahmed et.al, "F3TM: Flooding Factor based Trust Management Framework for secure data transmission in MANETs", Journal of King Saud University - Computer and Information Sciences, Volume 29, Issue 3, July 2017, Pages 269-280.

[9] JiaLiu et.al, "On throughput capacity for a class of buffer-limited MANETs", Ad Hoc Networks, Volume 37, Part 2, February 2016, Pages 354-367.

[10] SomayehTaheri et.al, "Anonymous group-based routing in MANETs", Journal of Information Security and Applications, Volume 22, June 2015, Pages 87-98.

[11] SrinivasAluvala et al, "A novel technique for node authentication in mobile ad hoc networks", Perspectives in Science, Volume 8, September 2016, Pages 680-682.

[12] Inderpreet Kaur, A. L. N. Rao, "A Framework to improve the Network Security with Less Mobility in MANET", International Journal of Computer Applications Volume167 – No.10, June 2017, Pages 0975 – 8887.

[13] Jaikumar Vinayagam, CH. Balaswamy , K. Soundararajan, "Certain Investigation on MANET Security with Routing and Blackhole Attacks Detection", Procedia Computer Science 165 (2019) 196–208.

[14] Houda Moudnia, Mohamed Er-rouidi, Hicham Mouncif, Benachir El Hadadi, "Black Hole attack Detection using Fuzzy based Intrusion Detection Systems in MANET", Procedia Computer Science 151 (2019) 1176–1181.

[15] N. Rajendran, P.K. Jawahar, R. Priyadharshini, "Cross centric intrusion detection system for secure routing over black hole attacks in MANETs", Computer Communications, Volume 148, 15 December 2019, Pages 129-135.

[16] ElbasherElmahdi, Seong-MooYoo, KumarSharshembiev, "Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks", Journal of Information Security and Applications, Volume 51, April 2020, 102425.

[17] SubramanianBalaji, Eanoch GoldenJulie, Yesudhas HaroldRobinson, RaghvendraKumar, Pham HuyThong, Le HoangSon, "Design of a security-aware routing scheme in Mobile Ad-hoc Network using repeated game model", Computer Standards & Interfaces, Volume 66, October 2019, 103358.

[18] Ningthoujam ChidanandaSingh, AvinashSharma, "Resilience of mobile ad hoc networks to security attacks and optimization of routing process", Material Systems: Proceedings, https://doi.org/10.1016/j.matpr.2020.09.622.

[19] BinYang, ZhenqiangWuaYulongShen, XiaohongJiang, "Packet delivery ratio and energy consumption in multicast delay tolerant MANETs with power control", Computer Networks, Volume 161, 9 October 2019, Pages 150-161.

[20] R. GaneshBabu, P.Karthika, G.Manikandan, "Polynomial Equation Based Localization and Recognition Intelligent Vehicles Axis using Wireless Sensor in MANET", Procedia Computer Science, Volume 167, 2020, Pages 1281-1290.

[21] ValantoAlappatt, P.M.Joe Prathap, "Hybrid cryptographic algorithm based key management scheme in MANET", Material Systems: Proceedings, https://doi.org/10.1016/j.matpr.2020.09.788.

[22] Salman AliSyed, "A systematic comparison of mobile Ad-hoc network security attacks", Material Systems: Proceedings, https://doi.org/10.1016/j.matpr.2020.12.617.

[23] DivyaGautam, VrindaTokekar, "A novel Approach for Detecting DDoS Attack in MANET", Material Systems: Proceedings, https://doi.org/10.1016/j.matpr.2020.07.332.

[24] SuneelMiriyala, M. SatyaSairam, "Improving privacy in SDN based MANET using hybrid encryption and decryption algorithm", Microprocessors and Microsystems, https://doi.org/10.1016/j.micpro.2020.103501.

