ISSN No. 0976-5697

Volume 2, No. 5, Sept-Oct 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Study of Secured and Energy Efficient Protocol for MANET

Awadhesh Kumar* and Dr. Neeraj Tyagi
Research Scholar, Computer Science & Engg., Mnnit Allahabad (UP)
awadheshkumar.knit@gmail.com
Associate Professor, Computer Science & Engg., Mnnit Allahabad (UP)
neeraj@mnnit.ac.in

Abstract— A Mobile Ad-Hoc Network (MANET) is a collection of wireless mobile nodes forming a temporary network without using any centralized access point, infrastructure, or centralized administration. One of the main design constraints in mobile Ad Hoc networks (MANETs) is that they are power constrained. Hence, every effort is to be channeled towards reducing power. More precisely, network lifetime is a key design metric in MANETs. The typical MANET routing protocols of (AODV, DSR and DSDV) are shortest routing protocols, that is, the least hops but do not consider the energy efficiency of the routes. Our goal in this paper is to study Active Communication Energy Efficient routing mechanisms and protocols, satisfying less energy consumption from the viewpoints of nodes and network. To achieve our goal, we studied the three typical MANET routing protocols (AODV, DSR and DSDV) using performance and energy aware metrics.

Keywords—Aodv, DSR, security. attacks.

I. INTRODUCTION

MOBILE Ad-hoc Network (MANET) is a collection of wireless mobile hosts without fixed network infrastructure and centralized administration (Figure-1). Communication in MANET is done via multi-hop paths. Lots of challenges are there in this area: MANET contains diverse resources; the line of defense is very ambiguous; Nodes operate in shared wireless medium; Network topology changes unpredictably and very dynamically; Radio link reliability is an issue; connection breaks are pretty frequent. Moreover, density of nodes, number of nodes and mobility of these hosts may vary in different applications. There is no stationary infrastructure. Each node in MANET acts a router that forwards data packets to other nodes. Therefore, selection of effective, suitable, adaptive and robust routing protocol is of utmost importance.

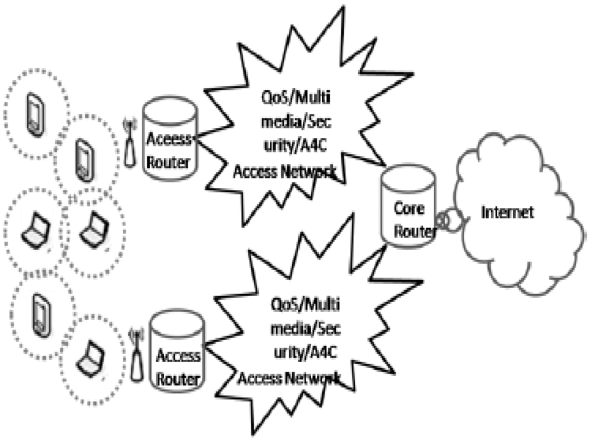
QoS/Multi media/Sec urity/A4C Access Network
Aceess Router
Core Router
Internet
QoS/Multi media/Sec urity/A4C Access Network
Access Router

Figure-1 Mobile Ad-hoc Network

There are three types of routing protocols:
Proactive Protocols, Reactive Protocols and Hybrid Protocols.

Proactive protocols are table-driven that constantly update lists of destinations and routes. Reactive protocols respond on demand. Hybrid protocols combine the features of reactive and proactive protocols. The main goal of routing protocols is to minimize delay, maximize network throughput, maximize network lifetime and maximize energy efficiency. In this paper, Sections II, III, IV and V looks at working of routing protocols like Destination Sequenced Distance Vector (DSDV), Dynamic Source Routing (DSR), Temporally-Ordered Routing Algorithm (TORA) and Ad-hoc On Demand Distance Vector (AODV); Section VI thoroughly explains the exact operation of AODV.

