Novel Defense Scheme for Static and Dynamic Wireless Mess Network

Jasmine David, Roopa Jayasingh

Abstract—In this paper we considered the security implication of using high-throughput metrics in multicast protocols in wireless mesh networks. In particular, we identified metric manipulation attacks that can inflict significant damage on the network. We overcome the attacks with our novel defense scheme, Rate-Guard that combines measurement-based attack detection and accusation-based reaction. We demonstrate through analysis and experiments that our defense is effective against the identified attacks, resilient to malicious exploitations and imposes a small overhead.

Index Terms— Wireless Mesh Network, Rate Guard , Attack Detection, Attack Reaction, Distance Vector.

1 Introduction

THIS WIRELESS mesh networks (WMNs) emerged as a promising technology that offers low-cost high-bandwidth community wireless services. A WMN consists of a set of stationary wireless routers that form a multihop backbone, and a set of mobile clients that communicate via the wireless backbone. Numerous applications envisioned to be deployed in WMNs, such as webcast, distance learning, online games, video conferencing, and multimedia broadcasting, follow a pattern where one or more sources disseminate data to a group of changing receivers. These applications can benefit from the service provided by multicast routing protocols. Multicast routing protocols deliver data from a source to multiple destinations organized in a multicast group. In the last few years, several protocols were proposed to provide multicast services for multihop wireless networks. These protocols were proposed for mobile ad hoc networks (MANETs), focusing primarily on network connectivity and using the number of hops (or hop count) as the route selection metric. However, it has been shown that using hop count as routing metric can result in selecting links with poor quality on the path, negatively impacting the path throughput. Instead, given the stationary nature of WMNs, recent protocols focus on maximizing path throughput by selecting paths based on metrics that capture the quality of the wireless links. We refer to such metrics as link-quality metrics or high-throughput metrics, and to protocols using such metrics as high-throughput protocols.

2 Routing Protocols in AD HOC Network

2.1 Table Driven

The nodes maintain a table of routes to every destination in the network, for this reason they periodically exchange messages. At all times the routes to all destinations are ready to use and as a consequence initial delays before sending data are small. Keeping routes to all destinations up-to-date, even if they are not used, is a disadvantage with regard to the usage of bandwidth and of network resources.

DSDV has one routing table, each entry in the table contains: destination address, number of hops toward destination, next hop address. Routing table contains all the destinations that one node can communicate. When a source A communicates with a destination B, it looks up routing table for the entry which contains *destination* address as B. Next hop address C was taken from that entry. A then sends its packets to C and asks C to forward to B. C and other intermediate nodes will work in a similar way until the packets reach B. DSDV marks each entry by sequence number to distinguish between old and new route for preventing loop.

DSDV use two types of packet to transfer routing information: full dump and incremental packet. The first time two DSDV nodes meet, they exchange all of their available routing information in full dump packet. From that time, they only use incremental packets to notice about change in the routing table to reduce the packet size. Every node in DSDV has to send update routing information periodically. When two routes are discovered, route with larger sequence number will be chosen. If two routes have the same sequence number, route with smaller hop count to destination will be chosen.

DSDV has advantages of simple routing table format, simple routing operation and guarantee loop-freedom. The disadvantages are (i) a large overhead caused by periodical update (ii) waste resource for finding all possible routes between each pair, but only one route is used.

2.2 On-Demand

These protocols were designed to overcome the wasted effort in maintaining unused routes. Routing information is acquired only when there is a need for it. The needed routes are calculated on demand. This saves the overhead of maintaining unused routes at each node, but on the other hand the latency for sending data packets will considerably increase.

In on-demand trend, routing information is only created to requested destination. Link is also monitored by periodical Hello messages. If a link in the path is broken, the source needs to rediscovery the path. On-demand strategy causes less overhead and easier to scalability. However, there is more delay because the path is not always ready. The following part will present AODV, DSR, TORA and ABR as characteristic protocols of on-demand trend.

