Enhance the Throughput of Wireless Network Using Multicast Routing

Ramya[1], Vadivel[2]
[1]PG Scholar,[2] Lecturer
M.Kumarasamy College of Engineering ,Karur Tamilnadu, India

Abstract: *Wireless Mesh Network is designed static or limited mobility environment .In multicast routing for wireless mesh networks has focused on metrics that estimate link quality to maximize throughput andtoprovide secure communication. Nodes must collaborate in order to compute the path metric and forward data.Node identify the novel attacks against high- throughput multicast protocols in wireless mesh network.. The attacks exploit the local estimation and global aggregation of the metric to allow attackers to attract a large amount of traffic These attacks are very effective based on high throughput metrics. The aggressive path selection is a double-edged sword: It is maximizes throughput, it also increases attack effectiveness. so Rate guard mechanism will be used.Rate guard mechanism means combines Measurement-based detection and accusation-based reaction techniques.The attacks and the defense using ODMRP, a representative multicast protocol for wireless mesh networks, and SPP, an adaptation of the well-known ETX unicast metric to the multicast setting.*

Keywords— *Wireless mesh network,high throughput metrics, secure multicast routing,metric manipulation attacks, Byzantine attacks*

I. INTRODUCTION

Wireless mesh network that offers low cost high bandwidth community wireless services.WMN consists of a set of stationary wireless router that form a multihop backbone and a set of mobile clients that communicate via the wireless backbone. Multicast routing protocols deliver data from a source to multiple destinations organized in a multicast group.Previous work primarily focused on maximizing throughput by selecting path based on metric that capture the quality of wireless links. ODMRP it is a mesh based protocol potential to be more attack resilient,Identify class of severe attacks in multicast protocols that exploit the use of high throughput. metrics, including local metric manipulation and global metric manipulation

In a typical high-throughput multicast protocol, nodes periodically send probes to their neighbors to measure the quality of their adjacent links. The path select the best metric. This assumption is difficult to guarantee in wireless networks that are vulnerable to attacks coming from both insiders and outsiders,if the attacks coming from insider node means its very effective. An aggressive path selection introduces new vulnerabilities and provides the attacker with an increased arsenal of attacks leading to unexpected consequencesAn aggressive path selection introduces new vulnerabilities and provides the attacker with an increased arsenal of attacks leading to unexpected consequences. For example, adversaries may manipulate the metrics in order to be selected on more paths and to draw more traffic, creating opportunities for attacks such as data dropping, mesh partitioning, or traffic analysis

II. RELATED WORK.

Attacks on routing protocols can target either the route establishment process or the data delivery process, or both. Ariadne [15] and SRP [6] propose to secure on-demand source routing protocols by using hop-by-hop Authentication techniques to prevent malicious packet manipulations on the route discovery process ODSBR provides resilience to colluding Byzantine attacks by detecting malicious links based on an end-to-end acknowledgment-based feedback technique.

secure unicast or multicast routing considers routing protocols that use only basic routing metrics, such as hop count and latency. None of them consider routing protocols that incorporate high-throughput metrics, which have been shown to be critical for achieving high performance in wireless networks symmetric links, correct trust evaluation on nodes, ability to correctly determine link metrics despite of attacks. In addition, none of them consider attacks on the data delivery phase high performance and security as goals in multicast routing and considers attacks on both path establishment and data delivery phases .

