Volume: 03 Issue: 05 Pages: 1352-1357 (2012)

Comparative Analysis of Routing Attacks in Ad Hoc Network

Bipul Syam Purkayastha
Department of Computer Science, Assam University, Silchar – 788011, India
Email: bipul_sh@hotmail.com
Rajib Das
Department of Computer Science, Assam University, Silchar – 788011, India.
Email: rajibdas76@gmail.com

----------ABSTRACT----------
In the mobile ad hoc networks the major role is played by the routing protocols in order to route the data from one mobile node to another mobile node. But in such mobile networks, routing protocols are vulnerable to various kinds of security attacks such as blackhole node attacks. The routing protocols of MANET are unprotected and hence resulted into the network with the malicious mobile nodes in the network. These malicious nodes in the network are basically acts as attacks in the network. In this paper, we modify the existing DSR protocol with the functionality of attacks detection without affecting overall performance of the network. Also, we are considering the various attacks on mobile ad hoc network called blackhole attack, flooding attack and show the comparative analysis of these attacks using network simulator ns-2.

Keywords: MANET, blackhole, flooding, DSR, ns-2.

Date of Submission: October 24, 2011 Date of Acceptance: December 10, 2012

I. INTRODUCTION

Mobile Ad hoc Networks (MANETs) are open to a wide range of attacks due to their unique characteristics like dynamic topology, shared medium, absence of infrastructure, multi-hop scenario and resource constraints. In such a network, each mobile node operates not only as a host but also as a router, forwarding packets for other nodes that may not be within direct wireless transmission range of each other. Thus, nodes must discover and maintain routes to other nodes. Data packets sent by a source node may be reached to destination node via a number of intermediate nodes. In the absence of a security mechanism, it is easy for an intermediate node to insert, intercept or modify the messages thus attacking the normal operation of MANET routing. This network is usually characterized by a dynamic topology, a limited bandwidth, energy constraints, the heterogeneity nodes, and a limited physical security. The applications having recourse to the ad hoc networks cover a very broad spectrum. For example in the tactical applications (fires, flood, etc.), in the soldier's field, in the monitoring systems, and the world of transport [1]. The problem of the MANET is how to find the investment of lower costs in rated capacities and reserves which ensures the routing of the nominal traffic and guarantees its reliability in the event of any breakdown of arc or node. That's why several families routing protocols emerged. Each protocol can be classified as a reactive like AODV (Ad hoc One Demand Distance Vector) and DSR (Dynamic Source Routing), proactive like OLSR (Optimized Link State Protocol), or hybrid like ZRP (or Routing Protocol Zones) [1].

In spite of the evolution of the ad hoc mobile networks during the last decade it still problems related security which remain unsolved. Although some solutions were proposed none of them can't satisfy all the constraints on the ad hoc networks.

In this paper we compare & analyze different routing attacks of ad hoc network & the performance evaluation of DSR under different attack. We use different methods to detect various security attacks in the MANET. Their performances were evaluated through simulations using network simulator (ns-2) and were analyzed and compared based on packet delivery ratio (%), throughput (kbps), average end to end delay (ms), and average jitter (ms).

II. DIFFERENT TYPES OF ATTACKS AND THEIR COUNTER MEASURES

The malicious node(s) can attacks in MANET using different ways, such as sending fake messages several times, fake routing information, and advertising fake links to disrupt routing operations. In the following subsection, current routing attacks and its countermeasures against MANET protocols are discussed in detail..

In **Blackhole Attack,** a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example, in AODV, the attacker can send a fake RREP (including a fake destination sequence

Volume: 03 Issue: 05 Pages: 1352-1357 (2012)

number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic. In a blackhole attack, where attacker A (say) sends a fake RREP to the source node S, claiming that it has a sufficiently fresher route than other nodes. Since the attacker's advertised sequence number is higher than other nodes' sequence numbers, the source node S will choose the route that passes through node A [1][2].

Several solutions exist to counter these types of attacks, among which we name the technical estimate relation. In this mechanism the authors classified the relation between the nodes and their neighbors in three cases: Unknown (node X sent forever (received) of messages to (from) the node y and the probability of the malevolent behavior are very high), acquaintance (node X sent (received) some messages to (from) the node y and the probability of the malevolent behavior must be observed) and Friend (node X sent (received) in abundance of the messages to (from) the node y and the probability of the malevolent behavior is too small. This mechanism is implemented in the routing protocol RDSR (Relationship enhanced DSR protocol) [3].