Moreover, Ad-hoc networks [1] are the networks that don't have any fixed infrastructure. Ad-hoc networks are often mobile and that is why the term MANET (Mobile Ad-hoc Network) is used. There are many applications for ad-hoc networks like conferencing, emergency services, personal area networks, embedded computing, and sensor dust. A MANET is a peer-to-peer network that allows direct communication between any two nodes, when adequate radio propagation conditions exist between these two nodes. If there is no direct link between the source and the destination nodes, multi-hop routing is used. In multi-hop routing, a packet is forwarded from one node to another, until it reaches the destination. A routing protocol is in general necessary in adhoc networks; this routing protocol has to adapt quickly to the frequent changes in the ad-hoc network topology. Ad-hoc routing protocols are classified into three categories. The first category is Table-driven (Proactive) routing protocols such as DSDV [2], CGSR [3], GSR [4], FSR [5], and OLSR [6]. The second category is on-demand (Reactive) routing protocols such as AODV [7], DSR [8], ABR [9], SSA [10], and TORA [11].

The third category is Hybrid (Reactive and proactive) routing protocols such as ZRP [12] and ZHLS [13]. AODV is a well known on-demand routing protocol where a source node initiates route discovery when it needs to communicate to a destination that doesn’t have a route to it. Once a route discovered between the two nodes, data transfer occurs through until the route broken due node movement or interference due the erroneous nature of wireless medium.

Route maintenance initiated when a route failure happens between two nodes. The upstream node of the failure tries to find a repair to the route and this process called local repair.

II. RLATED ROUTING PROTOCOLS

A. Destination-Sequenced Distance Vector (DSDV):

Destination-Sequenced Distance Vector (DSDV) is a traditional table-driven protocol for MANET. To solve the routing loop problem, it was invented by C. Perkins and P. Bhagwat in 1994. Routes are established based on constant control traffic and they are available all the time. Each node maintains one or more tables that contain route information to other nodes in the network. Nodes continuously update the tables to provide fresh view of whole network. Updates are so frequent that the advertisement must be made regularly enough to make sure that every node can almost always find every other node in the network. The data that is broadcast by the mobile node contains its new sequence number, destination address, number of hops needed to reach destination and sequence number of the information received for the destination.

The fundamental issue with DSDV is creation and maintenance of the tables. These tables need to be frequently updated by transmission of packets, even in traffic condition. Moreover, until updates about changes in topology are not sent across the network, DSDV does not function. In a large network with high density, mobile nodes often create broken links. Maintenance and modification of tables as well as advertising the modifications would be significantly complex in this kind of network. DSDV is effective for ad-hoc network with small number of mobile hosts with limited changes in network topology. Improved forms of DSDV have been suggested, but commercial implementation of the traditional DSDV has not been done.

B. Dynamic Source Routing (DSR):

Dynamic Source Routing (DSR) is a reactive kind of protocol which reacts on-demand. The main feature of DSR is source routing in which the source always knows the complete route from source to destination. It frequently uses source routing and route caching. Route Discovery and Route Maintenance are two main methods used in DSR. It is uncomplicated and efficient protocol. It does not depend on timer-based activities. It allows multiple routes to destination node and routing is loop-free here. Any broken link is notified to the source node with an error message. It works well in large networks where routes change quickly and mobility of routes is higher.

In DSR, intermediate nodes do not need to preserve the routing information. Instead the packets themselves contain every routing decision. DSR uses a route discovery process to find a route when a node in the network tries to send a data packet to a destination for which the route is unknown. A route is found by flooding the network with route requests. When a node receives this request, it broadcasts it again until it itself is the destination or it has the route to the destination. This node then replies to the request to the original source. The request and response packets are source routed. Request packet creates the path of traversal. Response packet creates the reverse path to the source by traversing backwards.

