International Journal of Engineering Applied Sciences and Technology, 2017
Vol. 2, Issue 5, ISSN No. 2455-2143, Pages 50-59
Published Online March-April 2017 in IJEAST (http://www.ijeast.com)

AN IMPROVED AND SECURE ROUTING USING EC-ANTSEC FRAMEWORK IN MOBILE AD-HOC NETWORK

Manisha Sharma
Research Scholar, CSE
DAVIET, Jalandhar

Parveen Kakkar
Department of CSE
DAVIET, Jalandhar

Raman Kumar
Department of CSE
I K Gujral Punjab Technical University,
Kapurthala, Punjab, India

Abstract— **Mobile ad hoc network comes in the category of wireless networks that do not require any fixed infrastructure or any base station. It is established by wireless mobile nodes. The topology of MANETs is dynamic in nature since the nodes can move randomly in any direction. Hence, due to this topology MANETs has to face various security challenges during routing and data transmission. In this paper EC-ANTSEC (Enhanced cluster based ANTSEC) framework is proposed that includes features like AODV+AntHocNet protocol, symmetric keys and clustering. Key management is an important part of any secure communication. So, in this paper a third party which is a certification Authority will generates symmetric keys using digital certificates to provide authentication check for network's nodes. This proposed work provides security to the data packets by injecting immunity packets thereby improving the packet delivery ratio, and throughput of the network and reduces the delay of the network. The main focus of this paper is to accommodate the large amount of traffic by using LmC clustering algorithm.**

Keywords— **Security, LmC, Routing, AntSec, Symmetric keys.**

I. INTRODUCTION

Previously there was a mainframe computer which is centrally located with terminals for various clients, as of now there is one or more than one computer for every individual. In Ubiquitous Computing, every individual will have numerous gadgets accessible in his or her surroundings (i.e., personal digital assistants, handheld digital devices, laptops or cell phones etc) and where power of computation will be accessible all over the place. The quality of devices of communication and ubiquitous computing makes remote systems a key answer for their collaboration. Consequently, the arena of wireless communication is developing to meet distinctive difficulties. Without a doubt, the most requested administration by versatile clients is connections of network and relating information administrations. The majority of the current associations among these devices which are wireless are based on infrastructure gave by private networks or providers of service. [1]

The popularity of wireless network in computing industry is increasing day by day. There are two types of mobile networks the one is infrastructure based network and other is infrastructure less network. In Infrastructure based network the mobile nodes will communicate with each other by using the base stations. The base stations acts as a bridge of the network. Office WLAN is one of the examples of such network. The infrastructure less network is also known as Ad-Hoc network with no fixed routers. In such network the movement and connections of the mobile nodes are random in nature. The nodes act as router that performs the functions of discovering and maintenance of route. Ad-Hoc network is useful in case if the cost of communication infrastructure is high or it is impossible to install a communication infrastructure. The Ad Hoc network is a collection of mobile nodes that form a network without the support of any central administration or pre-existing infrastructure. The nodes in such network can randomly move in any direction and organise themselves accordingly and makes the network dynamic in nature [2]. As the topology of MANETS changes rapidly that leads to various kind of security threats. In order to protect the network from such security threats various Secure Routing protocols has been invented but still sometime it becomes a challenging task to protect an open and distributed communication environment from attacks. There are various attacks and challenges that disrupt the communication process of the network like internal external attacks. Routing process in ad hoc network mainly disrupt by internal or external attackers [3]. Internal attacker basically accesses the network in an unauthentic way and stops the normal functioning of the network by changing the information that is transmitted within the network. An External attacker is an outside entity.

There is various type of attack that threatens the security of MANET. These attacks are classified in to two categories:

Active Attack: In this attack the data that is transmitted in the network is changed or destroyed by the attacker hence upset the normal functioning of the network [4]. Such type of attacks is very strict attack in MANETs that stop the network to perform reliable communication between nodes.

These attacks are divided into two sections:

- External Attack: In this attack the attackers are not the part of the network that means the attack is carried out by outside source.
- Internal Attack: In this attack the attacker accesses the network without any authentication and then stops the normal functioning of the network by changing the information that is transmitted within the network.

Passive Attack: In such type of attack the attackers listens the network communication without any authority. The passive attacks are less harmful since the hacker does not attempt to change the data that is transmitted in the network.

Hence, in order to prevent the network from such attacks major design like secure routing algorithm and other techniques like cryptography are required to making the network more secure and reliable.

II. RELATED WORK

Subbing Umamaheswari and Govindaraju Radhamani [5] proposes a secure AntHocNet framework that includes functions like ant colony based routing protocol, Artificial Immune system, Cross layer design and clustering. The security is provided by injecting immunity in data packets so that the packet delivery ratio increases and the end to end delay decreases. In this paper it is observed experimentally that the ANTSEC performed better as compare to AODV_COCA method in various scenarios.

Avita Katal et. al. [6] proposes a cluster based Datagram chunk detection and prevention technique which work efficiently if there is a datagram chunk dropping attacker in the network. The Datagram chunk dropping attack occurs in multimedia transmission. The quality of service of network is affected in this attack as the intermediate malicious node drops some data stream and decreases the throughput of the network. From the experimental results it is shown that the throughput of the network is improved by using this detection and prevention scheme. In this scheme numbers are assigned to the chunk that make easy to detect the dropping of packet. So this scheme makes the network more reliable and secure.

Wibhada Naruephiphat et. al. [7] proposes a clustering algorithm named Limiting member node. In this algorithm a cluster head is elected on the basis of a new cost function that includes residual battery, energy consumption and distance to the base station. Thus this proposed algorithm limits the number member for each cluster head. By using this algorithm, the packet delivery ratio increases while the delay time decreases efficiently. After comparing the LmC algorithm with some other methods like maximum battery clustering and minimum cost function show that it provides highest network lifetime as compare to other methods.