Besides attacks on the routing layer, wireless networks are also subject to wireless-specific attacks, such as flood rushing and wormhole attacks Techniques to defend against wormhole attacks include Packet Leashes which restricts the maximum transmission distance by using time or location information, Truelink which uses MAC level acknowledgments to infer if a link exists or not between two nodes, and the work in , which relies on directional antennas

III. PROPOSED METHODOLOGY

Retransmission diversity is mainly used. This is eliminate the malicious node from our multicast routing. There will be chance to packet loss will occur before the detection. Intermediate node make use of special buffer and store sensitive data. If packet loss will occur means the intermediate node successfully receives the lost packets and retransmitted, i.e which should act as a relay node. We investigate and motivate the need for a simple form of node cooperation, also popularly referred to as **retransmit diversity.**

In mesh networks, one has control over the deployment of atleast some nodes in the network, which can serve as relay points for traffic for other nodes. Such nodes are limited in number for easier network management and can be assumed to be stationary. Hence, it is possible to conceive such “special” nodes to be vested with smart antennas capabilities to improve the overall network performance. Other applications would include digital battlefields envisioned by DARPA, zeroconfiguration community networks, etc.

In simple form of retransmit diversity may not necessarily provide performance improvement in homogeneous omni-directional networks if the relay does not have a better link gain to the destination than the source, and if the fading is fast and independent from one packet to another.

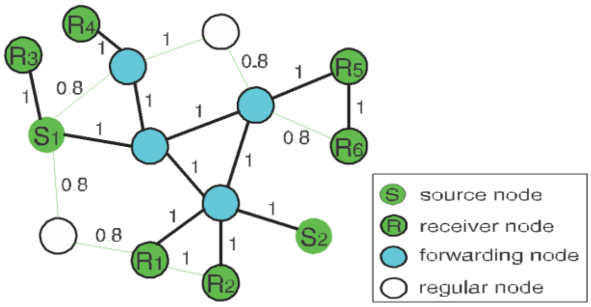
This has motivated researchers to consider more sophisticated forms of cooperation diversity such as distributed space-time codes, virtual MIMO, etc. in omni-directional networks. Such sophisticated approaches deliver good diversity gains at the cost of requiring synchronization, distributed code design, rate and/or power control amongst the cooperating nodes, which prevents their distributed implementation from being light weight. While such sophisticated approaches are warranted in omni-antenna networks, we show that even the simple form of retransmit diversity presented in the example above can provide significant performance improvement and hence has incentives to be exploited in heterogeneous smart antenna networks.

The transmitter continues to (re)transmit the packet on fading loss using its normal strategy of operation without any change for a maximum of F trials. If the link involves a smart node then the smart antenna gain on the link would contribute to reliability

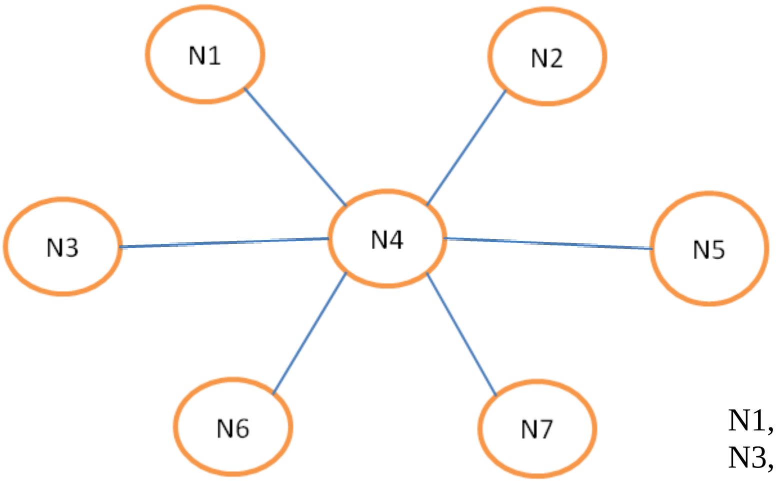
The transmitter transmits using its normal strategy of operation. On experiencing a fading loss, if there is a neighbor within the communication pattern of both the transmitter and receiver, then that node can potentially receive the packet from the transmitter due to wireless broadcast advantage and hence relay the packet (on successful decoding) to the receiver. In any case, the number of retransmissions for the packet (including transmitter and relay) is bounded by F, after which the packet is dropped. In the absence of a relay, the operation is the same as that of non-cooperation

