Trusted Secure Routng for Mobile Adhoc Networks using Hybrid Trust Model

M.Anugraha, S.H.Krishnaveni

Abstract: **Mobile ad ho network is a self-prepared network, in which each node acts as a router. In traditional routing methods for MANETs, optimization method is not considered for security. This paper, proposes the Hybrid Trust Model (HTM) in MANETs, here optimization techniques is used that is Ant Colony Optimization (ACO). ACO algorithm provides optimization method for emerging routing algorithms for mobile ad hoc networks. This ACO algorithm, find shortest path from the initial node to neighboring nodes and it will provide key for each and every nodes. This method is realistic to the mobile ad hoc. This paper carried out of some features as well as performance analysis of the proposed ACO based DSR routing protocols. In our simulation work considering the some parameters such as connectivity, Energy, Average Delay, Overhead, Packet delivery ratio, Throughput and Storage area. The simulation result shows performance analysis of the reliable security of HTM, increase the system efficiency and improve the security in data transmission.**

***Index Terms*: Ant Colony Optimization, Dynamic Source Routing, Hybrid Trust Model, Mobile Adhoc Network.**

I. INTRODUCTION

In today's world Mobile Ad hoc Network (MANET) is a leading sort of mobile ad hoc network among other networks. Mobile means the nodes are not fixed it can move in different location in different time interval [9]. They are wireless and don't have fixed infrastructure, these nodes are self-configured. Each node act as a router as they forward traffic to other specified node in the network. So this type of network is also called as self-organized network. As a part MANET may operate as a separate manner in larger network. The nodes are highly fixed independent topology with the presence of one or more transmitter and receiver between the nodes. The main challenge of MANET is securely maintaining the routing information. This can be used in road safety, disaster, health, etc. The MANET topology, nodes mainly uses neighbor node for transmitting data. So, in today's world trust between the neighbor nodes become a major challenge. So for managing trust between nodes the routes should be securely maintained.

The trusted data delivery is a difficult duty in Mobile Ad hoc Network. In out-dated routing methods for MANETs, security is the most considerable issue that is addressed lacking optimizing the routing performance. This work, proposes the Hybrid Trust Model (HTM) in MANETs, here optimization technique is used that is Ant Colony Optimization (ACO). ACO algorithm is the optimization process that is used for emerging routing procedures in mobile ad hoc networks. This ACO algorithm finds the shortest path between type nodes in the MANET. Now a day's, finding a shortest path became a major issue in Mobile Ad hoc network. So in order to solve this issue Ant Colony Optimization (ACO) technique is used. This algorithm is normally based on Ant's behavior. When an ant moves from nest to its food it releases a chemical from its body called pheromone. The following ants will find the path by smelling the pheromone. This pheromone will form a trail in ground surface, so that the ant will find good food by following previous ants. If any obstacles appear in their path the ant will scatters and form a new path. The pheromone will only remain for short time period. During obstacle period pheromone used to find a shortest path. The difference in pheromone content between two paths over time makes the ant chooses the shortest path. In this paper, ACO algorithm finds shortest path between source node and neighbor node, ACO will provide key for each and every node. By providing key to each node, the nodes are securely maintained. The key generation also helps to avoid the data duplication, data drop, etc.

The ACO algorithm will direct the data one by one so it will take some many times to deliver the data. In order to control the time, this paper uses DSR routing protocol. This routing protocol is a self-organized routing protocol in MANET. This protocol can function with number of nodes in mobile network. If a node sends data from source to destination, it will search route during the transmission time, it does not maintain previous information about nodes for future usage. In this paper, DSR maintains channel and gateway. First the nodes will send the data to the channel. The channel will check whether the nodes are authorized are not. If it is authorized the odes send the data through the gateway, so that the time is also consumed and the data is also securely maintained. This paper carried out some of characteristics as well as performance analysis based on some parameters such as connectivity, energy, average

Revised Manuscript Received on July 05, 2019.

Ms.M.Anugraha, Research Scholar ,Computer Science & Engineering, Noorul Islam University, Kumaracoil, India.

Dr.S.H.Krishnaveni, Associate Professor, Computer Science & Engineering, Baselios Mathew II College of Engineering , Kollam, *APJ Abdul Kalam Technological University* India.

delay, overhead, packet delivery ratio, and throughput and storage area. The performance analysis of the Trust Management by reliable security of HTM results shows in increase of system efficiency and improves the security in data transmission.

