International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Implementation and Comparison of Enhance SAODV Protocol against Blackhole Attacks in MANET using Network Simulator

Anil[1], Dr. Sudesh Kumar[2]

[1]M.Tech Scholar, Department of Computer, Science and Engineering BRCM CET, Bahal, Haryana, India

[2]Assistant Professor, Department of Computer, Science and Engineering BRCM CET, Bahal, Haryana, India

Abstract: ***Mobile Ad-Hoc Networks has the ability to deploy a network where a traditional network Infrastructure environment cannot possibly be deployed. Security of MANET is one of the important features for its deployment. In our proposed work we analyzed that Black Hole attack with three different scenarios with respect to the performance parameters of End-to-End Delay, Throughput and Packet Delivery Ratio. In a network it is important for a protocol to be redundant and efficient in term of security. We have analyzed the vulnerability of two protocols Secure AODV and AODV .The percentage of Packet Delivery Ratio of Secure AODV is better as compare to the AODV. The throughput of Secure AODV is better as compare of AODV. In case of End to End Delay however, there is effect on Secure AODV by the malicious node is similar to the AODV***

Keywords: MANET, Routing Protocol, Attack, AODV, Blackhole, SAODV

1. Introduction

Wireless cellular systems have been in use since 1980s. We have seen their evolutions to first, second and third generation's wireless systems. These systems work with the support of a centralized supporting structure such as an access point. The wireless users can be connected with the wireless system by the help of these access points, when they roam from one place to the other. The adaptability of wireless systems is limited by the presence of a fixed supporting coordinate. It means that the technology cannot work efficiently in that places where there is no permanent infrastructure. Easy and fast deployment of wireless networks will be expected by the future generation wireless systems. This fast network deployment is not possible with the existing structure of present wireless systems. MANETs face different securities threats i.e. attack that are carried out against them to disrupt the normal performance of the networks. These attacks are categorized in "security issues in MANET" on the basis of their nature. In these attacks, black hole attack is that kind of attack which occurs in Mobile Ad-Hoc networks (MANET). This Black Hole attack and other attacks that are carried out against MANETs. Two types of black hole attack can be described in AODV in order to distinguish the kind of black hole attack.1. Internal Black hole attack This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination. 2. External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET.

2. Related Work

Harmandeep Singh have implemented an AODV protocol that simulates the behaviour of a black hole in NS-2.In this method we have used very simple and effective way of providing security in AODV against black hole attack that causes the interception and confidentiality of the ad hoc wireless networks. The solution detects the malicious nodes and isolates it from the active data forwarding. Though the algorithm is implemented and simulated with AODV routing algorithm, we believe that the solution can also be used by other routing algorithm as well.

Satoshi Kurosawa have analyzed the blackhole attack and introduced the feature in order to define the normal state of the network. We have presented a new detection method based on dynamically updated training data. Through the simulation, our method shows significant effectiveness in detecting the blackhole attack.

Payal N. Raj have proposed a DPRAODV (Detection, Prevention and Reactive AODV) to prevent security threats of blackhole by notifying other nodes in the network of the incident. The simulation results in ns2 (ver- 2.33) demonstrate that our protocol not only prevents blackhole attack but consequently improves the overall performance of (normal) AODV in presence of black hole attack.

Sanjay Ramaswamy have studied the routing security issues of MANETs, described the cooperative black hole attack that can be mounted against a MANET and proposed a feasible solution for it in the AODV protocol. The proposed solution can be applied to 1.) Identify multiple black hole nodes cooperating with each other in a MANET; and 2.) Discover secure paths from source to destination by avoiding multiple black hole nodes acting in cooperation.

Heta Changela proposed a technique for black hole attack by using RREQ_ACK. If source node receive the RREQ_ACK then compare DSN and SSN value, if DSN greater than the SSN then discard that node from the quarantine list. With this scheme we compare some parameter like throughput, End-to-End delay and Packet delivery ratio. Throughput is increase as compare to attacker node and PDF will also increase. We

can apply this proposed solution to identify and remove any number of black hole in a MANET and discover a safe path from source to destination by diverting the malicious nodes.

