INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

TRUST BASED ROUTING SCHEME FOR MANETS IN ADVERSARIAL ENVIRONMENT THROUGH AASR PROTOCOL

Lavanya K N[1], Dr. Deepa Anand[2]

[1]Mtech (CNE) CMRIT, Bangalore, naubadelavanya.24@gmail.com
[2]Associate prof (MCA), CMRIT, Bangalore, India

Abstract: - Anonymous Communications are important for many applications of the MANETs deployed in adversary environments. Mobile ad hoc networks are vulnerable to security threats due to the open wireless medium and dynamic topology. The main need of network is to provide unidentifiability and unlinkability for mobile nodes. The existing protocol works on the basis of authentication by group signature and onion routing protocol on the authentication. AASR protocol concept is to defend the neighbour nodes attack by the way of key-encryption and decryption in route-request and route-reply. In this proposed system routing protocol method is Authenticated Anonymous Secure Routing with Trust based model.The Calculation of trust value of each node helps to avoid the end-to-end packet transfer delay between nodes.

Keywords*:* Trust Model, Authenticated Routing, Diffie-Hellman, Mobile Ad hoc Network.

1. Introduction

Mobile ad hoc network (MANET) is a set of wireless devices or nodes, which are dynamically, connect and survey information in a network. These wireless nodes may be personal computers (desktop/laptop) with wireless LAN cards, Personal Digital Assistants (PDA), or other types of wireless or mobile communication devices. Anonymous Communications are important for many applications of the MANETs deployed in adversary environments. Anonymity is defined as the state of being unidentifiable and unlinkability. Unidentifiable means the identities of the source and destination nodes cannot be revealed to other nodes. Unlinkability means that the route and traffic flow between the source and destination nodes cannot be pretended or the two nodes cannot be linked. The major aspect to provide an anonymous communication needs a secure routing protocol ie anonymous protocol. Many Anonymous protocol has been proposed in last decade based on topology on demand routing protocol. In order to provide an anonymous routing we need to anonymous the on-demand routing protocols. The protocols with this features are ANODR, SDAR, AnonDSR, MASK, and Discount ANODR, but these protocol are not fully satisfied with the concept of anonymity and are vulnerable to active attacks like denial of service and al. AASR protocol even though overcome all the problems pre-mentioned above, does not provide an sufficient to anonymous secure delay reduce scheme during packet transmission. After observing this protocol, we find the objectives for secure routing with reduce delay by authenticated anonymous secure routing (AASR) with trust based routing Scheme. Each node of AASR consists of public and private key for authentication purpose. The authentication of packet is provided by Diffie-Hellman key exchange

method, which will use the public and private key of a node. The calculation of trust value of node is to reduce the delay in anonymous routing path.

2. System Model (AASR with Trust Model)

AASR protocol has been combined with the trust model in order to increase the packet delay in the network. Trust model involves the calculation of the trust value of each node in a network depending on the behaviour of nodes, and it includes overhead, throughput, packet ration, packet dropping rate and delay, and on the link quality. The packet delivery ration of node is identified by the delivery of a packet from one node to other node in a network and comparing it with the original packets.

2.1 System Architecture

AASR protocol has been used in MANETs to provide a secure anonymous communication in adversarial environments. It adopted a key-encrypted onion to record a discovered route and designed an encrypted secret message to verify the RREQ-RREP linkage, and group signature is used to authenticate the RREQ packet per hop, to prevent intermediate nodes from modifying the routing packet.