[25] G.A.E.Satish Kumar, P.Rama Devi, "A novel proactive routing strategy to defend node isolation attack in MANETS", Material Systems: Proceedings, https://doi.org/10.1016/j.matpr.2020.11.361.

[26] Maruthupandi.J, Prasanna.S, Jayalakshmi.P, Mareeswari.V, Siva kumar.B, Sanjeevi.P, "Route manipulation aware Software-Defined Networks for effective routing in SDN controlled MANET by Disney Routing Protocol", Microprocessors and Microsystems, Volume 80, February 2021, 103401

Figures

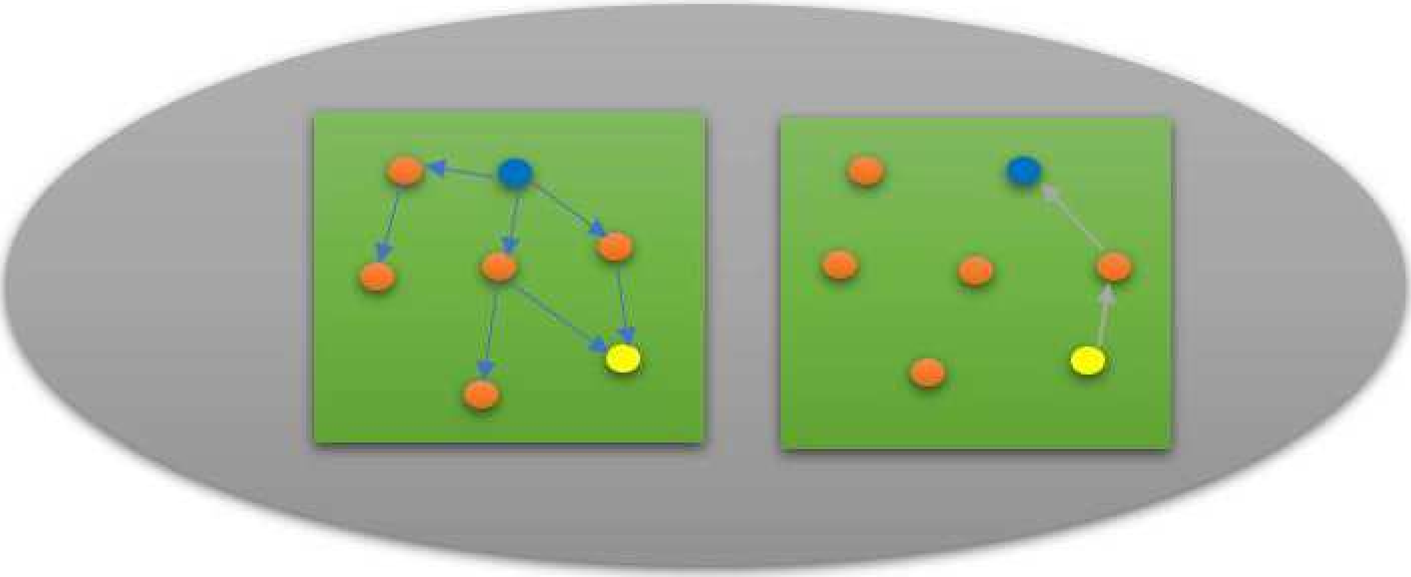


Figure 1

Route Discovery Phase of AODV and DSR protocols

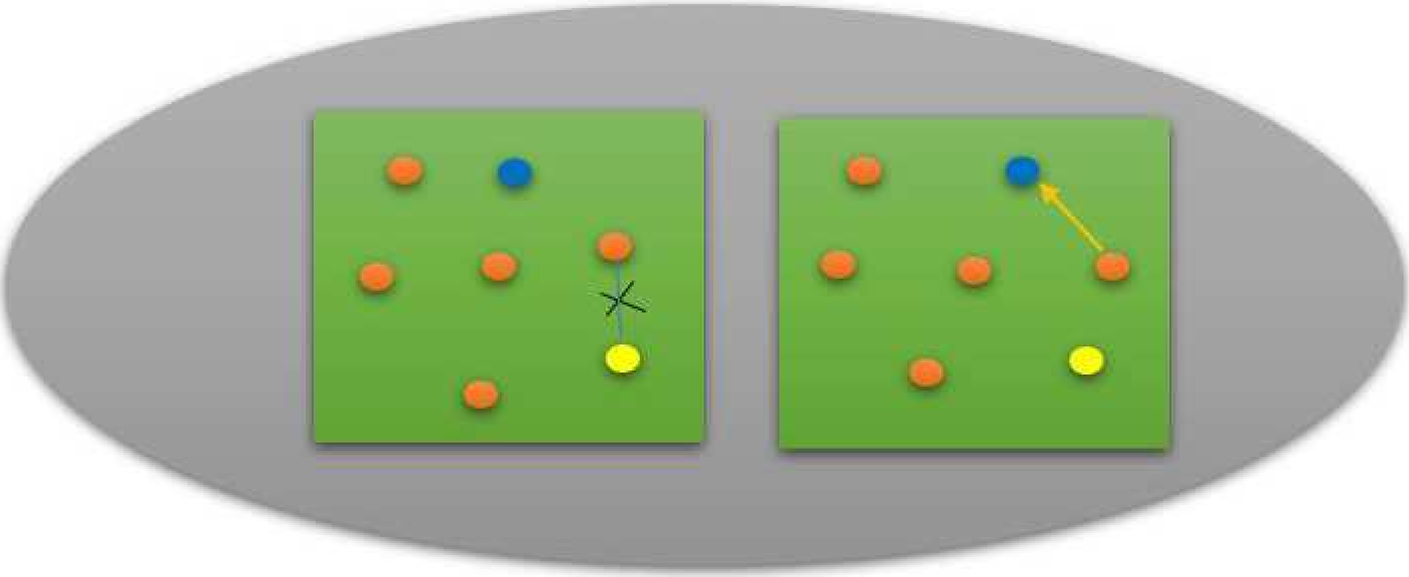


Figure 2

Route Maintenance Phase of AODV

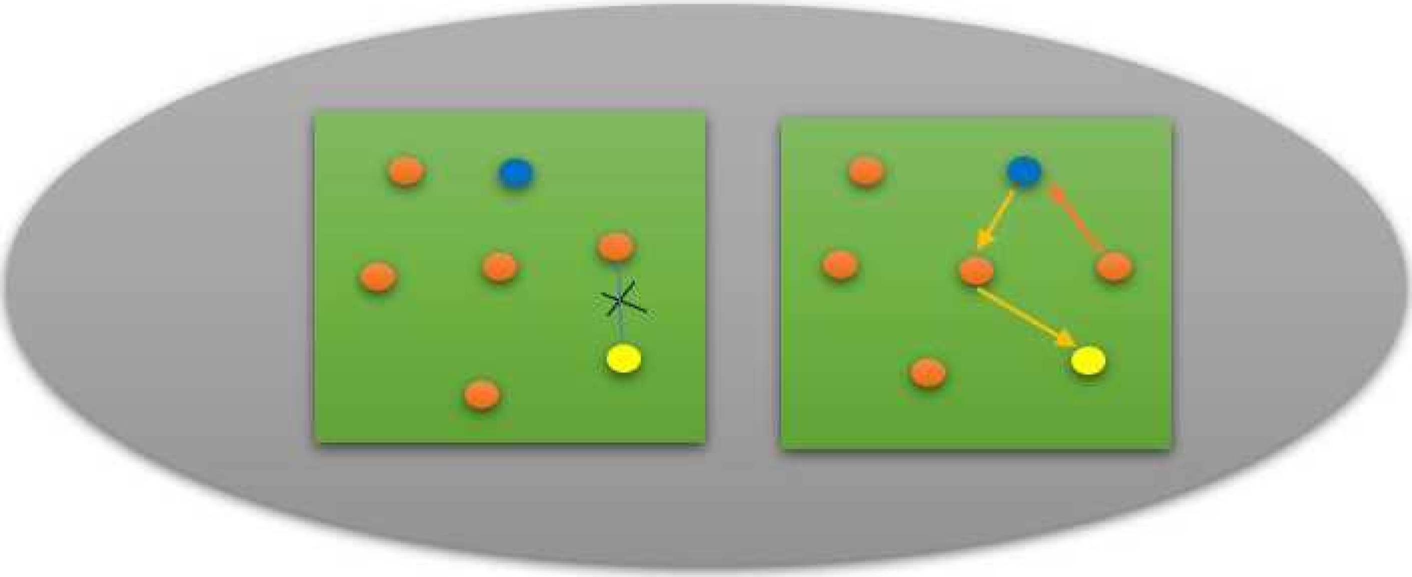


Figure 3

Route Maintenance Phase of DSR

