ISSN No. 0976-5697

Volume 5, No. 3, March-April 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Enhance RAODV Protocol using Multipath and Incentive System in MANET

Savitha Rohini K
P.G Scholar, Department of Computer Science and Engineering, Info Institute of Engineering,
Anna University,
Chennai, Tamil Nadu, India

Dhanasekar S
Assistant Professor, Department of Computer Science and Engineering, Info Institute of Engineering,
Anna University,
Chennai, Tamil Nadu, India

Abstract: Mobile ad hoc networks (MANETs) consist of a collection of wireless mobile nodes which dynamically exchange data among without reliance on a fixed base station or a wired backbone network and where the cooperation of nodes in packet forwarding is required for the network to function properly. However, since nodes in this network usually have limited resources, some selfish nodes might intend not to forward packets to save resources for their own use. In order to encourage the co-operation between the nodes in the system, many incentive mechanisms have been proposed like reputation system. In this paper, the efficiency of the incentive system has been analyzed based on past history of nodes in MANET and Enhanced The Reverse Ad Hoc on Demand Vector Routing Protocol (RAODV) by providing multipath packet forward system and Hybrid Reputation System (HRS) as Enhance Reverse Ad Hoc on Demand Vector Routing Protocol (ERAODV)..

Keywords: MANET; Reputation System; HRS; Packet Forward System; RAODV; Multipath Routing; ERAODV;

I. INTRODUCTION

A wireless ad hoc network is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding data. and MANETs are a kind of Wireless ad hoc network [17], [18] that usually has a routable networking environment on top of a Link Layer ad hoc network.

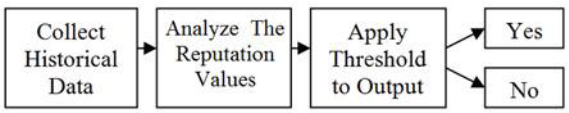
A MANET [1] is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. The network should be able to adaptively alter the routing paths to alleviate any of these effects. There are two types of routing protocols [3], [14] used in MANET, they are: Proactive and Reactive protocols.

Ad hoc On-Demand Distance Vector (AODV) Routing is a routing protocol for mobile ad hoc networks (MANETs) and other wireless ad-hoc networks. is a reactive routing protocol, meaning that it establishes a route to a destination only on demand. In contrast, the most common routing protocols of the Internet are proactive, meaning they find routing paths independently of the usage of the paths. Our aim is to design a new protocol based on Reverse Ad hoc On Demand Vector (RAODV) called as Enhanced Reverse Ad hoc On Demand Vector (ERAODV) which provides better security compared to AODV & RAODV

II. RELATED WORK

A. *Reputation System:*

The basic premise of a reputation system [2], [3] is that one can predict future behavior by looking at past behavior. This does not hold for all cases, since there can be erratic behavior that is completely inconsistent with past behavior, as in the case of sudden failure. But the assumption is that such cases are the exception and not the norm and that past behavior can be used as a basis for the prediction of future behavior. To provide this basis, the reputation system [4], [5], [6], [7], [8] has to keep track of past behavior. This can be done in several ways.



General framework of the Reputation System that decides whether to transact with a given node or not.

Figure.1 Reputation System

A reputation system [9], [10], [11] needs a way of keeping information about the entity of interest, of updating it and of incorporating the information about that entity obtained from others. Then the decision making itself has to take place to allow nodes to choose other nodes for cooperation. Keeping Track of Past Behavior, Reputation is a function of past behavior and time, so a reputation system needs to collect data about past behavior. These data can be stored in a centralized or in a distributed way. For self-organized networks, a distributed storage of reputation data

is needed, so ensure access to a centralized reputation authority.

B. Routing protocols:

Most currently proposed routing protocols for ad hoc networks are unipath routing protocols. In unipath routing, only a single route is used between a source and destination node. Two of the most widely used protocols are the Dynamic Source Routing (DSR) and the Ad hoc On-demand Distance Vector (AODV) protocols. AODV and DSR are both on-demand protocols.

Standard routing protocols [14], [18] in ad hoc wireless networks, such as AODV and DSR, are mainly intended to discover a single route between a source and destination node. Multipath routing consists of finding multiple routes between a source and destination node. These multiple paths between source and destination node pairs can be used to compensate for the dynamic and unpredictable nature of ad hoc networks. Multipath routing consists of three components: route discovery, route maintenance, and traffic allocation. Protocols are Split Multipath Routing and AOMDV.