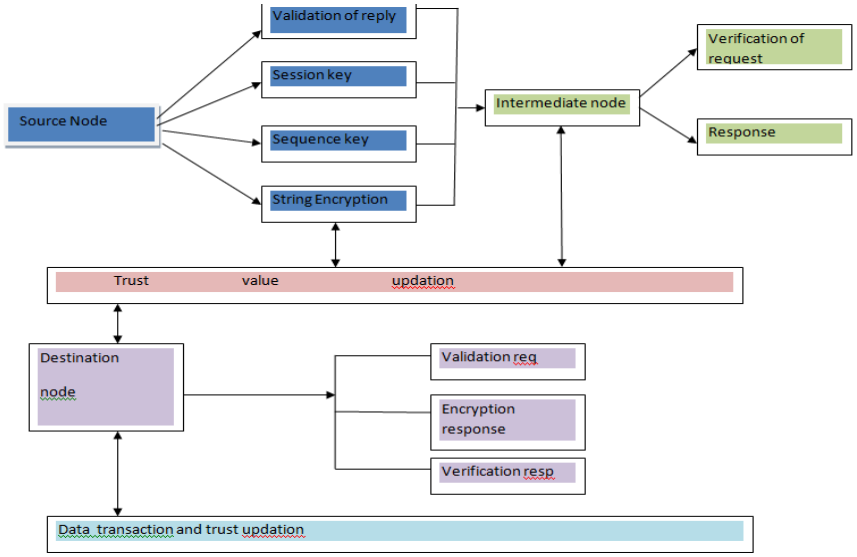


Fig 1. System Architecture

The source node generates the session and sequence number with the encrypted validation message and broadcast the request message to the trusted node. The intermediate nodes in the network with the public key verifies the route request and forwards it to destination node. The destination node in a session and with a public and private key do the validation of the route request and response back to the source with the same path .After route discovery the data transactions will take place between the source and destination node with validation process in a trustworthy network.

2.2 Trust Value Calculation and Authentication Procedure.

The trust level calculation is based on some basic parameters. They are:

Count Type	RREQ	RREP	Data
Success	Q_{rs}	Q_{ps}	Qds
Failure	Q_{rf}	Q_{pf}	Q_{df}

1.Q_{rs}- the query request success rate, which is calculated based on number of neighbouring nodes who have successfully received (rreq) from source node which has broadcasted it.

2.Q_{rf}- the query request failure rate which is calculated based on number of neighbouring nodes which have not received the query request.

3. Q_{ps}-the query reply success rate which is calculated as success replies (rrep) received by the source node which has sent the rreq.

4.Q_{pf}- the query reply failure rate which is calculated based on the number of neighbouring nodes which have not sent the replies for the query request received.

5. Q_{ds}- the data success rate calculated based on successfully transmitted data.

6. Q_{df}- data failure rate calculated based on data which have failed to reach destination.

$$Qr = \frac{q_{rs} - q_{rf}}{q_{rs} + q_{rf}}$$

$$Qp = \frac{q_{ps} - q_{pf}}{q_{ps} + q_{pf}}$$

$$Qd = \frac{q_{ds} - q_{df}}{q_{ds} + q_{df}}$$

Where Qr, Qp and Qd are intermediate values that are used to calculate the nodes Request rate , Reply rate and data transmission rate. The values of Qr , Qp, and Qd are normalized to fall in a range of -1 to +1.If the values fall beyond the normalized range then it clearly shows that the failure rate of the node is high and denotes that the corresponding node may not be applicable for routing.

TL=T(RREQ)*Qr+T(RREP)*Qp+T(DATA)*Qd

- TL is the trust value
- T(RREQ), T(RREP), and T(DATA) are time factorial at which route request, route reply and data are sent by the node respectively.

Authentication Procedure

For the authentication of a packet in a network it uses **Diffie-Hellman Key Exchange method.** This method has been used to encrypt the data while forwarding from one node to other by using public and private key of nodes after the verification of the packet in a network.

Diffie-Hellman Key Exchange method:

Diffie-Hellman Key Exchange method, which is a method for exchanging private keys using public key encryption. With Diffie-Hellman, asymmetric encryption is used to exchange session keys. These are limited-use symmetric keys for temporary communications; they allow two organizations to conduct quick, efficient, secure communications based on symmetric encryption. Diffie-Hellman provided the foundation for subsequent developments in public key encryption. Because symmetric encryption is more efficient than asymmetric for sending messages, and asymmetric encryption doesn't require out-of-band key exchange, asymmetric encryption can be used to transmit symmetric keys in a hybrid approach. Diffie-HeIlman avoids the exposure of data to third parties that is sometimes associated with out-of-band key exchanges.

