International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

Distributed certificate authority based trusted ad-hoc vector routing protocol in wireless mesh network.

Shalini Maurya[1] , Rishi Srivastava[2]

[1] *C.N Student, Dept of CSE, BBDU, U.P (Lucknow), India*
[2] *Assistant professor, Dept of CSE, BBDU, U.P (Lucknow), India*

Abstract - *Wireless mesh network is a technology that has evolved in recent years and fits well in today's technological needs. Shared nature of wireless medium, diversity nodes and static nature of multiple paths between source and destination nodes makes challenging task for wireless mesh network when time delay, network performance, and packet overhead taken into consideration. In wireless mesh network security is the major problem in routing packets from source to destination so will use trusted ad-hoc on demand vector routing protocol.*

Keywords: wireless mesh network, wireless mesh architecture, mesh clients, mesh routers, security attacks, security services, distributed certificate authority, trusted adv.

1.INTRODUCTION

Wireless mesh network is an eminent wireless networking technology. Wireless mesh network is a multihop, peer to peer wireless communication network which is made up of radio nodes organised in a mesh topology. It has the ability to cover a wide geographical area. Wireless mesh network composed of mesh clients and mesh routers. Mesh routers forward traffic peer to peer. Mesh routers have additional routing functionalities such as gateway and repeaters to support mesh networking. Mesh routers are fixed and static. On the other hand, mesh clients are dynamic, as mesh clients changes its position. Mesh clients are such as laptops, desktop/pc, etc.
Wireless mesh network is a kind of wireless multihop radio network whose promotion and deployment depend heavily on security issues relative to cable network and WLAN.

Many security schemes have been recommended in order to protect the routing information or data packets during communication. However most of the schemes presume that there are trusted third parties or centralized servers that are responsible for issuing digital certificates and keys or monitoring the behaviour of other nodes. Some scheme distributes the function of servers into each node of the network that introduces the significant performance overhead.

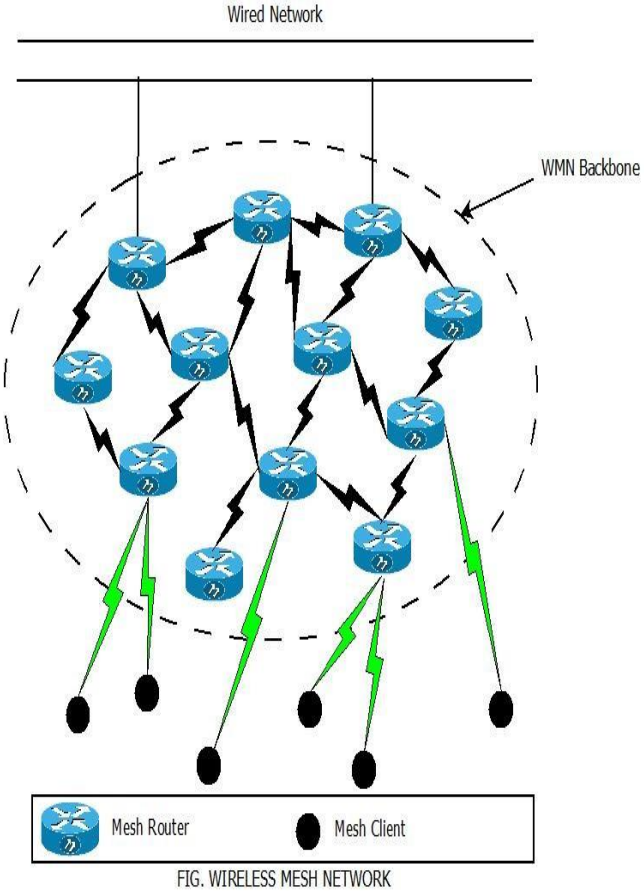


FIG-1: Wireless Mesh Network

In this paper, a trusted ad-hoc routing vector protocol is proposed which is based on distributed certificate authority and RSA public key cryptosystem concept. In order to provide trust between each node we need a self organised, light weighted security scheme for wireless mesh

network. The nodes are encrypted by the RSA algorithm for sharing of key between nodes also the certificate authority is distributed to the nodes by sending the copy of the certificate authority to the server. Server then distributed the certificate to the nodes and sends the packets to the nodes. In order to provide secure transmission of packets we proposed a trusted ad-hoc routing vector protocol which will provide trust between the nodes while communicating.

The rest of the paper is organised as follows: In section 2, we have discussed the architecture of wireless mesh network. In section 3, we discussed the related work on ad-hoc on demand vector routing protocol over wireless mesh network.

In section 4, Trusted ad-hoc vector routing protocol is discussed. In section 5, performance analysis is explained. Conclusion and future work are explained in section 6.