II. OPTIMIZATION TECHNIQUE IN MANET

MANET securely maintains the routing information. But maintaining trust between nodes is challenging issue in this work, so these issues are detected and evaluated by Hybrid Trust Model. By the use of Ant Colony Optimization (ACO) method, the nodes will send the data one by one to the destination via neighbor nodes in a shortest path. So during this transmission it takes many times to transfer the data, so to overcome this Dynamic Source Routing (DSR) protocol was introduced. DSR maintains channel and gateway, so the authenticated data will send to the gateway and then to the destination through a shortest path. By the ACO method, the source node generate AES key for each node, the key of each node is known only for source and destination. This key is used to avoid data drop and data duplication.

A. Ant Colony Optimization (ACO)

ACO algorithm provides optimization method for emerging routing algorithms in mobile ad hoc networks. This ACO algorithm finds the shortest path between source node and neighbor node. Now a day's, finding a shortest path became a major issue in MANET[11]. So in order to solve this issue ACOmethod is used. ACO technique is normally based on Ant's performance. When an ant moves from nest to its food it releases a chemical from its body called pheromone. The following ants will find the path by smelling the pheromone. This pheromone will form a trail in ground surface, so that the ant will find good food by following previous ants. If any obstacles appear in their path the ant will scatters and form a new path. The pheromone will only remain for short time period. During obstacle period pheromone used to find a shortest path. Finding a shortest path from nest to food

It is the experimental optimization algorithm which provides approximate solution to the complex optimization issues. ACO normally based on the Ant's behavior, which gives the existing results for the optimization problem. But in dynamic network, this technique admits a high version to variations in MANET outline. However in this type of networks, the connection will change due to the moving nodes.

B. Dynamic Source Routing(DSR) protocol

Dynamic Source Routing protocol is a self-organizing routing protocol for MANETs. From fig 5, this protocol can function with number of nodes in mobile network. By human administration the dynamic source routing network can independently organize or configure itself. If a node wants to send information, at that time it goes for searching route. It does not maintain any information for future usage.

In DSR each initial node communicates the packet to the particularend point. Two main components are described in DSR they are Route Discovery and Route Maintenance. Route discovery is the change of route during transmission; network condition changes as loop-free these remains optimum path transmission ensuring the Route maintenance.

C. AES Key Generation

Key generation is the process of generating keys for secure delivery of data. It includes key algorithms such as DES and AES and public key algorithm such as RSA. This work uses AES (Advanced Encryption Standard) as a key for secure transmission of data.

AES algorithm performs number of transformations and the data's are stored in an array, such a way the rounds are repeated. The rounds are specified by key length.

Symmetric key ciphers like AES are suitable for encrypting the actual data because they require less resource and are also much faster than other ciphers. AES uses same key for encryption and decryption, so the sender and destination node should use the same secrete key.

III. HYBRID TRUST MODEL

In current scenario, the communication in mobile Ad hoc network occurs in different manner. The network may have a fixed infrastructure like base station, access point, etc. [9]. In this type the devices will send the data to the base station then it will send to the destination. But if the network does not have any fixed infrastructure, each node act as access point and perform their on process this type of noes are said to be as self-organized nodes. In this many problems will occur like packet drop, delay, energy, overhead, throughput, packet delivery ratio, connectivity, malicious attackers, etc. So these issues are detected and evaluated by Hybrid Trust Model. By the use of Ant Colony Optimization (ACO) method, the nodes will send the data one by one to the destination via neighbor nodes in a shortest path. So during this transmission period due to any misbehavior there may be a possibility of having a packet drop and also it takes many times to transfer the data, so to overcome this Dynamic Source Routing (DSR) protocol was introduced. DSR maintains channel and gateway, here one node act as channel for two or more nodes in which the nodes will send the data to the channel, it will check whether the data is authenticated or not. Another one node will act as gateway, so the authenticated data will send to the gateway and then to the destination through a shortest path. By the ACO method, the source node generate AES key for each node, the key of each node is known only for source and destination. By the key generation the data's are securely maintained. This key is used to avoid data drop and data duplication.