3. Simulation Results

Scenario1-
Creation of nodes

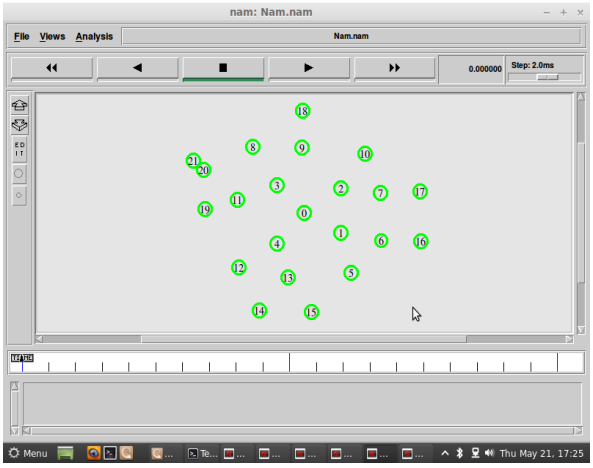
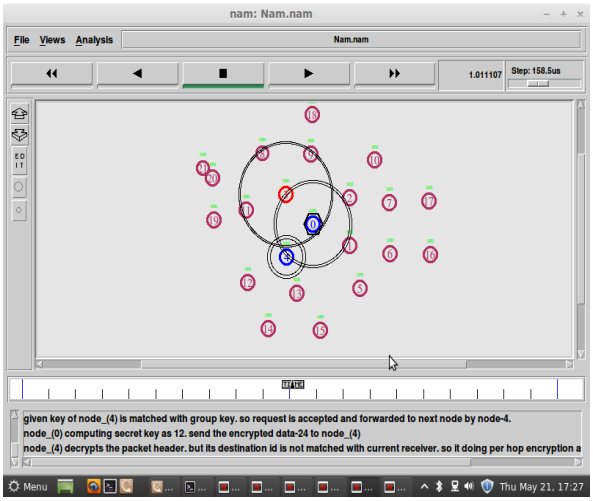
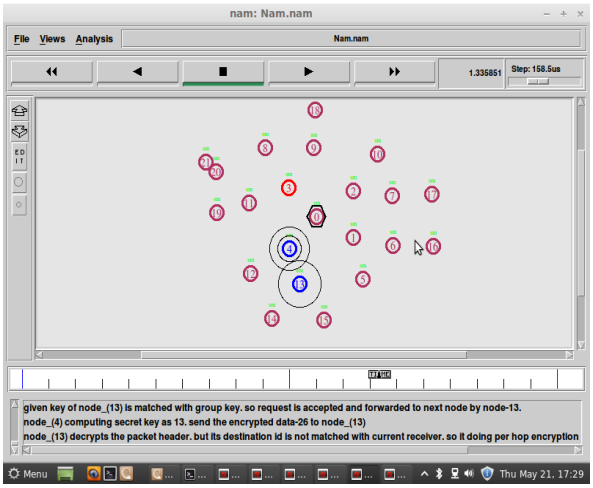


Fig 2 Node creation

Scenario2-
Node selection for data transmission and malicious node detection (red node)





