International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.06, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Routing and Security Enhancement in Mobile Ad-hoc network using Optimized Authenticated Routing Protocol (OA-AODV)

Dr. Gurbinder Singh Brar[1], Kirti Gupta[2]

Associate Professor, Computer Science Department,
Adesh Institute of Engineering & Technology, Faridkot
Research Scholar, Computer Science Department,
Adesh Institute of Engineering & Technology, Faridkot

ABSTRACT

With the advancement in the technology, communication becomes a very essential part of the human life and these results with the new emerging technologies like MANETs where users can communicate with each other but with infrastructure less network. MANETs are the dynamic network where topology can change with respect to time. So, the network topology becomes unstructured and node enters or leaves the network according to their need. As per considered a dynamic network, it is very difficult to maintain routing and transmission processes in this type of networks. Also there is a lack of security in this network because MANETs are vulnerable to various attacks. So, there is a need to overcome these challenges. In this paper, various challenges related to routing and security has been discussed and a new optimized authenticated protocol OA-AODV is proposed. This secure optimized protocol uses KNN clustering to handle different network areas and generates a path based on ant colony optimization mechanism. For more security, shared key mechanism is also added to this proposed protocol. Performance analysis of this proposed protocol is calculated on the basis of different parameter such as packet delivery ratio, end to end delay and throughput. Results show the performance improvement in terms of both routing and security.

Keywords *- Attacks, MANETs, Routing, Security, Optimization, Protocols, OA-AODV.*

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. Be that as it may, we are moving to the age of Ubiquitous Computing, in which one 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 MANET is a gathering of self-organizing radio gadgets. These radio nodes could be sent without necessity of any base. MANET is additionally perceived as a self-governing framework of remote hubs tho are connected up by remote associations without utilizing any current web framework. Each cell phone in this system goes about as a companion who can play out the undertaking of sending and getting information, every hub can be hosted or switch. MANET does not get any setup communication joins like a wired network; the correspondence is brought on by hubs by sending information in bundles to each other even to the goal gets that packet. [2]. the communication in MANET is completed by routing protocols. Subsequently the significant issue in the plan of MANET systems is the usage of adaptable routing protocols those can discover ways between the imparting hubs proficiently. Any routing protocol of MANET ought to be fit to hold up with the most astounding level of hubs portability as hub versatility habitually changes the topology of MANET drastically and randomly. This is likewise called as variations on link quality during communication in MANET. In this manner, joining the fluctuations in link quality because of the behaviour of broadcasting of MANET hubs brought about bearing in the exploration of remote systems administration, called, agreeable communication in MANET. [2]

1.1 ROUTING IN MANET

Routing is the procedure of selection of best path in the network so that the data is transmitted from one end to other through that path. Routing is meant for any kind of network it can be telephonic or transportation [23]. There are two steps that are involved in routing first is selection of optimal route and the second is transmission of data packets. The classification of routing protocol is done in this section according to their characteristics. Routing protocols is divided in three parts Table Driven(Proactive), Source initiated On demand Routing protocols (Reactive) and Hybrid.

1.1.1 On demand Routing protocols (Reactive)

In this protocol routes are created only whenever it is required [25]. There are two phases in this protocol one is Route discovery phase and other is maintance phase.The Route discovery phase initiate only when the node require route to its destination in the network. When the route is discovered after that route maintance phase started. AODV DSR are best known example of Reactive Routing protocol.

Ad hoc On-Demand Distance Vector (AODV)

Aodv protocol discover route to destination only whenever it is needed by source and the routes are maintained by source as long as it is needed. One of best advantage of this protocol is that the traffic problem is very less during communication along the links. In this protocol the source node start route discovery process whenever a source node wants to send a data packet to destination node by broadcasting route request to all its

neighbors[7]. When route request is recieved by its immidiate neighbours then they rebrodcast the same request to their neighbours . The process continue until the route request reaches to destination. When destination node gets the route request packet then it send the route reply to source node by using that reverse path through which it recive the route request.

