RESEARCH ARTICLE OPEN ACCESS

TAODV :Modification of AODV protocol using TRUST mechanism for mobile Ad Hoc networks

Deeksha Sohani[1], Ms. Manju Sachdeo[2]
M.Tech Scholor IIPS DAVV[1], Reader/Associate Professor[2] ,IIPS DAVV

Abstract:

This paper define a new approach for prevention of jamming attack in mobile ad-hoc networks . MANET's are easy prey to be caught by attackers because they are mobile and hence not attached to a fixed location and not exposed to similar threat. MANET is a collection of mobile nodes which can be configured by themselves where each node itself act as a router for other nodes.

The idea is to employ a trust mechanism in AODV protocol to prevent jamming attack. AODV protocol originally uses computational logic to provide authentication to newly arrived nodes while trust mechanism uses subjective logic. Trust model represents trust among nodes through a term called “opinion” . “opinion” is a 3 dimensional parameter having dimensions-Trust, Mistrust, Unknown. These parameters describe the authenticity of a node in MANET. The value of “opinion” keep updated during information exchange process. If a node perform normally ,it's authenticity from other node's viewpoint increases otherwise it looses it's trust from other nodes and the malfunctioning node is denied from network. The performance of new protocol is evaluated through analysis and simulation. The proposed protocol should provide better results relative to following parameter-Packet delivery ratio, end -to -end delay, energy and throughput. The results of both AODV and TAODV protocols are compared.

Keywords — **MANET, trust model, ad-hoc networks, jamming attack, TAODV.**

1. Introduction

A mobile ad-hoc network (MANET) is a network in which there is no central administration or base .It does not need any third party to coordinate and collaborate between the nodes. It is infrastructure-less network. The topology of network may change uncertainly and rapidly due to high mobility of independent nodes. Each node in MANET itself act as router to find suitable and shortest path . In this research paper MANET is taken as network due to its increasing demand and applications in emergency operations and military networks where mobility of node is large and security, reliability, deliberate jamming are main concern. Taking MANET for research can be justified by it's characteristics such as openness, mobility, change-prone topology and weak protocol.

All the security schemes that have been proposed in recent years are based on centralized units or third parties to issue digital authentication. The schemes that have been suggested till now are-secure routing protocol, intrusion detection mechanism, secure key management solutions, error distribution, and key exchange. However these mechanisms are threat to self - organization nature of MANET as these incorporate third party. Moreover these solutions bring huge computation overheads. Mechanism of trustworthiness employs the idea of subjective logic which avoids large computational overhead and motivate the self – organizing nature of MANETs.

The subjective logic used as security solution over jamming attack qualitatively defines the calculation and combination of trust. In recent years, research work has been conducted to incorporate trust model into security solutions of MANET. But till now no paper suggested specific use and implementation of trust mechanism to prevent jamming attack and there are no terse and applicable designs proposed for routing protocol security

solutions in MANETs.
Our derived protocol is based on existing protocol-AODV (Ad-hoc on demand distance vector routing protocol). The new protcol derived is named MAODV (modified AODV) protocol. Salient features of MAODV protocol are:
(1)Trustworthiness of a node is defined by trust relationship between the nodes.
(2)Digital signature authentication and verification is eliminated at each hop and hence performance improved to large extent.
(3)A node which performs unhealthy and produce "mistrust" is eliminated.
(4)If a node produce "Unknown" parameter then a digital certificate is required as suggested by original protocol.
The organization of rest of paper is as follows:

- insight of AODV protocol,subjective logic.
- System framework and network assumptions for MAODV protocol.
- Description of trust mechanism.
- More details of trust mechanisms and updating algorithms.
- Performance and security analyses .
- Conclusion.

