An Implementation and Performance Evaluation Study of AODV, MAODV, RAODV in Mobile Ad hoc Networks

E.Suresh Babu[1] **C.Nagaraju**[2] **MHM Krishna Prasad**[3]

Abstract: Mobile ad hoc network (MANET) is a new pattern of wireless networks, offering unrestricted mobility without any centralized infrastructure such as base station or mobile switching centers. Moreover, it is an autonomous system in which collection of mobile self organizing nodes connected by wireless links are free to move randomly and often act as routers at the same time by forming a multi-hop network. The MANETs are finding more likely importance due to the flexibility, ease and speed with which these networks can be deployed as well as reconfigured. This allows the use of this kind of networks in special circumstances, such as military battle field, natural disaster recovery, emergency medical services, etc. On one hand the security sensitive applications of MANETs require high degree of security; on the other hand they are inherently vulnerable to security attacks, the inherent features of MANETs make them more vulnerable to a wide variety of attacks such as DoS Attack. A malicious node drops packets solely to disrupt the network performance and prevent other nodes from accessing any network services. We represent the simulation study with DoS attack scenarios in the context of a different network nodes using AODV routing protocol. In this paper we will propose a feature to secure AODV against Denial of Service (DOS) attacks that protect data from the intrusion by malicious nodes.

Keywords: AODV, Routing, RAODV, DoS Attack, Ad hoc Networks,

1. INTRODUCTION:

Mobile Ad hoc networks, also known as MANETs, are a new and useful innovation in the field of mobile wireless communication. Due to the various applications that have been and can be developed under this technology including ocean and wildlife monitoring, manufacturing machinery performance monitoring, building safety and earthquake monitoring, and many military applications, MANETs have been attracting many researchers. Unlike other types of networks, MANETs are usually deployed without a centralized control unit; the devices participating in a MANET rely on other units to route information to their destinations. This, along with the fact that MANET nodes are often constrained in power, makes MANETs vulnerable to various malicious attacks and applying the routing techniques that work with wired networks is infeasible here. In contrast of the applications of ad hoc network, it is evident to realize that secure service delivery in such network has become a major concern of the related researchers. Particularly secure routing has become an excellent topic of open research because of the extraordinary gap between the nature of ad hoc network and the security required by its applications.

Most research efforts are concentrated on how to secure routing information on the mobile nodes. It is desirable that a good secure routing algorithm should not only prevent each of possible attacks, but also ensure that no node can prevent successful route discovery and maintenance between any other nodes other than by non-participation. Methodologically looking at many researches which were working towards the security of wireless ad hoc networks, these studies are based on two types of approaches. One approach is to develop the secure protocols for instance, secure routing algorithms. In past decades, there are many schemes of secure routing protocols designed for MANETs, unfortunately a limited number of these schemes are practically implemented, their feasibility and performance are yet to be studied. Further to the already implemented schemes, in case that there are two or more routes, none of them guarantee the communication nodes with the most secure route. Another problem is that the schemes are not capable of adapting to the changing in their topology.

2. OVERVIEW OF AODV ROUTING PROTOCOL

In E M. Belding-Royer Charles E. Perkins [7] proposed Ad-hoc On Demand Distance Vector (AODV) protocol is a reactive routing protocol; however it has a feature of proactive protocol in a sense that a source node stores the valid routes for the next hop node in routing table. AODV uses a distributed approach [1] meaning that source nodes do not know the routing sequence of the intermediate nodes it has to go through to reach the destination.