C. Temporally-Ordered Routing Algorithm (TORA):

Temporally-Ordered Routing Algorithm (TORA) is made to find routes on demand. It tries to achieve high scalability. It creates and maintains directed acyclic graph rooted at the destination node. TORA can establish routes rapidly and can provide multiple routes for a single destination. It doesn't give Shortest-Path Algorithm too much of importance. Instead it uses longer paths to avoid finding of new routes. TORA minimizes communication over as it reacts only when needed and doesn't react to every topological change as well as it localizes scope of failure reactions.

There are three main phases of the algorithm: Route Creation, Route Maintenance and Route Erasure. In the Route Creation phase, the query packet is flooded all over the network and if routes exist, an update packet is sent back. In the Route Maintenance phase update packets re-orient the route composition. The route erasure phase involves flooding of a broadcast clear packet all over the network to erase invalid routes. To simulate the protocol, size of network, rate of topological change and network connectivity should be kept in mind.

D. Ad-Hoc On Demand Distance Vector (AODV):

Ad-hoc On Demand Distance Vector (AODV) is a reactive protocol that reacts on demand. It is probably the most well-known protocol in MANET. It is a modification of DSDV. The demand on available bandwidth is significantly less than other proactive protocols as AODV does not require global periodic advertisements. It enables multi-hop, self-starting and dynamic routing in MANETs. In networks with large number of mobile nodes AODV is very efficient as it relies on dynamically establishing route table entries at intermediate nodes. AODV never produces loops as there cannot be any loop in the routing table of any node because of the concept of sequence number counter borrowed from DSDV. Sequence numbers serveas time stamps and allow nodes to compare how fresh information they have for other nodes in the network. The main advantage of AODV is its least congested route instead of the shortest path.

III. EXPLORING AODV

Route discovery process is started by a source node that wants to communicate with a destination node for which there is no routing information in its routing table. Each node broadcasts a HELLO message after a specific interval to keep track of its neighbors. Thus a node keeps track of only its next hop for a route instead of entire route. When a node wants to communicate with a node that is not its neighbor it broadcasts a route request packet called RREQ which contains RREQ ID, Destination IP Address, Destination Sequence Number, Source IP Address, Source Sequence Number and Hop Count. Destination Sequence Number is the latest sequence number received in the past by the source for any route towards the destination. Source Sequence Number is the latest sequence number to be used in the route entry pointing towards the source of RREQ. Every route table entry for every node must include the latest sequence number for the nodes in the network. It is updated whenever a node receives RREQ, RREP or RRER related to a specific node. Hop Count represents the distance in hops from the source to destination [3].

When a node receives an RREQ, it checks that whether it has already received an RREQ with the same Source IP Address and RREQID within PATH_DISCOVERY_TIME. If yes, it discards the newly arrived RREQ. If not, it increments the hop count value in RREQ by one. The route table entry for the destination will be updated with the new sequence number if:

a. Destination Sequence Number received from RREQ is greater than the existing value in the route table entry.
b. The Sequence numbers are equal, but the incremented hop count is smaller than existing hop count.
c. The Sequence number is unknown.

Soon after this updation valid sequence number field in the route table entry is set to true. The node searches for a reverse route towards the Source IP Address. If need be, route is created or updated using the Source Sequence Number. When the reverse route is created or updated following events are carried out:

a. If Source Sequence Number received from RREQ is greater than the existing value in the route table entry, it is updated.
b. The valid sequence number field is made true.
c. The next hop in the routing table becomes the node from which RREQ was received.
d. The value of hop count is copied from RREQ packet.

After updating the information the intermediate node forwards the RREQ packet until a node is found that is the destination itself or it has an active route to the destination with Destination Sequence Number greater than or equal to that of RREQ. This node replies back to the source node with a route reply packet RREP and discards the RREQ. If the node generating RREP is an intermediate node, it copies the known sequence into the Destination Sequence Number field in the RREP packet. RREP contains Destination IP Address, Destination Sequence Number, Originator IP Address and Lifetime. Lifetime represents the time in which nodes receiving RREP consider the route to be valid. When a node receives an RREP packet, it finds a route to the previous hop and increments the hop count value in the RREP by one [5]. The existing route table entry of the Destination Sequence Number is updated if:

a. The Destination Sequence Number in the RREP is greater than existing value and the value is valid.
b. The Sequence Numbers are same, but the incremented hop count is smaller than that of existing value.
c. The sequence number is marked as invalid in the routing table.
d. The sequence numbers are same, but the route is marked as inactive.