2. Background

2.1 AODV

AODV (ad-hoc on demand distance vector) protocol is a protocol for on- demand routing. It's on demand behavior makes it fittest for networks like MANET where routing is main concern due to mobility of nodes and nodes themselves act as router. On -demand routing means routing will be performed only when a transfer of packet is requested. It solely depends on node when to start routing hence efficiency of network increased to large extent. The two basic process that a node need to carry out while performing on-demand routing is routing discovery and routing maintenance. Routing discovery occurs when o some other node request transfer and host node does not contain any route entry for destination or requesting node. In this case Originator or source node will flood an RREQ (routing request) message that is broadcast this message to every other node. Every node which recieves such message will check in it's routing table whether it contains a path to this destination. If it does not contain any such path it will rebroadcast this routing request by sending RREQ back to sender. If it contains one or itself is destination then that particular node will generate RREP(request reply) message and send to sender or requesting node. All the nodes between intermediate or destination node and sender node aill update their entry in routing table for future references and then forward it to sender. In this way a two way path get established between the source and destination.

Routing maintenance may occur in two way-a node may broadcast HELLO message to connected nodes to confirm their connectivity and other way is to maintain connectivity locally from hop to hop using some network layer mechanism.

2.2 Security Issue In Manet

Types of attack in MANET-

I. External attack, in which aim of attacker is to cause congestion, propagate fake routing information or disturb nodes from providing services.
II. Internal attacks ,is attack in which attacker wants to gain the normal access to network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node,or by directly compromising a current node and using it as a basis to conduct it's malicious behaviors.
III. Denial Of service attack
IV. Impersonation
V. Eavesdropping.
VI. Attack against routing

2.3 Jamming

Jamming attack is a type of denial of service attack where a malicious node continuously transmit radio signal in order to obstruct legal access to medium. The adversary which attack network are called jammers. Jammers require powerful signal transmitters which intercept the original signals and block communication. In this type of attack attacking adversary aims at getting frequency of transmission to establish jammers in MANET.

In jamming attack attacker node acts as if it is node shortest in distance for destination node and receives all data.

3. Proposed Solution

3.1 Subjective Logic

Subjective logic is a term used for subjective beliefs and

uses the term "opinion" to represent credibility of a node for another node. A node's trustworthiness for another node depends upon the value of "opinion". The term "opinion" may contain three values -trust, mistrust, unknown.

Every value denotes different subjective logic. Trust means that node found target node as trustworthy to initiate communication. Mistrust value of node denotes target node is malicious and must be denied of network. If a node is uncertain about the credibility of a node then it takes unknown value in parameter "opinion". In case of node containing the value "unknown" need to perform digital signature authentication for that node and based on that value host node update it's value of "opinion" in it's routing table. The "opinion" can be defined as measure of probability.

The uncertainty about any node's trustworthiness is common phenomenon as MANET are frequently exposed to change in location and hence nodes are unable to collect enough evidences for calculating authentication. This uncertainty is incorporated in trust model. Trust model is derived from this subjective logic for MANET.

3.2 Proposed Protocol

3.2.1 Overview Of Trusted AODV (MAODV)

Some of the assumptions I made in this model are-

1. Each node in the network has the ability to recover all of its neighbors.
2. Each node in the network can broadcast some essential messages to neighbors with reliability.
3. Each node in the network contains a unique ID.
4. In the TAODV, it is also assumed that system contains some intrusion detection mechanism in network or application layer. This work has been proposed in some previous work, such as intrusion detection system and watchdog technique .

In MAODV, self-organized key management system is incorporated for issuing public key certificates which can be used for verification and generation of digital signatures during the initialization of TAODV or a newly arrived node.

3.2.2 Framework of Trusted AODV (MAODV)

The basic four module of MAODV framework are:
Basic routing protocol, trust model, trusted routing protocol, and self-organized key management mechanism as illustrated in fig. 1. This work focuses on the idea of trust model and modified routing protocol. The module modified routing protocol contains are trust recommendation, trust combination, trust judging, signature authentication routing trusted authentication routing and trust update. These modules are discussed in detail in upcoming sections 4 and 5.

This idea of trust model can be applied to different protocols but AODV protocol is taken to demonstrate idea.