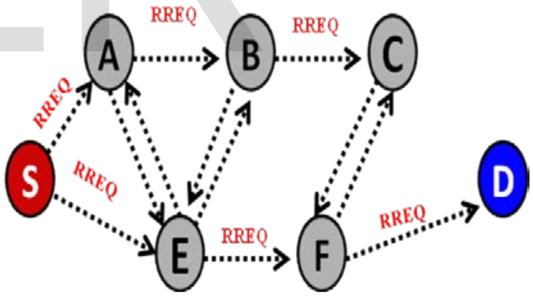


Fig-1: RREQ Broadcast

AODV uses the route discovery and route reply process to create and maintain a route on demand. In the route discovery phase for a source node to send information to a destination node, it first looks up its own routing table to see if a valid route exists. If a valid route does not exist, a source node broadcasts a global route request message (RREQ) that contains the source address, source sequence number, destination address, destination sequence number, broadcast ID, and hop count. The combination of the source address and the broadcast-ID is used to uniquely identify each RREQ message. A node that receives the RREQ message which is usually the nearest node to the source node replies immediately with a routing reply (RREP) if it has a fresh route. Otherwise, it forwards the RREQ message to establish the route to the destination. The sender selects the first node to respond with a RREP (Routing Reply) as the intermediate node to send messages through. During the route discovery phase a forward pointer link between source node, destination node, and all the intermediate nodes as the RREQ messages propagate in the routing discovery as shown in Fig-1. Similarly, backward pointer links between all nodes as the RREP messages propagate back to the source node, Fig-2.

- ***Mr. E. Suresh Babu** is pursuing PhD in Computer Science & Engineering from J.N.T.University Kakinada. Currently, he is working as an Associate Professor in the Department of CSE in PACE Institute of Technology & Sciences, Ongole.. suresh_esb551@yahoo.co.in*
- ***Dr. C. Naga Raju** Completed PhD in digital Image processing from J.N.T.University Hyderabad. Currently, he is working as a Associate professor in YSR College of Engineering of YV University, Poddutur. .*
- ***Dr. MHM. Krishna Prasad** PhD in Computer Science & Engineering from J.N.T. University Hyderabad. Currently, he is working as a Associate professor in the Dept of Computer Science Engineering JNTUK University.*

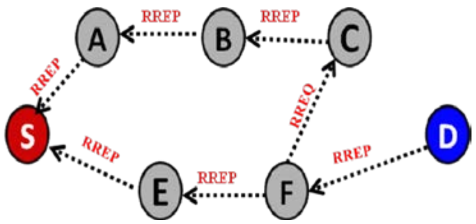


Fig-2: RREP Propagation.

3. VARIOUS ATTACKS IN MANETS

There are a wide variety of attacks that target the weakness of MANET. Some attacks apply to general network, some apply to wireless network and some are specific to MANETs. These security attacks can be classified according to different criteria, such as the domain of the attackers, or the techniques used in attacks.

3.1 Passive Vs. Active Attacks:

The attacks in MANET can roughly be classified into two major categories, namely passive attacks and active attacks [4][5]. A passive attack obtains data exchanged in the network without disrupting the operation of the communications, Examples of passive attacks are eavesdropping, traffic analysis, and traffic monitoring while an active attack involves information interruption, modification, or fabrication, jamming, impersonating, denial of service (DoS), and message replay thereby disrupting the normal functionality of a MANET.

4. SECURITY PROBLEMS IN AODV ROUTING PROTOCOL

AODV is vulnerable to a well known malicious node called DoS attacks. These nodes are planted by a hacker. In this paper we present some interesting DoS attacks in the wireless environment and suggest possible solutions. Our description is brief as exhaustive listing of such attacks; we consider various traffic patterns that an intelligent attacker(s) might generate in order to cause denial of service. Denials of Service (DoS) attacks are common place in the Internet. Guarding against DoS attacks is a critical component of any security system. While DoS has been studied extensively for the wire-line networks, there is lack of research for preventing such attacks in mobile ad hoc networks. Due to deployment in tactical battlefield missions these networks are susceptible to attacks of malicious intruders. These intruders might attempt to disrupt/degrade the functioning of the whole network or may harm a specific node. Traditional DoS attacks involve overwhelming a particular host. However, in mobile ad hoc networks, mobility, limited bandwidth, routing functionalities associated with each node, etc, present many new opportunities for launching a DoS. we point out that these attacks might be at the routing layer or at the MAC layer. But In this paper we focus on DoS attacks in wireless ad hoc networks. More specifically, we investigate attacks at the routing layer. For instance, In AODV, a malicious node that receives a RREQ could return a RREP to the source node with a destination sequence number that is far greater than that in the RREQ to ensure that it is on the selected path. In this an attacker may damage the other nodes just by dropping the Packets. This can cause a severe degradation of network performance in terms of the achieved throughput and latency. In wireless networks, DoS attacks are difficult to prevent and protect against.