Neetika Bhardwaj have studied the effect of Blackhole Attack on AOMDV protocol and the results were obtained by varying the number of malicious nodes. We have also proposed a new approach to detect and prevent the Blackhole attack in AOMDV protocol and have implemented the same using NS 2 simulation tool. Simulation results show that the proposed technique was found to increase the packet delivery ratio and throughput near to the original values that were obtained when there were no malicious nodes in the network. Even when the number of malicious nodes was incremented the proposed approach did not waver and produced the same results. Also the proposed approach has negligible false detection ratio and can detect single, multiple and cooperative blackhole attacks. It does not even require any extra memory and has nominal routing overhead so it is found to be better than the approaches yet proposed for detecting and preventing the Blackhole attack.

3. Black Hole Attack in MANET

MANETs face different securities threats i.e. attack that are carried out against them to disrupt the normal performance of the networks. In these attacks, black hole attack is that kind of attack which occurs in Mobile Ad-Hoc networks (MANET). In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it . In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address . The method how malicious node fits in the data routes varies.

Objectives: Study of Mobile Ad hoc network(MANET)

1) Detail study of AODV Routing protocols
2) The study focus on analysis of black hole attack in MANET and its consequences.
3) Analyzing the effects of black hole attack in the throughput, packet delivery ratio and end-to-end delay in MANET.
4) Simulating the black hole attack using AODV routing protocol.
5) Discuss the result of the proposed work with existing black hole attack in MANET.

4. Ad-Hoc on Demand Distance Vector Protocol (AODV)

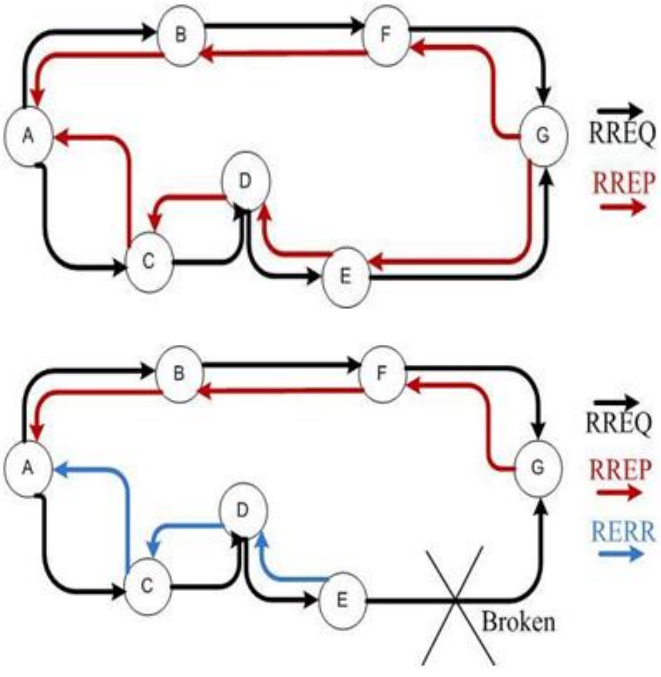
AODV is reactive protocol, when a node wishes to start transmission with another node in the network to which it has no route; AODV will provide topology information for the node. AODV use control messages to find a route to the destination node in the network. There are three types of control messages in AODV which are discussed bellow.

Route Request Message (RREQ): Source node that needs to communicate with another node in the network transmits RREQ message. AODV floods RREQ message, using expanding ring technique. There is a time to live (TTL) value in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted.

Route Reply Message (RREP): A node having a requested identity or any intermediate node that has a route to the requested node generates a route reply RREP message back to the originator node.

Route Error Message (RERR): Every node in the network keeps monitoring the link status to its neighbor's nodes during active routes. When the node detects a link crack in an active route, (RERR) message is generated by the node in order to notify other nodes that the link is down.