1.ARCHITECTURE OF WIRELESS MESH NETWORK

Wireless mesh network consists of three architectures such as:

- Infrastructure/ Backbone Wireless Mesh Network
- Client Wireless Mesh Network
- Hybrid Wireless Mesh network

Infrastructure/ Backbone Wireless Mesh Network:

Infrastructure/ Backbone WMNs the mesh routers forms a infrastructure or backbone for mesh clients through which client can access and connect with the internet with the help of (DSL) cable. Examples- wireless sensor network, wi-max, wi-fi, etc.

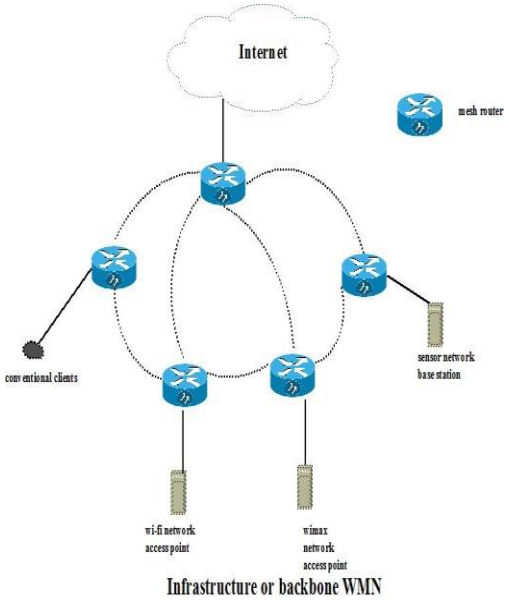


FIG-2: Infrastructure or Backbone WMN

Client Wireless Mesh Network:

Client WMNs is a peer to peer connection between the Mesh Clients. In client WMN mesh clients are self configured as well as self organised. Mesh routers are not required in client WMN because client nodes initiate the actual network to perform the routing and other configuration functionalities.

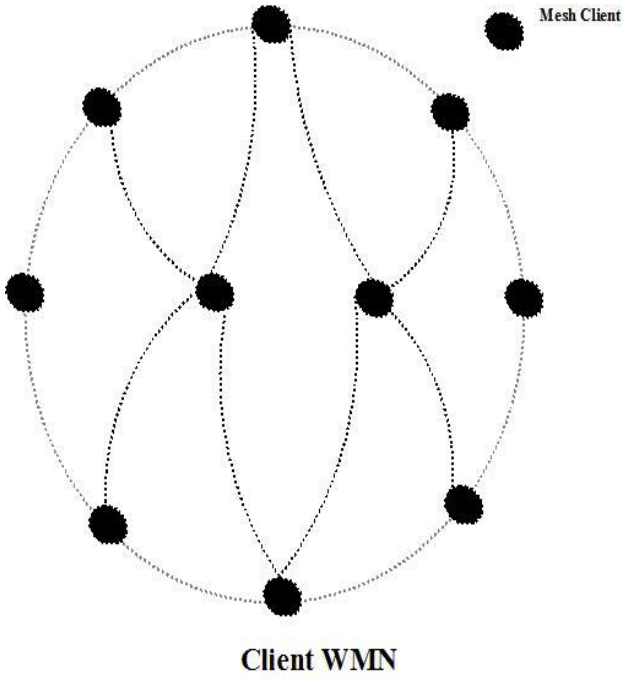


FIG-3: Client WMN

Hybrid Wireless Mesh Network:

Hybrid WMN is a combination of infrastructure/ backbone WMN and client WMN. It consists the attributes of both Infrastructure WMN and client WMN. Mesh clients can access internet through Mesh router Infrastructure.