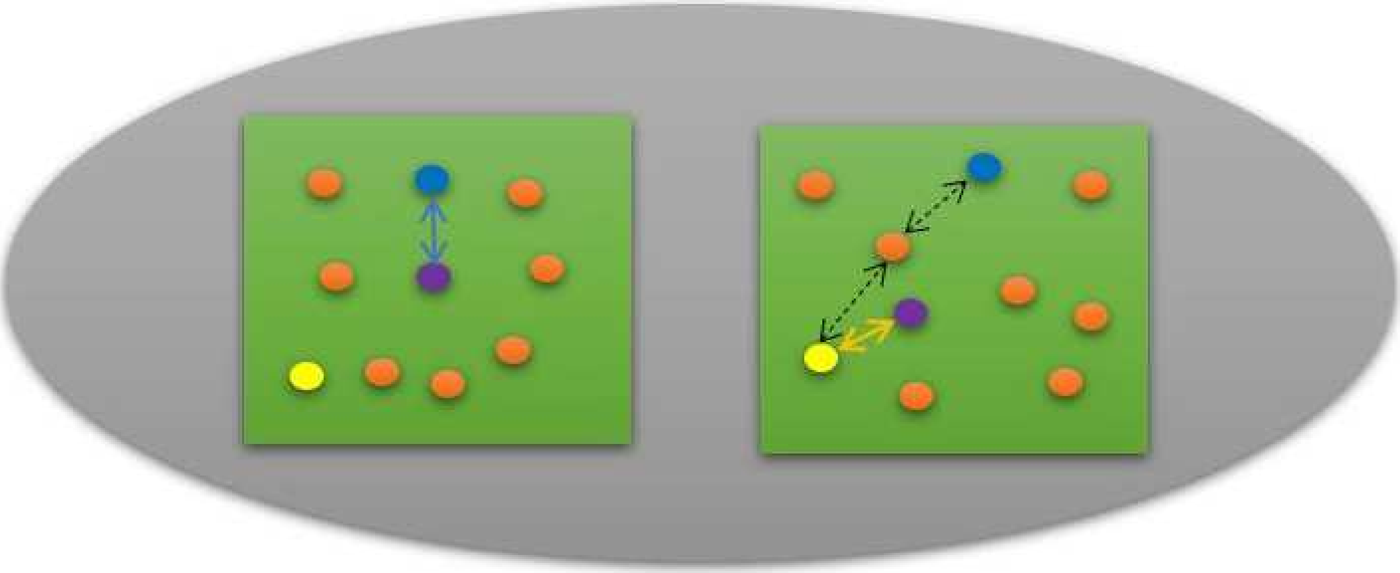


Figure 4

(a) and (b) Illustration of MDKGA

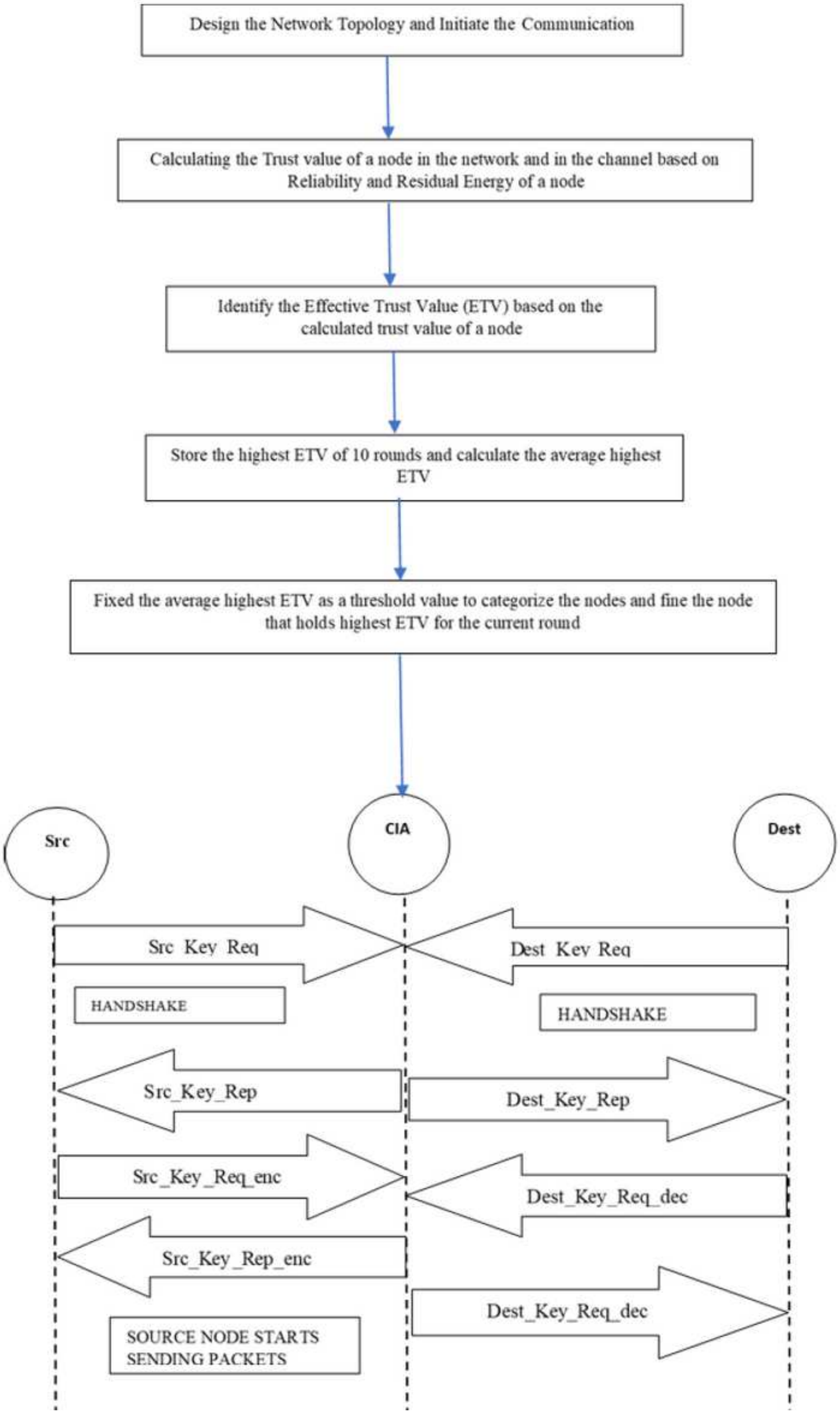

Design the Network Topology and Initiate the Communication
Calculating the Trust value of a node in the network and in the channel based on Reliability and Residual Energy of a node
Identify the Effective Trust Value (ETV) based on the calculated trust value of a node
Store the highest ETV of 10 rounds and calculate the average highest ETV
Fixed the average highest ETV as a threshold value to categorize the nodes and fine the node that holds highest ETV for the current round
Src
CIA
Dest
Src_Key_Req
Dest_Key_Req
HANDSHAKE
HANDSHAKE
Src_Key_Rep
Dest_Key_Rep
Src_Key_Req_enc
Dest_Key_Req_dec
Src_Key_Rep_enc
Dest_Key_Req_dec
SOURCE NODE STARTS SENDING PACKETS