Here, on a fading loss, the transmitter reduces its transmission rate to a low value which helps improve BER performance. Any available antenna gain on the link contributes to reliability as well. However, this increases the average SNR consumed per transmission and also the delay (which impacts throughput directly) although the number of re-trials required during correlated fading is reduced

Attacks



All the nodes in an network are categorized as **friends, acquaintances** or **strangers** based on their relationships with their neighboring nodes. During network initiation all nodes will be *strangers* to each other. A **trust estimator** is used in each node to evaluate the trust level of its neighboring nodes. The trust level is a function of various parameters like length of the association, ratio of the number of packets forwarded successfully by the neighbor to the total number of packets sent to that neighbor, ratio of number of packets received intact from the neighbor to the total number of received packets from that node, average time taken to respond to a route request etc. Accordingly, the neighbors are categorized into *friends* (most trusted), *acquaintances* (trusted) and *strangers* (not trusted). In an ad hoc network, the relationship of a node *i* to its neighbor node *j* can be any of the following types



N1,N2- Friend node
N3,N6Acquaintance
N7,N5-Stranger

(i) Node i is a **stranger** (S) to neighbor node j:

Node i have never sent/received messages to/from node j. Their trust levels will be very low. Any new node entering ad hoc network will be a stranger to all its neighbors. There are high chances of malicious behavior from stranger nodes.

(ii) Node i is an **acquaintance** (A) to neighbor node j:

Node i have sent/received few messages from node j. Their mutual trust level is neither too low nor too high to be reliable. The chances of malicious behavior will have to be observed.

(iii) Node i is a **friend** (F) to neighbor node j:

Note i sent/received plenty of messages to/from node j. The trust levels between them are reasonably high. Probability of misbehaving nodes may be very less. The above relationships are computed by each node and a friendship table is maintained for the neighbours.

Neighbors	Relationship
N1	F
N2	F
N3	A
N4	S
N5	A
N6	S

To prevent RREQ flooding, the threshold level is set for the maximum number of RREQ packets a node can receive from its neighbors. To prevent DATA flooding, the intermediate node assigns a threshold value for the maximum number of data packets it can receive from its neighbors. If Xrs, Xra, Xrf be the RREQ flooding threshold for a stranger, acquaintance and friend node respectively, Xrf > Xra > Xrs. If Yrs, Yra, Yrf be the DATA flooding threshold for a stranger, acquaintance and friend node respectively then Yrf > Yra > Yrs. If the specified threshold level is reached, further RREQ packets from the initiating node are ignored and dropped.

Let X[i] denotes the number of packets delivered from neighboring node i, where $1 \leq i \leq n$. Xrf, Xra and Xrs are the threshold values set for *friends*, *acquaintances* and *strangers*. Let Z[i] is a Boolean array to activate or stop the prevention algorithm. The algorithm for preventing RREQ flooding . The algorithm to prevent DATA flooding is similar to the algorithm flooding. The threshold values for DATA flooding can be set as per the requirements of the application software

In evaluate the performance of the Flooding Attack Prevention algorithm, WLAN throughput and delay in the network are considered. In the default setup, the nodes communicate using the AODV protocol which shows the degradation in throughput of the network and increased delay in the presence of malicious nodes. With the implementation of flooding attack prevention algorithm over AODV, the flooding attacks are constrained and this results in increased throughput and reduced delay

IV. RESULT

This section provides the results of Packet delivery ratio performance and packet drop performance and throughput performance using secure on demand multicast routing protocol

1.Packet Delivery Ratio Performance:

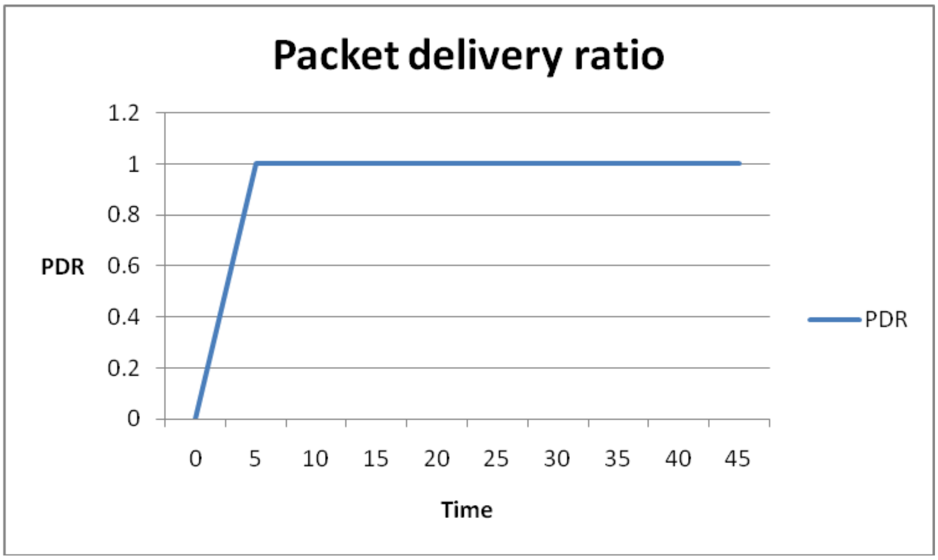


Fig 1.packet delivery ratio performance

Fig 1. represent the attackers do not perform any action in the network. where the attackers are identified and completely isolated in the network, and serves as the baseline for evaluating the impact of the attack.packet delivery ratio will be occurs on 0 to 1

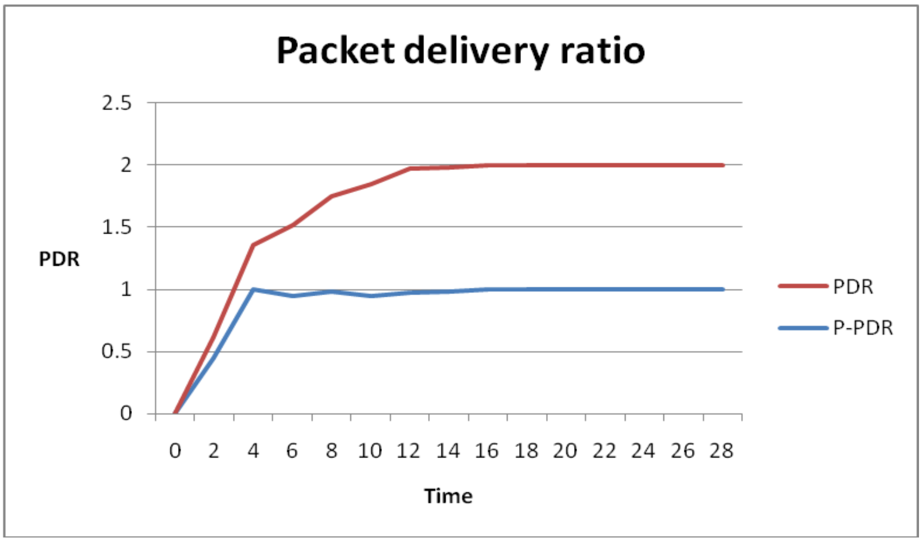


Fig2. packet delivery ratio performance comparision

Fig 2.represent packet delivery ratio will be high. The attackers combine local metric manipulation with the data dropping attack. The attackers conduct the LMM attack by readvertising the same metric they received in JOIN QUERY, which is equivalent to making their link metric of the previous hop equal to 1

2.PACKET DROP PERFORMANCE:

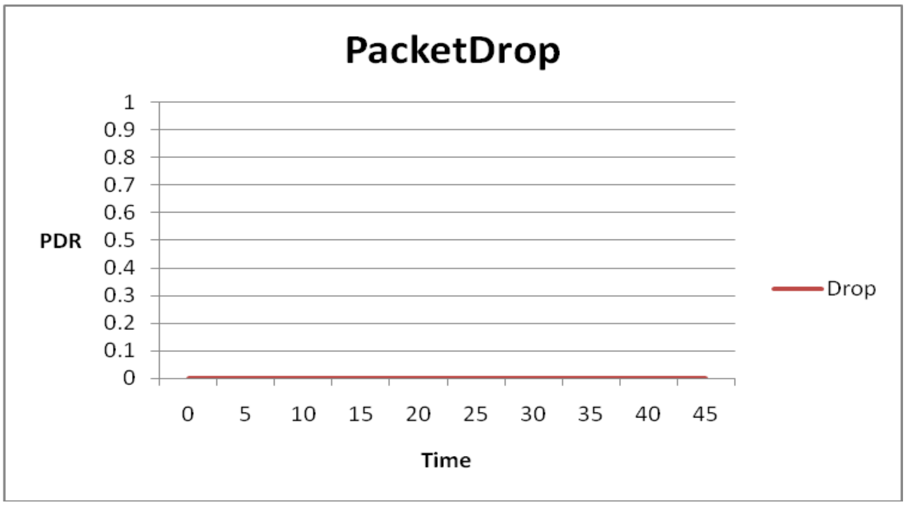


fig 3. Packet drop Performance

Fig 3. represent the attackers do not perform any action in the network. the neighbour node identified the attacker node. so there is no packet drop will be occur.

Fig 4.represent the attackers do not perform any action in the network. where the attackers are identified and completely isolated in the network, The attackers drop data packets, but participate in the protocol correctly otherwise. The attack has effect only when attackers are selected in the forwarding group.

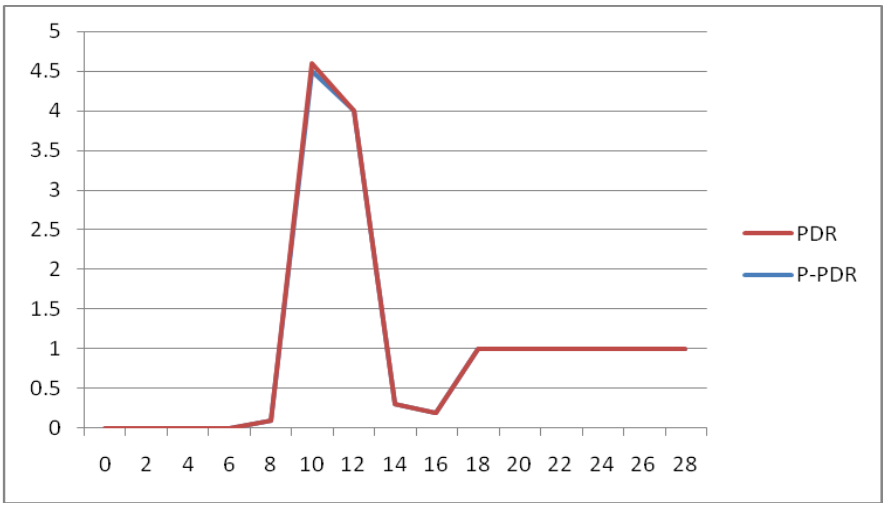


Fig 4. Packet drop Performance comparision

3.THROUGHPUT PERFORMANCE:

All the nodes send the hello packet to its neighbor.our approach eliminate the malicious node from our multicast routing.packet loss will be occur.node 2(source) only retransmit the lost packet.In our approach node 24(intermediate node) make use a special buffer and store the sensitive data.if packet loss will be occur means node 24 successfully receive the lost packet and retransmitted