4. TRUST MODEL FOR MAODV

4.1 Trust Representaion

Trust model is a modification of original trust model defined in subjective logic(see section 3.1). Here opinion is a three dimensional metric and is defined as :

Definition 1-Opinion – let $w^A_B = (b^A_B , d^A_B , u^A_B)$ denote any node A's opinion about any node B's trustworthiness in a MANET ,where the first ,second and third component corresponds to trust ,mistrust and unknown respectively. These three elements satisfy:

$$b^A_B + d^A_B + u^A_B = 1 \quad (1)$$

In this definition Trust means the probability of a node B can be trusted by a node A, and mistrust means the probability of B cannot be trusted by A. then unknown fills the void in the absence of both trust and mistrust ,and sum of these three elements is 1.

4.2 Mapping between The Evidence and Opinion Spaces

Opinion value of a node for other node is obtained through evidences by applying some mapping equation. Evidences collected by a node about other node's trustworthiness can be positive or negative . To find opinion values with the help of collected evidences we need to use mapping equation .

Definition 2- Mapping – let $w^A_B = (b^A_B , d^A_B , u^A_B)$ node A's opinion about node B's trustworthiness in a MANET , and let p and n respectively be the positive and negative evidences collected by node A about node B's trustworthiness , then w^A_B can be expressed as a function of p and n according to :

$$b^A_B = p/(p+n+2)$$

$$d^A_B = n/(p+n+2) \text{ ,where } u^A_B \neq 0$$

$$u^A_B = 2/(p+n+2)$$

4.3 Trust Combination

In this trust model, every node collect opinion about every neighboring node and combine them together using some combination operation to generate opinion of those nodes not neighbour to it. Hence when several nodes are present in a network , a particular node can easily make an objective judgment about other node's trustworthiness .the combination operations which nodes can perform are – Discounting combination and consensus combination.

4.3.1 Discounting Combination

Let us understand this combination operation with an example. Let A wants to know opinion about C's trustworthiness and also A already has opinion about B's trustworthiness and B has opinion about C's trustworthiness. Then in order to obtain opinion about C's trustworthiness A will combine two opinion :A to B and B to C to obtain a recommendation opinion A to C . This is discounting combination.

Definition 3: (Discounting combination). Let A,B and C be three nodes in a MANET where $w^A_B = (b^A_B , d^A_B , u^A_B)$ is A's opinion about B's trustworthiness and $w^B_C = (b^B_C, d^B_C, u^B_C)$ is B's opinion about C's trustworthiness then $w^{AB}_C = (b^{AB}_C , d^{AB}_C , u^{AB}_C)$ is A's opinion about C's trustworthiness such that

$$b^{AB}_C = b^A_B b^B_C$$
$$d^{AB}_C = d^A_B d^B_C$$
$$u^{AB}_C = d^A_B + u^A_B + b^A_B u^B_C$$

w^{AB}_C is called discounting of w^B_C by w^A_B which expresses A's opinion about C's trustworthiness as a consequence of B's advice to A. By using the symbol '$\otimes$' to represent this operator , we define $w^{AB}_C = w^A_B \otimes w^B_C$. The recommendation path makes use of discounting combination .

4.3.2 Consensus Combination

In trust model when a node collect opinion about a particular node it may differ or conflict other node's opinion for same node. To combine this contrary opinions together to reach a single relative objective evaluation about that node's trustworthiness consensus combination is used.

Definition 4(Consensus combination): Let $w^A_C=(b^A_C , d^A_C ,u^A_C)$ and $w^B_C=(b^B_C , d^B_C ,u^B_C)$ be node A's and node B's opinions respectively about node C's trustworthiness then $w^{A,B}_C=(b^{A,B}_C , d^{A,B}_C ,u^{A,B}_C)$ is node A's opinion about node C such that

$$b^{A,B}_C = b^A_C u^B_C + b^B_C u^A_C$$
$$d^{A,B}_C = d^A_C u^B_C + d^B_C u^A_C$$
$$u^{A,B}_C = u^A_C u^B_C /k$$

where $k=u^A_C + u^B_C - 2u^A_C u^B_C$ such that k is not equal to 0 , then $w^{A,B}_C$ is called consensus between w^A_C and w^B_C representing node [A,B]'s opinion about node C's trustworthiness. The symbol used to represent consensus combination is '$\oplus$' .hence it is defined as $w^{A,B}_C = w^A_C \oplus w^B_C$. Consensus combination can reduce uncertainty that is 'unknown' parameter in opinion value of a node.

