IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 73-78

Performance Comparison of AODV and DSR Using Fuzzy Approach in MANET

K. Thamizhmaran
Assistant Professor in ECE, Department of ECE, Annamalai University, Annamalainagar, Chidambaram, Tamilndu, India-608002,

Abstract: *Mobile Adhoc Networks (MANETs) is particularlyvulnerable to security attacks due to its characteristics. Wirelesscommunication is vital during disaster, natural climates andmilitary operation. In this paper,theyproposesecured network scheme that fuzzy logic scheme is used to detectblack-hole attack based on certificate authority and trust node toimprove the performance of network and compare with existing protocols namely,Adhoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR) protocols with fuzzy logic. Fuzzy logic is used to detectmisbehaving node by giving certificate to only trusted node. Theproposed technique is more secure and reliable to increase the network lifetime, packet delivery ratio, throughput and routing overhead with fixed topology size by continuously monitoring the individual nodes in the network. Network Simulator 2(NS2) is used to employ and investigation our proposed system.*

Keywords: *MANET, fuzzy logic, Routing Protocol,network lifetime, PDR, RO.*

I. INTRODUCTION

A MANET is infrastructure less and self-configuring network of mobile device. Each device in MANET isfree to move independently in any direction and will therefore changeits links to other devices frequently. MANET is a type of ad-hocnetwork that can change the location and configure itself on the fly.Because MANET is mobile device they are wireless connection tovarious networks. MANET is particularly vulnerable to securityattacks due to its characteristics, such as wirelessly connectingmedium, dynamic natured topology used, distributed cooperatednetwork. MANETs are easy to set up and use since their operationdoesn't depend on any fixed infrastructure. There are manyapplications that can benefit from MANETs such as military tactical operations,rescue missions, disaster relief, lawenforcement, commercial useMANETs are unique among communication networks, as can beobserved from the vital application areas. However, the uniquecharacteristics required by these applications necessitate uniquesolutions and differentiate MANETs from other conventionalnetworks. There are various challenges that have to be taken intoaccount when designing a MANET.In MANET the energy of one node is powered by batteries withlimited energy. Therefore the minimal energy node can roll as selfishnode. The energy of a node is calculated by the energy spent ontransmission and the reception of data packets andacknowledgements. MANET attracted by the attackers because itsunique features like dynamic topology, variable capacity, openmedium, local physical security and energy constrained operation.Inmilitary application mobility is a critical factor because mission willstart at certain coordinate and will end up at the other coordinate. Inthe battle field soldiers exchange the message like voice recording,video tapes, images and quality of services to other field unit.Unfortunately the communication can have delay of message,dropped message and delivery of erroneous. To improve theperformance the proposed scheme provides trust based dataexchange, certificate authority and fuzzy based analyzer to detect themisbehaving node.AODV and DSR routing protocols usedin military application because the source node maintains the routesas long as need by itself. It is reactive protocols, when a node wishesto start transmission with another node in a network to which it hasno route; the topology information is provides by the AODVand DSR protocols.

II. BACKGROUND

The ad-hoc on-demand distance vector protocol was done by Royer, et al (2000). Calculating a node's reputation in a mobile ad-hoc network was done by Adams, et al (2005). Prevention of co-operative black-hole attack in MANET was done by LathaTamilselvan (2008). A dynamic learning system against black-hole attack in AODV based MANET was done by Payal and Prashant (2009). Performance analysis of AODV, DSR & TORA routing protocols was done by Gupta, et al (2010). Avoiding black hole and cooperative black-hole attacks in wireless ad-hoc networks was done by Baddache and Belmehdi (2010). Comparison between various black-hole detection techniques in MANET was done by AkankshaSaini and Harish Kumar (2010). Vulnerabilities in network layer at WMN were done by Imani, et al (2010). A new protocol for detecting black-hole nodes in ad-hoc networks was done by Yaserkhamayseh, et al (2011). Impact of selfish node concentration

in MANETs was done by Shailender Gupta, etal (2011). Fuzzy based trusted ant routing protocol in mobile ad-hoc networks was done by Sethi, et al (2011).