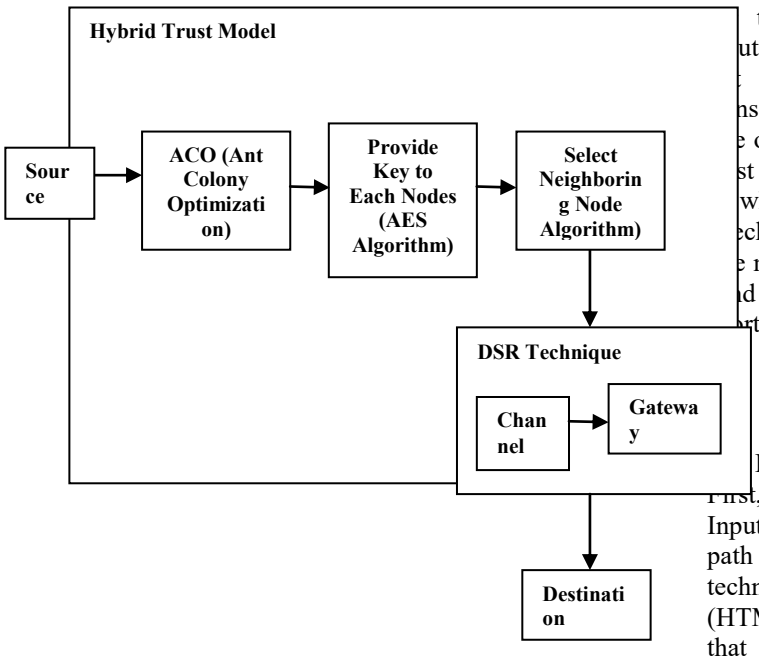

Figure1: Architecture of Hybrid Trust Model

Figure1 shows that the initial ants to transfer the data to the endpoint. If the endpoint is neighbor to the initial node, then it can have a straightinteraction, if not it uses an intermediary node for transferring the data. Due to the dynamic behavior, trusting a node is a difficult task in mobile ad hoc network. So, this work intends a Hybrid Trust Model. In this Ant Colony Optimization (ACO) is used so that it creates a shortest path and sends the data one by one. It takes more time to transfer the data and also traffic occurs during transformation. So, to overcome this Dynamic Source Routing (DSR) protocol was used, it generates channel and gateway which helps the data to reach the destination in a given time period. By ACO, the source node generate key for each node so that the data is securely maintained.

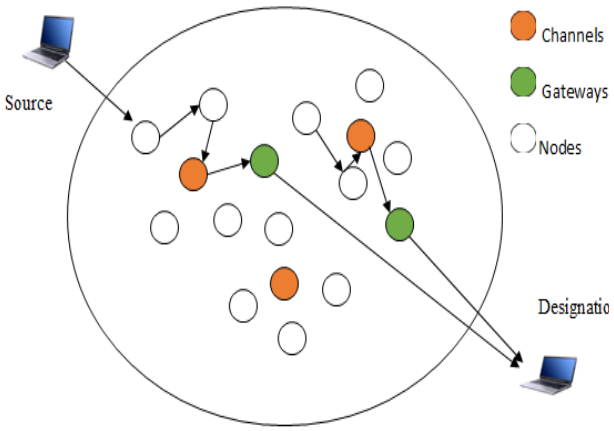

Figure2: Data Transaction

Figure 2 explains the transaction process from initialdevice to endpointthrough intermediary devices. In this type of network, each node does not have any history of a node ie., previous experience about a node. During transaction period only it collects the information based on some parameters like delay, throughput, packet delivery ratio, connection, energy, etc and these are stored in cache temporary usage. Here based on Dynamic Source uting protocol, the transaction between nodes is carried by channel and gateway. Channel refers to as a nsaction medium. It is used to convey information from or several senders to one or several receivers. In hybrid st model one node act as channel for two or more nodes which the nodes will transfer the packet to channel, it cks whether the packet is authenticated or not. Another node will act as gateway. So the authenticated data will d to the gateway and then to the destination through a rtest path.