5. Routing Operations in TAODV

In this section we are going to define trust recommendation mechanism for MAODV. Also we will define some rules which makes these nodes to obey routing decision according to opinion values. To update opinions of nodes for other nodes need to be updated time to time hence we defined some policies for updation of opinion values. I then describe MAODV protocol extensions and different scenarios of trusted routing discovery operation.

5.1 Trust Recommendation

In existing trust model ,there is no mechanism for exchanging trust information and hence updation of opinions is cumbersome. In my trust model I tried to incorporate an information exchange mechanism which makes use of trust recommendation .recommendation procedure makes use of two types of messages – Trust Request Message (TREQ) and Trust Reply Message(TREP). The formats of two types of messages are described in fig 2 and fig 3. When a node A wants to know opinion about node B 's trustworthiness it sends a TREQ message to all it's neighbors using broadcasting . Following the depicted format with type field set to 0 and and recommendee field containing the IP address of node B. Let C be any neighbor of A receives TREQ message then it will check in it's routing table whether it contains any opinion value for node B if it does then it will reply with message TREP where type field is set to 1 and

opinion field contains C's opinion for B's trustworthiness. If it does not contain opinion value for B then it will resend TREQ message to A. In 1 TREQ or TREP a node can ask for several opinion values for several nodes using recommendation protocol. Hence this trust model enable easy trust information exchange without incurring much packet overhead

Figure 2. Trust Request Message Format (TREQ)

.

Trust	Mistrust	Unknown	Actions
		> 0.5	Request and verify digital signature
	> 0.5		Mistrust a node for an expire time
> 0.5			Trust a node and continue routing
<= 0.5	<= 0.5	<= 0.5	Request and verify digital signature

Table 1 .criteria for judging trustworthiness

Trust Judgement

What actions need to be taken by a node after receiving opinion values of intending node is described by some set of rules called rules for trust judgment. These are as follows:

- If a node A's opinion about node B's trustworthiness w^A_B contains value greater than 0.5 for 'Trust' parameter then that node is accepted in network and can perform routing behavior or data transmission
- If node A's opinion about node B's trustworthiness w^A_B contains value greater than 0.5 for parameter 'mistrust' then A will not trust B and destroy B from network and refuse any sort of communication.
- If node A's opinion about node B's trustworthiness w^A_B for the third parameter 'unknown' is greater than 0.5 than A will request and perform digital signature authentication for node B to get it's trustworthiness.
- If node A's opinion about node B's trustworthiness w^A_B for all the three parameters 'trust' 'mistrust' and 'unknown' is less than 0.5 than A will request and perform digital signature authentication for node B to get it's trustworthiness.
- If node A's route table has no route entry for node B then A's opinion about node B is initialized as(0,0,1).

5.3 Trust Update

Some policies are defined for updating trust opinion of nodes . These opinions change dynamically due to successful or failed communication among nodes. These policies are as follows:

- Each time A has performed successful communication with B normally , B's successful events is increased by 1 in A's routing table by 1.
- Each time A has performed failed communication with B , B's failed events is increased by 1 in A's routing table by 1.
- each time when field related to successful or failed events affected,the corresponding value of opinion will be reevaluated using equation 2 , which is a mapping function from evidence space to opinion space.
- If A's route table lost entry of any node B's opinion value due to expiry ,the opinion will be set back to the initial value (0,0,1).

5.4 Route Table Extensions

The extension is as follows:

I add three fields to route table of each node . These fields are – positive events,negative events and opinion.