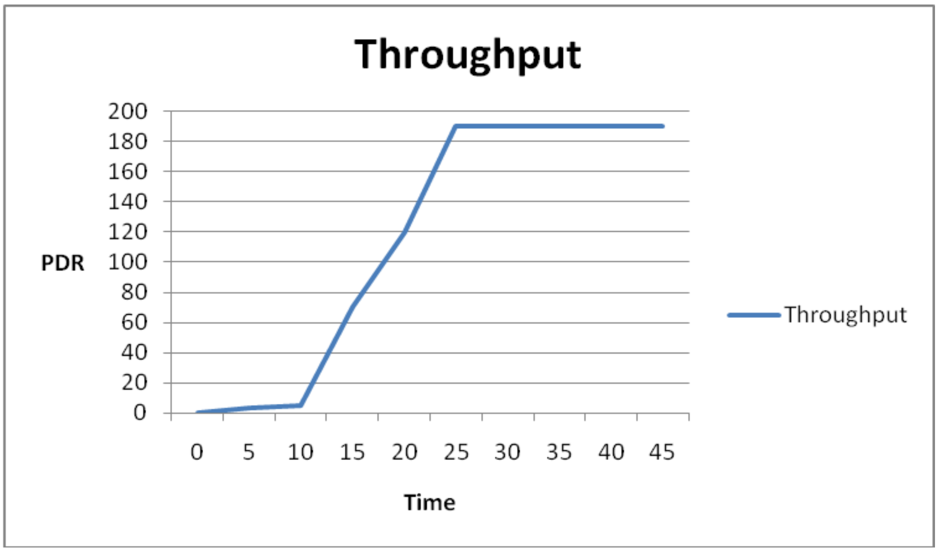


Fig 5 **Throughput Performance**.

Fig 5 represent maximize throughput will be occur.How much packet will be send that packet will be received in particular time and also the attacker do not perform any action in the network

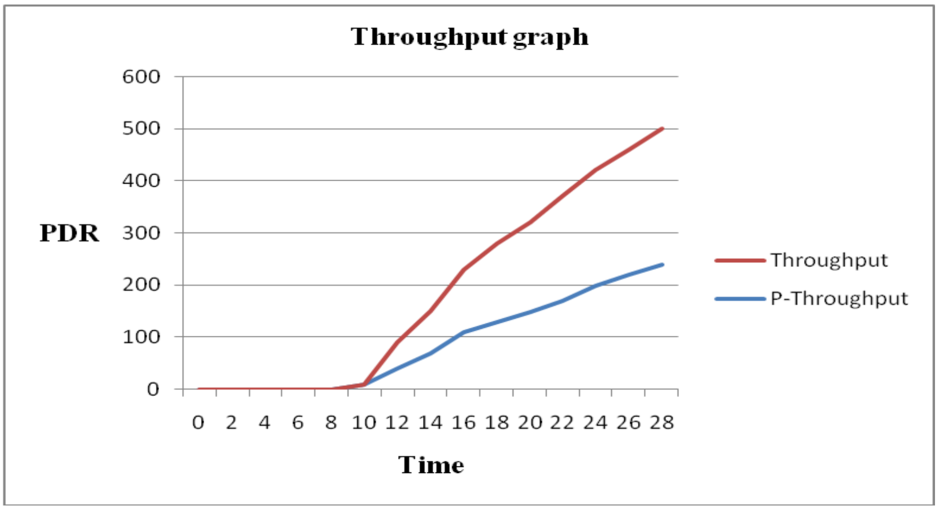


Fig 6. Throughput Performance comparision

Fig 6 represent throughput performance will be high . neighbour node identified the attacker node based on the trust level.and the neighbour node create one alarm meg and send the alarm meg all the node except the attacker node.so all the node identified the attacker node.so how much packet will be send that packet will be received in particular time and also the attacker do not perform any action in the network

V. CONCLUSION AND FUTURE WORK

The security implication of using high- throughput metrics in multicast protocols in wireless mesh networks. In particular, node identified metric manipulation attacks that can inflict significant damage on the network. The attacks not only have a direct impact on the multicast service, but also raise additional challenges in defending against them due to their metric poisoning effect. This paper overcome the challenges with our novel defence scheme, Rate Guard, that combines measurement-based attack de- taction and accusation-based reaction. Our defence also copes with transient network variations and malicious attempts to attack the network indirectly by exploiting the defense itself. This paper demonstrate through analysis and experiments that our defense is effective against the identified attacks, resilient to malicious exploitations, and imposes a small overhead

References

[1]. **1** J. Dong, R. Curtmola, and C. Nita-Rotaru, "On the Pitfalls of Using High-Throughput Multicast Metrics in Adversarial Wireless Mesh Networks," Proc. Fifth Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and AdHoc Comm.andNetwork s(SECON'08),2008.