III. PROPOSED SYSTEM

In this section we propose selection of most secure and reliable route by implementing the trust value management between two nodes with fuzzy logic rule prediction method. In the proposed scheme each node maintains trust value for its neighbor node. In MANET by using AODV and DSR protocols, before packet transmission process compute the trust value, based on trust value compute the route trust and update the trust value in the routing table of the node. If the route is valid route then select most trusted node route then transmit the packets else compute the trust route for the particular packet transmission. The trust value calculated as

$Ti(j) = \alpha Ti(self)(j) + \beta Ti(neighbor)(j)$
Where Ti (j) is the trust of node i on neighbor node j.
Ti(self)(j) represent the trust value of node i on nodej.
Ti(neighbor)(j) represent the trust that neighbor ofnode I has on node j,and α, β are weighting factor that is $\alpha + \beta = 1$.

The neighbor node establishes three structures like toforward and forwarded and source list. To forward store thenumber of packet to be forwarded and forwarded store thenumber of packet that are already forwarded and source listdefine the progenitor of the packet to be forwarded. Toforward count of node j is incremented by one when node I find that node j has received the packets which are to beforwarded further. Forwarded count is incremented by onewhen node j has forwarded that packet which is received.During the packet transmission process the algorithm is, immoral node maintains the source list (S_List) and observes thesource packet.

If [(Forwarded) node j and (S_List Contains Immoral node)]
(Forwarded) node j++;
(ToForward) node j++;
(Forwarded) node j ≥ Limit
Else
Calculate the trust value again.If immoral node fails to update forwarded and To Forwardedcount of node j then detect as a malicious node else securetransmission.

IV. ENERGY AUDITOR

In MANET the nodes energy is consuming whenreceiving and forwarding data to neighbor nodes. Initially allthe nodes have full battery capacity with maximum energy.According to energy consumption the selfish nodes utilize lessenergy because they only receive data packets they won'tforward data packets to neighbors. Whereas the trusted nodeconsuming more energy because they will receive and forwardthe packets to its neighbors. Each node has different energycalculation based on initial node configuration. Theconfiguration requires following parameters when it'sconfiguring like receive power consumption, transmissionpower consumption, ideal power consumption.In MANETenergy consumption monitored by energy supervisor (EA) foreach node when sending and receiving data packets toneighbor.Generally all nodes behave selfish to save batterypower without forwarding the packets to the neighbor due tolimited resource availability. Energy supervisor monitorpackets received by a node, forwarded by a node and batterypower affects by each node.

EA = Σ (Packet received + Packet forwarded+ Batter power) / Node

V. TRUST MANAGER

Trust value calculated by direct observation ofneighbors. In the network every node monitors the behaviourof its neighbors. Every node monitors its neighbor node byusing watch dog mechanism whether neighbor node reallyforward or drop the packets. The neighbor node is monitoredby passively observing communication for detecting delayedpacket, dropped packet and forward packets. Theseobservations are abnormal action of any node and detectdirectly to determine the trust value. When communicationbegins the total trust value (TV) calculated with node indexand direct trust value and stored in trust table for each node.

TV = Node index + Direct trustthe recommended trust obtaining indirect trust on destination from Node (N).