II. CLUSTERING IN MANET

Clustering is the most popular method developed to provide resource management over mobile ad hoc networks .This technique based on partitioning the network in smaller and manageable group, each group called cluster. Clustering offers, several benefits when it is used with MANETs listed as follows:

- Provides hierarchical architecture.
- Performs key management
- Helps to perform more efficient resource allocation
- Enhances routing process and mobility.

The purpose of a clustering algorithm is to produce and maintain a connected cluster. In most clustering techniques, nodes are selected to play different roles according to a certain criteria.

Cluster head**:** Can be defined as a local coordinator for its cluster. It performs key management, data forwarding and many other operations. Since cluster heads must perform extra work with respect to ordinary nodes, they can easily become a single point of failure within a cluster. In our work we are using KNN Clustering.

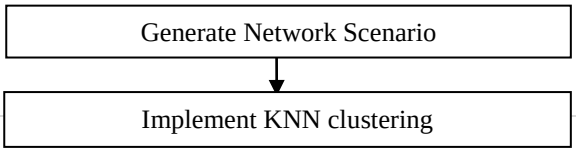
III. PROPOSED SCHEME

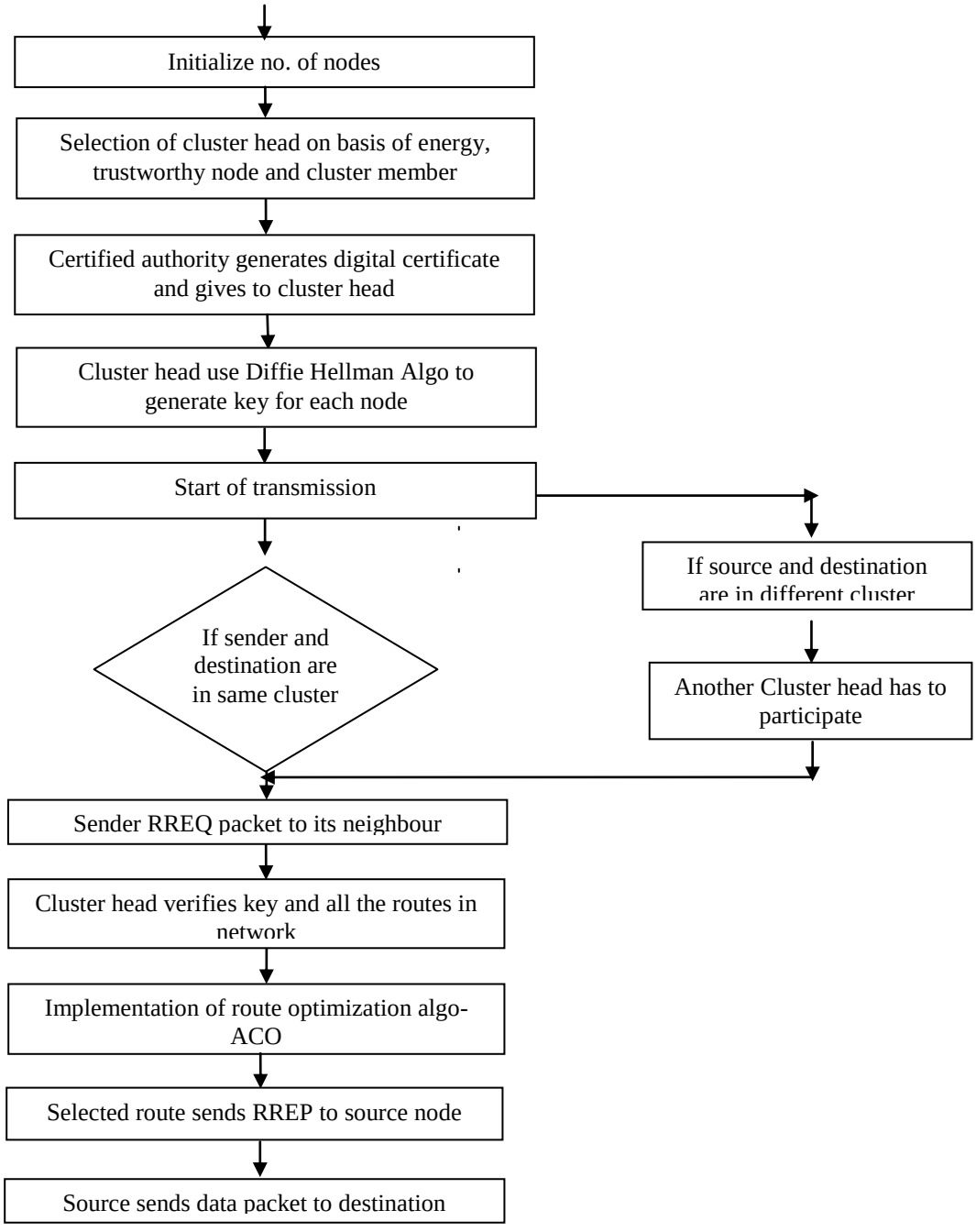
This proposed work provides security to the data packets by injecting immunity packets. The ANTSEC framework is proposed to evaluate the ACO based routing protocol with an enhanced security mechanism using key distribution to cluster heads. This framework combines the features of the Ant-Hoc Net protocol, symmetric keys and clustering. The main components of the ANTSEC framework are the cluster heads and the trusted third party. The main features include:

- To generate network scenario.
- To divide the network into different clusters.
- To implement shared key algorithm where trusted third party generates key and shared it to all nodes.
- 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, shared key mechanism and ACO to make routing more secure. This work explores solutions to address a few of the security challenges.

3.1 Flowchart





Pseudo Code for Proposed Algorithm

#start

Generate 'n' no. of nodes in the network area 'x*y'.

Implement K-mean clustering to divide the network area into k-clusters.

{

Initialize:

```
//choose 'k' random vectors to start clusters.
For i=1 to k
        J=rand (|n|)
        C[k]=n[j]
        n=n-{c[k]}
//assign initial clusters
For i=1 to |n|
        A[i]=argmax(j=1 to k) {sim(n[i],c[j])}
End
Run:
Let change=true
While change
Change=false //assume there is no change in the location of nodes
//reassign nodes to clusters
For i= 1 to |n|
        a= argmax(j=1 to n) {sim (n[i], c[j])}
        if a! = A[i]
        A[i] =a
        Change =true //recomputed clusters
        End
End
//recalculate cluster location
If change
For i= 1 to n
Mean,count=0
For j=1 to |n|
        If A[j]==i
        Mean = mean+n[j]
        count= count+1
        end
end
c[i]= mean/count;
end
end

}
```

Certification Authority (CA) is used to select cluster head and for authentication purposes. In this CA checks the previous transmission status of nodes and set as cluster head. CA generates Digital certificate and distribute it to clusters.

select s ← sender node

R ← receiver node

#start communication between s and r

#'s' sends RREQ packet to its neighbours and so on. Here ACO works for selecting optimize path.

{

Input ← ProblemSIze (Network Area), PopulationSize (number of nodes)

Start

Pbest ← CreateHeuristicSolution(ProblemSIze)

PbestEnergy← Energy (path)

Pheromone_init ← $\frac{1}{\text{ProblemSIze} \times \text{PbestEnergy}}$

Pheromone ← InitializePheromone(Pheromone_init)

While (!stopcondition())

For (i=1 to m)

S_i ←ConstructSolution(Pheromone,ProblemSize,β,q_0)

S_iEnergy ← Energy (S_i)

If (S_iEnergy ≤PbestEnergy)

PbestEnergy ← S_iEnergy

Pbest ← S_i

End

Local Update and Decay Pheromone(Pheromone, S_i, S_iEnergy,σ)

End

Global Update and Decay Pheromone (Pheromone, Pbest, PbestEnergy, ρ)

End

Return (Pbest)

}

now data will be transferred through this Pbest. Data is First Encrypted using Shared Key Mechanism then it will be transmitted.