2.3 AODV Routing

Ad hoc on demand distance vector routing (AODV) is the combination of DSDV and DSR. In AODV, each node maintains one routing table. Each routing table entry contains

1. Active neighbor list: a list of neighbor nodes that are actively using this route entry.

2. Once the link in the entry is broken, neighbor nodes in this list will be informed.

- Destination address.
- Next-hop address toward that destination.
- Number of hops to destination.
- Sequence number: for choosing route and prevent loop.
- Lifetime: time when that entry expires.

Routing in AODV consists of two phases: Route Discovery and Route Maintenance. When a node wants to communicate with a destination, it looks up in the routing table. If the destination is found, node transmits data in the same way as in DSDV. If not, it start Route Discovery mechanism: Source node broadcast the Route Request packet to its neighbor nodes, which in turns rebroadcast this request to their neighbor nodes until finding possible way to the destination. When intermediate node receives a RREQ, it updates the route to previous node and checks whether it satisfies the two conditions: (i) there is an available entry which has the same destination with RREQ (ii) its sequence number is greater or equal to sequence number of RREQ. If no, it rebroadcast RREQ. If yes, it generates a RREP message to the source node. When RREP is routed back, node in the reverse path updates their routing table with the added next hop information. If a node receives a RREQ that it has seen before (checked by the sequence number), it discards the RREQ for preventing loop. If source node receives more than one RREP, the one with greater sequence number will be chosen. For two RREPs with the same sequence number, the one will less number of hops to destination will be chosen. When a route is found, it is maintained by Route Maintenance mechanism:

Each node periodically send Hello packet to its neighbors for proving its availability. When Hello packet is not received from a node in a time, link to that node is considered to be broken. The node which does not receive Hello message will invalidate all of its related routes to the failed node and inform other neighbor using this node by Route Error packet. The source if still want to transmit data to the destination should restart Route Discovery to get a new path. AODV has advantages of decreasing the overhead control messages, low processing, quick adapt to network topology change, more scalable up to 10000 mobile nodes. However, the disadvantages are that AODV only accepts bi-directional link and has much delay when it initiates a route and repairs the broken link

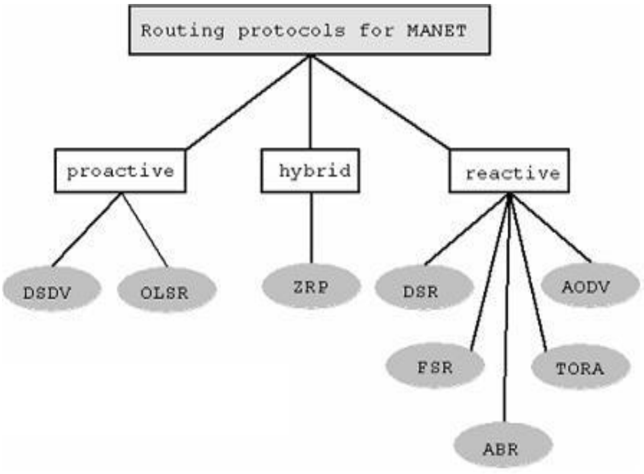

FIg 1 Routing Protocols for Mane

.

2.4 Dynamic Source Routing Protocol

DSR is a reactive routing protocol which is able to manage a MANET without using periodic table-update messages like table-driven routing protocols do. DSR was specifically designed for use in multi-hop wireless ad hoc networks. Ad-hoc protocol allows the network to be completely self-organizing and self-configuring which means that there is no need for an existing network infrastructure or administration.

For restricting the bandwidth, the process to find a path is only executed when a path is required by a node (On-Demand-Routing). In DSR the sender (source, initiator) determines the whole path from the source to the destination node (Source Routing) and deposits the addresses of the intermediate nodes of the route in the packets.

DSR is beacon-less which means that there are no hello-messages used between the nodes to notify their neighbors about her presence.