1. Node Source (S) sends Recommendation TrustRequest to node(s) N.
2. If S has direct trust value on D, then it will replyback with Recommendation Trust Reply.
3. Else If S does not have direct trust value record itwill discard the Recommendation Trust Request
4. After receiving Recommendation Trust Reply fromneighbors consider the trust value of the node with maximumdirect trust value by applying fuzzy logic technique.
5. Integrate all the obtained trust value fromneighbors to calculate the indirect trust value

VI. PACKET VERACITY CHECK

To maintain the integrity of the packetcommunication the modified message by the intermediatenode can be discarded. Initially the packet veracity checkvalue (PVC value) is positive,if any modification then PVCvalue will be decreased. Each message generated by a nodeincludes digital signature through its private key,based oncryptography technique when a node receives a messagedecrypt using digital signature and public key to authenticatemessage from neighbor node. Similarly all the intermediatenodes authenticate the message and forward to the neighbor, ifany modification in the message content then PVC value willbe decremented. In our proposed scheme compared to otherasymmetric key algorithms, RSA algorithm is implemented toperform digital signature verification and incur least cost.

VII. FINAL TRUST MANAGER

Final trust value of destination node is calculatedwith energy value, trust value and packet veracity check value.These values are assigned by each node and generate nodetrust table for each node. The table contains Node ID, Trustvalue, Trust type and Trust timeout. The centralized authoritynode request the final trust manager torecompute the trustvalue, the trust value of the node gets expired. Every timenode trust table updated when ever final trust managercomputing trust value,the final trust value is calculated as

FTValue = Evalue + Tvalue + PVCvalue

VIII. CERTIFICATE AUTHORITY

Any node with maximum trust value is elected ascertificate authority node. Final trust table helps to certificateauthority to obtain the trust value of each node. Based oncertificate authority only the network ensures the securetransmission and segregate the node with in time. Our valuenode get certificate from certified authority else node have tobe renewed again. When centralized authority moves out ofrange then the next maximum trust value elected as acentralized authority node.Source and destination nodes are certified bycentralized authority, and then it is eligible for packettransmission. The packet is encrypted using public key fromsource node and forwards it to the destination. In betweenpacket transmission the intermediate node cannot decrypt andview the message only, the destination node can decrypt thepacket using private key and view the message. In theproposed scheme MD4 algorithm used to hash the packetbecause it is least complex and incurs least energy cost.ISAKMP secure transmission started before theactual transmission between the source and destination node.Source node send request to certified authority node, thiscertified authority node encrypt it with shared key SKs. Afterreceiving this request certified authority node verifies whetherthe source and destination nodes are valid and also verifywhether the destination in its range. Certified authority nodesgenerate CERTA and CERTB encrypt with shared key SKs,SKd and forward to source and destination node. Both sourceand destination node decrypt CERTA and CERTB, makeauthentication and start communication if certificates arevalid.

IX. FUZZY BASED ANALYZER

Node reliability increases its trust level, when trustlevel represents positive experience and node reliabilitydecreases, when trust level represents negative experience.Fuzzy logic has trust values ranging between 0 and 1. Thetrust values of node can be calculated based on the computedEv, Tv, PVCv and FTv. These values are the fuzzy input valueand node mark as trusted node or malicious node based onfuzzy logic algorithm. When node establishes communicationto exchange packet data then fuzzy logic algorithm calledautomatically. If the fuzzy values falls below a criticalthreshold value then node marked as malicious.When communication initializes between two nodes,source node sends request to certified authority for certify thenode trust value, now fuzzy analyzer is invoked. Fuzzyanalyzer verifies the trust level of source node and performfuzzy table based on fuzzy analyzer algorithm. Certifiedauthority determines the node is TRUSTED or MALICIOUSbased on trust value. Certified authority find the requestingnode as malicious then generate ALARM message and send tothe entire trusted node in its range. Requester node is trustedthe certificate authority to generate certificate based on fuzzybased analyzer and sends to the request node. Node makessecure transmission when fuzzy values are VERY HIGH,HIGH and MEDIUM. Node fuzzy values are

LOW andVERY LOW is marked as malicious node, certified authoritydenies certificate for malicious node in the network. Whennode certificate expired issued by the certificate authority,then trust node send request for renewal of certificate before itstarts transmission.