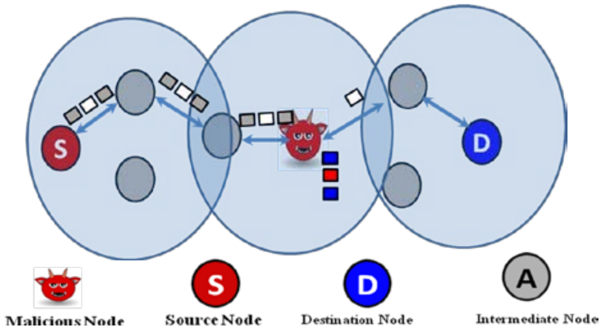


Fig-3: Dos Attack in AODV Protocol

5. OVERVIEW OF RAODV ROUTING PROTOCOL:

Analyzing AODV protocols, we can say that most of on-demand routing protocols based on unicast route reply along a reverse path to establish a routing path and use complex methods to build multipath. Our RAODV method distinguishes due to its simplicity of building multipath.
Specifically, the R-AODV protocol discovers routes on-demand using a reverse route discovery procedure. During route discovery procedure source node and destination node plays same role from the point of sending control messages. Thus, after receiving RREQ message, destination node floods *reverse request* (R-RREQ), to find source node. When source node receives an R-RREQ message, data packet transmission is started immediately.

5.1 Route Discovery In R-AODV

Since R-AODV is reactive routing protocol, no permanent routes are stored in nodes. The source node initiates route discovery procedure by broadcasting. Whenever the source node issues a new RREQ, the broadcast ID is incremented by one. Thus, the source and destination addresses, together with the broadcast ID, uniquely identify this RREQ packet [1, 17]. The source node broadcasts the RREQ to all nodes within its transmission range. These neighboring nodes will then pass on the RREQ to other nodes in the same manner. As the RREQ is broadcasted in the whole network, some nodes may receive several copies of the same RREQ. When an intermediate node receives a RREQ, the node checks if already received a RREQ with the same broadcast id and source address. The node cashes broadcast id and source address for first time and drops redundant RREQ messages. The procedure is the same with the RREQ of AODV.

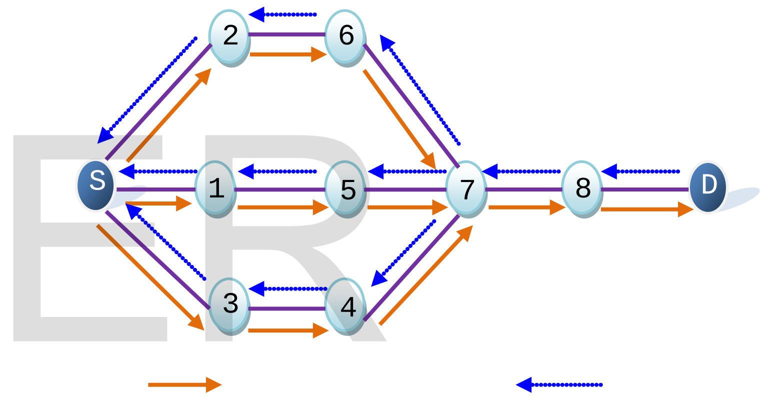


Fig-4 (a): R-RREQ Message Flow (b) RREQ Message Flow

When the destination node receives first route request message, it generates so called reverse request (R-RREQ) message and broadcasts it to neighbor nodes within transmission range like the RREQ of source node does. R-RREQ message (table-1) contains following information: reply source id, reply destination id, reply broadcast id, hop count, destination sequence number, reply time (timestamp).
When broadcasted R-RREQ message arrives to intermediate node, it will check for redundancy. If it already received the same message, the message is dropped, other-wise forwards to next nodes.