The Threshold of sequence number consists in performing a check to find if RREP_seq_no is higher than the threshold value. The threshold value is dynamically updated in each time interval. As the value of RREP_seq_no proves higher than the threshold value, one suspects the node to be malicious and adds it to the black list. This mechanism is implemented in the routing protocol DPRAODV (Detection, Prevention and Reactive AODV) [10].

The Watchdog or monitoring (watchdog) is a solution which makes it possible to identify malicious nodes. The Watchdog assigns positive values with a node which successfully forwarded packages and a negative value after a threshold level of bad behavior was observed. It's implemented in SWAN (mobile Secure Watchdog for Ad hoc Network). Pathrater which makes it possible the protocol to avoid nodes corrupted register in a black list [9].

The DRI or the data table of information's routing which is used to identify nodes of cooperative blackhole, it consists in adding two additional bits of information. These bits have as values 0 for "FALSE" and 1 for" TRUE " for intermediate nodes answering the RREQ of node source, AODV implements this mechanism [11][12]. The Cross checking solution which consists in hoping on reliable node (nodes by which node source has forwarded the data) to transfer from the packets of data.

Wormhole Attack is one of the most sophisticated and severe attacks in MANETs. In this attack, a pair of colluding attackers record packets at one location and replay them at another location using a private high speed network. The seriousness of this attack is that it can be launched against all communications that provide authenticity and confidentiality [1][2]. To fend off the Wormhole attacks some authors proposed to use the concept of Hop-count Analysis. In this mechanism, a route which has a low or high hop counted is considered to be nonusable. A so low hop counted can imply an attack of wormhole; while a high hop can also slow down the transmission. The protocol Multipath Hop-count Analysis (MHA) implements this mechanism and also protocol AODVWADR (AODV Wormhole Attack Detection Reaction) [8] .The clustering consists in dividing the network clusters with for each one a head and members. When a node in the item cluster suspect an attack wormhole of the layer1 in the cluster, it informs the head of the item cluster. The heads of the clusters of the layer1 inform its members respectively. This mechanism is implemented in the protocol in AODV [9]. The packet leash which can be geographical which ensures that the recipient of the packet is in at certain distance from the sender or temporal who ensures that the packet has a superior i.e. sender node which deals the time to live. The protocols LAR (Location Aided Routing) et AODVWADR (AODV Wormhole Attack Detection Reaction) implement this mechanism [1][7] and also the directional antennas (Directional antenna) which consists in using the direction of the packets of arrival to detect if the packets come from their own neighbors. This solution is implemented in DREAM (Distance Routing Effect Algorithm for Mobility).

The Selfish Attack consists in not collaborating for the good performance of the network. We can identify two types of nodes which do not wish to take part in the network. Defective nodes i.e. do not work perfectly. Those which are malevolent, it is those which intentionally, try to tackle the system: attack on the integrity of the data, the availability of the services, the authenticity of the entities (denial-of-service, interception of messages, usurpation of identity, etc). Selfish nodes are entities economically rational whose objective is to maximize their benefit. To prevent the selfish nodes some solutions were proposed.

Among these we have a solution based on the Negative Selection Algorithm (NSA). It's based on the principles of the discrimination of self or no self in the immune system (to define it to oneself like a collection S of elements in a characteristic space X, a collection which needs to be supervised). The detection of anomaly aims at distinguishing a new model like part of self or no-self, given a model of system of self. Structured GA (SGA) is a type of evolutionary algorithm which incorporates the redundant genetic material, which is controlled by a mechanism of gene activation. It uses the multi-layer genomic structures for its chromosome i.e. all the genetic material (expressed or not) is structured in a hierarchical chromosome. The activation and deactivates mechanism these coded genes. This

Volume: 03 Issue: 05 Pages: 1352-1357 (2012)

solution is implemented in AODV [10].

A solution based on the reputation (CORE and CONFIDANT) which consists in collecting information on an old behaviour of the tested entity by others [4][5][6]. A solution based on the payment (Nuglet) which requires with nodes which benefit from the resources of the network (transmitters and/or receivers) to pay "service providers" (intermediate nodes) [9][6] and a solution based on the localization (directional antennas).