RESULT AND DSCUSSION

Figure3demonstrations a flow chart for overall method. First, mobile devices are ordered in a diverse atmosphere. Input node is considered as a source node and the shortest path is created for transferring the data by using ACO technique. This paper, proposes the Hybrid Trust Model (HTM) in MANETs, here optimization techniques is used that is Ant Colony Optimization (ACO). ACO algorithm provides optimization method for emerging routing algorithms for MANET. This ACO algorithm, find straight path from the initialdevice to neighboring devicesand it will provide key for each and every devices. This method is applied to the mobile ad hoc. This paper carried out of some features as well as performance analysis of the proposed ACO based DSR routing protocols. In our simulation work considering the some parameters such as connectivity, Energy, Average Delay, Overhead, Packet delivery ratio, Throughput and Storage area. The simulation result shows performance analysis of the reliable security of HTM, increase the system efficiency and improve the security in data transmission.

The Hybrid Trust Model is executed in NS2 to attainimprovedenhanced data broadcast using ACO-DSR algorithm. The ACO technique is used to obtain the optimized-path. It will send the data one by one so it takes so much time for transferring the data through a shortest path and AES key for trusted communication in MANET. DSR maintains channel and gateway. First the nodes will send the data to the channel. The channel will check whether the nodes are authorized are not. If it is authorized the nodes send the data through the gateway, so that the time is also consumed and the data is also securely maintained.

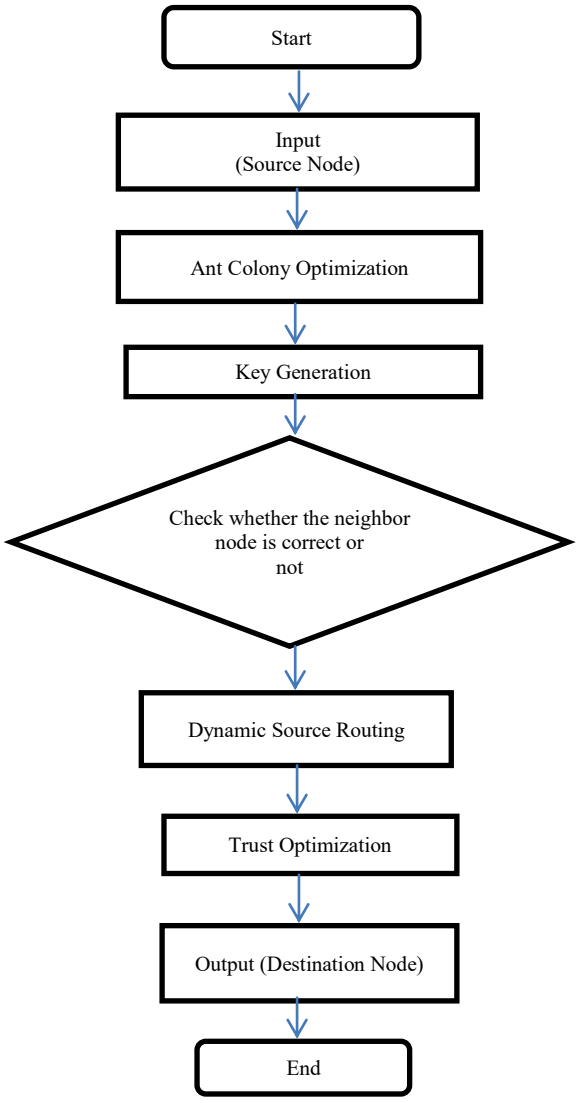

Figure3: flow chart of Hybrid Trust Model

Hybrid Trust Model delivers the packet trustfully by securing the routing [17]. The parameters are compared with existing methods.

a. Connectivity

Wireless network uses wireless data connection between network nodes. Most of the issues that occur in network due to connectivity are

- Node Failure
- Weak Points
- Link Failure
- Battery Failure

Node or device failure means individual nodes fail to operate when they lose touch with the network. This can occur due to the event of hardware or software failure, also due to the loss of network connectivity. Link failures can be caused by equipment problems due to switch or router, power failure.

b. Energy

Energy is termed as the ability to do work. Wireless network mainly uses battery as an energy source.

$$\text{Energy} = \frac{\min\_ttl \times \min\_energy}{Hopcount} \quad (1)$$

In this formula, min_ttl is minimum time to live of links in the path, min_energy is minimum energy of the path nodes and Hop count is path length.