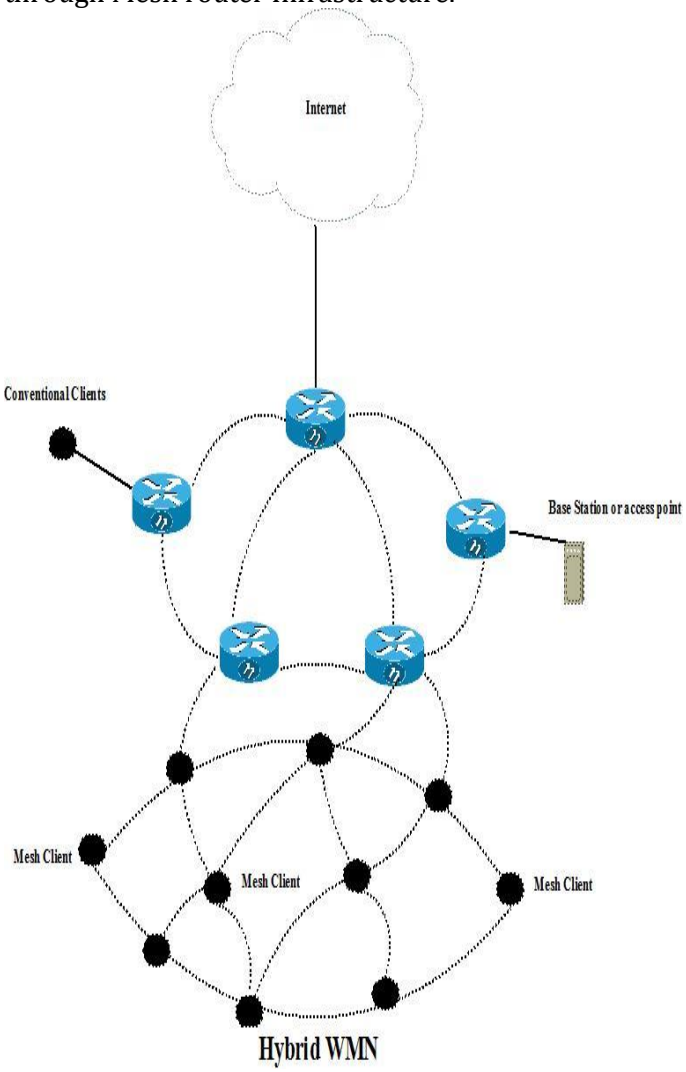


Fig-4: Hybrid WMN

1.RELATED WORK

The security scheme over wireless mesh network has been studied. In [1] Tainan ago talk about the combination of the proxy group signature and identity based-group signature, based on designated hierarchical proxy architecture for WMN in which the signing rights can be delegated in turn from the initial signer to proxy signer then to group manager. In [2] Muhammad Shoaib Siddiqui talk about the characteristics of the WMN and the essential issue of the network management in WMN. In [3],[4] Mohammad Sheikh Zefreh[3] talk about the key establishment and certificate authority over wireless ad-hoc network. They discussed that each clusters head has a split of CA's private key, which it can contribute with other cluster heads to produce new certificate or update them. Ping yi[4] discussed solution regarding key management and routing security as well as intrusion detection. In[5] Mandeep Singh talk about clustering algorithm on the basis of security and energy in which the cluster head is selected according to number of nodes which handles the cluster had battery power, transmission power and mobility of nodes. In [6][7], Andre Egners[6] has discussed about the PANA based security architecture and Mrs.K.Sudha[7] has discussed about the Deffie Hellman algorithm with the key management protocol.

1.TRUSTED AD-HOC ON DEMAND VECTOR ROUTING PROTOCOL

In trusted AODV we assume the each node in the network has the ability to recover all of its neighbours as well as each node in the network can broadcast some essential messages to its neighbours with high reliability, and each node in the network possess a unique id that can be distinguished from others.

There are basically the three prime modules in the trusted AODV system that is – basic AODV routing protocol, a trust model and a trusted AODV routing protocol.

4.1 Framework for Trusted AODV

Based on the trust model, the Trusted AODV routing vector protocol contains the procedures such as:

- Trust recommendation
- Authentication: Registration Authority, Certificate Authority and RSA algorithm.
- Trustupdating