Type	Reserved	Hop Count
Broadcast ID		
Destination IP address		
Destination Sequence Number		
Source IP address		
Replay Time		

Table -1: R-RREQ Message Format

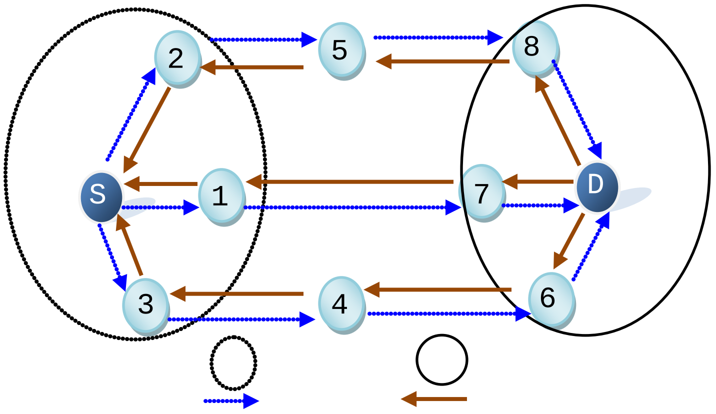


Fig -5(a) RREQ Message Flow (b) R-RREQ Message Flow

6. A POSSIBLE SECURITY SOLUTION OF DOS ATTACK IN AODV

To prevent denial of service attack on AODV protocol based network from an external malicious node and intruder or from an internal misbehaving node that can flood the network with any kind of control messages, such as RREQ and RREP. In this study we implement path-hopping routing based on reverse AODV. In R-AODV, which is an easy multipath searching method, the destination node uses reverse RREQ to find the source node rather than a unicast reply. Hopping paths means source node sends each data packet through different paths each time, therefore traffic is well distributed among paths and intrusion of malicious node effect to network become weaker. Let's assume node 5 is a malicious node. How can this influence on two protocols. Node intrusion for AODV case will be 100% due to single path. On AODV intrusion of malicious nodes may cause serious impairment to the security. Node intrusion for RAODV will be 33%. Therefore, we can conclude that more paths reduce malicious node intrusion to network.

Let's assume some parameters: Np is the number of nodes in routing paths, N_{all} is the number of all nodes in network, M is the number of malicious nodes, S is the number of paths from a source to a destination, P_m is probability of active malicious nodes.

$$P_{M} = \frac{N_p . M}{N_{all}}$$

Therefore, we can calculate P_i, malicious node intrusion rate, as follows

$$P_{i} = \frac{P_m}{S}$$

7. SIMULATION ENVIRONMENT

Our Simulation used for experiments and provides an analysis of the AODV, DoS in AODV and ROADV is implemented using NS-2. A mobile ad hoc network consisting of 50,150,100,200 nodes in a simulation area of 750m×750m is simulated. The link layer model of the IEEE 802.11 wireless LAN standard. The radio model uses the frequency hopping spread spectrum technology with 2 Mbps capacity. The radio propagation range for each node is 250 meters. In order to get realistic performance, the results are averaged for a number of scenarios. We tried to measure

Parameter	Value
Channel	Channel/Wireless Channel
Propagation model	Propagation/Two Ray Ground
Antenna	Antenna/Omni Antenna
Simulator	NS-2
No of Nodes	50,100,150,200
Routing Protocols	AODV,AODV with DoS Attack and RAODV
MAC Layer	802.11 IEEE
Simulation Time	150 Second
Simulation Area	750m X 750m
Transmission Range	250m
Node Movement	Model Random Waypoint
Traffic Type	FTP
Data Payload	512 Bytes/Packet

Table-2: Simulation Parameters

The protocols performance on real life scenario at a speed of 10 m/s. The simulation time was taken to be of 150 seconds for FTP traffic type with a packet size of 512 Byte. Also, we have considered nodes with Omni-Antenna and Two Ray Ground Radio Propagation method. Simulation parameters are appended in Table-2.