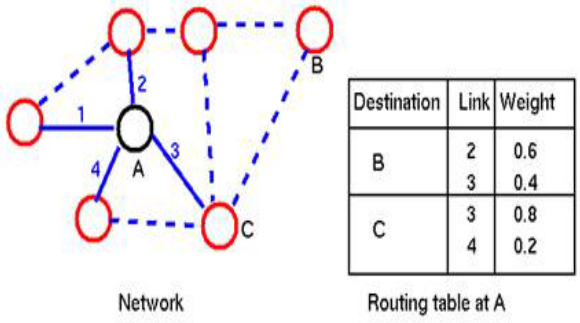
A reverse AODV which tries multiple route replies. The extended AODV is called reverse AODV (R-AODV), which has a novel aspect compared to other on-demand routing protocols on Ad-hoc Networks: it reduces path fail correction messages and obtains better performance than the AODV and other protocols have. Since R-AODV is reactive routing protocol, no permanent routes are stored in nodes. The source node initiates route discovery procedure by broadcasting. The

C. Multipath Routing System:

Multipath routing is the routing technique [14], [18] of using multiple alternative paths through a network, which can yield a variety of benefits such as fault tolerance, increased bandwidth, or improved security. The multiple paths computed might be overlapped, edge-disjointed or node-disjointed with each other. Extensive research has been done on multipath routing techniques, but multipath routing is not yet widely deployed in practice.

To improve performance or fault tolerance: CMR (Concurrent Multipath Routing) is often taken to mean simultaneous management and utilization of multiple available paths for the transmission of streams of data emanating from an application or multiple applications. In this form, each stream is assigned a separate path, uniquely to the extent supported by the number of paths available. If there are more streams than available paths, some streams will share paths. This provides better utilization of available bandwidth by creating multiple active transmission queues. It also provides a measure of fault tolerance in that, should a path fail, only the traffic assigned to that path is affected, the other paths continuing to serve their stream flows; there is also, ideally, an alternative path immediately available upon which to continue or restart the interrupted stream.

It is desirable to allow packets with the same source and destination to take more than one possible path. This facility can be used to overcome node failures and improve security. To operate such a scheme consistently nodes must maintain routing tables specifying what goes where. The mechanisms for this differ with datagram and virtual circuit transport.



Destination	Link	Weight
B	2	0.6
	3	0.4
C	3	0.8
	4	0.2

Figure. 2 Multipath Routing

The network above has all the links to node A numbered, its datagram routing table is shown. The weights in the table represent the probability of the link being chosen for the destination specified. A random number will decide where the packet actually goes. The weights represent ratios of some metric of path length. All virtual circuit packets in a given conversation must take the same route. When a conversation's first packet arrives at a node, it allocates the conversation a virtual circuit number on a selected link and sets this on the virtual circuit routing table, as shown. This allows the numbers of virtual circuits on a given link to be set (in relation to capacity etc.) at set-up and subsequently allocated as required by the network system.

III. PROPOSED SYSTEM

In our propose system, rather than integrating different incentive strategies [13], we focus on reputation based system alone and enhance it for the better identification and prevention of selfish nodes.

The main goal of this project is to detect the selfish nodes (Non co-operative nodes) [12], [14], [15], [16], [19], [25] in the network and avoid them to conserve computational resources such as power consumptions etc. And choose a trustworthy node in order to forward a packet in the network. We face problems while forwarding the packets in a single best path chosen as they are chance that the node in the path may drop the packets in order to retain its CPU resources. So our main goal is to efficiently increase the Throughput and finally provide Security by using hybrid reputation system. System Architecture fig 3 shows below for this system.

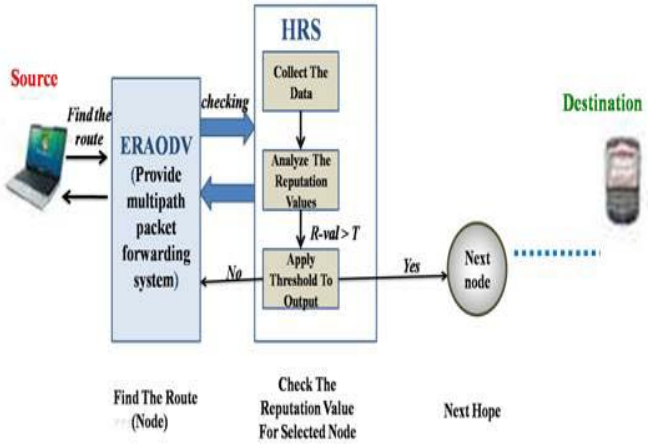


Figure.3 System Architecture

Secondly we provide essential security by using ERAODV that forwards the packet in a multi path manner, which provides security against the sniffing attacks on the network. So, by integrating both the hybrid system and the ERAODV, high throughput with security is achieved.