Ratish Agarwal et.al. [29] presented various clustering algorithm for ad-hoc network. In this paper a sequence wise classification has done for various clustering algorithm with their improvements. As nodes in MANETs changes frequently and changes the topology of network and increases the overhead ratio. The clustering algorithms keep the number of nodes with in cluster by using pre-defined threshold value. The Cluster head election helps in reducing computation and communication costs. Hence this paper provides a complete survey of different clustering algorithm.

Abdelhak Bentaleb et. al [32] discussed various clustering schemes in MANETS like topology based clustering, Mobility based clustering, Energy based clustering etc in hierarchal manner with their objective, characteristics and limitations. In this paper various clustering schemes are compared according to their performance and best clustering scheme is suggested. After the comparison they have concluded in various clustering scheme the routing overhead is high since the cluster Head changes frequently and the strength of cluster are also high. Hence they proved that the Weight based clustering approach functions well rather than ID-Neighbour, topology, mobility and energy based clustering scheme. By using this clustering scheme various goals are achieved like decreases the routing overhead, lifetime of mobile node are maximum, minimum changes in CH etc.

Aida Ben Chehida Douss et. al. [8] proposes a validation process that validates the delegation trust mobility-based clustering scheme. This scheme basically protects the Mobile ad hoc network from malicious nodes. In validation process it firstly proposes a language named Secured Clustered MANETs specification language that defines notations and semantics for the validation process and secondly checks the consistency and completeness checks for validation process. The validation process proves that DTMCA works well in every situation and there is no inconsistency in security procedures. So After validating the DTMCA scheme it i clear that this scheme makes the mobile ad hoc network more secure and reliable.

Claude Crepeau et. al. [9] presents a routing protocol named Robust Source Routing. This protocol is a secure on-demand routing protocol that helps in transferring the data packet safely from source to destination. As MANETs suffering from various security challenges so this protocol helps in reducing such challenges like dropping of data packet by malicious nodes and modification of data packet. After the experimental results it is clear that this Robust Source Routing protocol makes transmission process more reliable even if the numbers of malicious nodes are high in the network.

Panayiotis Kotzanikolaou et. al. [10] Proposes an on-demand routing protocol named Secure Multipath Routing protocol. This protocol protects the network against Denial of Service\attacks in MANETs. As various security solution has been proposed for secure routing like key agreement, intrusion detection etc. but these solutions does not prevent denial of service attack because they are applicable only for single path routing protocols. The Security concern of this protocol is based on authentication of neighbours. The use of encryption technique named public key cryptography is reducing in this protocol. Thus this protocol is capable of identifying and preventing this denial of service attack in case of multi-path Routing protocol.

S.Neelavathy Pari et al. [11] Proposes a secure protocol named Multi point Relay based Recommendation protocol. This protocol uses a trust model as well as SHA-1 key methods that detects and prevent the malicious node to enter the network. The trust value is calculated on the basis of knowledge and suggestion of the neighbouring nodes. Thus by using these trust model and SHA-1 encryption method the security of the network in MANETs increases effectively by reducing the presence of malicious node in the network. The simulation results show that the throughput of the network becomes high by using this proposed method.

Jubil Jose, Rigi C.R [12] compares the working of ad hoc on demand multipath distance vector routing protocol and describes the topology information with topology hiding multipath protocol. In this paper the topology exposure problem is proposed in order to point out the need of topology hiding in multipath routing protocol. The attackers are mostly affecting the AOMDV as compare to THMR. This paper basically figure out the need of hiding topology information in order to design the routing protocols in Mobile ad-hoc networks after the examining the various attacks and network topology.

Jie Niu [13] discusses the topology hiding multipath routing protocol and their necessity in preventing major security attacks in MANETs. Routing is major concern in mobile ad hoc network due to their unsecure routing architecture. So to overcome the challenge of security in routing the comparison of AOMDV routing protocol is done with topology hiding routing protocol to show that the effect of attackers in THMR in small degree as compare to AOMDV.

Bhuvaneswari M, Dinesh Naik [14] discussed about secure routing protocol in Manets. MANET consists of the number of mobile nodes that form a wireless communication. In MANETs the nodes can move randomly in any direction and dynamically join the network at any time which is known as self configuring network. Manet is helpful in industrial, vehicular communication and natural disaster management like flood, fire, earthquake etc. In this paper studies are done on routing protocols in order to improve their quality and efficiency. But still it lacks in security due to their characteristics. So, a algorithm is proposed that uses public key cryptographic technique to protect the protocol from various attack. Hence, Cryptography provides more security and reliability.

Waleed S. Alnumay, Uttam Ghosh [15] presented an identity (ID) based protocol that protects the AODV and TCP from various attack in MANETs. To protect AODV from attacks a Sequential Aggregate signature is used which is based on RSA. In this proposed protocol a session key is generated for each pair of source and destination node to make the data transmission process more secure and reliable. Each node in network has an unique ID which is evaluated by using public key and message Is authenticated with a signature. In this proposed technique, the id of node remain same throughout the network lifetime so that network is protected from various attacks that targeting the AODV and TCP in MANETs.