[2]. **2.** Y.B. Ko and N.H. Vaidya, "Flooding-Based Geocasting Protocols for Mobile Ad Hoc Networks," Mobile Networks and Applications, vol.7,no.6,pp.471-480,2002.

[3]. **3.** R. Chandra, V. Ramasubramanian, and K. Birman,

[4]. "Anonymous Gossip: Improving Multicast Reliability in Mobile Ad-Hoc Networks," Proc. 21st IEEE Int'l Conf.,Distributed Computing Systems(ICDCS'01),2001.

[5]. **4.**Y.-B. Ko and N.H. Vaidya, "GeoTORA: A Protocol for Geocasting in Mobile Ad Hoc Networks," Proc. Int'l Conf. Network Protocols(ICNP), pp. 240-250, 2000.

[6]. **5**. E.L. Madruga and J.J. Garcia-Luna-Aceves, "Scalable Multicasting: the Core-Assisted Mesh Protocol," Mobile Networks and Applications, vol. 6, no. 2, pp. 151-165, 2001.

[7]. **6**. S.J. Lee, W. Su, and M. Gerla, "On-Demand Multicast Routing Protocol in Multihop Wireless Mobile Networks," Mobile Networks and Applications, vol. 7, no. 6, pp. 441-453, 2002.

[8]. **7**. E.M. Royer and C.E. Perkins, "Multicast Ad-Hoc On-Demand Distance Vector (MAODV) Routing," Internet Draft, July 2000.

[9]. **8**. J.G. Jetcheva and D.B. Johnson, "Adaptive Demand-Driven Multicast Routing in Multi-Hop Wireless Ad Hoc Networks," Proc. ACM MobiHoc, 2001.

[10]. **9.** H. Lundgren, E. Nordstrom, and C. Tschudin, "Coping with Communication Gray Zones in IEEE 802.11b Based Ad Hoc Networks," Proc. Fifth ACM Int'l Workshop Wireless Mobile Multimedia(WOWMOM '02), 2002.

[11]. **10.** D.S.J.D. Couto, D. Aguayo, J.C. Bicket, and R. Morris, "A High- Throughput Path Metric for Multi-Hop Wireless Routing," Proc. ACM MobiCom, 2003

[12]. **11**.S. Roy, D. Koutsonikolas, S. Das, and C. Hu, "High-Throughput Multicast Routing Metrics in Wireless Mesh Networks," Proc. 26th IEEE Int'l Conf. Distributed Computing Systems (ICDCS),2006.

[13]. **12**.A. Chen, D. Lee, G. Chandrasekaran, and P. Sinha, "HIMAC: High Throughput MAC Layer Multicasting in Wireless Networks,"Proc. IEEE Int'l Conf. Mobile Adhoc and Sensor Systems (MASS '06),200

[14]. **13**.. B. Awerbuch, D. Holmer, and H. Rubens, "The Medium Time Metric: High Throughput Route Selection in Multirate Ad Hoc Wireless Networks," Mobile Networks and Applications, Special Issue on Internet Wireless Access: 802.11 and Beyond, vol. 11, no. 2, pp. 253-266, 2005

[15]. **14**.P. Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad Hoc Networks," Proc. SCS Comm.Networks and Distributed Systems Modeling and Simulation Conf. (CNDS), pp. 27-31, Jan. 2002.

[16]. **15**.Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Proc. Fourth IEEE Workshop Mobile Computing Systems and Applications

[17]. (WMCSA), 2002.