A. Hybrid Reputation System:

The Hybrid reputation system [20], [21], [24] has to have a mechanism to make decision and classifications. the concern ourselves mainly with the reputation information itself which uses the history. As time passes, the importance of parts of the reputation data collected can change. For instance, recent steady behavior is probably a better predictor of future behavior than behavior observed a long time ago. On the other hand, looking only at the most recent behavior can yield a distorted picture of past behavior as one instance observed is not enough to measure a trend. Fig. 4 shows the workings of an Hybrid reputation system. Several sources contribute to the generation of reputation values: direct (own) observations, indirect information from others, and time passing. Once the reputation value is determined, the subjects of interest can be classified and reactions according to these classifications can be triggered.

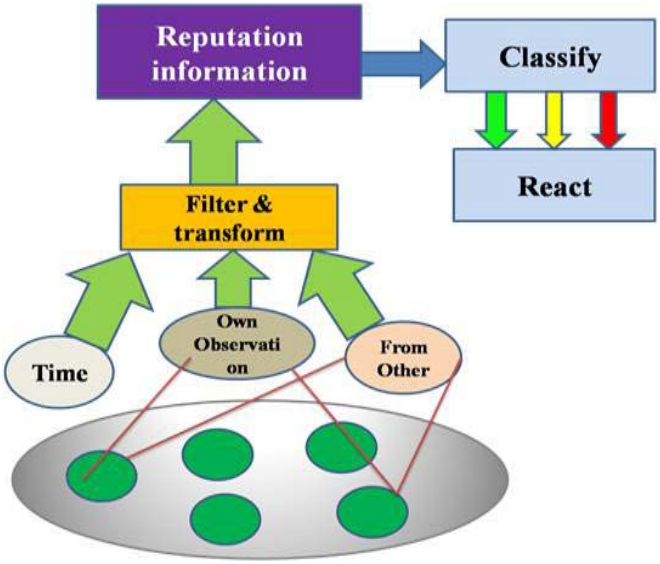


Figure.4 System Architecture for HRS

B. ERAODV Route Discovery:

When source node wants to communicate with destination and if path is not available to destination, then source floods or broadcasts RREQ. *i.e.* request packet to all its neighbors in the network. This RREQ message contains source and destination node's IP address, sequence number of destination, its current sequence number, hop count and RREQ ID. RREQ ID is monotonically increasing number. It gets incremented after each node initiates RREQ. Figure 5 illustrates this flooding procedure. When intermediate node receives RREQ, they create reverse link to previous node. They first of all check whether, valid route to destination is present or not. If, valid route is present then another condition must hold. i.e. intermediate node's sequence number should be at least as great as destination sequence number in RREQ packet. If both conditions hold, then that node generates RREP i.e. reply packet. If valid route is not present then RREQ is further forwarded. As RREQ is forwarded, hop count is incremented.

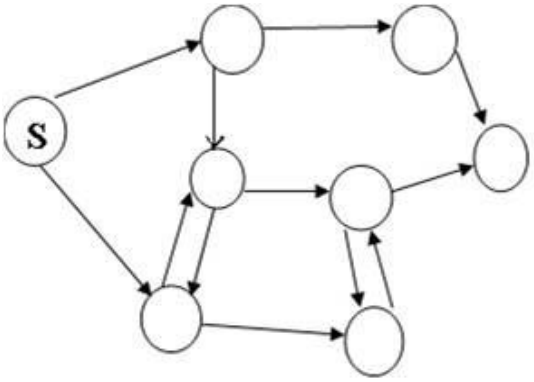


Figure 5 RREQ Broadcast

While sending RREQ, intermediate nodes start a timer. If reply doesn't come within that time means, there is no more active route or link failure has occurred. RREP contains IP address of source as well as destination, and destination sequence number. Once the node creates the forward route entry, it forwards the RREP to the destination node. The RREP is thus forwarded hop by hop to the source node. Once the source receives the RREP, it can utilize the path for the transmission of data packets.