Thus, an intermediate node or a source node updates its corresponding route table entry. When the RREP reaches to the source node, it can now send the data packets through the route that is set up.

A node generates router error packet RRER in the following situations:

a. While transmitting the data, if it notices a link break for the next hop (neighbor) of an active route in its routing table. Here the node first makes the list of unreachable destinations along with unreachable neighbors in the routing table.
b. If it receives a data packet that is to be sent to a destination node for which it does not have an active route.
c. If it gets an RERR from a neighbor for one or more active routes.

RERR packet allows AODV to adjust routes when a node moves around in a MANET. The RRER indicates those destinations that are unreachable; each node keeps a “precursor list containing the IP address for each of its neighbors that are likely to use it as a next hop towards destination. The information in the precursor list is acquired during the generation of a RREP packet.

A. Working of AODV:

To show the working of AODV we take an example of five mobile nodes as shown in Figure-2. The circles indicate the range of communication for the nodes. As each node has a limited communication range, it can communicate with its neighbor nodes only. At an instant, Node 4 wants to communicate with Node 3, but it is uncertain of the route. Node 4 broadcasts RREQ that is received by its neighbors Node 1 and Node 5. Node 5 doesn’t have any route to Node 3 and therefore it rebroadcasts RREQ that is received back by Node 4. Node 4 drops it. On the other side, if Node 1 has a greater sequence number than RREQ, it discards RREQ and replies with RREP. If not, it updates the sequence number in its routing table and forwards RREQ to Node 2. As Node 2 has a route to Node 3, it replies to Node 1 by sending an RREP. Node 1 sends RREP to Node 4 and route Node 4-Node 1-Node 2-Node 3 is confirmed to send data packets. Node 4 can now send data packets to Node 3 through the specified route. Imagine a Node 6 in the communication range of Node 1 and Node 2. As shown in Figure-3, Node 1 moves out of network. Suppose Node 6 detects it first by not getting any HELLO message from Node 1and marks the respective route table entry for route as invalid. It sends out an RERR with the invalid route which is received by Node 2. This is how Node 2 comes to know from Node 6 that Node 1 is no longer its neighbor

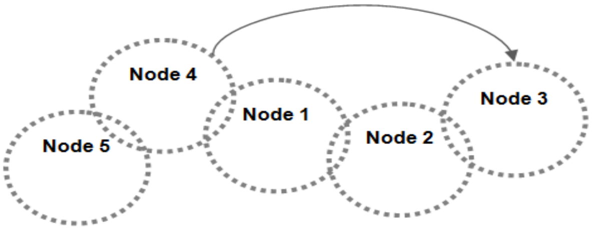

Figure-2 Communication between nodes in a Mobile Ad-hoc Network

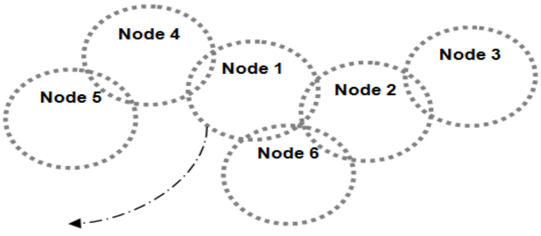

Figure-3 Node 1 moves out of communication range

B. Security Attacks against AODV :

As MANETs are unwired network with dynamic topology associated with them, they are very vulnerable to MANET attacks. In protocol stack, Physical layer has security issues like Denial of Service (DoS) attacks and preventing signal jamming. Network layer has to deal with security of ad-hoc routing protocol and related parameters. Transport layer has issues with end to end data security with encryption methods and Authentication. Application layer has security concerns with prevention, worms, malicious codes, application abuses as well as virus detection.