X. SIMULATION CONFIGURATIONS

When comparing the simulation results with other research works, it is clear that the default scenario setting in NS 2.34 has been adopted. The maximum hops allowed in this configuration setting.

Table 1 Simulation parameter

Parameter	Value
Simulation area	680m * 680m
Routing Protocol	AODV & DSR
Number of nodes	1000
Average speed of nodes	0–20 meter/second
Mobility model	Random waypoint
No. of packet per/sec	4
Transmission range	300 m
Constant bit rate	3 (packets/second)
Packet size	512 bytes
Node beacon interval	0.5 (seconds)
MAC protocol	802.11 DCF
Initial energy/node	100 joules
Antenna model	Omni directional
Simulation time	600 sec

XI. RESULT & DISCUSSION

In this research work, simulated network consists of nodes like, 20, 40, 60, 80, 100 mobile nodes placed randomly within fixed topology size. In this model, a node selects a destination randomly within the roaming area and moves towards that destination at a predefined speed 30 m/s. our results analysis the following parameters packet delivery ratio, routing overhead and throughput.

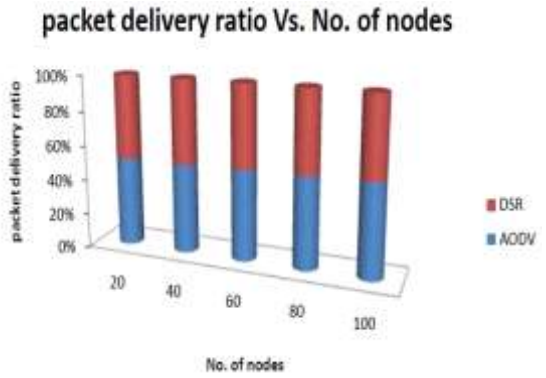

Fig 1 packet delivery ratio Vs. Number of nodes

From Figure 1it's clear that our proposed scheme AODV surpassed DSR performance by above 2% when there are 20 to 100 nodes in the network. This method is able to detect misbehaviours in the presence of block-hole attacks.

Table 2 Results of RO and Throughput

Routing Overhead					
DSR	**0.36**	**0.34**	**0.32**	**0.30**	**0.28**
AODV	**0.27**	**0.25**	**0.23**	**0.21**	**0.19**
Throughput					
DSR	**0.47**	**0.45**	**0.43**	**0.41**	**0.39**
AODV	**0.53**	**0.51**	**0.49**	**0.47**	**0.45**

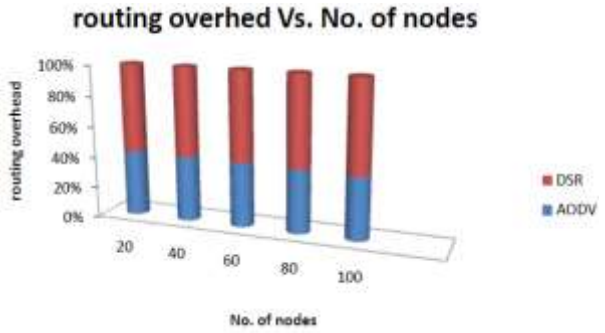

Fig 2 Routing overhead Vs. Number of nodes

From Figure 2and Table 2 it's clear that the comparing of the AODV with corresponding misbehaviour detection algorithm shows the routing overhead reduced with increase in the number of nodes by 20 to 100.

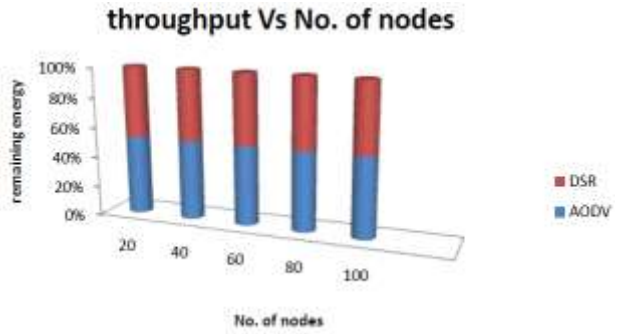

Fig 3 Throughput Vs. Number of nodes

Figure 3 and Table 2 clearly depict comparison of DSR with corresponding misbehaviour detection algorithm along with AODV where it shows the throughput increases with increase in the number of nodes on by 20 to 100.