Route Discovery Mechanism in AODV: When a node "A" wants to initiate transmission with another node "G" as shown in the Fig. it will generate a route request message (RREQ). This message is propagated through a limited flooding to other nodes. This control message is forwarded to the neighbors, and those node forward the control message to their neighbors' nodes. This process of finding destination node goes on until it finds a node that has a fresh enough route to the destination or destination node is located itself. Once the destination node is located or an intermediate node with enough fresh routes is located, they generate control message route reply message (RREP) to the source node. When RREP reaches the source node, a route is established between the source node "A" and destination node "G". Once the route is established between "A" and "G", node "A" and "G" can communicate with each other. Fig. depicts the exchange of control messages between source node and destination node.



When there is a link down or a link between destinations is broken that causes one or more than one links unreachable from the source node or neighbors nodes, the RERR message is sent to the source node. When RREQ message is broadcasted for locating the destination node i.e. from the node "A" to the neighbors nodes, at node "E" the link is broken between "E" and "G", so a route error RERR message is generated at node "E" and transmitted to the source node informing the source node a route error, where "A" is source node and "G" is the destination node.

5. Security Issues in MANET

Security in Mobile Ad-Hoc Network (MANET) is the most important concern for the basic functionality of network. MANET often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats.

In the last few years, security of computer networks has been of serious concern which has widely been discussed and formulized. Most of the discussions involved only static and networking based on wired systems. However, mobile Ad-Hoc networking is still in need of further discussions and development in terms of security . With the emergence of ongoing and new approaches for networking, new problems and issues arises for the basics of routing. With the comparison of wired network Mobile Ad-Hoc network is different. The routing protocols designed majorly for internet is different from the mobile Ad-Hoc networks (MANET). Traditional routing table was basically made for the hosts which are connected wired to a non dynamic backbone. Due to which it is not possible to support Ad-Hoc networks mainly due to the movement and dynamic topology of networks. Due to various factors including lack of infrastructure, absence of already established trust relationship in between the different nodes and dynamic topology, the routing protocols are vulnerable to various attacks . Major vulnerabilities which have been so far researched are mostly these types which include selfishness, dynamic nature, and severe resource restriction and also open network medium. Despite of the above said protocols in MANET, there are attacks which can be categorized in Passive, Active, Internal, External and network-layer attacks, Routing attacks and Packet forwarding attacks. MANET work without a centralized administration where node communicates with each other on the base of mutual trust. This characteristic makes MANET more vulnerable to be exploited by an attacker from inside the network. Wireless links also makes the MANET more susceptible to attacks which make it easier for the attacker to go inside the network and get access to the ongoing communication.

6. Methodology

Network Simulator

A network simulator is software that predicts the behavior of a computer network. Nowadays, there are many network simulators that can simulate the network scenario. In simulators, the computer network is typically modeled with devices, links, applications etc. and the performance is analyzed.