There can be two kinds of attacks: passive and active. A passive attack does not disturb the normal network operation while an active attack does it. In passive attack, attacker sneaks data without altering it. Passive attacks are difficult to detect as there is no change in the functionality of the network. Active attacks can be internal or external. Internal attacks are carried out by nodes within the network while external attacks are carried out by nodes outside the network. Modification, Impersonation and Fabrication are some of the most common attacks that cause a big security concern for MANET.

C. Attacks using Modification :

A node may attack by altering the protocol fields in messages or injecting routing messages with false values. To determine the shortest path, AODV uses the hop count parameter. A malicious node can set the false hop counts. Also, it can set false value of route sequence numbers. This may cause redirection of network traffic. A DoS attack may be launched by modifying source routes as well. DoS attack is easy to carry out but it is difficult to detect.

D. Attacks using Impersonation :

By impersonating a node (spoofing), a malicious node cancause lots of attacks in MANET. For example, traffic that belongs to the impersonated node may be redirected to the malicious node. Loops may also be created by spoofing. The malicious node may take up identity of multiple nodes; it does not need to impersonate any node of the network.
8 7.3 Attacks using Fabrication.

In fabrication attacks, false routing information is generated by an intruder. For example, false route error messages (RERR) and routing updates may disturb the network operations or consume node resources. Some well-known fabrication attacks are described here:

a. ***Blackhole attacks:*** A black hole is a malicious node that falsely replies for route requests without having an active route to the destination. It exploits the routing protocol to advertise itself as having a good and valid path to a destination node. It tries to become an element of an active route, if there is a chance. It has bad intention of disrupting data packets being sent to the destination node or obstructing the route discovery process. Cooperative black hole attack is caused by many neighbor black holes co-operating each other. Black hole attack may be internal or external.

b. ***Grayhole attacks*:** A gray hole may forward all packets to certain nodes but may drop packets coming from or destined to specific nodes. In other type of attack, node may behave maliciously for some time but later on it behaves absolutely normally. Sometimes, a node may combine the behavior of attacks discussed above. Due to this uncertainty in behavior of gray hole, this type of attacks are more difficult compared to black hole attack. Like black holes, cooperative gray hole attacks may be possible against AODV.

c. ***Wormhole attacks:*** In this type of attacks, the attacker disrupts routing by short circuiting the usual flow of routing packets. Wormhole attack can be done with one node also. But generally, two or more attackers connect via a link called „wormhole link‟ . They capture packets at one end and replay them at the other end using private high speed network. Wormhole attacks are relatively easy to deploy but may cause great damage to the network.

E. Securing AODV :

To make AODV secure, we need to understand security attributes and mechanisms. Security is applied with the mixture of processes, procedures, and systems which are used to ensure confidentiality, authentication, integrity, availability, access control, and non repudiation [6].

As MANETs use an open medium, all nodes can access data within the communication range. Therefore, **confidentiality** should be obtained by preventing the unauthorized nodes to access data. **Authentication** should be used to ensure the identity of source as well as neighbor nodes to prevent a node from accessing unauthorized resources and confidential information as well as to stop it from interfering operations of other nodes. **Integrity** helps to prevent malicious nodes from altering data and resending it (called replay attack e.g. wormhole attack). Also, if a node sends a message, that node cannot deny that the message was sent by it which is called **non repudiation** [8] [6].

To defend against passive attacks conventional approaches like digital signature, encryption, authentication and access control (whether a node having appropriate access rights to access the network) should be considered. To defend against active attacks intrusion detection systems and cooperation enforcement mechanisms (reducing selfish behavior of a node) are useful. Encryption and authentication are based on asymmetric and symmetric cryptography [11]. To achieve data integrity and authentication, hash functions and digital signatures are really useful.