David Airehrour et. al. [16] presented a secure trust based routing protocol for MANETs. This scheme is very effective in protecting the network from malicious nodes in MANETs. In this paper a GradeTrust is proposed which is a secure Routing protocol that uses trust level of network nodes. By isolating the black hole routing attack proposed scheme provides secure data transmission and improved packet delivery ratio. The simulation results shows that Grade Trust based routing protocol provides better packet delivery ratio as compare to traditional routing protocol like AODV and FSR

Morli Pandya, Ashish Kr. Shrivastava [17] discussed discussed about the improvement in security of AODV routing protocols in MANETs. The popularity of network has motivated the development of MANETs which is a decentralized wireless system. As the network is a fast changing is known as dynamic in nature that faces various security challenges due to their characteristics. In this paper the performance of AODV reactive protocol is evaluated with their possible attacks. The two layer signature scheme is also discussed with security that contains secure hash algorithm to improve the AODV's performance. Hence the proposed scheme improves the security as well as performance of the network.

Rakesh Ranjan et al. [18] discuss various security issues occurring in MANETs. One of the major security concerns are security attacks that interrupt the normal functioning of the network like black hole attack grey hole and worm hole. In black hole attack the malicious node breaks the security of network and stops the normal functioning resulting in packet loss. Hence this paper provides various security issues that make the communication process unreliable.

M. Rmayti et. al. [19] proposes an approach which is watchdog based that uses two Bayesian filters: Bernoulli and Multinomial to detect the packet dropping attacks in MANETs. To detect the denial of service, attack the watchdog mechanism is used which is an intrusion detection scheme. By using these filters, the attacks are detected with high rate of accuracy. By using this approach, it becomes easy to transfer the data packet through a secure path from source to destination. So, this approach avoids or detects the attack that leads to denial of service. After experimental results it is proved that if the rate of malicious node is greater than 25% then Bernoulli model is used and in case of detection rate of malicious node is less than 25% then Multinomial model is used.

Albandari Alsumayt and John Haggerty [20] discuss various methods to handle the Denial of service attack. Due to the characteristic like dynamically changing network makes the MANETs vulnerable to various kinds of security attacks and one of the serious attacks is Denial of service attack. Denial of service prevents the legitimate users from accessing service and disrupts the functioning of the network. So, main aim of this paper is to provide some traditional methods with their advantages and disadvantages so that they help in designing a new method to detect and prevent this attack. The pro and cons of the current method provides various keys point that helps in handling the denial of service attack that are mainly occur in MANETs.

Quan Jia et. al. [21] proposes a secure mechanism which is based on capability known as CapMan. The main focus of this approach to prevent the Denial-of-service attacks in the network which is multipath in nature. There are two components in CapMan one is capability distribution and other is capability enforcement. In this approach the capability message is distributed among all the nodes within the routing path to maintain the throughput of the network. Thus this approach efficiently identifies and prevents the Denial of service attack in the network which is multi-path in nature. This mechanism works effectively even if the initiator and responder of the network is malicious insider. The experimental result shows that this mechanism mitigates all denial of service attack and reduces their impact during communication in the network.

Yinghua Guo and Matthew Simon [22] Discuses one of denial of service attack named distributed denial of service attack. This paper proposes a quantitative model that helps in designing the various features of ASF attack traffic to determine if there is any attack launched in the network and the time when the attack is launched. Thus this model help in protecting the network from Denial of service attack by identifying the various anomalies in the traffic so that it becomes easy to detect the DoS attack.

S.Sasirehka et. al. [23] proposes a technique that increases the security of the network named unified trust management technique. This technique detects various packet dropping attacks by calculating the trust value. There are two methods that are used in trust management scheme for calculating the trust value one is direct and other indirect observation. The trust value is calculated from neighboring node through dempster-shafer and Bayesian inference theory. The unified trust management scheme helps in enhancing the security of MANETs by increasing the packet delivery ration and decreasing the end to end delay. So the throughput of the network is improved effectively by using this technique.

Syed Jalal Ahmad et al. [24] discuss a scheme that provides security to the network by using linear block coding in MANETs. The linear block coding helps the network to detect the malicious node by creating a security code vector and by matching the code word in the network. In this scheme whenever a source node wants to transfer the data packet a security code vector is combined to the packet header and then forwarded to the next nodes in the network. The data in the network is transferred only when the security bits of current node matches with source node. Thus this approach is very efficient since it saves energy and reduces computational operations.

III. Enhanced Cluster Based ANTSEC Framework

The proposed work improves the security of Mobile ad hoc network by injecting immunity to the data packets. The EC-ANTSEC framework basically evaluate the ACO based routing protocol with improved security method. The security is improved by distributing keys to each cluster head present in the network. This framework constitutes various features like AODV+AntHocNet protocol, Symmetric keys and clustering. The main components of the framework are the cluster heads and the trusted third party. The main features includes in this framework are:

- To generate network scenario.
- To divide the network into different clusters.
- To implement key distribution algorithm where trusted third party generates key and distributed it to all cluster heads.
- To implement routing based on ant colony optimization with secure key mechanism.
- To apply the proposed algorithm and compare the results.

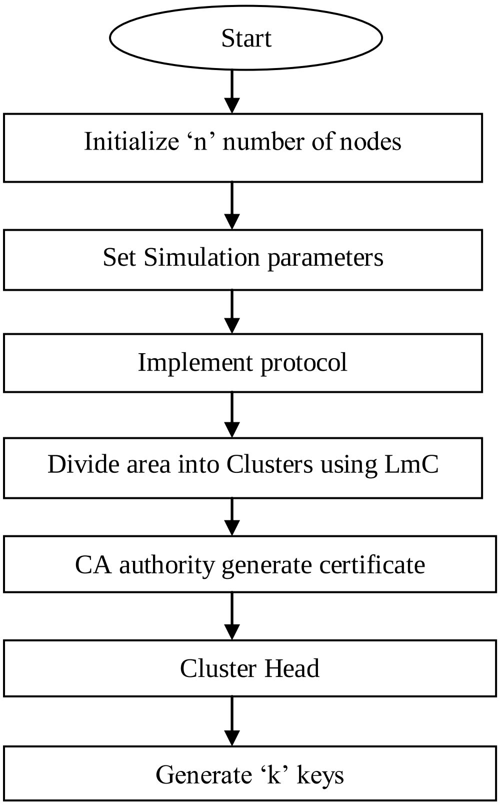
The proposed work is basically to provide a secure environment in mobile ad hoc networks. In this proposed work, the focus is on three major techniques to do the analysis. The techniques focused are clustering, key distribution and ACO to make routing more secure. This work explores solution to address few of security challenges.