Number of Nodes	Energy	
	AODV	ACO
10	0.1743	0.3238
20	0.3245	0.6398
30	0.4870	1.1035
40	0.6453	1.9645

Table No: 1 Energy

In above table no 1 the X axis denotes the communication range and the Y axis denote the number of nodes. Here energy is described by the amount of energy source (eg., battery) used for each node with in a communication range for the communication. Energy is compared between AODV and ACO. They are measured in form of miliseconds. The below graphical figure 4 demonstrates that by using ACO, the given energy is used by number of nodes with in a communication rage for transmitting data.

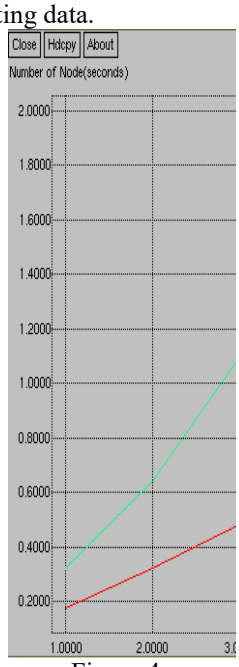

Figure 4: Comparison between

ACO and AODV for Energy

c. Average Delay

Delay means to cause to be late during data transmission. Network delay is an important design and performance characteristics of a network [10]. The delay in network specifies how long it takes for a data to travel across the network from one node to another node. Delay is measured in fraction of seconds. Delay may differ slightly, depending on the pair of node where is located.

$$\text{Average Delay}=\frac{Sum\ of\ all\ packets\ Delay}{Total\ No.of\ Received\ Packets} \quad (2)$$

Number of Nodes	Average Delay	
	Transmission time	Delivery Packet
10	0.1743	0.2456
20	0.3245	0.3343
30	0.4870	0.6543
40	0.6453	0.5245

Table No 2: Average Delay

In above table no 2 the X axis denotes the number of nodes and the Y axis denotes the delivery delay of packet [19]. Average Delay is compared between Transmission time and Delivery packet. They are measured in form of milliseconds. The below graph figure 5 shows that a node delivers the packet in a given transmission time interval but due to delay it takes more time to deliver data.

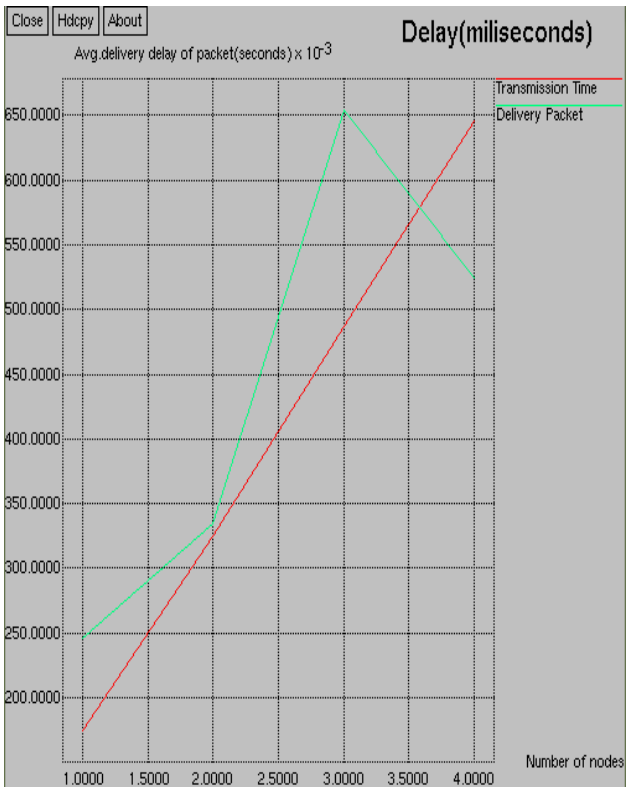

Figure5: Comparison between Transmission Time and Delivery Packet for Average Delay

d. Routing Overhead:

The Routing overhead denotes to the time that is needed for transmitting the data in MANET.

$$\text{Overhead}=\frac{Data\ packets\ Received}{Control\ packets\ generated} \quad (3)$$

Number of Nodes	Routing Overhead	
	AODV	ACO
10	0.1743	0.3238
20	0.6245	0.6398
30	0.3870	1.1035
40	0.2453	1.9645

Table No 3: Routing Overhead

In above table no 3 the X axis denotes the number of nodes and the Y axis denotes the Routing Overhead. Here Routing Overhead is compared between ACO and AODV. They are measured in form of milliseconds. The below graph figure 6 shows that by using ACO model there is increase in routing overhead for a set of nodes in a network.