Routing Tables Overflow consists of malicious nodes to cause the overflow routing tables of nodes being used as relay [13][14]. To fend off this attack the named solution Trust evaluation was proposed. It's based on the evaluation of confidence to ensure a secure routing in MANETs. The success of a communication through a node will increase the index of confidence of this node and the failure by this node will decrease the index of confidence. If this value reaches zero this node is registered in a blacklist and we inform the other neighbors. TRP (Trust-based Routing Protocol) implements this solution.

Flooding Attack, which makes it possible for an adversary to carry out a DoS by saturating the support with a quantity of broadcasting messages, by reducing the output of nodes, and in the worst case, to prevent them from communicating [15][16]. To prevent saturation on the level of nodes two principal approaches were proposed. An approach based on the Relationship, in this mechanism, all the nodes in an ad hoc network are classified by categories: friends, knowledge or foreigners, based on their relationship with their neighbor nodes. During the initialization of the network all the nodes will be foreigners between them. A confidence estimator is used in each node to evaluate the degree of confidence of his neighbors. This solution is implemented in protocol AODV) [17][18][19]. An approach based on the virtual currency which uses the concept of credit or micro payment to compensate for the node service. An approach based on the method of neighbor suppression (FAP). When the attacker diffuses a large number of RREQ packets, the neighbor nodes to the attacker record the rate of requests for routes. Once the threshold is exceeded, the neighbor nodes deny all the future packets of request of the attacker.

There are many attacks and the protocols which implement these above mentioned mechanisms do not resist with these types of attacks. The following table recapitulates the protocols and the attacks which the protocols can counter.

III. MODELING OF ATTACKS

In order to model the attacks in ns-2 it is important to understand at which layer of the protocol stack the attack is launched. Since we are currently only dealing with attacks on routing protocols we delved into the ns-2 code that dealt with the network layer. The modeling of attacks in ns-2 can be better understood by examining node behavior and composition in the simulator. A node in ns-2 consists of two TclObjects a address classifier and a port classifier object, a node id, an address or id_, monotonically increasing by 1 (from initial value 0) across the simulation namespace as nodes are created, a list of neighbors, a list of agents , a node type identifier, and a routing module [20].

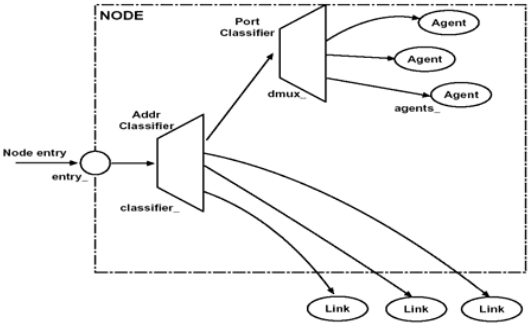

Fig 1: Modeling of Attacks in ns-2

The function of a node when it receives a packet is to examine the packet's fields, usually its destination address, and on occasion, its source address. It should then map the values to an outgoing interface object that is the next downstream recipient of this packet. This task is done by the classifier object. The classifier looks at the packet and then determines which agent to forward the packet. An agent is service or connection TCP/UDP with which two nodes in the simulator are connected. The actual processing of a packet received by the node is done by the agent. Each node can have more than one agent attached to it. An agent in ns is analogous to a port in a TCP connection to which a particular flow of data is associated.

An attack model in ns-2 can be implemented at the MAC layer that is changing the code for classifier in the simulator or at the network layer i.e. the node agent. After investigating over this issue in detail we have determined it is much easier and flexible to implement the attack model at the agent level. Implementing the attack model at the agent level gives much more flexibility in terms of operation that can be performed on the packet. An agent is equipped with function such as send, drop, forward and receive, which essentially are functions to launch an attack.

Given below is the list of actions that are taken by a node agent when it receives a packet.

- Extract the IP header from the packet, determine the source and destination
- Extract the common header from the packet. The common header consists of information about the previous hop and next hop
- Extract protocol specific header from the packet e.g

RREP, Route Request etc.

- If the packet already has been seen or has information older than it currently has, then discard the packet by dropping.
- If the packet has latest information then forward it to the next hop in the packet, it has a route to the next hop.
- If the destination in the packet is the node itself then, generate a reply packet and then send it to the prev hop in the packet header.