BASIC DESIGN FLOW:

In this design flow firstly ‘n’ number of nodes is initialized and then it sets general simulation parameters. After that AODV+ANTHOCNET protocol is implemented. In next stage the area is divided into clusters by using LmC that is limited member node Clustering. A Certificate Authority then generate a unique certificate that includes unique keys is distributed to each cluster head. Each cluster Head distributes these unique keys to the nodes and then node will submit their key information to CA.

Pseudo Code for Proposed Algorithm:

```
Step1: Generate a network Scenario. Initialize 'n' number of nodes.
Step 2: Implement Limited member node based Clustering where n number of node distributed in 'k' clusters according to their distance. Cluster includes limited number of nodes according to total number of nodes in the area. Cluster Head selections are on the basis of cost function. Where cost is calculated on the basis of transmissions done by the node (maximum number of transmissions).
Step 3: CA Authority generates Digital Certificate and distributes it to each Cluster Head. Each Cluster Head has a unique Certificate and Certificate includes 'n' number of unique keys.
Step 4: Cluster Head distributes Keys to the nodes present in the Clusters.
Step 5: Nodes submit their Keys information to Certificate Authority.
Step 6: When Transmission starts then generate path on the basis of ANTSEC Framework.
Step 7: Calculate the Parameters on the basis of transmissions for different scenarios (n=100, n=150)
```


Start
Initialize 'n' number of nodes
Set Simulation parameters
Implement protocol
Divide area into Clusters using LmC
CA authority generate certificate
Cluster Head
Generate 'k' keys

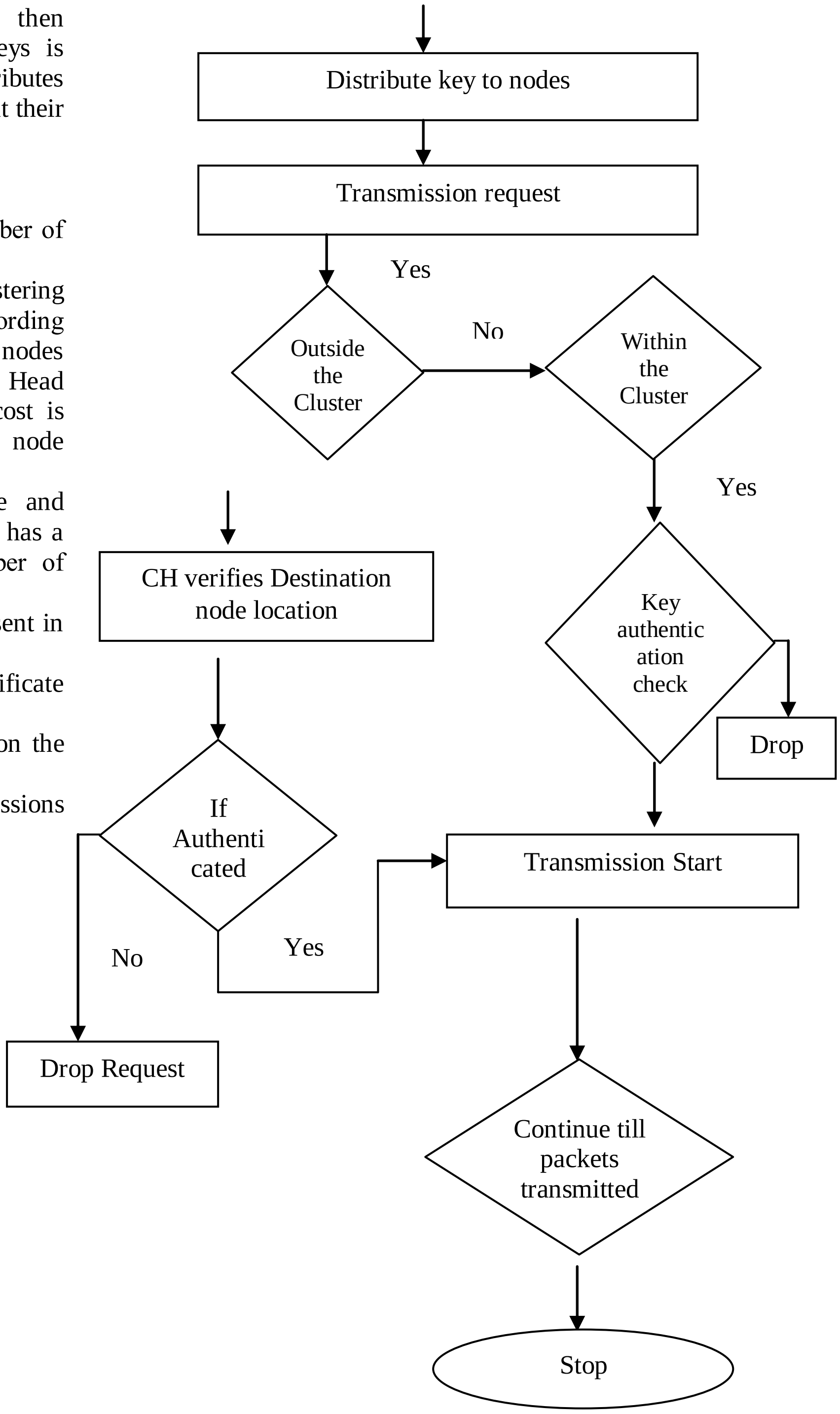


Fig. 1: Basic Flow Design

Detailed Explanation of algorithm:

The step wise detail of the proposed algorithm is explained in the following steps.