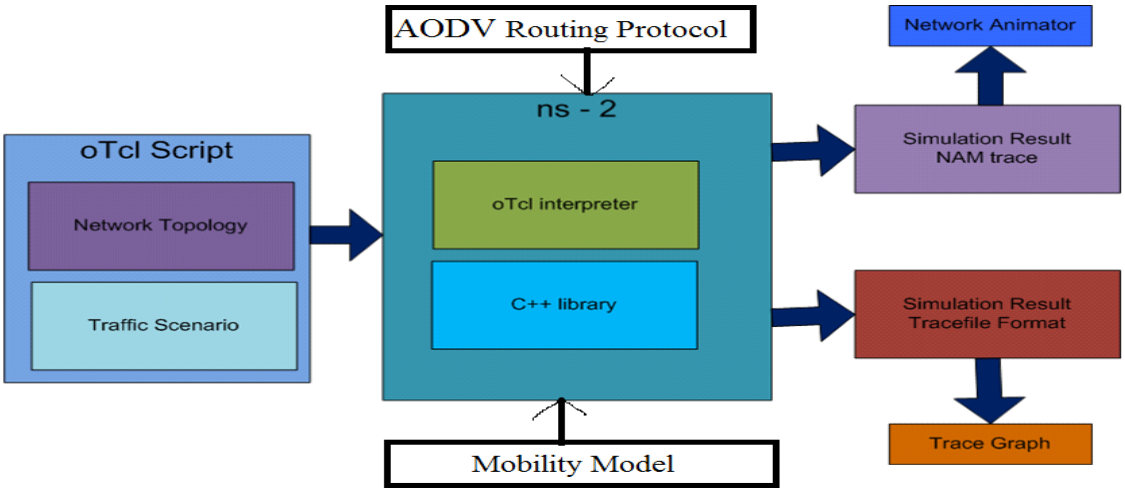


Figure: NS2 Working

Experimental Work & Results

Parameters Used

Simulation Parameters	*Value*
Network Simulator	NS-2.35
Routing Protocols	AODV, BlackholeAODV, SAODV
Simulation Area	2000m x1500m,
Number of Nodes	50,100,150,225,315
MAC Protocol	IEEE802.11b
Simulation Time	100 sec.
Connection Type	TCP
Packet Size	1500 Bytes
Data Rate	1 Mbps
Mobility Model	Random waypoint model
Pause Time	2 sec.
Nodes Speed	20 m/ sec.
Antenna	Antenna/OmniAntenna
Propagation Model	Propagation/TwoRayGround
Channel	Channel/WirelessChannel
Attack Type	Blackhole Attack

Secure AODV

1 Algorithms

Assumption: RREP header is modified with additional field that is Speed of node.

Step 1: Source S broadcasts RREQ message to the network with digital signature.

Step 2: If **Destination D** replies RREP with digital signature then S will start transmission.

END

Step 3: If **intermediate node (say Y)** replies with RREP and when packet reaches node Y's **precedingnode@ (say X),** it checks the following:

if (RREQ digital signature match with RREP digital signature)

GOTO Step 5.

else

GOTO Step 4.

Step 4: If (digital signature S key1 ‡ digital signature D key2)

Node X will send a Modified Hello signal (**MHELLO**) with key1 to a **Node@@ (say Z)** which is few hops away from X.

If X receives acknowledgment from Z successfully then

X forwards RREP to S and S will transmit the data.

Else

Node next to Y is Blackhole and an alert signal will be transmitted by X to S.

Else

Node Y is Blackhole node and an alert signal will be transmitted by X to S.

Step 5: X forwards RREP to S and S will transmit the data.

7. Simulation Results

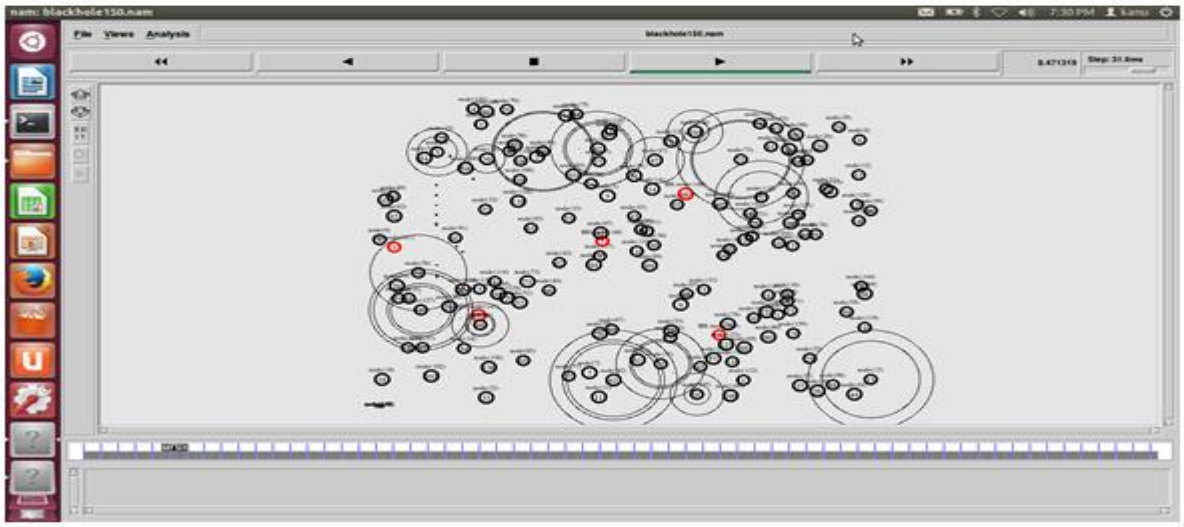
Performance Metrics

There are following performance matrices to evaluate the performance of the routing protocols.