DSR was developed for MANETs with a small diameter between 5 and 10 hops and the nodes should only move around at a moderate speed. DSR is based on the Link-State-Algorithms which mean that each node is capable to save the best way to a destination. Also if a change appears in the network topology, then the whole network will get this information by flooding. The DSR contains 2 phases

- Route Discovery
- Route Maintenance

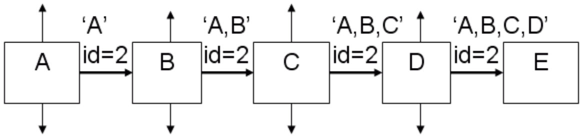

Fig 2 Route Discovery

3 Secure Multicast Routing

Multicast protocols provide communication from sources to receivers organized in groups by establishing dissemination structures such as trees or meshes, dynamically updated as nodes join or leave the group. Tree-based multicast protocols (e.g., MAODV) build optimized data paths, but require more complex operations to create and maintain the multicast tree, and are less resilient to failures. Mesh-based multicast protocols (e.g., ODMRP) build more resilient data paths, but have higher overhead due to redundant retransmissions. We focus on ODMRP as a representative mesh-based multicast protocol for wireless networks. Below, we first give an overview of ODMRP, then describe how it can be enhanced with any link-quality metric. The protocol extension to use a high-throughput metric was first described by Royetal .We refer to the ODMRP protocol using a high-throughput metric as ODMRP-HT in order to distinguish it from the original ODMRP protocol.

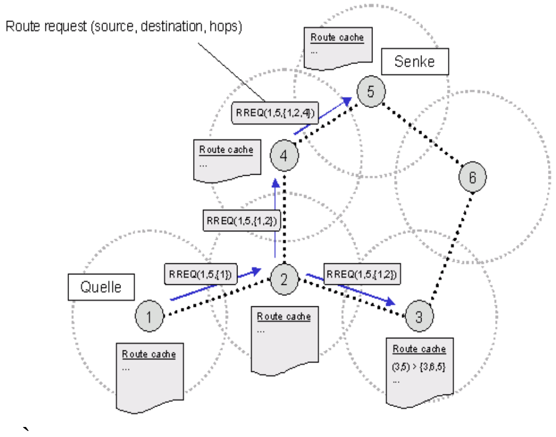

Fig 3 Route Request

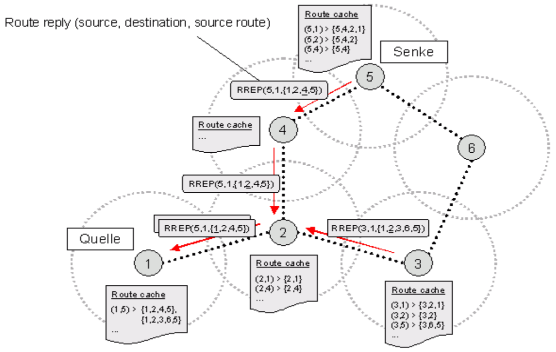

Fig 4 Route Reply

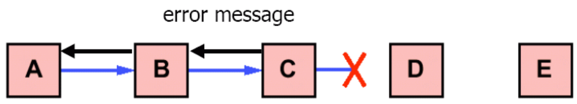

Fig 5.Route Maintenance

4 Modules

S-ODMRP ensures the delivery of data from the source to the multicast receivers even in the presence of Byzantine attacks targeting JOIN QUERY and JOIN REPLY messages, and the injection of corrupted data packets. Modules are

- Topology Formation and Hello packet sending
- High-throughput Metrics
- Attack against High-throughput multicast

5 Secure High Throughput Muticast Routing

5.1 High-Throughput Mesh-Based Multicast Routing

Multicast protocols provide communication from sources to receivers organized in groups by establishing dissemination structures such as trees or meshes, dynamically updated as nodes join or leave the group. Tree-based multicast protocols (e.g., MAODV) build optimized data paths, but require more complex operations to create and maintain the multicast tree, and are less resilient to failures. Meshbased multicast protocols (e.g., ODMRP) build more resilient data paths, but have higher overhead due to redundant retransmissions.

We focus on ODMRP as a representative mesh-based multicast protocol for wireless networks. Below, we first give an overview of ODMRP, then describe how it can be enhanced with any link-quality metric. The protocol extension to use a high-throughput metric was first described by Roy et al. We refer to the ODMRP protocol using a high-throughput metric as ODMRP-HT in order to distinguish it from the original ODMRP protocol.