Step 1: The scenario of 100 and 150 nodes has been generated and distributed to the area of 3000*3000 m.
Step 2: Set Simulation parameter.

Table 1: Simulation Parameter

Parameter	**Value**
Channel	Wirelesss
Radio Propagation Model	Two ray Ground
Network Interface	Wireless Physical
MAC	802.11
Link Layer	LL
Antenna	Omni directional
Queue Length	50
Number of Nodes	100.150
Area	3000*3000
Routing protocol	Ant Colony Optimization
Simulation Time	2000 sec
Transmission Range	250 m
Bandwidth	3 mbps
Nodes (m/s)	0-10
Pause Time	100
Maximum Number of Packets	1000

Step 3: Implement protocol system.
Classification of routing protocol:
The classification of routing protocol is done in this section according to their characteristics. Routing protocols is divided in three parts Table Driven, Source initiated and Hybrid.

A. Table Driven Routing Protocols (Proactive)
In Proactive routing protocol each node in the network maintain a routing table that is determined in advance without requiring it and the routing table updated whenever the topology of the network changes [25]. DSDV, WRP are the best known example of the Proactive Routing Protocols in MANETs.

B. On demand Routing protocols (Reactive)
In this protocol routes are created only whenever it is required [26]. There are two phases in this protocol one is Route discovery phase and other is maintance phase. AODV DSR are best known example of Reactive Routing protocol.

C. Hybrid Routing Protocols:
The Hybrid protocol constitutes the characteristics of both the proactive and reactive routing protocols. As the parameters latency is low and overhead is large in case of proactive and opposite in case of reactive routing protocol. So, the hybrid protocol helps in recovering from such shortcoming of both reactive and proactive routing protocols [26]. ZRP is an example of a Hybrid Routing Protocol.

D. Optimized Routing protocol:
This protocol works on the basis of intelligency where it select the optimized route as per the required criteria. These algorithms will help the networks to find out the best path from source to destination. In this various algorithm were introduced which inspired by both natural phenomenas and biological phenomenas.

ACO based Routing Protocol: This is one of the optimized algorithm which is based on the behaviour of ants and determines the shortest path based on the value of pheromone. ACO is based on the foraging behaviour of ants.There are various paths from nest to food then ants randomly walk from nest to food. During their walk from nest to food they lay a chemical substance called pheromone[27]. After that the newer ants will follow that path where the concentaration value of pheromone is high and also reinforce the path they have taken So, therby they find the shortest path from source to destination.

In proposed work AODV+ANTHOCNET prtocol is used. This protocol initiated by sending a route-request packet to the neighbors of source node untill it reaches the destination node. When Destination node receives the route request packet then it wait for a default time interval that is 3 seconds. The selection of best route is done on the basis of intelligency that includes shortest path and energy of the path.The route through which the route request packet is propagated uses the same route to forward the route reply packet to the source node. After reciving the route reply packet the source node will starts the data transmission process.

Step 4: Implement Clustering:
In Clustering the network is devided into small groups which is known as cluster. The Clustering is very popular method in MANETs since it perform the managements of resource in an appropreat manner.
There are various benefits while using the Clustering in MANETs are as follows:

- Hierarchical architecture.
- Key management process.
- The resource allocation process is more efficient.
- The routing and mobility process is enhanced.

The clustering algorithm basically generates and maintains a connected cluster. In clustering techniques, nodes plays different role in a cluster are selected on the basis of certain criteria. Three types of nodes are defined in clustering are[28]:

1. Cluster head: Cluster Head acts as a local coordinator in its cluster. The functions that are performed by the cluster head are Key management, data forwarding etc. The concept of cluster head is similar to the base station concept in current cellular system. But in case of cluster head there is no need of special hardware as required in case of conventional base station concept. The selection of cluster head is among the set of stations that represents a dynamic and mobility behaviour. As the cluster heads execute more work as compare to the ordinary nodes present in the cluster so it become a single point of its failure within the cluster.
2. Gateway: Gateway nodes basically are the nodes that are positioned at edge of a cluster in a non cluster head state. Such type of nodes can listen the transmission information from another node which is located at different clusters. In order to achieve this, there should be a member of cluster that act as a neighbor of a gateway node.
3. Cluster Member or Ordinary Nodes: Ordinary nodes are also the members of a cluster. These nodes do not have any neighbors that are belonging to any member of the different clusters.

Different Clustering in Network [29]:

Lowest ID Cluster algorithm: In this algorithm the node with the minimum id is chosen as a cluster head so the node other than cluster head must have id higher than that cluster head. The gateway node must lies in the transmission range of two or more cluster heads. Gateway node mainly performs the function of routing between the clusters. In this algorithm each node is assigned with a distinct id and during communication the node broadcasts the packets to the list of nodes that it can hear.

Highest connectivity Clustering Algorithm: In this Algorithm the degree of a node is calculated on the basis of their distance from others. The node with the maximum number of neighbours has the maximum chances of elected as cluster head. The neighbours of the cluster head act as members of a cluster and also cannot take part in election process for long time. Hence the rate of change of Cluster Head is very low in this algorithm. Typically some resources are assigned to each cluster and shared by the members of the cluster that increases the traffic rate and makes the throughput of the network low.