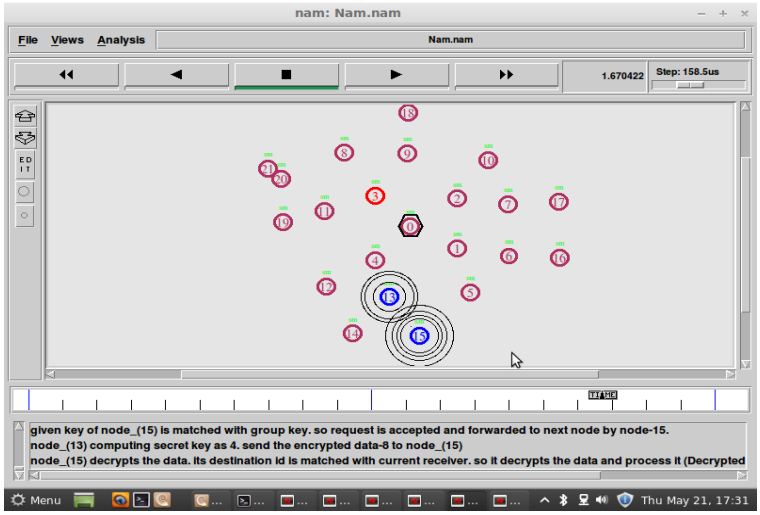
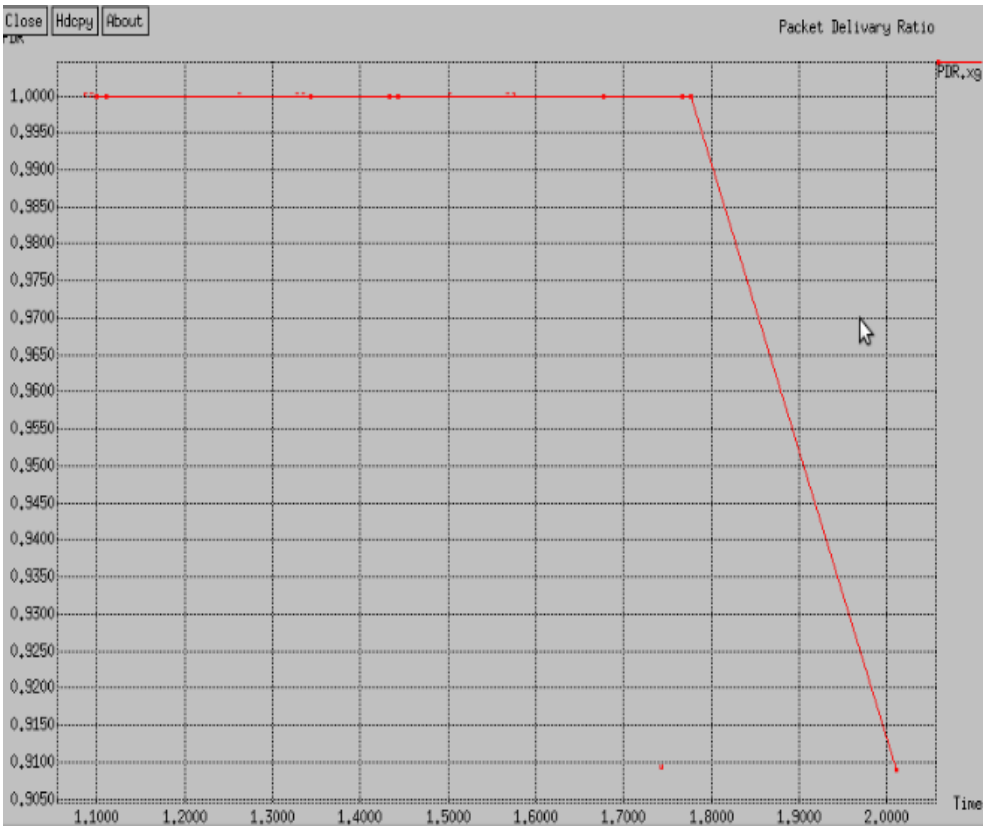


Fig 3 Node selection and data transmission.

Scenario3-
Throughput, Packet Delivery ration, Energy Consumption, Packet drop graphs.
Packet Delivery Ration