Figure 5

MDKGA Process Flow

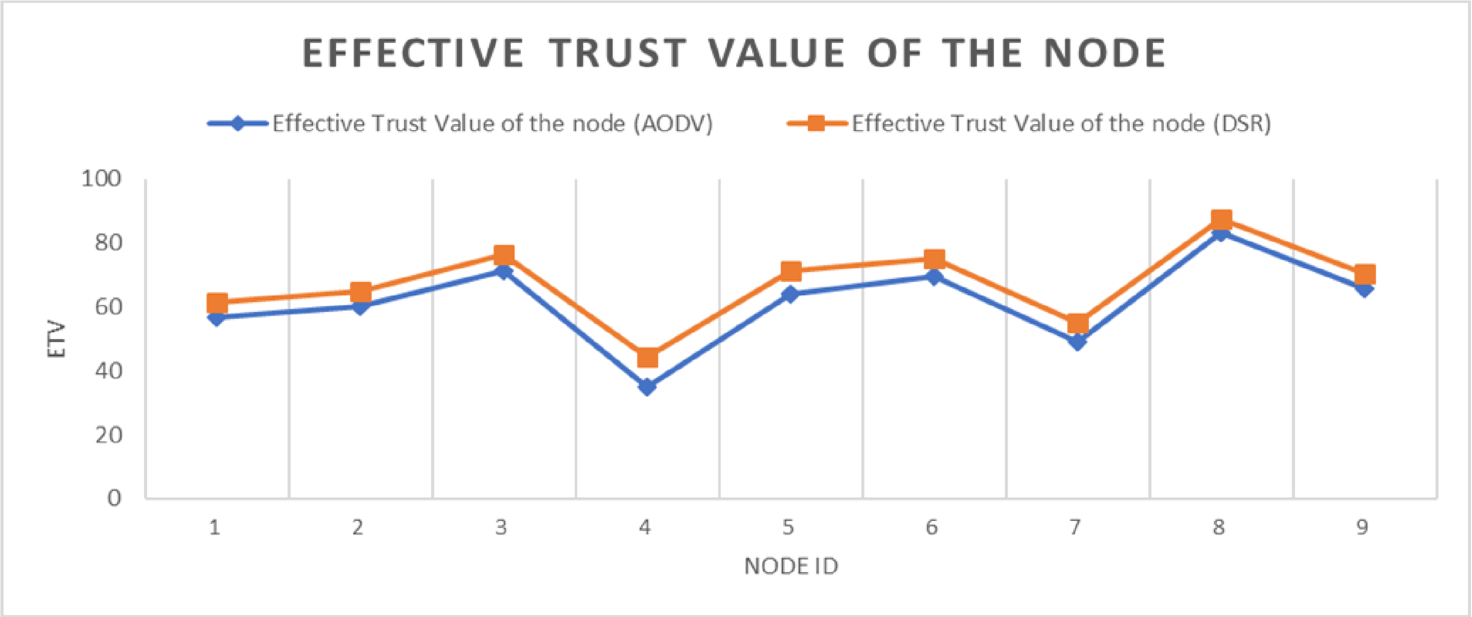


Figure 6

Effective Trust value of the nodes using AODV and DSR