ODMRP is an on-demand multicast routing protocol for multihop wireless networks, which uses a mesh of nodes for each multicast group. Nodes are added to the mesh through a route selection and activation protocol.

The source periodically recreates the mesh by flooding a JOIN QUERY message in the network in order to refresh the membership information and update the routes. We use the term round to denote the interval between two consecutive mesh creation events. JOIN QUERY messages are flooded using a basic flood suppression mechanism, in which nodes only process the first received copy of a flooded message.

When a receiver node gets a JOIN QUERY message, it activates the path from itself to the source by constructing and broadcasting a JOIN REPLY message that contains entries for each multicast group it wants to join; each entry has a next hop field filled with the corresponding upstream node. When an intermediate node receives a JOIN REPLY message, it knows whether it is on the path to the source or not, by checking if the next hop field of any of the entries in the message matches its own identifier. If so, it makes itself a node part of the mesh (FORWARDING GROUP) and creates and broadcasts a new JOIN REPLY built upon the matched entries. Once the JOIN REPLY messages reach the source, the multicast receivers become connected to the source through a mesh of nodes (FORWARDING GROUP) which ensures the delivery of multicast data. While a node is in the FORWARDING GROUP, it rebroadcasts any non-duplicate multicast data packets that it receives.

5.2 Attacks against High-Throughput Multicast

In general, the attacker can achieve the goal of disrupting the multicast data delivery by either exhausting network resource (resource consumption attacks), by causing incorrect mesh establishment (mesh structure attacks), or by dropping packets (data forwarding attacks). The packet dropping attack is straightforward: The attacker node on the data delivery path simply drops data packets instead of forwarding them.

S-ODMRP ensures the delivery of data from the source to the multicast receivers even in the presence of Byzantine attackers, as long as the receivers are reachable through non adversarial paths. To achieve this, S-ODMRP uses a combination of authentication and rate limiting techniques against resource consumption attacks and a novel technique, Rate Guard, against the more challenging packet dropping and mesh structure attacks, including metric manipulations and JOIN REPLY dropping.

Rate Guard Over View

Rate Guard relies on the observation that regardless of the attack strategy, either by dropping JOIN REPLY, metric manipulations, or by dropping packets, attackers do not affect the multicast protocol unless they cause a drop in the packet delivery ratio (PDR). We adopt a reactive approach in which attacker nodes are detected through a measurement- based detection protocol component, and then isolated through an accusation-based reaction protocol component.

5.3 Attack Detection

We detect attacks using a measurement-based mechanism, where each FORWARDING GROUP and receiver node continuously monitors the discrepancy between ePDR and pPDR and flags an attack if ePDR _ pPDR .

The most straightforward method for estimating pPDR is to use a sliding window method, with pPDR calculated as pPDR ¼ r=w, where r is the number of packets received in the window and w is the number of packet sent by the source (derived from packet sequence numbers) in the window. Albeit being simple, this method is sensitive to bur sty packet loss. In addition, this approach requires a node to wait until at least w packets are sent in a round before being able to make any decision.

Therefore, setting w too large causes delay in making decisions, whereas setting w too small results in inaccurate pPDR estimation and hence more frequent false positives. In general, it is difficult to determine the optimal value for w, as it depends on the network conditions and the specific position of a node. To avoid these shortcomings, we propose an efficient statistical-based estimation method for pPDR that naturally adapts to the network environment of each node.

5.4 Attacks Reaction

To isolate attackers, our protocol uses a controlled-accusation mechanism which consists of three components, staggered reaction time-out, accusation message propagation and handling, and recovery message propagation and handling. When a node detects attack behavior, it starts a React Timer with time-out value ePDR, where is a system parameter that determines the maximum time-out for reaction timer (line 1).Since ePDR decreases monotonically along a multicast data path, nodes farther away from the source will have a larger time-out value for the React Timer.

5.5 Fall Back Recovery

The accusation mechanism ensures that when the metric is refreshed in the round after the attack detection, the accused nodes are isolated. However, during the round when an attack is detected, the receiver nodes in the sub tree of the attacker need to find alternative routes to “salvage” data for the rest of the round.