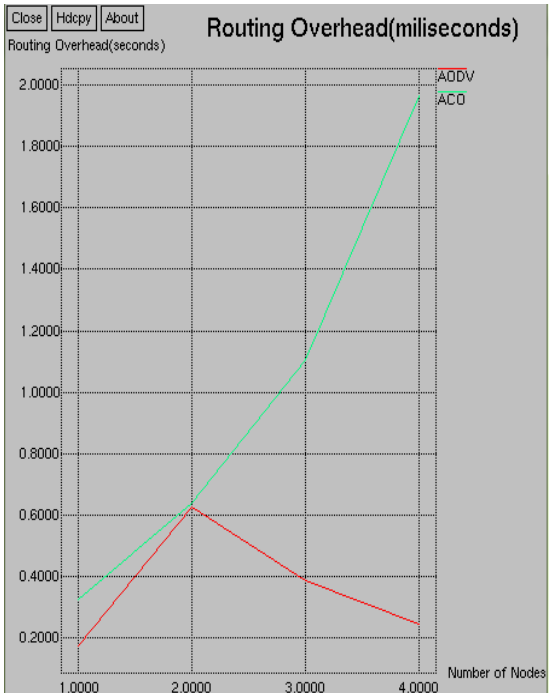

Figure6: Comparison between ACO and AODV for Routing Overhead

e. Packet Delivery Ratio

Packet delivery ratio (PDR) is defined as the portion of number of packets delivered in conflict of the number of packets sent.

$$\text{Packet delivery ratio} = \frac{Received\ Packets}{Send\ packets} \times 100 \qquad (4)$$

Number of Nodes	Packet Delivery Ratio	
	AODV	ACO
10	0.1743	0.2456
20	0.3245	0.1343
30	0.4870	0.3543
40	0.6453	0.5245

Table no 4: Packet Delivery Ratio

In above table no 4 the X axis denotes the execution time and the Y axis denotes the ratio of packet delivery. It is compared between ACO and AODV. They are measured in form of milliseconds. The below graph figure 7 shows by using ACO, the data reaches the destination within a short time period. For example, if data want to reach destination in a minutes it takes only seconds to transfer the data.

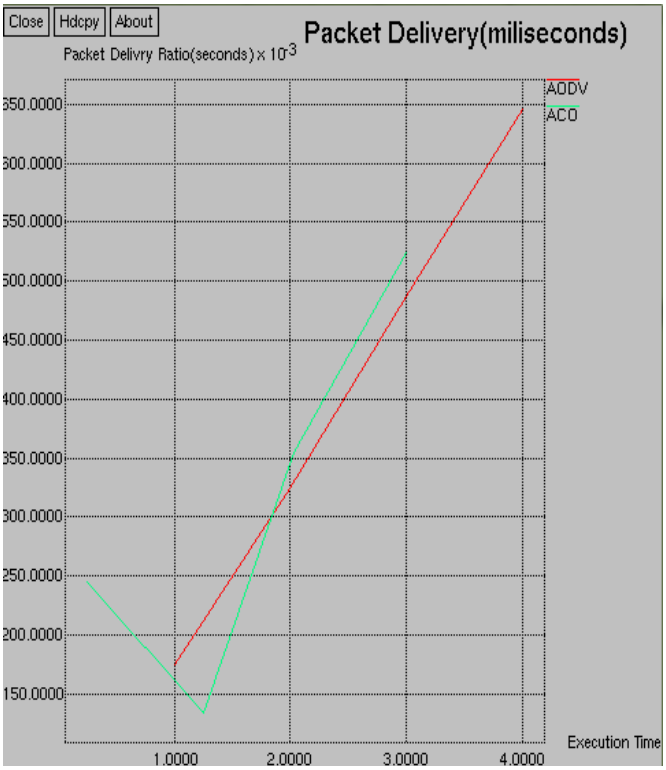

Figure7: Comparison between ACO and AODV for Packet Delivery Ratio

f. Throughput

Throughput is normally represented as average and measured in bits per second (bps). The high ratio of unsuccessful message delivery leads to lower throughput. Throughput indicates the level of successful packet delivery from one point on the network to another [20].