Throughput

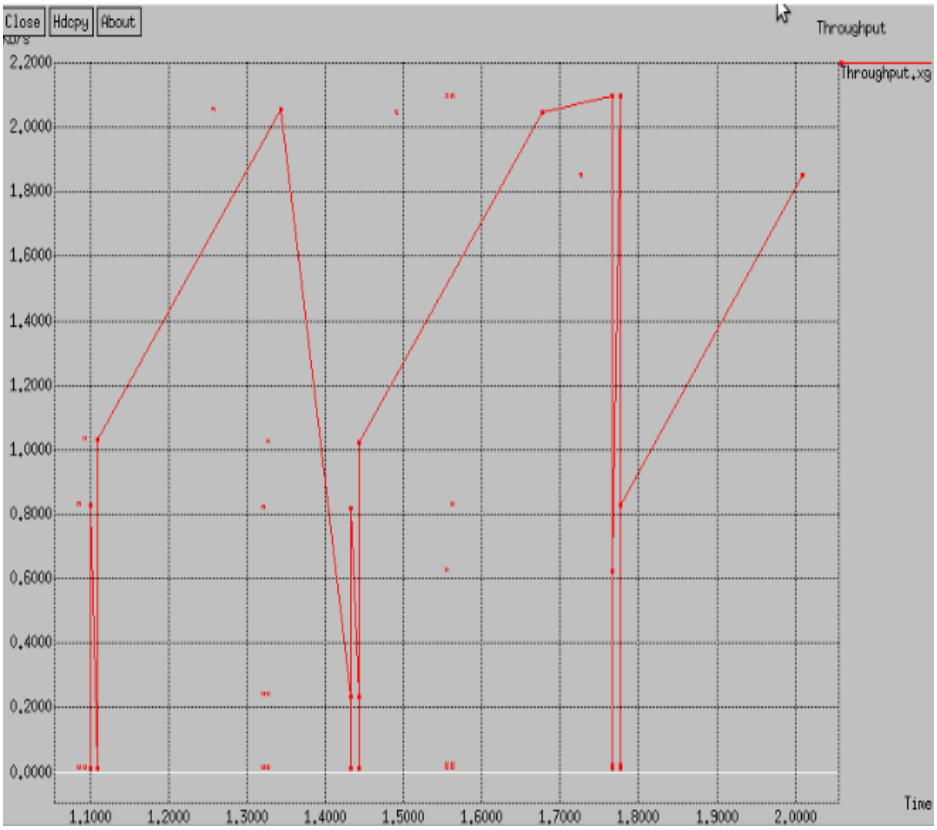
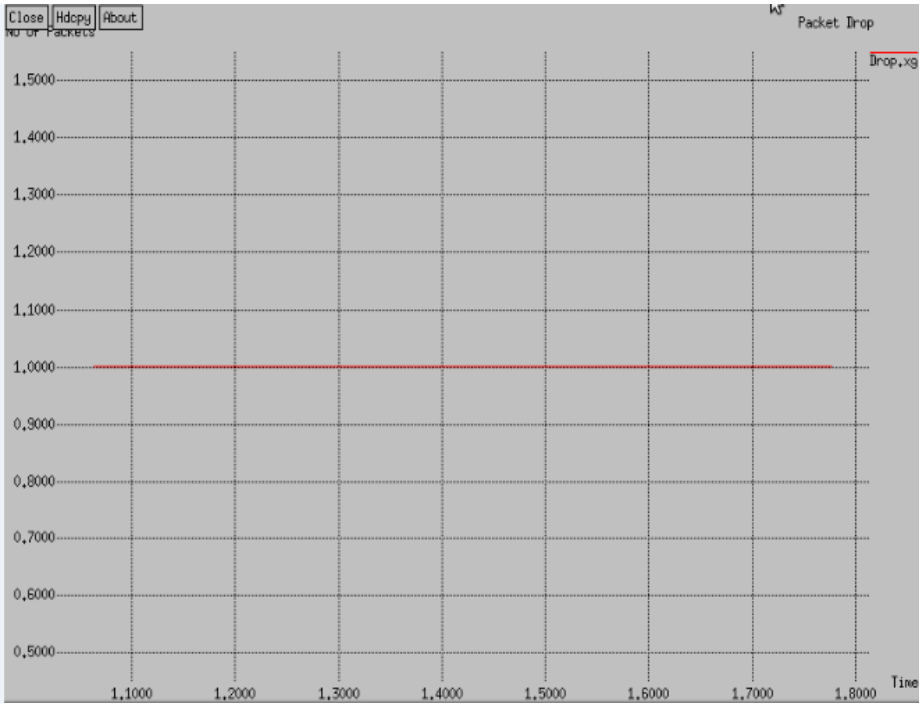