6 PROPOSED WORK

We have altered the normal DSR Protocol by finding the local broken link from the reply message and finding another efficient way to transfer the data between the nodes without any loss in data. The below are the simulation settings we have used.

Table1.Simualtion Setting

Parameters	Value
Channel	Wireless Channel
Propagation	Radio Propagation
MAC Type	802.11
Antenna Type	Omni Antenna
Routing Protocol	DSR
Energy Mode	Mode 1
Initial Energy	100

- Calculating the nearest neighbouring node:

The distance between the neighbouring nodes has been calculated using two points distance formula the points are taken from the x and y axis points of a particular node from the mesh network. Then the distance value is compared with a threshold value as the mac type is known and the values are compared to find the nearest node. Usually this routing can be compared with the AODV, DSR, DSDV algorithms.

- High Throughput metrics:

Then we are calculating the high Throughput metrics. From the shortest node found from the earlier step we are finding the link quality for the shortest node. To find the link quality the packet delivery ratio between the two nodes are calculated. The link quality from the awk file is collected and the Packet Delivery Ratio (PDR) is calculated between two nodes. From the received PDR the threshold is set and the Rate Guard is calculated. The difference between the expected PDR and the perceived PDR is calculated and is checked with the Threshold value and thus the link with the high throughput is calculated.

- Flooding the Information

Based on the AMF the shortest high throughput information is sent to all the nodes in the wireless mesh networks and sent through joint query and joint reply. If there is any distortion is found in between the nodes then that input is sent and the PDR rate varies and the nodes check for another short and high throughput link to the destination. we propose a secure high-throughput multicast protocol S-ODMRP that incorporates a novel defense scheme Rate Guard. Rate Guard combines measurement-based detection and accusation-based reaction techniques to address the metric manipulation and packet dropping attacks. We perform a detailed security analysis and establish bounds on the impact of the attacks under our defense scheme. Extensive simulations with ODMRP and SPP confirm our analysis and show that our strategy is very effective in defending against the attacks, while incurring a low overhead.

7 OUTPUT &DISCUSSION

We have calculated nearest node for transmission, calculated high ThroughPutmetrics and flooding the information about the packet drop and the output obtained in showcased below.

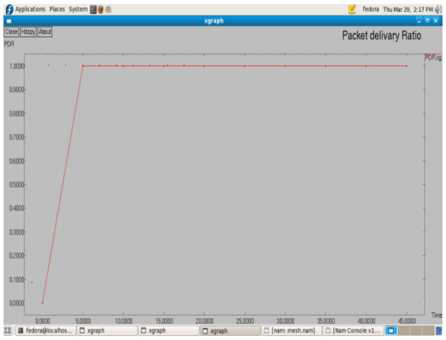

Fig 6 PDR for Static Network

Packet Delivery Rate is high for Static Network.

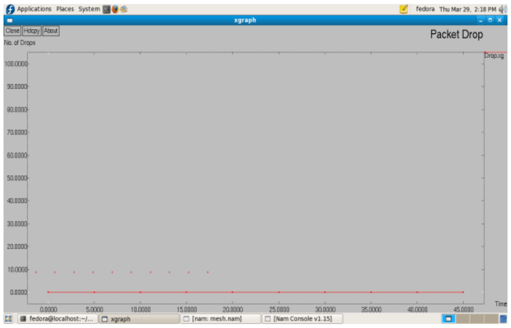

Fig 7 Packet Drop for Static Network

Packet Drop is very less for Static Network

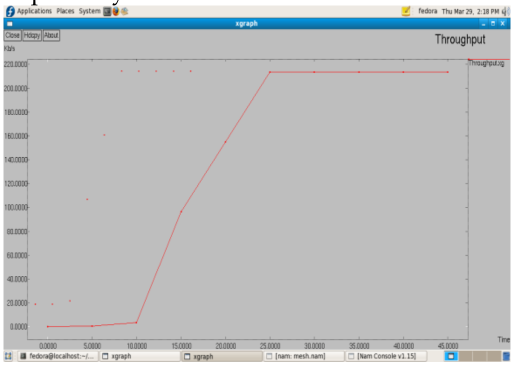

Fig 8 Throughput for Static Network

Efficiency is high in Static Network.