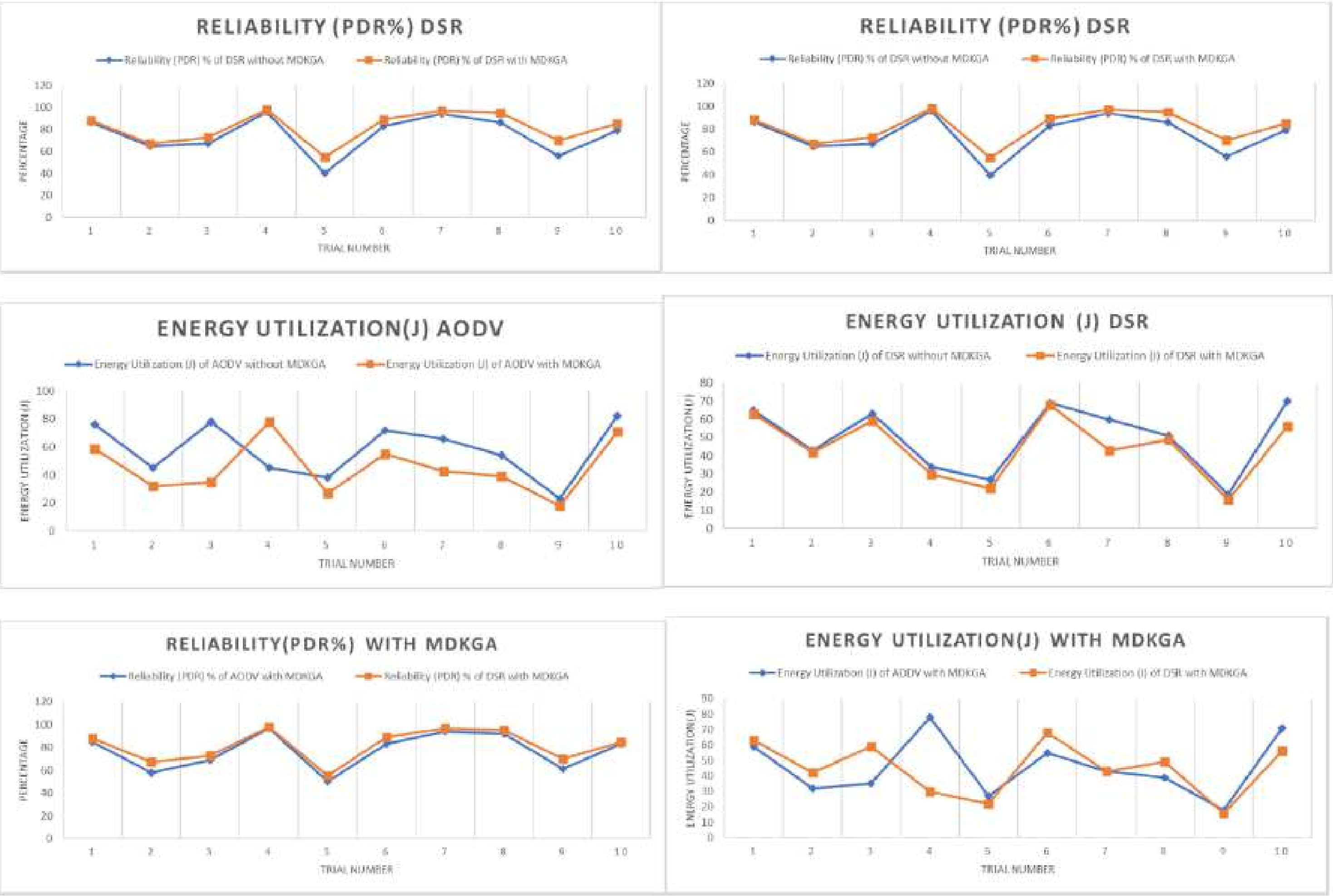


Figure 7

Comparisons of reliability (%) and Energy Utilization with and without using DKGM using AODV and DSR