Positive events are frequency of successful communication between the two nodes . Negative events are frequency of failed communication between the two nodes and opinion field contains parameter value('trust','mistrust','unknown') of intending node for host node. The main parts of route table of any node using trust model is illustrated in figure 4.

5.5 ROUTING MESSEGE EXTENSIONS

AODV routing messages also needs to be extended to incorporate trust information field. 2 main types of extensions are – TRREQ(Trust routing request) and TRREP(Trust routing reply) .formats of these messages

are depicted in fig 5 and 6. when we talk about trusted routing discovery procedure every routing request and reply message carries trust information which includes opinion towards both originator and destination ,which is employed to calculate the credibility of both .when a node is asked to provide it's certificate information it simply fills these information with it's own signature proposed by traditional security mechanisms.

In case if a node A is unable to pass the critical signature Authentication ,it's opinion from another node B' point of view will be set to (0,1,0) which means 'mistrust' and B will broadcast an RERR message . Any node which receive this message will verify B's trustworthiness and then perform update.

5.6 Trusted Routing Discovery

now we will formulate trusted routing discovery procedure with an example shown in fig 7. in this fig route path is uncovered . The originator S will generate a TRREQ message to discover a route path to destination D. node N is intermediate node while nodes N1 to N4 are neighboring nodes. When node N receives the re-broadcast message TRREQ from N1 it will perform operations depicted in algorithm 1.

Algorithm 1 General Procedure of Node N in Performing Trusted Routing Discovery Receive an TRREQ(S,D) or an TRREP(S,D) from N 1;

/*Verify the trustworthiness of N 1*/
Broadcast TREQ(N1) to request the opinions from N 's neighbors to N 1;
Receive opinions from N 's neighbors: ω^{N1}_{N2} , ω^{N3}_{N1} , ω^{N4}_{N1} ;

Combine these opinions together and get a latest ω^{N}

/*Check each component in ω^{N}
using the criteria in Table 1*/ **if** unknown> 0.5 $_{N1}$;
then
Request and verify N 1's $_{N1}$, and judge the next step certificate;

else if mistrust> 0.5 **then**
Update the N 1 entry in the route table; Distrust N 1 for an expiry time;

else if trust> 0.5 **then**
Calculate ω^{N}_{S} , and ω^{N}_{D} using the latest ω^{N}_{N1} ;
Update the S and D entries in the route table;
Trust N 1 and re-broadcast TRREQ/TRREP;

else
/*Do not have much confidence about N 1's trustworthiness.*/
Request and verify N 1's certificate, by default; **end if**

if Succeed in verifying N 1's certificate **then**
Calculate ω^{N}_{S} , and ω^{N}_{D} using the latest ω^{N}_{N1} ;
Update the S and D entries in the route table;
Trust N 1 and re-broadcast TRREQ/TRREP;

else
/*N1 doesn't pass the certificate verification*/
Set ω^{N}_{N1} to (0, 1, 0);
Broadcast TRERR(N1) to N 's neighbors; Update the N 1 entry in the route table; Distrust N 1;
end if

In algorithm 1, I tried to calculate node N1's trustworthiness from node N's point of view .Node N has it's original opinion for it's neighboring nodes N1,N2,N3,N4: w^{N1}_{N}, w^{N2}_{N} ,w^{N3}_{N},w^{N4}_{N}. By collecting node N1's opinion on behalf of node N from all the neighboring nodes N1, N2, N3, N4 are- w^{N2}_{N1}, w^{N3}_{N1} ,w^{N4}_{N1}. After collecting opinion of all the neighboring nodes for node N1,the different opinions are combined using combination equation described in section 4.3 to yield a single opinion . I illustrate the trust recommendation relationship in figure 8.