8. PERFORMANCE EVALUATION

The performance evaluation is based on the comparison of following metrics

- **Packet Delivery Fraction (PDF):** The ratio of the data packets delivered to the destination and the total number of data packets generated by the sources. Mathematically, it can be expressed as:

$$P = \frac{1}{c}\sum_{k=0}^{s}\frac{R_k}{N_k}$$

  Where, P is the fraction of successfully delivered packets, C is the total number of flow or connections, k is the unique flow id serving as index, R_k is the count of packets received from flow k and N_k is the count of packets transmitted to k.
- **Average End to End Delay (AEED):** It is an aggregated average of the time taken by a packet for the successful delivery at the destination. The time for the successful delivery is the interval between the packet is generated at the source and the time when it is delivered to the application at the destination. It includes all the delays that can occur due to waiting in the data buffer, in the network interface queue and the time taken in propagation.

$$D = \frac{1}{N}\sum_{i=1}^{s} R_i - S_i$$

  Where N is the number of successfully received packets, i is unique packet identifier, R_i is time at which a packet with unique id i is received, S_i is time at which a packet with unique id i is sent and D is measured in ms.
- **Routing Load (RL):** It is the ratio of the routing packets generated to the data packets delivered at the destination. Sometime it also renamed as throughput.

$$\text{Throughput } (T) = \frac{r_a}{g_a}$$

  r_a: total no. of received packets at application layer; g_a: total no. of generated packets at application layer

8.1 Performance Analysis

It is observed that from Table-3 and Figure-6 shows End-2-End delay for AODV, AODV with DoS attack, RAODV as you can see RAODV has less delay due to distributed traffic load among paths.

Nodes	End-To-End Delay		
	AODV	AODV with DoS Attack	RAODV
50	123.555	4189.31	166.304
100	334.119	3157.71	251.541
150	498.191	1246.43	187.654
200	201.545	1201.54	198.395

Table -3: End-To-End Delay with Varying No of Nodes of AODV, MAODV & RAODV

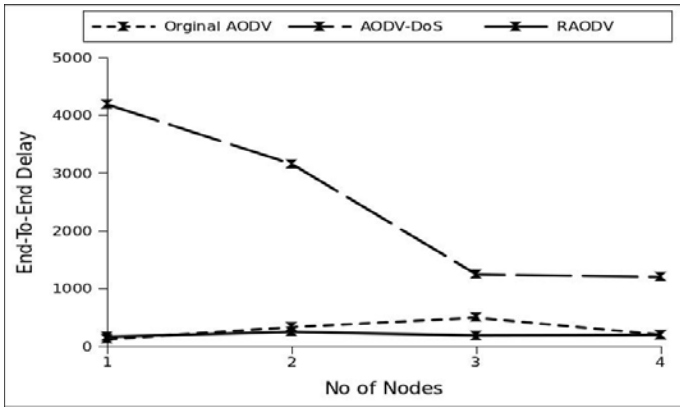
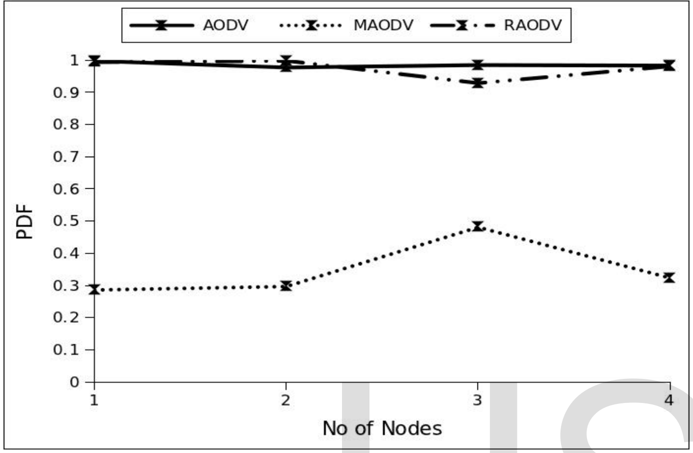


Fig -6: End-To-End Delay with Varying No of Nodes of AODV, MAODV & RAODV

Nodes	Packet Delivery Fraction		
	AODV	AODV with DoS Attack	RAODV
50	0.9976	0.2857	0.9938
100	0.9960	0.9771	0.9681
150	0.9908	0.7848	0.9286
200	0.9831	0.9831	0.9880

Table-4: Packet Delivery Fraction with varying number of Nodes AODV, MAODV & RAODV