Secure Ad-hoc On Demand Distance Vector (SAODV) is an extension of AODV in which digital signature and has chains mechanisms are used. Every node uses digital signature for authentication and integrity in routing messages like RREQ, RREP and RRER. This signature is verified by neighbor nodes that receive the message. Hash chains are used to secure hop-count mechanism. Thus, SAODV addresses security of routing messages only; security of data exchange still remains unaddressed. Moreover, due to digital signatures, messages get bigger. Also, generating and verifying signatures add to the overhead, especially when double signatures mechanism is used.

F. Performance Parameters:

This section presents the performance parameters used to evaluate the proposed AODVLRT routing protocol against the original AODV routing protocol. The main performance parameters are Routing message overhead, average end to end delay, and throughput. Under each main performance parameters, there are secondary performance parameters which affect it or depend on it.

a. Routing Message Overhead:

Routing message overhead is calculated as the total number of control packets transmitted. The increase in the routing message overhead reduces the performance of the ad-hoc network as it consumes portions from the bandwidth available to transfer data between the nodes.

b. Average End to End Delay:

Average end to end delay is used to measure the latency. It is calculated as the total summation of the division of total end to end delay (DT) by the number of packets delivered (NPD) divided by the number of nodes (NN) as in Eq. (1).

$$\Sigma\left(\frac{D_T}{N_{PD}}\right) \Big/ (N_N) \qquad (1)$$

Average end to end delay is affected by path length as when the path lengths get longer the average end to end delay gets larger. Average path length is used to measure path lengths and it is calculated as the total summation of the division of the number of hop counts (NHC) by the number of data packets received (NPR) divided by the number of nodes (NN) as in Eq. (2)

$$\Sigma\left(\frac{N_{HC}}{N_{PR}}\right) \Big/ (N_N) \qquad (2)$$

Average end to end delay is affected by the broken links as the increase in the number of broken links gets the average end to end delay increased. Broken links is calculated as the number of broken links for all the nodes. The increase in the number of local repair retrials attempts after the first local repair attempt increase the delay of repairing a route. The percentage of local repair retrials to local repair first trails attempts is calculated as the division of the summation of the number of local repair retrials attempts (NLRR) by the summation of the number of local repair first trials attempts (NLRF) as in Eq. (3).

$$\frac{\Sigma(N_{LRR})}{\Sigma(N_{LRF})} \qquad (3)$$

c. Throughput:

Throughput is a very important parameter in evaluating the modifications performance. It is calculated as the number of bits received per second. Throughput is affected by the number of packets dropped or left wait for a route which is evaluated as the summation of the number of packets dropped or left wait for a route for all the nodes.

IV. CONCLUSION

MANETs require a reliable, efficient, scalable and most importantly, a secure protocol as they are highly insecure, self-organizing, rapidly deployed and they use dynamic routing. AODV is prone to attacks like modification of sequence numbers, modification of hop counts, source route tunneling, spoofing and fabrication of error messages. Although fabrication of source routes (cache poisoning) is not possible in AODV while DSR is prone to it. Wormhole attack is a real threat against AODV protocol in MANET. Therefore, trustworthy techniques for discovering and detection of wormhole attack should be used. We should keep in mind that some solutions may not work well in the presence of more than one malicious node, while some require special hardware and some solutions are very expensive. So, there is still a lot of room for research in this area to provide a more secured MANET.

V. REFERENCES

[1]. Z. J. Haas, J. Deng, B. Liang, P. Papadimitratos,a nd S. Sajama: Wireless Ad-Hoc Networks, Encyclopedia of Telecommunications, 2002.

[2]. G. He: Destination-Sequenced Distance Vector(DSDV) Protocol, Networking Laboratory, Helsinki University of Technology, 2002.

[3]. C. C. Chiang: Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel, Proc. IEEE SICON '97, April 1997, pp. 197– 211.