C. ERAODV Route Maintenance:

As MANET is dynamic i.e. mobility and topology of nodes always change, link break occurs. When path breaks, both the nodes inform their end nodes about link failure, who were using that path by sending RERR i.e. error message as illustrated in Figure 3. End nodes delete their entries from route table, as path is no longer useful. If source node still wants to communicate with destination, it reinitiates RREQ broadcasting or path finding process or repair broken link.

D. Algorithm:

Begin

a. Initialize source and destination.
b. Find neighbors of source node.
c. Select the node which has the maximum reputation value.
d. Find the Reputation value using the formula
e. Reputation value = Last five reputations / 5;
f. Compare that value with the threshold value as
g. Reputation value >= threshold value.
h. If that returns true, declare that node as co-operative and send RREQ request to that neighbor.
i. Otherwise, do declare that node as non-cooperative and repeat steps 2-7 until the request is reached at the destination.
j. Reply via same path on which request is reached.

End

E. Enhanced Reverse Ad hoc On Demand Vector Routing Protocol (ERAODV):

Enhanced RAODV is our proposed protocol, which extends the Reverse AODV protocol. In Ad hoc networks, malicious nodes can enter in radio transmission range on the routing path and disrupt the network activity and also affect the performance of the whole network. Therefore, protecting the network from intrusion of malicious node and enhance data security is an important issue on Mobile Ad hoc networks. Enhanced RAODV provides a path hopping

method based on reverse AODV (R-AODV). By Reverse AODV, source node builds a multipath to the destination and adaptively hops all available paths for data communications. Hopping paths can protect data from the intrusion of malicious nodes.

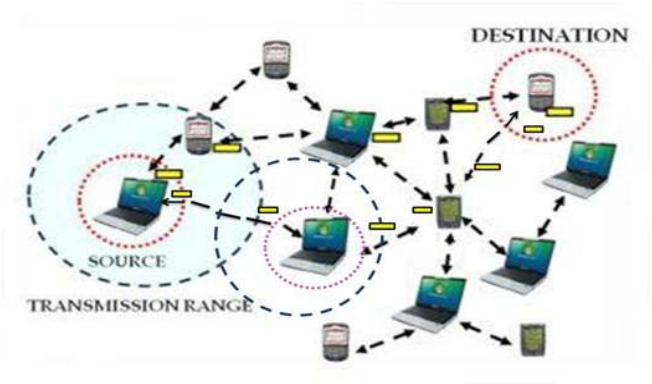


Figure.6 Working of ERAODV

We propose an analytic method to expect selfish nodes and a multi path hopping routing mechanism to implement simulation models and using NS-2(Network Simulator 2). Also it integrates the Hybrid Reputation System, which identifies and thereby avoids the non-cooperative and malicious nodes in the network.

IV. SIMULATIONS

The existing RAODV is compared with the proposed ERAODV using Network Simulator 2 (NS2). The topology we have used is shown. The total band-width considered is 2 Mbps and the radio range of each node varies randomly. At first UDP connection is established between nodes S and D. A new communication has been set up that connects node-2 to node-30 using the HRS and Multipath routing systems. The results are shown in figure 3(b). At first the node chooses single path routing without having any cooperation incentive strategy, when using the original routing protocols, RAODV. The same experiment carried out with ERAODV leads to a very different result

Network Simulator 2 (NS2) [22], [23] is used to evaluate the performance of ERAODV. To compare ERAODV with prior work in routing RAODV, this uses flooding. CBR traffic flows were selected, originating from randomly-selected sending nodes. Each CBR flow uses 512-byte packets. Each simulation lasts for 10 seconds of simulated time. The following aspects of ERAODV are emphasized:

a. Increased Throughput
b. Increased Security
c. Low latency/delay.

A. Simulation Parameters:

a.	Simulation time	: 10 mins
b.	Number of nodes	: 100
c.	Topology area	: 1611m x 766 m
d.	Mobility model	: Random way point
e.	Traffic type	: UDP
f.	Maximum speed	: 20 m/s
g.	Packet size	: 512 bytes for UDP
h.	Propagation	: Two Ray Ground
i.	Channel type	: Wireless channel

B. Network Topology:

Network topology is the arrangement of the various elements of a computer or a biological network. Essentially, it is the topological structure of a network, and may be depicted physically or logically. Physical topology refers to the placement of the network's various components, including device location and cable installation, while logical topology shows how data flows within a network, regardless of its physical design. Distances between nodes, physical interconnections, transmission rates, and/or signal types may differ between two networks, yet their topologies may be identical.