Fig 4 Performance Graph

Packet Drop



Energy Consumption

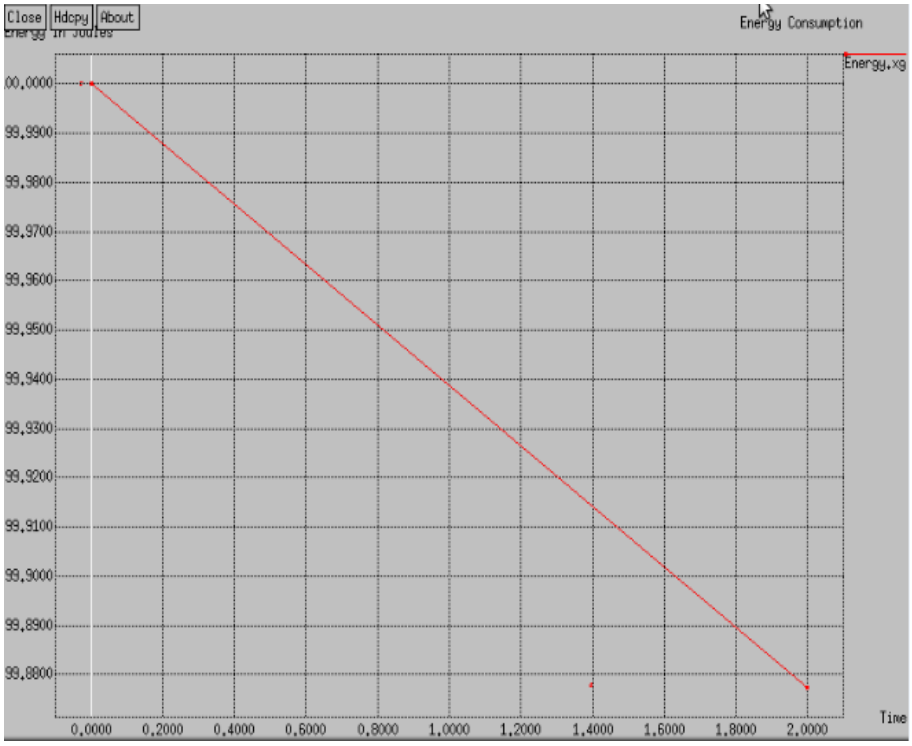


Fig 5 Performance Graph

4. Conclusion and Future Scope

In this paper, we design a trust based authenticated anonymous routing protocol design for MANETs in adversarial environment through AASR protocol. It uses a trust value and link quality based concept in forwarding the favor packet to the next node. The route request packets are authenticated by using diffie-Hellman encryption method, which can defend the potential active anonymous attacks without unveiling the node identities. In this proposed scheme, authorized node has high throughput, and packet delivery ratio can be improved significantly with decreasing average end to end delay by increasing trust value. The same scheme can also be implemented on other MANET routing protocols and also implement some techniques for authenticating the packet and the node which take part in routing.

Future Scope: The future work can be to find an alternative path in detection of any malicious node in data transmission route. A possible method is to use any different encryption method in the authentication of nodes.

REFERENCES

[1] D. Kelly, R. Raines, R. Baldwin, B. Mullins, and M. Grimaila, "Towards a taxonomy of wired and wireless anonymous Networks, "in *Proc. IEEE WCNC'09*, Apr. 2009.

[2] C. Perkins, E. Belding-Royer, S. Das, *et al.*, "RFC 3561 - Ad hoc On-Demand Distance Vector (AODV) Routing," *Internet RFCs*, 2003.

[3] D. Johnson, Y. Hu, and D. Maltz, "RFC 4728 - The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4," *Internet RFCs*, 2007.

[4] J. Kong and X. Hong, "ANODR: Anonymous on Demand Routing with Untraceable Routes for Mobile Ad hoc networks," in *Proc. ACM MobiHoc'03*, Jun. 2003, pp. 291–302.

[5] J. Kong, X. Hong, and M. Gerla, "ANODR: An identity-free and on demand routing scheme against anonymity threats in mobile ad hoc networks," *IEEE Trans. on Mobile Computing*, vol. 6, no. 8, pp. 888–902, Aug. 2007.

[6] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: a Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Adhoc Networks," in *Proc. IEEE Int'l Conf. Local Computer Networks (LCN'04)*, Nov. 2004, pp. 618–624.
[7] R. Song, L. Korba, and G. Yee, "AnonDSR: efficient anonymous dynamicm source routing for mobile ad hoc networks," in *Proc. ACM Workshop Security of Ad Hoc and Sensor Networks (SASN'05)*, Nov. 2005.
[8] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in *Proc. IEEE INFOCOM 2005*, vol. 3, Mar. 2005, pp.1940–1951.
[9] Y. Zhang, W. Liu, W. Lou, and Y. G. Fang, "MASK: Anonymous On-Demand Routing in Mobile Ad hoc Networks," *IEEE Trans. on Wireless Comms.*, vol. 5, no. 9, pp. 2376–2386, Sept. 2006.
[10] L. Yang, M. Jakobsson, and S. Wetzel, "Discount anonymous on demand routing for mobile ad hoc networks," in *Proc. Int. Conf. on SECURECOMM'06*, Aug. 2006.
[11] M. Yu and K. Leung, "A Trustworthiness-based QoS routing protocol for ad hoc networks," *IEEE Trans. on Wireless Comms.*, vol. 8, no. 4, pp.1888–1898, Apr. 2009.