Table-4 & Figure 7 shows packet deliver ratio of each protocol when the number of nodes increases. RAODV delivery ratio is slightly less than AODV, because it maintains more paths than the other does and path break rate may be higher. However, when more nodes become available in network, RAODV can build more stable multi-paths and hence increase packet delivery ratio



. **Fig-7: Packet Delivery Fraction with varying number of Nodes AODV, MAODV & RAODV**

Table-5& Figure-8 illustrates the throughput curve under AODV, AODV with DoS packet attack and ROADV. The Throughput of RAODV less than AODV but traffic is well distributed among paths and intrusion of malicious node effect to network becomes weaker. This is obvious gives better throughput than when the normal AODV is under attack.

Nodes	**Throughput**		
	AODV	**AODV with DoS Attack**	**RAODV**
50	547.81	0.9876	516.66
100	292.50	0.9245	301.33
150	420.00	12.345	202.84
200	546.59	40.450	499.22

Table-5 : Throughput with varying number of Nodes of AODV, MAODV & RAODV

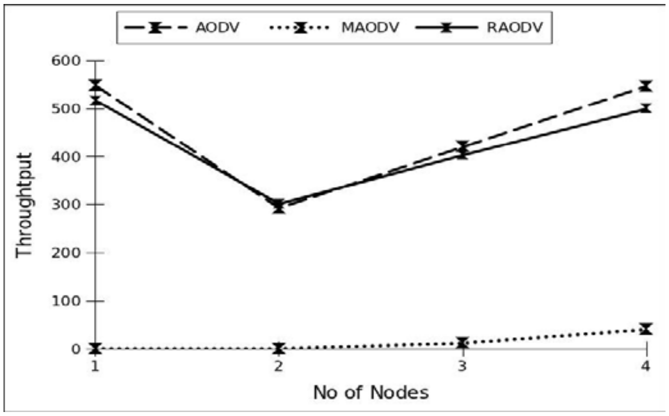


Fig-8: Throughput with varying number of Nodes of AODV, MAODV & RAODV

9. CONCLUSION AND FUTURE WORK

In this paper we have analyzed AODV, AODV with DoS Attack and RAODV routing protocols and we have developed a practical solution that solves security issue of the DoS Attack and Intrusion of malicious nodes gives security solution using RAODV protocol. In the presented work, the Passive DoS Attack are dealt with; it would be interesting to note the behavior of a routing protocol capable of handling both selfish and malicious nodes using Biological Inspired cryptography.

REFERENCES

1 Elizabeth M. Belding-Royer, Charles E. Perkins Evolution and future directions of the ad hoc on-demand distance-vector routing protocol-Elsevier 2003

2 C. E. Perkins. *Ad Hoc Networking*. Addison-Wesley Professional, first edition, 2000.

3 S. R. Medidi, M. Medidi, and S. Gavini. Detecting packet-dropping faults in mobile ad-hoc networks. In *Proceedings of The Thirty-Seventh Asilomar Conference on Signals, Systems & Computers*, pages 1708–1712, November 2003.

4 S. Medidi, M. Medidi, S. Gavini, and R. Griswold. Detecting packet mishandling in manets. In *Security and Management*, pages 159–162, 2004.

5 R. Griswold and S. Medidi. Malicious node detection in ad-hoc wireless networks. In *Proceedings of SPIE AeroSense, Digital Wireless Communications V*, April 2003.

6 R. Griswold. Malicious node detection in ad hoc wireless networks. Master's thesis, Washington State University, Pullman, 2003.

7 E.M. Belding-Royer, Hierarchical routing in ad hoc mobile networks, Wireless Communications and Mobile Computing 2 (5) (2002) 515–532.