C. Performance Analysis:

Performance analysis deals with the comparison of the results over RAODV and ERAODV protocols using x-graph tool with the parameters, throughput and delay. The analysis result is found by comparing the trace files generated by the protocol in discussion. Trace graph is a tool, which is used to extract the values needed to perform a comparative analysis of the parameters considered throughput and delay. The result generated by the trace graph is given to the x-graph tool of NS2 to plot the comparative graph.

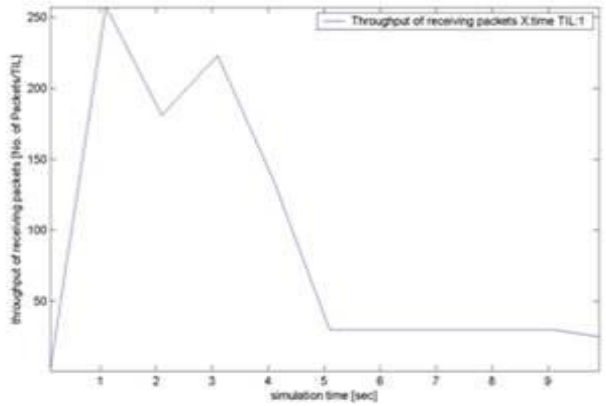


Figure.7 (a) Throughput of RAODV

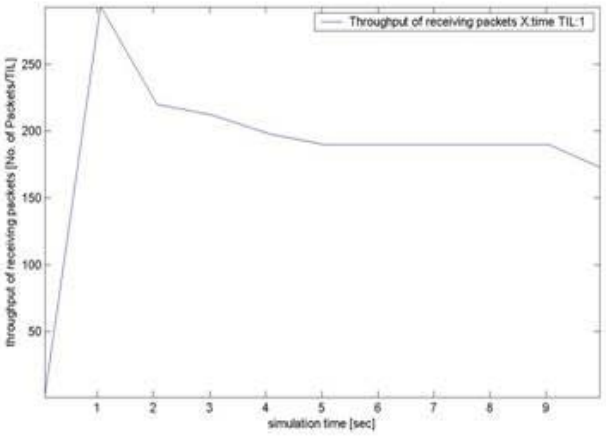


Figure.7 (b) Throughput of ERAODV

The number of packets originated by the source at application layer to number of packets received by the destination node, which also known as the packet delivery ratio or throughput. Following figure 3(c) shows that the delivery ratio in which result is shown between packet ratio and Time.

Figure.7 (c) Comparison result of RAODV & ERAODV (Throughput Vs Time)

V. CONCLUSION AND FUTURE WORK

A mobile Ad-hoc network provides the mobility of nodes which is so helpful in any emergency situations. However, if security accidents and packet loss occurs, ruinous economic damages are inevitable. Our project proposed a new hybrid reputation system that focuses on detection on malicious node and avoids them to increase the Qos parameters. Proposed method provides how we decrease the traffic and rate of vulnerability in the system using ERAODV protocol. Implementing the same concept in wireless sensor networks which may be helpful in real-time.

In future we propose to improve the Hybrid Reputation System for achieving null packet loss and simultaneous multi path packet forwarding may be done to reduce the transmission time. Cryptographic systems can also be included to encrypt the packets that we sent during transmission for security. Packet forwarding will be done by considering the energy resources of each node, so that energy efficient transmission can be achieved.

VI. REFERENCES

[1] S. Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," *Proc. ACM MobiCom*, 2000.

[2] J.J. Jaramillo and R. Srikant, "DARWIN: Distributed and Adaptive Reputation Mechanism for Wireless Networks," *Proc. ACM MobiCom*, 2007.

[3] K. Balakrishnan, J. Deng, and V.K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Netwotks," *Proc. IEEE Wireless Comm. and Networking Conf. (WCNC)*, 2005.

[4] P. Dewan, P. Dasgupta, and A. Bhattacharys, "On Using Reputations in Ad Hoc Networks to Counter Malicious Nodes," *Proc. Int'l Conf. Parallel and Distributed Systems (ICPADS)*, 2004.