The opinion which N calculate using equation 3:

$$\omega^{N\,N2}_{N1} = \omega^{N}_{N2} \otimes \omega^{N2}_{N1}$$
$$\omega^{N\,N4}_{N1} = \omega^{N}_{N3} \otimes \omega^{N4}_{N1}$$
$$\omega^{N}_{N1} = \omega^{N}_{N4} \otimes \omega^{N}_{N1}$$

The new opinion Wnn1 can be combined as :

$$W^{NN} = W^{N(N2,N3,N4)}\,N1$$
$$= (\omega^{N}_{N2} \otimes \omega^{N2}_{N1}) \oplus (\omega^{N}_{N3} \otimes \omega^{N3}_{N1}) \oplus (\omega^{N}_{N4} \otimes \omega^{N4}_{N1})$$

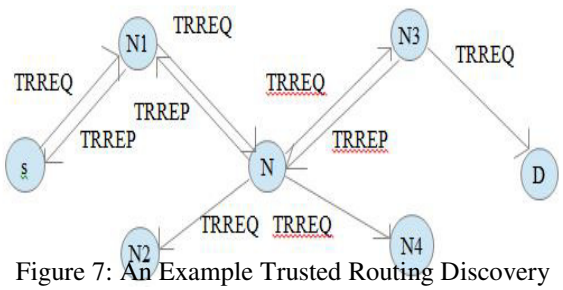


Figure 7: An Example Trusted Routing Discovery

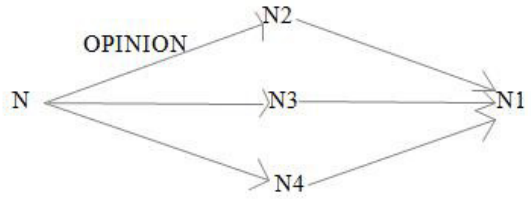


Figure 8: An Example For Trust Combination

5.7 Initiation of TAODV MANET

To understand our implementation of protocol MAODV let us consider a MANET of 4 nodes :A,B,C,D as shown in figure 9.In this figure node A has 2 neighbors B and D and B has C and A as neighbors while C has neighbors B and D and node D has A and C as neighbors. In the beginning every node's routing table has no entry for opinion and initialized to (0,0,1) . now let us suppose node A wants to discover a route path to node C ,the process for same is as follows:

1.A broadcast an RREQ request to all it's neighbors i.e. B and D for requesting route path to C and wait for an RREP message from it's neighbors.

2. since both B and D contains node C as their neighboring node both will perform following steps:

I am taking only node B to explain process --

a) Checks a route to C and opinion for example opinion for node B is w^{B}_{A} and w^{B}_{c} since it is beginning of network $w^{B}_{A} = w^{B}_{A}=(0,0,1)$.

by 1 and new opinion will be somewhat like $w^{B}_{A}=(0,0.22,0.67)$and B will cancel RREQ and does not forward it.

c) If C is also certified as authenticated node by B ,it's route table is updated and B will re-broadcast the message RREQ else B won't forward it.

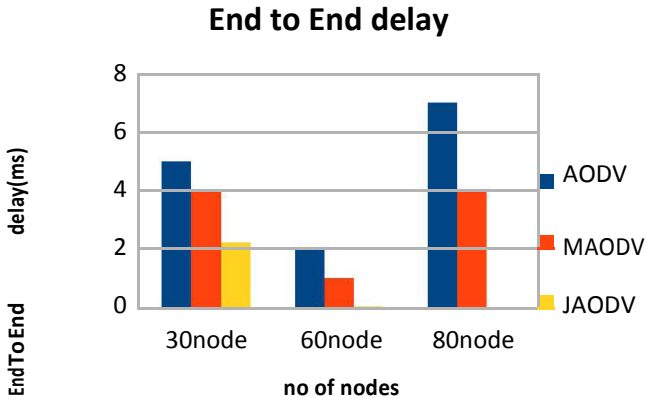
3. C receives this RREQ from B and check B's authenticity. If B passes, then C will generate RREP back to B, if not then C will drop request.