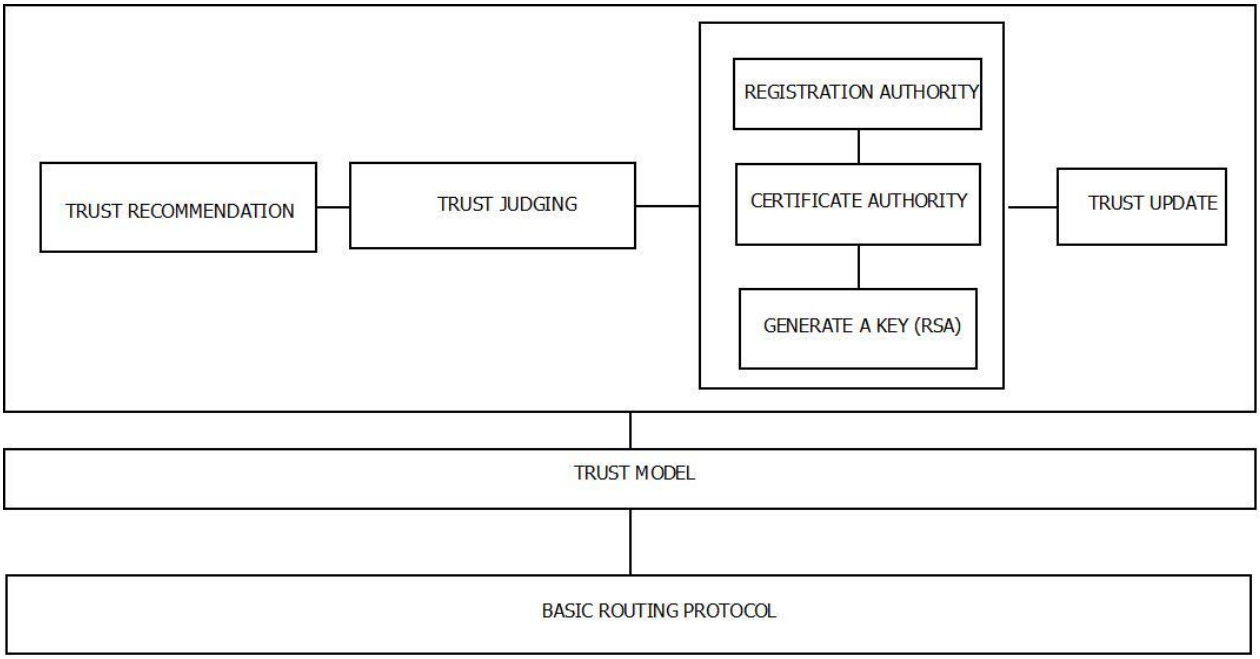


FIG- 5: Framework of Trusted AODV

The basic routing protocol

The algorithm can be given as.

1. While discovering the route, a source node sends RREQ packet to its neighboring nodes. RREQ packets send its security related information such as key information with the regular information.
2. When once RREQ packets are received by intermediate node. Then the node places the link trustworthiness. This process continues till it reaches the destination.
3. At the destination, the node waits for a fixed no of RREQs before it make decision. It then unicasts the RREP back to source node. When the source node receives the RREP, it starts data communication by using the route.
4. Once the route is established the intermediate node monitors the link status of the next hops in the active routes.
5. When a link breakage is detected in an active route is detected, a route error(RERR) packet is used to notify the other nodes that the loss of the link has occurred.

Trust recommendation

The existing trust model rarely concern the exchange of trust information. In the trust recommendation protocol, consists of three types of messages: Trust Request Message(TREQ), Trust Reply Message(TREP) and Trust Warning Message(TWARN).

Authentication

- Registration Authority: Which is the authority in the network for verifying the users request for digital certificate and certificate authority to issue it.
- Distributed Certificate Authority: The services of the certificate authority will be distributed in all the nodes using secret sharing. It reduced the communication delay and it also improves availability.
- RSA Algorithm: RSA is developed by Ron Rivest, Adi Shamir, Len Adleman. RSA generates public key and private key that encrypt information and also decrypt the information.