[5] S. Bansal and M. Baker, "Observation-Based Cooperation Enforcement in Ad Hoc Networks," Arxiv preprint cs/0307012, 2003.

[6] K. Liu, J. Deng, P.K. Varshney, and K. Balakrishnan, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs," *IEEE Trans. Mobile Computing*, vol. 6, no. 5, pp. 536-550, May 2007.

[7] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," *Proc. Sixth Joint Working Conf. Comm. and Multimedia Security (CMS)*, 2002.

[8] Q. He, D. Wu, and P. Khosla, "SORI: A Secure and Objective Reputation-Based Incentive Scheme for Ad-Hoc Networks," *Proc. IEEE Wireless Comm. and Networking Conf. (WCNC)*, 2004.

[9] S. Buchegger and J.Y. Leboudec, "The Effect of Rumor Spreading in Reputation Systems for Mobile Ad Hoc Networks," *Proc. Workshop Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WIOPT)*, 2003.

[10] M.T. Refaei, L.A. DaSilva, M. Eltoweissy, and T. Nadeem, "Adaptation of Reputation Management Systems to Dynamic Network Conditions in Ad Hoc Networks," *IEEE Trans. Computers*, vol. 59, no. 5, pp. 707-719, May 2010.

[11] S. Buchegger and J.Y. Le Boudec, "A Robust Reputation System for Mobile Ad-Hoc Networks," *Proc. Second Workshop Economics of Peer-to-Peer Systems (P2PEcon)*, 2004.

[12] L. Buttyan and J.P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Network," *ACM J. MONET*, vol. 8, pp. 579-592, 2002.

[13] J. Crocraft, R. Gibbens, F. Kelly, and S. Ostring, "Modeling Incentives for Collaboration in Mobile Ad Hoc Networks," *Performance Evaluation*, vol. 57, pp. 427-439, 2004.

[14] L. Anderegg and S. Eidenbenz, "Ad Hoc-VCG: A Truthful and Cost-Efficient Routing Protocol for Mobile Ad Hoc Networks with Selfish Agents," *Proc. ACM MobiCom*, 2003.

[15] H. Janzadeh, K. Fayazbakhsh, M. Dehghan, and M.S. Fallah, "A Secure Credit-Based Cooperation Stimulating Mechanism for MANETs Using Hash Chains," *Future Generation Computer Systems*, vol. 25, pp. 926-934, 2009.

[16] A. Urpi, M. Bonuccelli, and S. Giordano, "Modeling Cooperation in Mobile Ad Hoc Networks: A Formal Description of Selfishness," *Proc. Workshop Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt)*, 2003.

[17] V. Srinivasan, "Cooperation in Wireless Ad Hoc Networks," *Proc. IEEE INFOCOM*, 2003.

[18] M. Felegyhazi, L. Buttyan, and J.P. Hubaux, "Nash Equilibria of Packet Forwarding Strategies in Wireless Ad Hoc Networks," *IEEE Trans. Mobile Computing*, vol. 5, no. 5, pp. 463-476, May 2006.

[19] H. Kameda and E. Altman, "Inefficient Noncooperation in Networking Games of Common-Pool Resources," *IEEE J. Selected Area in Comm.*, vol. 26, no. 7, pp. 1260-1268, Sept. 2008.

[20] Z. Li and H. Shen, "A Hierarchical Account-Aided Reputation Management System for Large-Scale MANETs," *Proc. IEEE INFOCOM*, 2011.

[21] H. Shen and Z. Li, "ARM: An Account-Based Hierarchical Reputation Management System for Wireless Ad Hoc Networks," *Proc. Int'l Workshop Wireless Security and Privacy (WISP)*, 2008.

[22] C.Z. Mooney, *Monte Carlo Simulation: Quantitative Applications in the Social Sciences.* Sage, 1997.

[23] The Network Simulator - ns-2, http://www.isi.edu/nsnamns, 2012.

[24] Z. Li and H. Shen, "Analysis of a Hybrid Reputation Management System for Mobile Ad Hoc Networks," *Proc. 18th Int'l Conf. Computer Comm. and Networks (ICCCN)*, 2009.

[25] Haiying Shen and Ze Li, "Game-Theoretic Analysis of Cooperation Incentive Strategies in Mobile Ad Hoc Networks," IEEE Transactions on Mobile Computing, vol. 11, no. 8, pp. 1287-1303, Aug. 2012.