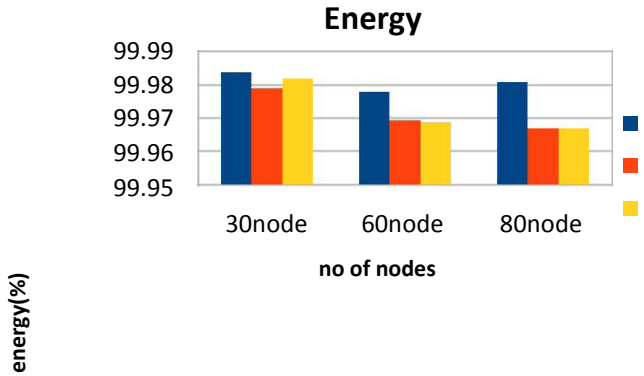
b) If u^{B}_{A} >0.5 then node B will authenticate node A and successful events is increased by 1. Also new opinion contains some value say $w^{B}_{A}=(0.22,0,0.67)$. If A does not manage to pass the authentication then failed events is increased

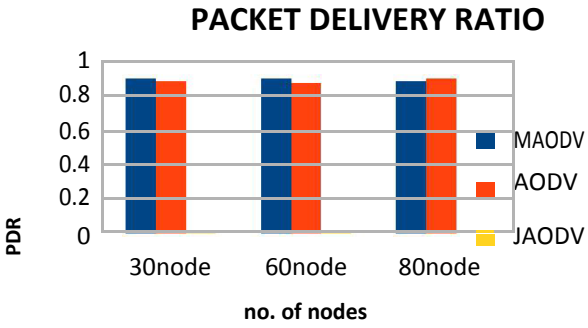
6. Analysis and Simulation

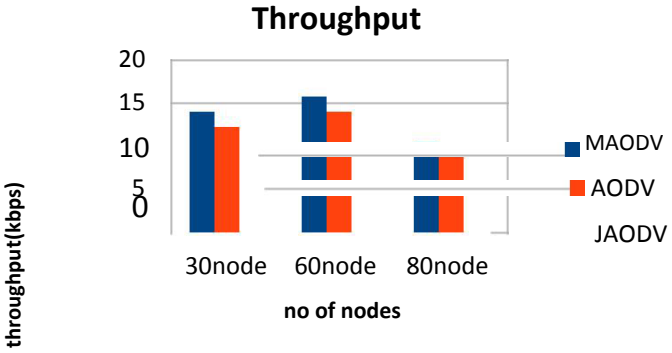
6.1 Analysis

It will analyze the network by evaluating the computation overhead of single node in MAODV MANET in certain routing traffic and then comparing it to general secure routing solution which employs digital signature authentication.




Energy
99.99
99.98
99.97
99.96
99.95
30node
60node
80node
no of nodes
energy(%)


PACKET DELIVERY RATIO
1
0.8
0.6
0.4
0.2
0
MAODV
AODV
JAODV
30node
60node
80node
no. of nodes
PDR


Throughput
20
15
10
5
0
MAODV
AODV
JAODV
30node
60node
80node
no of nodes
throughput(kbps)

8. References

[1] Y.Kim,J.Jung,S.Lee,C.Kim,A Belt-Zone Method for Decreasing Control Messages in Ad Hoc Netowkrs.ICCSA.2006:42-46.

[2] L. Abusalah, A. Khokhar, and M. Guizani, A survey of secure mobile ad hoc routing protocols,. Commun. Surveys Tuts., 2008;10(4):78–93.

[3] Marchang Ningrinla. Light-weight trust-based routing protocol for mobile ad hoc networks. J IET Information Security, 2012;6(2):77-83.

[4] Nakayama Hidehisa, Kurosawa, Satoshi, etc. a dynamic anomaly detection scheme for AODV-Based mobile ad hoc networks. J IEEE Transactions on Vehicular Technology, 2009; 58(5):2471-2481.

[5] Lee Breslau Deborah Estrin etc. Advances in Network Simulation. IEEE Computer,2000;5:78-85.

[6] R. Choudhary, S. Bhandhopadhyay and K. Paul. A Distributed Mechanism for topology discovery in Ad Hoc Wireless Networks Using Mobile Agents.2000;(5):96-101.