4.2 Flow chart for Trusted AODV

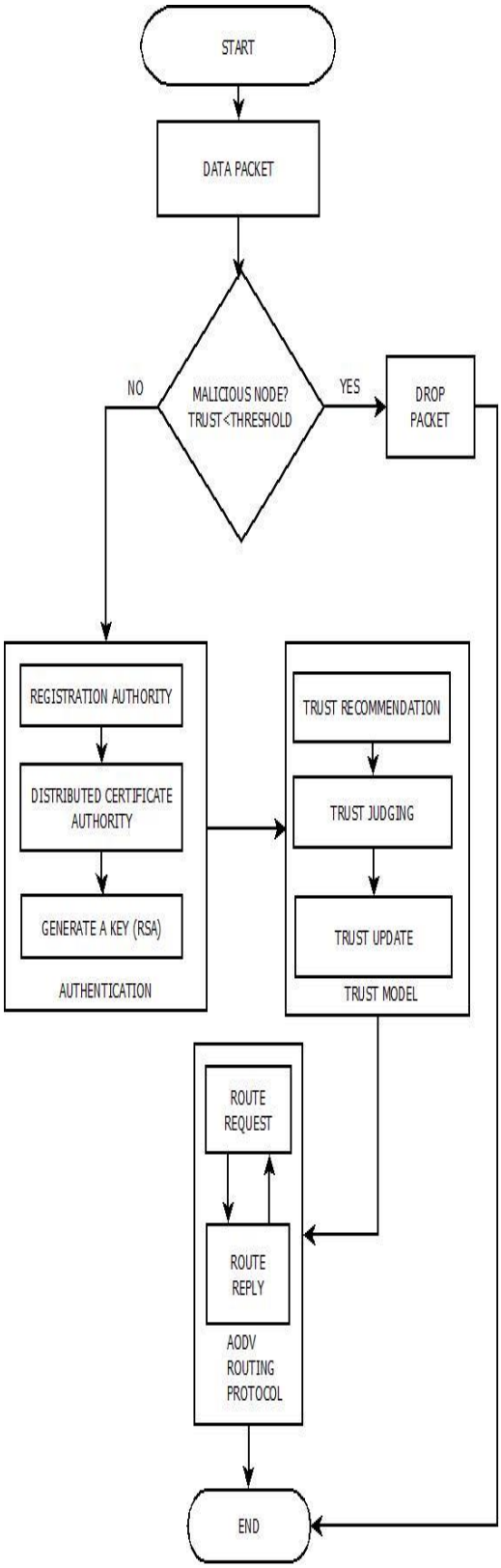


FIG-6: Flowchart of TAODV

4.3 Algorithm for Trusted AODV

1. Check for malicious nodes
   - Begin
   - If(sender node trust value<threshold)then
   - Drop packet
   - End if
2. Register nodes with Registration Authority()
3. Generate RSA with Certificates()
4. Generate data() for transmission
5. Enqueue data packets and raise RREQ
   - If(Data packet) then
   - Call recvAODV(packet)
   - End if
   - If(have route for destination) then
   - Call forward(packet)
   - Call data insert(packet)
   - Else
   - Generate RERR()
   - End else
   - End
6. For sending request
   - Procedure recvRequest(packet)
   - Begin
   - Update routing table
   - Call forward(packet)
   - Call rreq_insert(packet)
   - End
7. For sending reply
   - Procedure recv(packet)
   - Begin
   - If(dest_sequence_no<repthreshold) then
   - Update routing table
   - Call forward(packet)
   - Call rrep_insert(packet)
   - End

5 ANALYSIS OF SIMULATION RESULTS

In this thesis we implement trusted AODV with distributed certificate authority using network simulator 2 version 2.35. The simulation is tested for random 63 nodes.
Implementation study begins with the simulation of network environment. These require setting of simulation network parameters. These parameters

are depicted in table1. The simulation results from running the script in NS-2 include an input to the graphical simulation display tool called network animator(NAM).

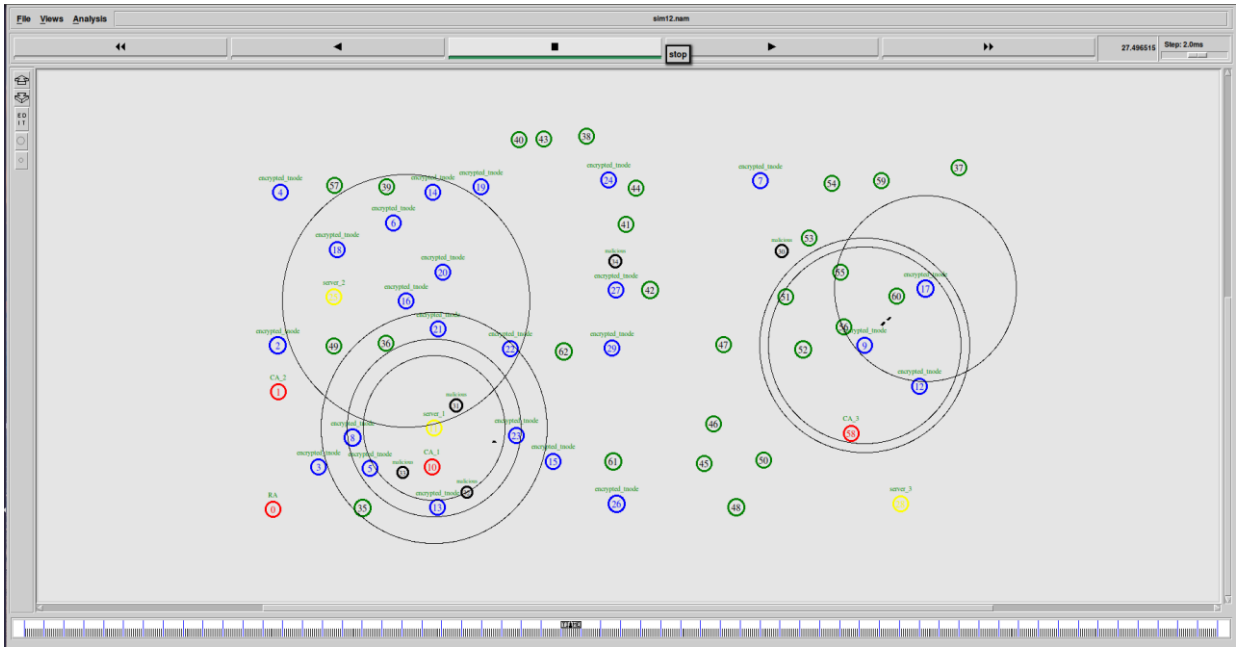


FIG-7: Screenshot of NAM window.

Table1. Simulation Parameters

Parameter	Values
Examined protocols	AODV, TAODV
Traffic type	UDP
Transmission area	1000*1000 m^2
Packet size	512 bytes
Data rate	600kb/s
Simulation time	60s

NAM is an animation tool for viewing network simulation traces. Fig 2. Shows snapshot of NAM for a 63 node network with data rate of 600kb/s. X-Graph is the geographical representation tool which is used for representing nodes properties with respect to the simulation time. This is characterised to only one route per destination maintained by AODV. Each packet that the Mac layer is unable to deliver is dropped since there are no alternate paths.