[4]. T. Chen, M. Gerla: Global State Routing: A New Routing Scheme for Ad-hoc Wireless Networks, In Proceedings of IEEE ICC'98, Atlanta, GA, June 1998, pp. 171-175.

[5]. G. Pei, M. Gerla, and T. Chen: Fisheye State Routing in Mobile Ad Hoc Networks, ICDCS Workshop on Wireless Networks and Mobile Computing, 2000.

[6]. T. Clausen, P. Jacquet: Optimized Link State Routing Protocol (OLSR), Network Working Group, IETF RFC, RFC 3626, October 2003.

[7]. C. Perkins, E. Belding-Royer, S. Das: Ad hoc On-Demand Distance Vector (AODV) Routing Network Working Group, IETF RFC, RFC 3561, July 2003.

[8]. D. B. Johnson, and D. A. Maltz: Dynamic Source Routing in Ad-Hoc Wireless Networks, Mobile Computing, T. Imielinski and H. Korth, Eds., Kluwer, 1996, pp. 153–81.

[9]. C. K. Toh: Ad Hoc Mobile Wireless Networks: Protocols and systems, Chapter 6, p.p. 80-95, Prentice-Hall, 2002.

[10]. Komala CR, Srinivas Shetty, Padmashree S., Elevarasi E., "Wireless Ad hoc Mobile Networks", National Conference on Computing Communication and Technology, pp. 168-174, 2010

[11]. Samir R. Das, Charles E. Perkins and Elizabeth M. Royer, "Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks"

[12]. Ramanarayana Kandikattu, and Lillykutty Jacob, "Secure Internet Connectivity for Dynamic Source Routing (DSR) based Mobile Ad hoc Networks", International Journal of Electronics, Circuits and Systems, pp. 40-45, 2007

© 2010, IJARCS All Rights Reserved

[13]. David B. Johnson, David A. Maltz and Josh Broch, " DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks", http://www.monarch.cs.cmu.edu/

[14]. Josh Broch, David A. Maltz, David B. Johnson, Yih-Chun Hu and Jorjeta Jetcheva, "A Performance Comarison of Multi-hop Wireless Ad Hoc Network Routing Protocols", ttp://www.monarch.cs.cmu.edu/

Short Biodata of the Author

Awadhesh Kumar graduated from Govind Ballabh Pant Engineering college, Pauri (Garhwal) in Computer Science & Engineering in 1999. He obtained his Master degree (M.Tech.) in Computer Science from Uttar Pradesh Technical University, Lucknow in 2006. He joined the department of Computer Science & Engineering at Kamla Nehru Institute of Technology, Sultanpur (Uttar Pradesh) as Lecturer in 2000 and Assistant Professor in 2007. His teaching and research interests include Computer Networks, Wireless Networks and Mobile Ad-Hoc Networks. He is pursuing PhD in the department of Computer Science & Engineering, MNNIT, Allahabad (Uttar Pradesh) in the area of Mobile Ad-hoc Networks.
Email: awadheshkumar.knit@gmail.com

Dr. Neeraj Tyagi has completed B.E. degree in Computer Science & Engineering from Motilal Nehru National Institute of Technology, Allahabad (Uttar Pradesh) in 1987, his M.E. degree in Computer Science & Engineering from MNNIT, Allahabad (Uttar Pradesh) in 1997 and PhD degree in Computer Science & Engineering from MNNIT, Allahabad (Uttar Pradesh) in 2008.His teaching and research interests including Computer Networks, Mobile Ad-Hoc Networks, wireless Networks and Operating Systems. He joined the department of Computer Science & Engineering in 1989 at MNNIT, Allahabad and he has Also worked in Warman International- Australia, G.E (Capital) - U.S.A, Electronic Data Systems- U.S.A during 1999-2001. Presently he is working as Associate Professor in the department of Computer Science & Engineering, MNNIT, Allahabad (Uttar Pradesh), India.
Email:neeraj@mnnit.ac.in

© 2010, IJARCS All Rights Reserved