Adaptive Multihop clustering: This is a multihop clustering scheme having a load balancing capability. Every node broadcasts the information like ID, Cluster Head ID, and status of members to other within the same cluster. On the basis of the information each mobile node has the topology information of its cluster. The gateway nodes also exchanges their information with neighbouring gateways in different clusters and also reports to the Cluster Head. The cluster members are assigned with an upper and lower bounds within a cluster. If the number of members in a cluster are low than that of the lower bound then the cluster has to merge one of the neighbouring cluster. Hence the Cluster head has to know about the cluster size of neighbouring clusters so that the cluster members in a merged cluster should not exceeded from the upper bound. In case if the members of a cluster are higher than that of the upper bound then the cluster is divided in to two clusters. Though, this algorithm hasn't provided any criteria for selecting a proper node as a cluster head.

KNN: KNN is an instance-based learning algorithm that is used for classification and regression [30]. It can also be used in estimation and prediction. This algorithm is the simplest one among all machine learning algorithms. In this algorithm a set of training data is given. The classification of new data is done by comparing it to the most similar data in the training dataset. The process of building KNN classifier involves identifying k value, the number of the most similar classes to be considered in the training dataset. It checks its nearest neighbours and then it checks for the similar pattern in the training dataset. If it gets the similar pattern then it will added that node in its own cluster.

LmC: LmC is known as Limiting member node Clustering (LmC) [7] that uses a threshold value in order to limits the number of member nodes presents in each cluster. In this scheme a cluster head is selected on the basis of a new cost function where Cost is calculated on the basis of number of transmissions done by the node. The ratio of packets delivery are high in case of limiting member node clustering (LmC) approach with high network lifetime and low delay time

Step 5: Key Generation & Distribution:
In this step CA authority generates a Digital Certificate and distributes it to each Cluster Head. Each Cluster Head has a unique Certificate and Certificate includes 'n' number of unique key. Cluster Head distribute these keys to the nodes present in Clusters and then nodes submit their keys information to CA.

Step 6: Transmission Request: When a node send route request packet, this route request packet is forwarded to every neighbour in the network then ACO based routing protocol is propagated and best route is selected based on the value of pheromone in pheromone table.

Step7: Key Authentication Check:
In this step best route selected by ACO is verified by Cluster Head. In verification Cluster Head verifies destination key in between nodes (hops) and also verify source node key to ensure that the sender which initiate request is genuine and also the destination and hops which are receiving data are genuine nodes.

Step 8: Transmission Start and Continue:
Any data packet transmitted through the network first encrypted by using ECC algorithm then only it will be transmitted.
ECC: Elliptic curve cryptography [31] uses an algebraic structure of elliptic curve over finite fields. It requires smaller keys to provide the security. This public -key cryptography technique is applied for digital signatures, encryption and pseudo-random generators. ECC works on groups of points over an elliptic curves and the security is derived by using elliptic curve discrete logarithm problem (ECDLP).

IV. RESULTS & DISCUSSIONS

This proposed framework is simulated using network simulator-2. It is discrete event simulator for networking research and works at packet level.
The parameters considered in the simulation are Packet delivery Ratio, Average Delay, Throughput.
Each mobile node in Simulation area follows the random way-point mobility model that is used for simulate the moving pattern of mobile nodes in MANET. The simulation for 100 and 150 nodes were performed in a 3000*3000 area.
The Performance metrics were used in the simulation experiment:

- PDR: It is the ratio of the number of packets received at the destination to the total number of packet sent by all sources.

$$PDR = (R_p/S_p) * 100$$

Where, R_p is total packet received and S_p is total packet sent.

- End to End delay: It includes the average delay that is caused by buffering during route discovery, latency, and retransmission by intermediate nodes etc for receiving the packet

$$D = (R_T - S_T)$$

Where, R_t is receive time and S_t is sent time of the packet.

- Throughput: It is the amount of data packets that are transferred successfully from source to destination in a particular time instance.

The performance of the proposed work is evaluated by conducting the simulations for 100 and 150 nodes and on the basis of this simulation the parameters i.e. the packet delivery ratio, average delay, and throughput is evaluated. As MANETs faces various security challenges like interference that increases delays and also reduces the throughput of the network. So to overcome this problem EC-ANTSEC that is enhanced cluster based ANTSEC framework is proposed.