From all the figures it's clear that the comparison of the AODVandDSR with misbehaviour detection algorithm shows the turnout and packet delivery ratio increase with the rise within the range of number of nodes and additionally throughput and routing overhead decease with the rise within the range of nodes.

XII. CONCLUSION AND FUTURE WORK

In this research paper, they focus on black-hole security attack based ontrust metrics and fuzzy logic and avoid black-hole attackduring route discovery. Normally AODV and DSR protocols are affecteddue to selfish node, which results in high packet delivery ratio and throughput. Fuzzy trust model proposed to detect theblack-hole attack in AODV and DSR protocol. NS 2.34 simulation usedto simulate the MANET and experiment the performance ofpacket delivery ratio, throughput and routing overhead. Theexperimental setup of proposed fuzzy trust scheme givesbetter delivery ratio, throughput, less congestion.

REFERENCE

[1]. Perkins and Royer (2000) "The Ad-hoc On-demand Distance Vector Protocol", Ad hoc Networking, pp. 173–219, Addison-Wesley.
[2]. Adams, et al (2005) "Calculating a Node's Reputation in a Mobile Ad Hoc Network," Proc. 24th IEEE International Conference, Vol. 7, No. 9, pp. 303-307.
[3]. Sen, et al (2008) "Wireless Ad Hoc Networks; In: Chapter 17-Intrusion Detection in Mobile Ad Hoc Networks", Springer.
[4]. LathaTamilselvan and Sankaranarayanan (2008) "Prevention of Co-operative black-hole Attack in MANET" JOURNAL OF NETWORKS, Vol. 3, No. 5.
[5]. Payal and Prashant (2009) "DPRAODV: ADynamic Learning System against black-hole attack in AODVbased MANET ", International Journal of Computer Science,Vol. 2.
[6]. AkankshaSaini and Harish Kumar (2010) "Comparison between various black-hole Detection techniques in MANET" NCCI 2010, INDIA.
[7]. Baddache and Belmehdi (2010) "Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks," International Journal of Computer Science and Information Security, Vol. 7, No. 1, pp. 10-16.
[8]. Imani, et al (2010) "Vulnerabilities in network layer at WMN," International Conference on Educational and Networking Technology, pp. 487-492.
[9]. Gupta, et al (2010)"Performanceanalysis of AODV, DSR & TORA Routing Protocols, International Journal of Engineering and Technology, Vol.2,No.2.

[10]. khamayseh, et al (2011) "A New Protocol for Detecting Black -hole Nodes in Ad Hoc Networks" International Journal ofCommunication Networks and Information Security.
[11]. Shailender Gupta, et al (2011) "Impact of Selfish Node Concentration in MANETS, International Journal of Wireless & Mobile Networks, Vol. 3, No. 2.
[12]. Sethi, et al (2011) "Fuzzy-based trustedant routing (FTAR) protocol in mobile ad hoc networks",Multi-disciplinary Trends in Artificial Intelligence, Springer, pp. 112-123.

Biography:

K. Thamizhmaran received his BE and ME from Annamalai University, Tamilnadu, India in 2008 and 2012, respectively. He is currently working as an Assistant Professor of ECE in the Department of Electronics and Communication Engineering, Annamalai University, Annamalai Nagar, Chidambaram, Tamilnadu, India. His research interest includes networks security, ad-hoc networks, mobile communications, and digital signal processing. He has published more than 89 technical papers at various national / international conferences and in journals. He is a life member of IAENG and IACSIT.