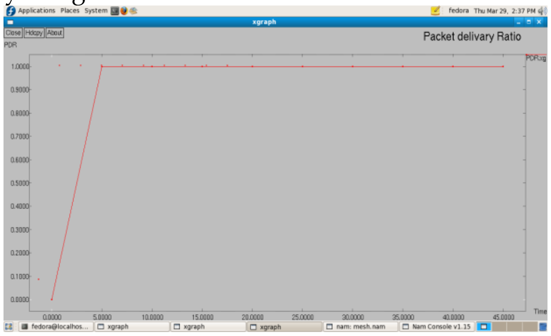

Fig 9 PDR   for Dynamic Network

Packet Delivery Rate is very high in Dynamic Network.

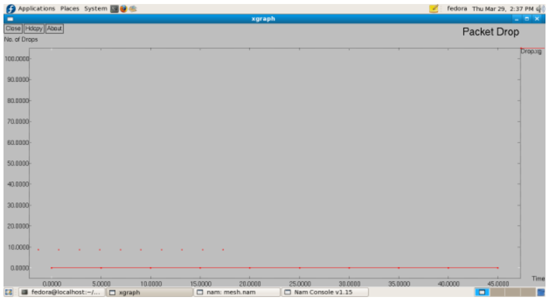

Fig 10 Packet Drop for Dynamic Network

Packet Drop is very less for Dynamic Network

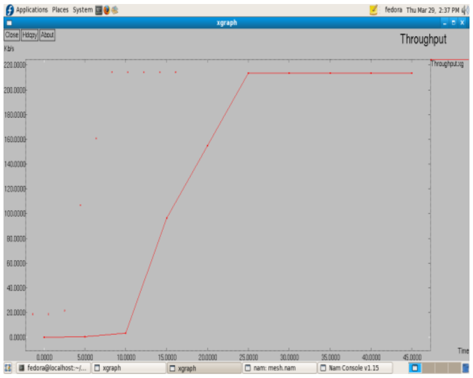

Fig 11. Throughput for Dynamic Network

Efficiency is high in Static Network.

We infer that our proposal is efficient than the previous methods as it gives more security to the data and high throughput. Our defense scheme proves to be one of the efficient ways to find and fight the attackers which causes packet drop. Thus our proposal is effective against the identified attacks, resilient to malicious exploitations, and imposes a small overhead.

8 Conclusion

We considered the security implication of using high-throughput metrics in multicast protocols in wireless mesh networks. In particular, we 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. We overcome the challenges with our novel defense scheme, Rate-Guard that combines measurement-based attack detection and accusation-based reaction. Our defense also copes with transient network variations and malicious attempts to attack the network indirectly by exploiting the defense itself. We 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] 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 Ad Hoc Comm. and Networks (SECON '08), 2008.

[2] Baruch Awerbuch, David Holmer, and Herbert Rubens' *High Throughput Route Selection in Multi-rate Ad Hoc Wireless Networks "*.

[3] R. Chandra, V. Ramasubramanian, and K. Birman, "*Anonymous Gossip: Improving Multicast Reliability in Mobile Ad-Hoc Networks*,"Proc. 21st IEEE Int'l Conf. Distributed Computing Systems (ICDCS '01), 2001.

[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.

[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.

[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.

[7] Thomas Kunz and Ed Cheng," *Multicasting in Ad-Hoc Networks:Comparing MAODV and ODMRP "*

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

[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.

[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.

Jasmine David was born in Nagercoil, India in 1977.She received her BE degree in Electronics and Communication Engineering from Bharathiyar University in 1998 and ME degree from Bharathiyar University in 2001.She is currently pursuing her PhD in Karunya University and working as Assistant Prof (SG) in Karunya University.

Roopa Jayasingh was born in Coimbatore, India, in 1974. She received the B.E degree in Electronics and communication engineering from the Bharathiar University in 1996 and M.E degree from Bharathiar University in 2002. She is currently pursuing her PhD in Anna University and working as an Assistant Professor (SG)in Karunya University.
Email id: **roopa.jayasingh@gmail.com**