Stop

IV.RESULTS AND DISCUSSIONS

The tool used for the simulation of results is NS-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 nodes was performed in a 1500*1000 area. The secure optimized Routing protocol is used in simulation. The Performance metrics were used in the simulation experiment.

Table1: Simulation Parameters

Parameter	**Value**
Channel	Wireless
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	150
Area	1500*1000
Routing Protocol	OA-AODV
Simulation time	2000sec
Transmission Range	250m
Bandwidth	3mbps
Nodes(m/s)	0-10
Pause Time	100
Maximum number of packets	1000

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

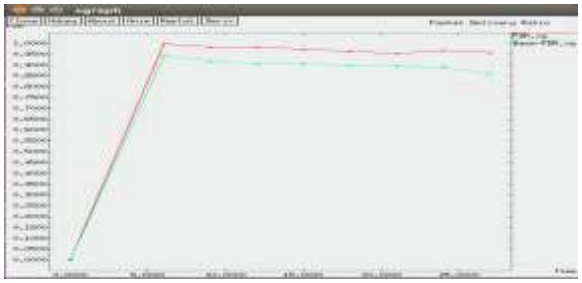


fig.1: Packet delivery Ratio with 150 nodes.

TIME	0	3	6	9	12	15	18
BASE PDR	0	0	0.9435	0.9168	0.90736	0.8963	0.8953
NEW PDR	0	0	0.9982	0.9837	0.9836	0.9735	0.9536

- 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

fig.2: Delay with 150 nodes.

TIME(s)	0	3	6	9	12	15	18	21
BASE AVG DELAY	0	0	0	0	0.0584	0.0418919	0.0418518	0.319919
NEW AVG DELAY	0	0	0	0	0.028	0.0218	0.0118	0.0119919

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

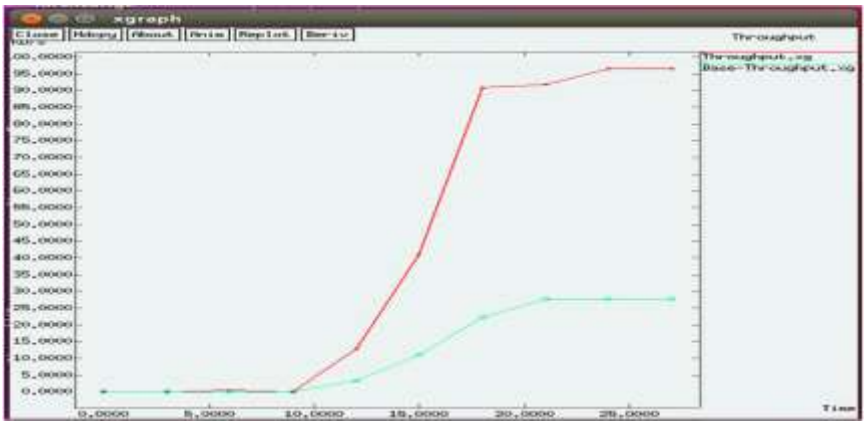


fig.3: throughput with 150 nodes.

TIME(s)	0	3	6	9	12	15	18	21
BASE THROUGHPUT(kb/s)	0	0	0	0	3.413	10.922	22.18	27.648
NEW THROUGHPUT	0	0	0.365	0	12.970	40.960	90.920	91.88

The performance of the proposed work is evaluated by conducting the simulations for 100 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 secure routing based ant colony optimization and secure shared key mechanism using KNN is proposed that helps in accommodating the high network traffic rate and makes the network more secure and reliable.

V. CONCLUSION & FUTURE SCOPE

In this paper, the secure and optimized framework is proposed to evaluate the ACO based routing protocol with an enhanced security mechanism using shared key mechanism. This framework combines the features of the Ant-hoc Net protocol, shared keys and KNN clustering. The main components of this framework are the cluster heads and the Certification authority. 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. In Future, proposed protocol is testing on high traffic scenario with varying mobility.

REFERENCES

[1] 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.*

[2] 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.*

[3] 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.*

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

[5] 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.*

[6] 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.*

[7] 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.*

[8] 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.*