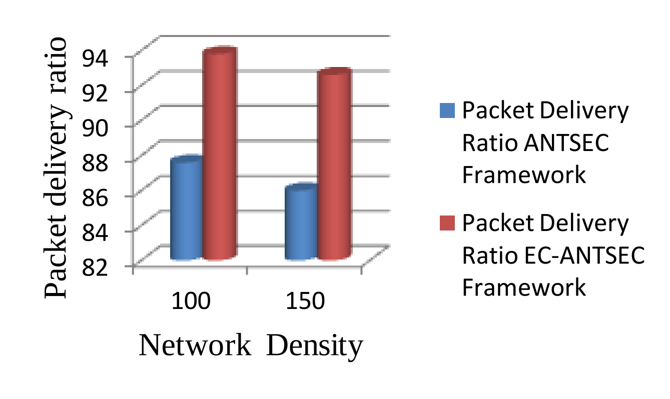


Fig 2: Packet Delivery Ratio with 100 and 150 Nodes

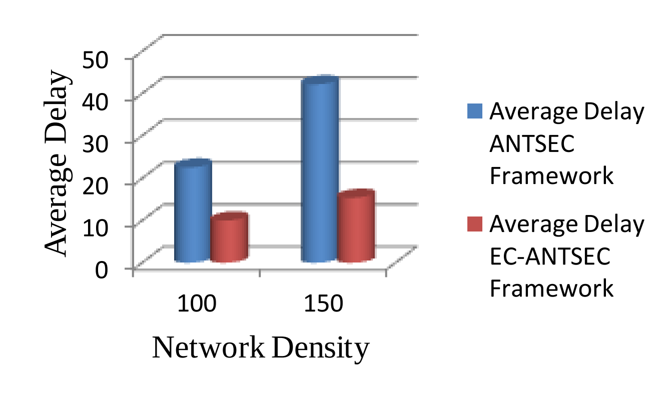


Fig 3: Average Delay with 100 and 150 Nodes

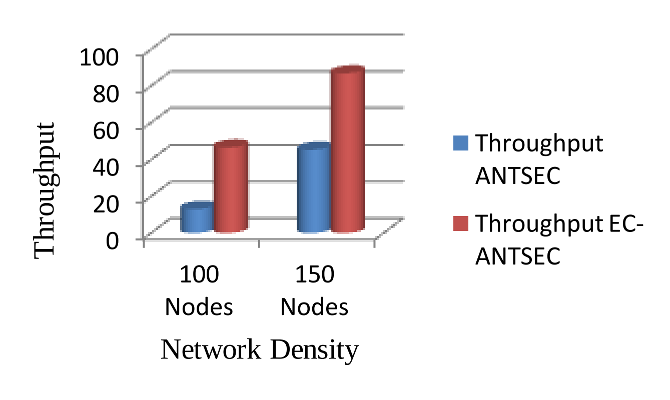


Fig 4: Throughput with 100 and 150 Nodes.

Table 2: Performance on 100 and 150 nodes

	PDR		**Delay**		**Throughput**	
Scenario	ANTSEC	EC-ANTSEC	ANTSEC	EC-ANTSEC	ANTSEC	EC-ANTSEC
100 Nodes	87.6	93.8	22.6	10	13	46.6
150 Nodes	86	92.6	42.2	15.4	45.4	86.8

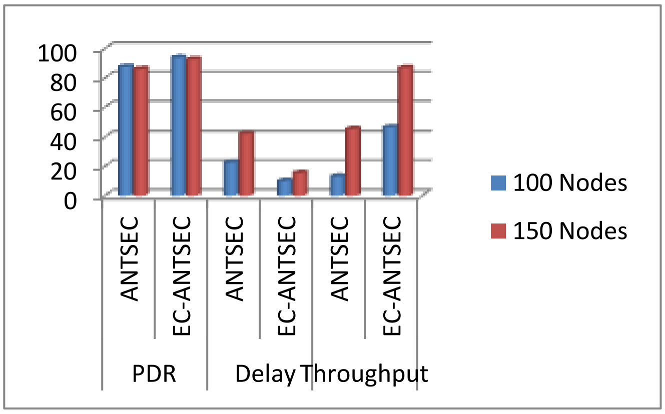


Fig 5: Comparison of ANTSEC AND EC-ANTSEC Framework with 100 and 150 nodes

The PDR, Average Delay and Throughput were evaluated by us ing two scenarios 100 and 150 nodes. The values for PDR, delay and throughput are shown in table 2 that dipicts superior performance as comapre to ANTSEC framework.

The Proposed work functions well in case if the traffic of the network is very high as in this work we have used a clustering algorithm named LmC Limited member node Clustering. LmC clustering mainly accommodate the traffic by limiting the number of nodes present in the Cluster. The proposed algorithm selects a cluster head on the basis of a cost function where cost is calculated on the basis of number of transmission done by the node. The results proof that the proposed work performs well in case of large network including the malicious node.

VI.CONCLUSION & FUTURE SCOPE

In this paper, the EC-ANTSEC framework is proposed to evaluate the ACO based routing protocol with an enhanced security mechanism using key distribution to cluster heads. This framework combines the features of the AODV+AntHocNet protocol, symmetric keys and clustering. The main components of this framework are the cluster heads and the trusted third party. So, focus of this proposed work is to provide a secure environment in mobile ad hoc networks. In order to accommodate the high traffic rate in network the Limited member node based clustering is used that limits the numbers of nodes present in the cluster according to total number of nodes in the area. Hence it can be concluded from the results that the proposed work performed better in most of the scenarios as compare to the ANTSEC method. Hence the proposed work can achieve a high rate of packet delivery with shortest delay and high amount of throughput. In Future, this proposed approach will be tested by using different simulation parameters to analyse its performance.

VII. REFERENCES

[1] Thair Khdour, Abdullah Aref, "A Hybrid Schema Zone-Based Key Management for MANETs", Journal of Theoretical and Applied Information Technology, Vol. 35, No. 2, January 2012.

[2] Sandhya Onkar Ahire, Dr. D.K. Shedge, "ECORMAN: Extended Cooperative Opportunistic Routing Scheme (CORMAN) with Efficient MAC Base Channel Reuse Technique for Mobile Ad Hoc Network (MANET)", IEEE UP Section Conference on Electrical Computer and Electronics (UPCON), IEEE, 2015.

[3] Ms.Supriya and Mrs.Manju Khari, "MANET Security Breaches:threat to a Secure communication Platform, International Journal on AdHoc Networking System (IJANS) Vol.2, No. 2, April 2012.

[4] Nishu Garg et.al., "MANET Security Issues", International Journal of Computer Science and Network security", Vol 9 No.8, August 2009

[5] Subbian Umamaheswari and Govindaraju Radhamani, "Enhanced ANTSEC Framework with Cluster based Cooperative Caching in Mobile Ad Hoc Networks" Journal of Communications and Networks, Vol. 17, No. 1, February 2015.