TAODV allow packet to stay in send buffer for 30s for route discovery. And if

Once the routes are discovered the data packets are sent on that route to be delivered at the destination. Each packet that a MAC layer is unable to deliver is dropped since there is no alternate path.

Table 2. Shows the performance metrics of AODV and TAODV

Metrics	AODV	TAODV
No of nodes	63	63
Throughput(kbps)	285.27	320.32
Send packets	7303	7864
Received packets	6980	7345
End to end delay(ms)	67.89	61.34
Packet loss(bytes)	78956	74556

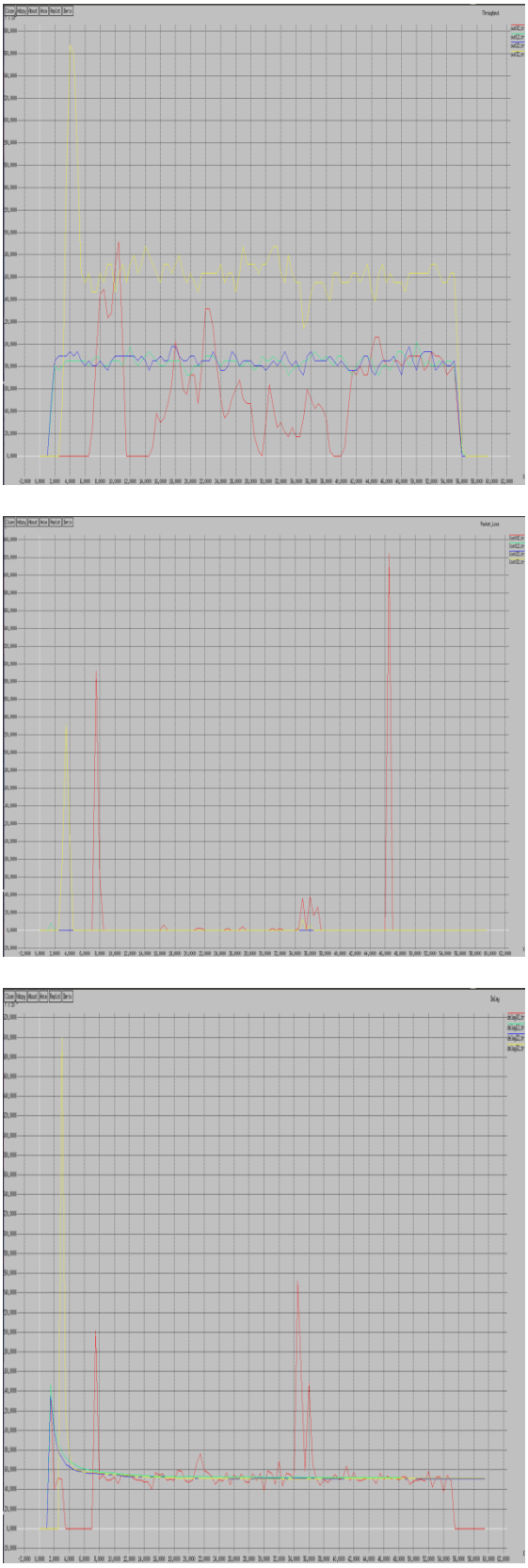


FIG-8: Shows various x graphs of the throughput, packet dropped and delay of TAODV