$$\text{Throughput} = \frac{Total\ Number\ of\ packet\ delivered\ Successfully}{Total\ Number\ of\ Internal} \qquad (5)$$

Number of Nodes	Throughput	
	AODV	ACO
10	0.1743	0.4543
20	0.3245	0.1856

30	0.4870	0.6432
40	0.6453	0.1987

Table no 5:Throughput

In above table no 5 the X axis denotes the number of nodes and the Y axis denotes the throughput. Throughput is compared between ACO and AODV. They are measured in form of milliseconds. The below graph figure 8 shows comparing with AODV, ACO's processing time is better. Processing time is low, so the data will reach soon to destination.

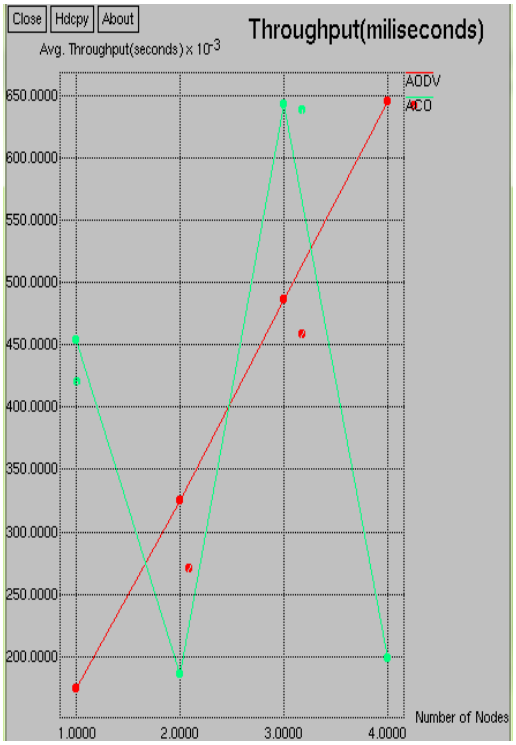

Figure8: Comparison between ACO and AODV for Throughput

V. CONCLUSION

This paper proposed the Hybrid Trust Model (HTM), in ACO method has been generate the key values in each nodes by using the RNG (Random Number Generator) as the identify the malicious nodes. From the proposed method improve some parameters such as connectivity, Energy, Average Delay, Overhead, Packet delivery ratio, Throughput and Storage area. Here NS-2 simulation is used; it will provide the good system performances, less execution time and improves the different types of parameters in MANET environment. In future any other optimization techniques or routing protocols are developed for security propose in the data transmission time and improve the system performance.

REFERENCES

[1]. AnjaliAnand; HimanshuAggarwal; RinkleRani,"Partially distrib uted dynamic model for secure and reliable routing in mobile ad hoc networks", *IEEE Journal of Communications and Networks*, Vol.18, pp.938-947, 2016.

[2]. BanothRajkumar, Dr.G.Narsimha, "Trust Based Certificate Revocation for Secure Routing in MANET", 2nd International Conference on Intelligent Computing, Communication & Convergence, Vol.92, pp.431-441, 2016.

[3]. CHEN Xi1,3, SUN Liang2, MA JianFeng 3, MA Zhuo, "A Trust Management Scheme Based on Behavior Feedback for Opportunistic Networks", *Network Technology and Application*, pp.117-129, April 2015.

[4]. Debjit Das, KoushikMajumder,and AnuragDasgupta, "Selfish Node Detection and Low Cost Data Transmission in MANET using Game Theory", *Procedia Computer Science,* Vol.54, pp. 92-101, 2015.

[5]. DipikaSarkar, SwagataChoudhury, "Enhanced-Ant-AODV for optimal route selection in mobile ad-hoc network" *Journal of King Saud University – Computer and Information Sciences*, 2018.

[6]. J. Sengathir , R. Manoharan "Exponential Reliability Coefficient based Reputation Mechanism for isolating selfish nodes in MANETs", *Egyptian Informatics Journal* , Vol.16, pp.231–241, July 2015.