8 University of Southern California Information Sciences Institute (USC/ISI). The network simulator - ns-2. Computer software. Available from http://www.isi.edu/nsnam/ns/

9 WPI. NS by Example. Online. Accessed from http://nile.wpi.edu/NS/.

10 M. Greis. Tutorial for the Network Simulator "ns". Online. Accessed from http://www.isi.edu/nsnam/ns/tutorial/.

11 Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks by Vikram Gupta+, Srikanth Krishnamurthy§, and Michalis Faloutsos in 2010

12 Manikandan, and R. Manimegalai S.P.SURVEY ON MOBILE AD HOC NETWORK ATTACKS AND MITIGATION USING ROUTING PROTOCOLS American Journal of Applied Sciences, 2012, 9 (11), 1796-1801

13 L. Zhou and Z. Haas. Securing ad hoc networks. IEEE Network, 13(6):24--30, November / December 1999.

14 Y. Zhang and W. Lee, "Intrusion detection in wireless ad hoc networks," ACM MOBICOM, 2000.

15 P.Papadimitratos and Z.J. Haas, "Secure Routing for Mobile Ad Hoc Networks," SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002.

16 Zhi Li and Yu-Kwong Kwok, "A New Multipath Routing Approach to Enhancing TCP Security in Ad Hoc Wireless Networks" in Proc. ICPPW 2005.

17 3. Chonggun Kim, Elmurod Talipov, and Byoungchul Ahn, "A Reverse AODV Routing Protocol in Ad Hoc Mobile Networks" in EUC Workshops 2006, LNCS 4097, pp. 522 – 531, 2006.

18 4. Rendong Bai and Mukesh Singhal, "Salvaging Route Reply for On-Demand Routing Pro-tocols in Mobile Ad-Hoc Networks" in MSWIM 205, Montreal, Quebec, Canada. Oct 2005

19 5. C. K.-L. Lee, X.-H. Lin, and Y.-K. Kwok, "A Multipath Ad Hoc Routing Approach to Combat Wireless Link Insecurity," Proc. ICC 2003, vol. 1, pp. 448–452, May 2003.

20 6. S.-J. Lee and M. Gerla, "Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks," Proc. ICC 2001, vol. 10, pp. 3201–3205, June 2001.

21 7. M. K. Marina and S. R. Das "On-Demand Multi Path Distance Vector Routing in Ad Hoc Networks," Proc. ICNP 2001, pp. 14– 23, Nov. 2001.

22 8. A. Nasipuri and S. R. Das, "On-Demand Multipath Routing for Mobile Ad Hoc Net-works," Proc. ICCN 1999, pp. 64–70, Oct. 1999.

23 Elmurod Talipov, Donxue Jin, Jaeyoun Jung, Ilkyu Ha, Youngjun Choi, and Chonggun Kim, "Path hopping based on Reverse AODV for Security" APNOMS2006, LNCS 4283, pp. 574 – 577, 2006.

ABOUT THE AUTHORS

Mr. E. Suresh Babu received his B.Tech degree in Computer Science from RGM College of Engineering, Nandyal, M.Tech degree in Computer Science from V.T.University Belgaum and pursuing PhD in Computer Science & Engineering from J.N.T.University Kakinada. He has published 5 research papers in various International Journal and 5 research papers in various National and International Conferences. He has attended 10 seminars and workshops. His areas of interests are wireless communication and MANETs.

Dr. C. Naga Raju received his B.Tech degree in Computer Science from J.N.T.University Anantapur, M.Tech degree in Computer Science from J.N.T.University Hyderabad and PhD in digital Image processing from J.N.T.University Hyderabad. Currently, he is working as a Associate professor in YSR College of Engineering of YV University, Poddutur. He has got 16 years of teaching experience. He has published thirty Five research papers in various National and International Journals and about twenty eight research papers in various National and International Conferences. He has attended twenty seminars and workshops. He is member of various professional societies like IEEE, ISTE and CSI.

Dr. MHM. Krishna Prasad received his B.Tech from CBIT Hyderabad, M.Tech degree in Computer Science from J.N.T. University Hyderabad and PhD in Computer Science & Engineering from J.N.T. University Hyderabad. Currently, he is working as a Associate professor in the Dept of Information Technology JNTUK University College of Engineering Vizianagaram. . He has got 19+ years of teaching experience. He has published Twenty research papers in various National and International Journals and various research papers in National and International Conferences. He has attended twenty seminars and workshops. He is member of various professional societies like IEEE, ISTE and CSI.