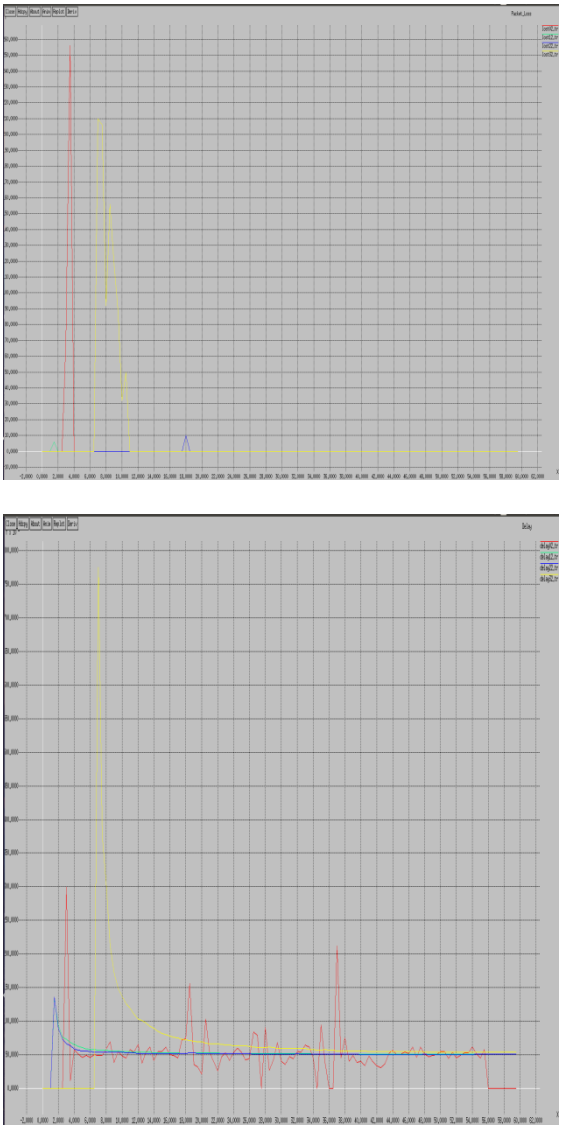


FIG-9: Shows various X-graphs of the throughput, packet dropped and delay of AODV.

By using AWK script, we got the performance metrics as shown in table2.

Now we simulate network for different no of nodes to find out the performance of our proposed system under various routing conditions and we plot it as a graph. Fig5 shows the routing protocol performance during malicious node. TAODV provide better performance evaluation metrics values than AODV

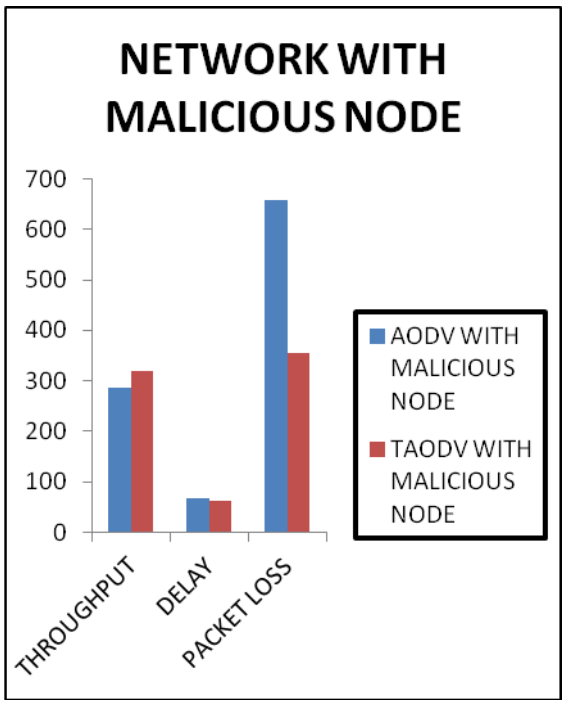
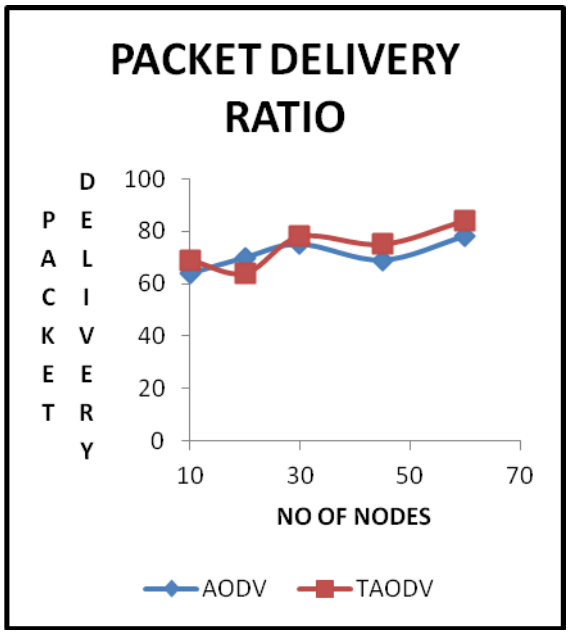
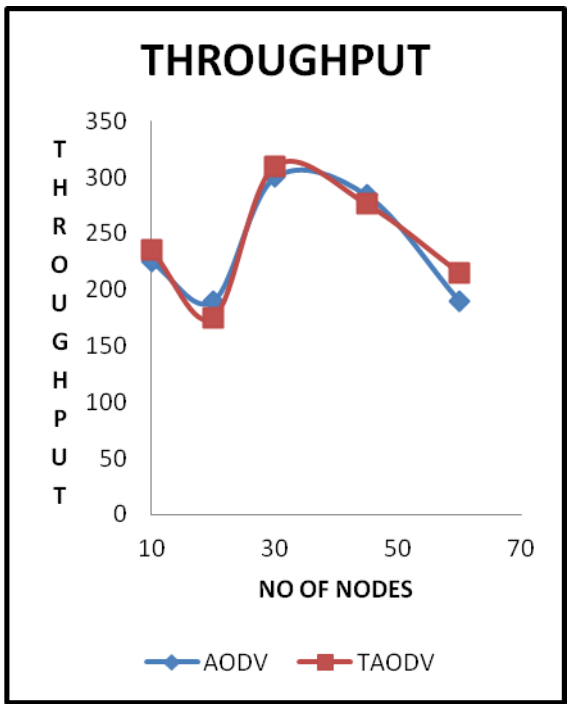


Chart-1: Performance analysis of malicious nodes.