[6] AvitaKatal, Mohammad Wazid, R H Goudar and D P Singh "A Cluster Based Detection and Prevention Mechanism against Novel Datagram Chunk Dropping Attack in MANET Multimedia Transmission" IEEE Conference on Information & Communication Technologies (ICT), 2013.

[7] Wibhada Naruephiphat, Chalermpol Charnsripinyo, "The Clustering Algorithm for Enhancing Network Lifetime in Wireless Sensor Networks" Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing, 2009.

[8] Aida Ben Chehida Douss, Ryma Abassi, Sihem Guemara El Fatmi, "A Model for Specification and Validation of a Trust Management based Security Scheme in a MANET Environment" 10th International Conference on Availability, Reliability and Security 2015.

[9] Claude Crepeau, Carlton R. Davis, Muthucumaru Maheswaran, "A secure MANET routing protocol with resilience against byzantine behaviours of malicious or selfish nodes" 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW),2007.

[10] Panayiotis Kotzanikolaou, Rosa Mavropodi, Christos Douligeris, "Secure Multipath Routing for Mobile Ad Hoc Networks" Second Annual Conference on Wireless On-demand Network Systems and Services (WONS),2005.

[11] S.Neelavathy Pari, Sabarish Jayapal, Sridharan Duraisamy, "A Trust System in MANET with Secure key Authentication Mechanism" ICRTIT, 2012.

[12] Jubil Jose, Rigi C.R, "A Comparative Study of Topology Enabled and Topology Hiding Multipath Routing Protocols in Manets" Electrical, Electronics, Signals, Communication and Optimization (EESCO), 2015.

[13] Jie Niu, "Based on social network theory security identity authentication protocol research on MANET" International Conference on Intelligent Transportation, Big Data & Smart City, 2015.

[14] Bhuvaneswari M, Dinesh Naik, "Secure optimal routing protocol in Manets", 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), IEEE, 2014.

[15] Waleed S. Alnumay, Uttam Ghosh, "Secure Routing and Data Transmission in Mobile Ad Hoc Networks", International Journal of Computer Networks & Communications (IJCNC), Vol. 6, No. 1, January 2014.

[16] David Airehrour, Jairo Gutierrez, Sayan Kumar Ray, "GradeTrust: A Secure Trust Based Routing Protocol for MANETs", 2015 International Telecommunication Networks and Applications Conference (ITNAC), IEEE, 2015.

[17] Morli Pandya, Ashish Kr. Shrivastava, "Improvising the Performance with security of AODV Routing Protocol in MANETs", 2013 Nirma University International Conference on Engineering (NUiCONE), IEEE, 2013.

[18] Rakesh Ranjan, Nirnemesh Kumar Singh, Mr. Ajay Singh, "Security Issues of Black Hole Attacks in MANET" International Conference on Computing, Communication and Automation (ICCCA), 2015.

[19] M. Rmayti, Y. Begriche, R. Khatoun, L.Khoukhi, D. Gaiti, "Denial of Service (DoS) Attacks Detection in MANETs Using Bayesian Classifiers" IEEE 21st Symposium on Communications and Vehicular Technology in the Benelux (SCVT), 2014.

[20] Albandari Alsumayt and John Haggerty "A survey of the mitigation methods against DoS attacks on MANETs" Science and Information Conference, August 27-29, 2014,london, UK.

[21] QuanJia, Kun Sun and Angelos Stavrou" CapMan: Capability-based Defense against Multi-Path Denial of Service (DoS) Attacks in MANET" 20th International Conference on Computer Communications and Networks (ICCCN), 2011.

[22] Yinghua Guo and Matthew Simon" Network forensics in MANET: traffic analysis of source spoofed DoS attacks" 4th International Conference on Network and System Security (NSS), 2010.

[23] S.Sasirehka, S.Vijayakumar, K.Abinaya, "Unified Trust Management Scheme that enhances the Security in MANET using Uncertain Reasoning" 2nd International Conference on Electronics and Communication System (ICECS), 2015.

[24] Syed Jalal Ahmad, P. RadhaKrishna, "Security on MANETs Using Block Coding" International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2015.

[25] Patel Dhaval, Rana Arpit, "Power Aware Routing Protocol to Extend Life-Time of MANET" International Journal of Engineering Research & Technology (IJERT), 2012.

[26] Vidya Shree, P. Sophia Reena G "A Survey of various Routing Protocols in Mobile ad-hoc networks" IJCSET, 2012.

[27] Saab Ghaleb Yaseen et. al., "Ant Colony Optimization, International Journal of Computer Science and Network Security", Vol.8 No.6, June 2008

[28] Mohamed Dyabi, Abdelmajid Hajami, Hakim Allali, "An enhanced MANETs clustering algorithm based on node performances", IEEE, 2014.

[29] Ritesh Agarwal, Dr. Mahesh Motwani, "Survey of clustering algorithms for MANET", International Journal on Computer science and Engineering Vol.1(2), 2009.

[30] Shubair Abdulla et. al., "kEFCM:kNN-Based Dynamic Evolving Fuzzy Clustering Method", International Journal of Advanced Computer Science and Application Vol.6, 2015.

[31] Julio Lopez and Ricardo Dahab, "An Overview of Elliptic Curve Cryptography", 2000.

[32] Abdelhak Bentaleb, Abdelhak Boubetra, Saad Harous, "Survey of clustering Scheme in Mobile ad hoc Networks", Communication and Network,2013

[33] Raman Kumar, Manisha Sharma, "Design and Analysis of Secure Routing Protocol for Mobile ad hoc Network", SP-CRTPNFE October 2016