[7]. J. Sengathir, R. Manoharan, "Laplace Stleltjes Transform based Conditional Survivability Coefficient Model for mitigating Selfish Nodes in MANETs", *Egyptian Informatics Journal* , Vol.15, pp.149–157, Aug 2014.

[8]. Jin-Hee Cho, Ing-Ray Chen,"On the tradeoff between altruism and selfishness in MANET trust management", *Ad Hoc Networks*, Vol.11, pp.2217-2234, Nov 2013.

[9]. M. Anugraha, S. H. Krishnaveni. "Recent survey on efficient trust management in mobile ad hoc networks", 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT), 2016.

[10]. Malik N. Ahmed, Abdul Hanan Abdullah, Hassan Chizari, OmprakashKaiwartya, "F3TM: Flooding Factor based Trust Management Framework for secure data transmission in MANETs", *Computer and Information Sciences*, Vol 29, pp. 269–280, 2017.

[11]. Mukesh Kumar Garg, Neeta Singh, PoonamVerma, "Fuzzy rule-based approach for design and analysis of a Trust-based Secure Routing Protocol for MANETs",*International Conference on Computational Intelligence and Data Science*, Vol.132, pp.653-658, 2018.

[12]. P.B. Velloso, R.P. Laufer, D. de O Cunha, O.C. Duarte, G. Pujolle, "Trust management in mobile ad hoc networks using a scalable maturity-based model", *IEEE Trans. Netw. Serv. Manage*, Vol. 7, No. 3, pp. 172–185, Sep 2010.

[13]. Radha Krishna Bar, Jyotsna Kumar Mandal, "QoS of MANet Through Trust Based AODV Routing Protocol by Exclusion of Black Hole Attack" *International Conference on Computational Intelligence: Modeling*

Techniques and Applications CIMTA), pp. 530 – 537, 2013.

[14]. Radu-IoanCiobanu,CiprianDobre , MihaiDascălu, ŞtefanTrăuşan-Matu, ValentinCristea, "SENSE: A collaborative selfish node detection and incentive mechanism for opportunistic networks",*Journal ofNetwork and Computer Applications*, Vol 41, pp.240-249, May 2014.

[15]. Rajesh Kumar M, SudhirK.Routray, "Ant Colony Based Dynamic Source Routing For VANET", *International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, pp. 279 – 282, 2016.

[16]. Saju P John , Philip Samuel, "Self-organized key management with trusted certificate exchange in MANET",*Ain Shams Engineering Journal* Vol.6, pp.161–170, Mar 2015.

[17]. ShubhajeetChatterjee, Swagatam Das, "Ant colony optimization based enhanced dynamic source routing algorithm for mobile Ad-hoc network" *Information Sciences*, Vol 295, pp 67-90, 2015.

[18]. SinaShahabi, MahdiehGhazvini, "A modified algorithm to improve security and performance of AODV protocol against black hole attack" *Wireless Netorks*, Vol 22, pp 1505–1511, July 2016.

[19]. Sreevidya R C, Nagaraja G S, "Secure Multicast Routing for Wireless Sensor Networks using ACO-AODV with DHKE Cryptosystem*", International Conference on Computing Methodologies and Communication (ICCMC),*pp. 733 – 737, 2018.

[20]. ZhongLuo, Liuzheng Lu, "An Ant Colony Optimization-based Trustful Routing Algorithm for Wireless Sensor Networks" *International Conference on Computer Science and Network Technology (ICCSNT)*, pp.1128-1131, 2015.

AUTHORS PROFILE

Ms M.Anugraha received the ME Degree in Computer and Engineering from Noorul Islam University, Kumaracoil. She is a Research Scholar at Noorul Islam University Her research interests include Trusted data transmission in MANET.

Dr.S.H. Krishna Venireceived her M.E. Computer Science and Engineering from Anna University and Ph.D. Computer Science and Engineering M.S. University. Presently he is working as Associate professor in CSE department ofofBaselios Mathews II College of Engineering , Kollam, Kerala. He has 15years of diverse experience in teaching, Life member of ISTE, and IEEE Member. Her Research interests in Image processing, network Security , Data Mining and Soft Computing.