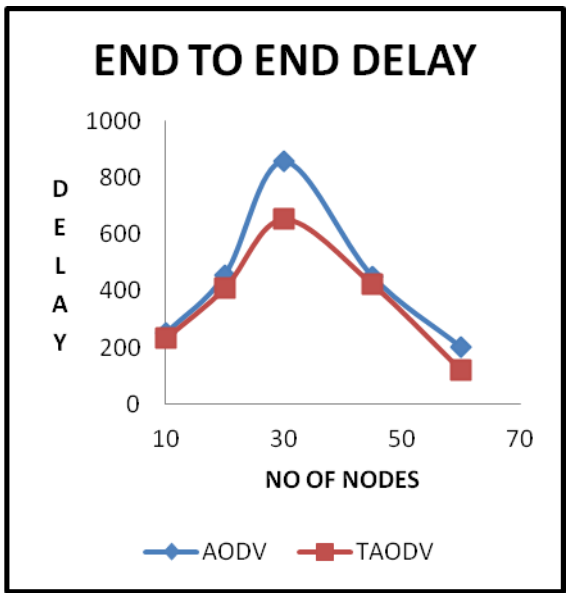


Chart-2: Performance analysis using various metrics

6 CONCLUSION

With the growing interest and development in wireless technology, the user expects better and more services that can be access at anywhere and anytime. The backbone of Wireless mesh network has facilitated the user to access the internet at anytime and anywhere.

The performance of AODV protocol has been modified by including the source route accumulation feature. As the low transmission power of each ad-hoc node limits its communication range, the node must assist and trust each other in forwarding packets from one node to another. However this implies trust relationship can be threatened by malicious nodes that may modify or disrupt the orderly exchange of packets. Security demands that all packets to be authenticated before being used.

Based on this trust model, we have designed our trust routing protocol for wireless mesh network called TAODV routing protocol. Through simulation we can see that bad nodes are clearly separated from the good nodes. Although a comparison of the performance between AODV and TAODV routing protocol under different experiments was achieved.

As the future work, we focus on identifying more different types of attack using TAODV for secure transmission. And work at applying this trust model in other routing protocol of wireless mesh network.

REFERENCES

1. Tianhan Gao,Fangting Peng and Nan Guo, "Anonymous authentication scheme based on identity-based proxy group signature for wireless mesh network", EURASIP journal on wireless communications and networking(2016).
2. Muhammad Shoaib Siddiqui, Syed Obaid Amin, Choong Seon Hong, "An Efficient Mechanism for Network Management in Wireless Mesh Network", IITA-2006-C1090-0602-0002, ISBN: 978-89-5519-136-3, feb 17-20, 2008 ICACT 2008.
3. Mohammad Sheikh Zefreh, Ali Fanian, Sayyed Mahdi Sajadieh, Mahdi Berenjkoub, Pejman Khadivi, "A Distributed Certificate Authority and Key Establishment Protocol for Mobile Ad Hoc Networks", dept of electrical and computer engg, Isfahan university of technology, Isfahan, Iran, ISBN: 978-89-5519-136-3, feb 17-20, 2008.
4. Ping Yi, Yue Wu, Futai Zou and Ning Liu, "A Survey on Security in Wireless Mesh Networks" , IETE technical Review, vol 27, issue 1, Jan-feb 2010.
5. Mandeep Singh , Mr.Gagangeet Singh, "A Secure and Efficient Cluster Head Selection Algorithm for MANET ", journal of network communication and emerging technologies, vol 2, issue 2, June 2015, ISSN: 2395-5317.
6. Andre Egners and Ulrike Meyer, UMIC research centre," Wireless mesh network security: State of Affairs", RWTH Aachen University.
7. Mrs.K.Sudha , Mr. J.Prem Ranjith, Mr. S.Ganapathy, Mr.S.Ranjith Sasidharan, "Secure transmission over remote group: A new key management protocol",IPASJI international Journal of Computer Science, vol 2, issue 1, January 2014, ISSN: 2321-5992.
8. Y.Dong, Victor O.K.Li, Lucas C.K.Hui, S.M. Yiu."Dynamic distributed certificate authority services for mobile ad hoc networks". IEEE , 1525-3511/07, 2007.
9. Spinder kaur, harpreet kaur, "implementing RSA algorithm in MANET and comparison with RSA digital signature", internal journal for advance research in engineering and technology.(2015)
10. Senthilkumar subramaniyan, William Johnson, and karthikeyan subramaniyan, "a distributed framework for detecting selfish nodes in manet using record and trust based detection technique", EURASIP journal on wireless mesh network.(2014)