Throughput

It measures how well the network can constantly provide data to the destination**.** It is the ratio of the total amount of data that reaches a receiver from a sender to the time it takes for the receiver to get the last packet.

Simulation scenario of 150 Nodes



Throughput=(Received byte*8)/ (Simulation time 1024*1024)

It is derived in Mbps. For achieving better performance it should be high.

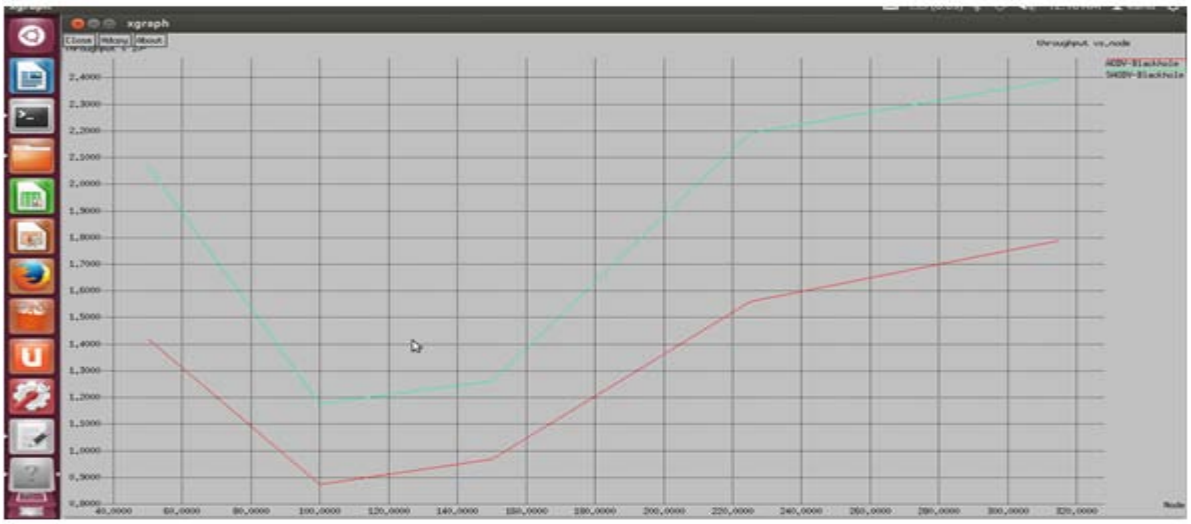
Packet Delivery Ratio

The ratio of the number of data packets delivered to the destination nodes and the number of data packets sent by source nodes.

Packet delivery ratio= (Received packet)/ (Sent packet);

Packet delivery ratio %= [(Received packet)/ (Sent packet)]*100;

PACKET DELIVERY RATIO



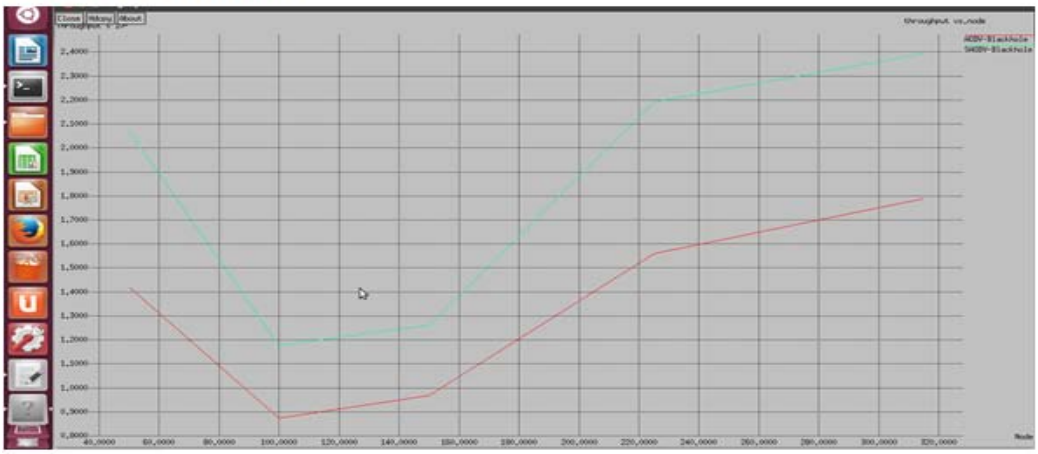
The performance would be better when it is high. It measures the loss rate as seen by transport protocols and as such, it characterizes both the correctness and efficiency of ad hoc routing protocols. A high packet delivery ratio is desired in any network.