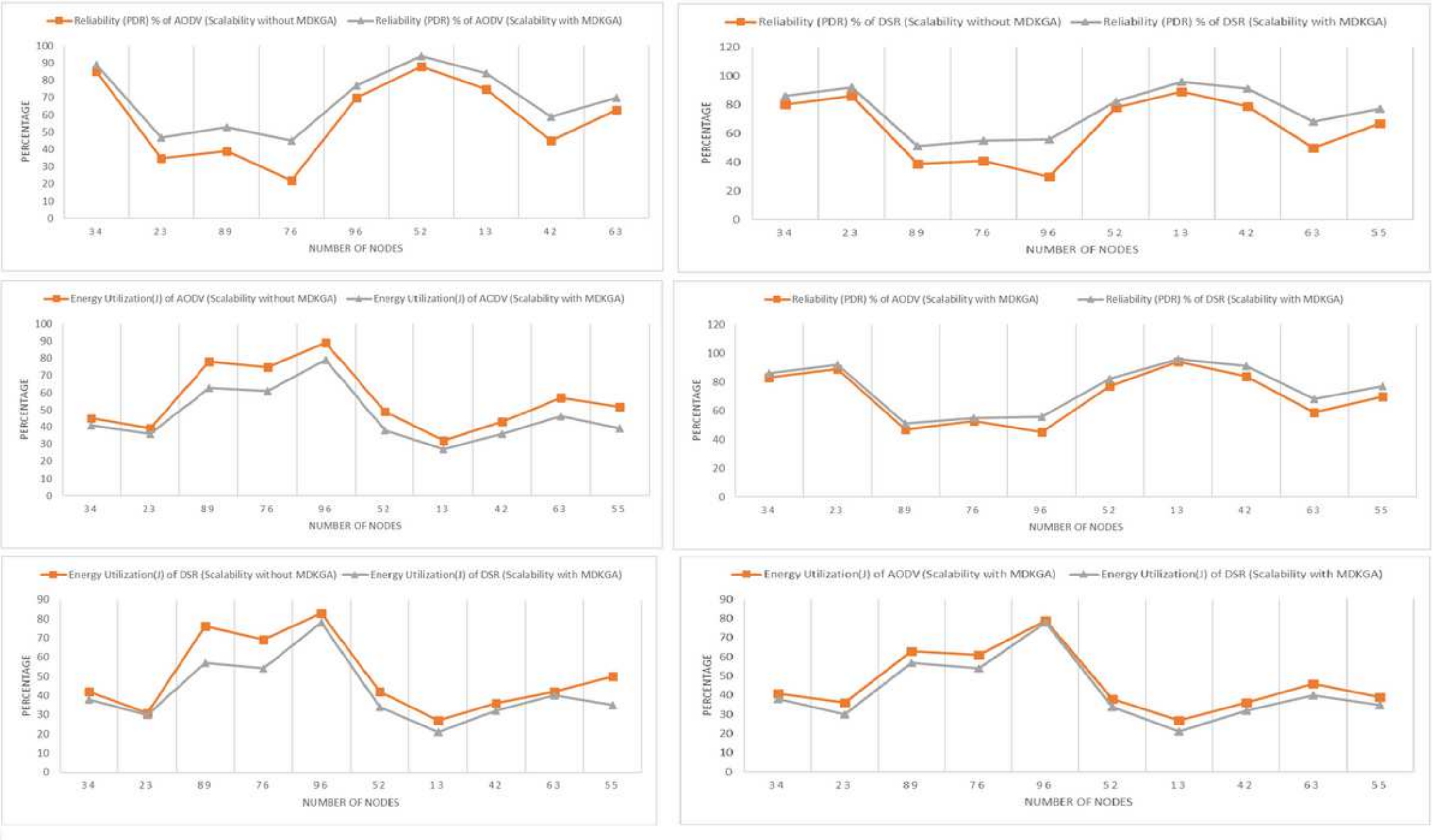


Figure 8

Reliability (%) and Energy Utilization based on scalability with and without using DKGM using AODV and DSR