End to end delay

The average time interval between the generation of packets in a source node and successfully delivery of it in a destination node.

End-to-end delay= Delay sum/ Received packets

END TO END DELAY



The performance would be better when it is low. It therefore includes all the delays in the network such as buffer queues, transmission time and delays induced by routing activities and MAC control exchanges.

8. Conclusion and Future Scope

Mobile Ad-Hoc Networks has the ability to deploy a network where a traditional network Infrastructure environment cannot possibly be deployed. Security of MANET is one of the important features for its deployment. In our proposed work we analyzed that Black Hole attack with three different scenarios with respect to the performance parameters of End-to-End Delay, Throughput and Packet Delivery Ratio. In a network it is important for a protocol to be redundant and efficient in term of security. We have analyzed the vulnerability of two protocols Secure AODV and AODV .The percentage of Packet Delivery Ratio of Secure AODV is better as compare to the AODV. The throughput of Secure AODV is better as compare of AODV. In case of End to End Delay however, there is effect on Secure AODV by the malicious node is similar to the AODV.Based on our research and analysis of simulation result we draw the conclusion that Secure AODV is more vulnerable to Black Hole attack than AODV.

For future work several directions are possible. Like by apply Prevention and detection technique of blackhole attack on Secure AODV routing protocol and compare with the existing Secure AODV routing protocol.

References

[1] Harmandeep Singh, Manpreet Singh, “Securing MANETs Routing Protocol under Black Hole Attack” International Journal of Innovative Research in

Computer and Communication Engineering , www.ijircce.com, Vol. 1, Issue 4, June 2013.

[2] Satoshi Kurosawa , Hidehisa Nakayama , Nei Kato , Abbas Jamalipour, and Yoshiaki Nemoto, **"Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method"** International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007.

[3] Payal N. Raj, Prashant B. Swadas, **"DPRAODV: A Dyanamic learning system against blackhole attack in AODV based MANET",** IJCSI International Journal of Computer Science Issues, Vol. 2, 2009, ISSN (Online): 1694-0784.

[4] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, **"Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks".**

[5] Heta Changela, Amit Lathigara, **"Algorithm to Detect and Overcome the Black Hole Attack in MANETs",** International Journal of Computer Applications (0975 – 8887) Volume 124 – No.8, August 2015. [6] Steve Ford, "American Radio Relay League", ARRL's VHF Digital Handbook, p 1-2, 2008.

[6] Neetika Bhardwaj, Rajdeep Singh, **"Detection and Avoidance of Blackhole Attack in AOMDV Protocol in MANETs"**, International Journal of Application or Innovation in Engineering & Management (IJAIEM) Web Site: www.ijaiem.org Email: editor@ijaiem.org, Volume 3, Issue 5, May 2014, ISSN 2319 – 4847.

[7] C. R. Lin and J.-S. Liu, "QoS routing in ad hoc wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 17, no. 8, pp. 1426–1438, Aug. 1999.

[8] "Distance-vector routing protocol," *Wikipedia, the free encyclopedia*. 07-Jun-2016.

[9] Qi Xue , Aura Ganz, "Ad hoc QoS on-demand routing (AQOR) in mobile ad hoc networks." Journal of Parallel and Distributed Computing Volume 63, Issue 2, February 2003, Pages 154–165.