The functionality of the node assumes behavior of an uncompromised node; however the scenario becomes totally different when dealing with compromised or malicious nodes. The information that is available by looking at the packet header is sufficient to launch any kind of attack that has been mentioned in the classification. A malicious node can look at the IP header of a packet and determine nodes to which most number of packets is sent. This information could be sufficient to launch a DoS attack on a vital node of the network. The malicious node can launch a gray hole or black hole attack by determining the prev hop and next hop that are listed in the packet header. After learning the topology the malicious node can also fabricate packets containing false information and hence causing disruption in routing.

IV. SIMULATION ENVIRONMENT OF THE ATTACK ANALYSIS

To evaluate the malicious behaviour of the attacks we used the software of ns2. The parameters of our simulation are given in the Table 1.

To study the attacks we focus on parameters quoted below. These parameters are chosen because in Selfish as well as in blackhole the number of sent packets is lower than the number of received packets. For Overflow the energy consumption differs because each received packet corresponds to a loss of energy. The parameters are: a) The number of packets sent; b) the number of packets received; c) The number of packets lost; d) The consumption of energy.

The rate of lost packets is equal to the number of lost packets divided by the number of sent packets. The output is number of received packets divided by the number of sent packets in the application layer.

Parameter	Value
Simulator	NS-2 (ver 2.29.3)
Simulation Time	500 sec
Number of Mobile Nodes	20
Transmission Range	250 m
Topology	1000 m X 1000 m
Routing Protocol	DSR
Maximum Bandwidth	1 Mbps
Traffic	CBR (UDP)
Maximum Speed	5 m/s
No. of Malicious node	1 to 10
Packet Size	512
Sending – Receiving Energy	(0.3) – (0.5) J

Table 1: Simulation Parameter

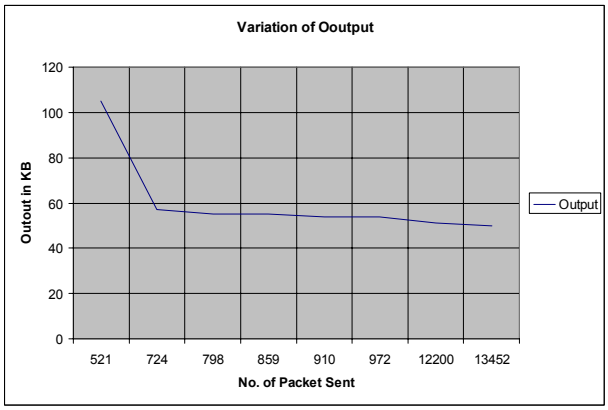

Fig 2: Output Variation

Figure 2 illustrates the change of the output according to the number of packets sent in time. We noted that the output is equal to 105 bit/Sec when the number of received packets is equal to 521 and suddenly the output falls and reaches the 56 bit/Sec, that finds its explanation in the fact that the goal of the attacker is to saturate the network thus making the bandwidth no available from where reduction in the output.

The figure 3 shows the effect to the packet delivery ratio (PDR) measured for the DSR protocol when the node mobility is increased. The result shows both the cases, with the black hole attack and without the black hole attack. It is measured that the packet delivery ratio dramatically decreases when there is a malicious node in the network. For example, the packet delivery ratio is 100% when there is no effect of Black hole attack and when the node is moving at the speed 10 m/s. but due to effect of the Black hole attack the packet delivery ratio decreases to 82%, because some of the packets are dropped by the black hole node.

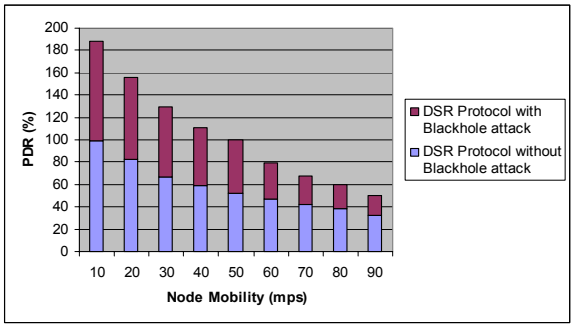

Fig 3: Impact of Black hole attack on PDR

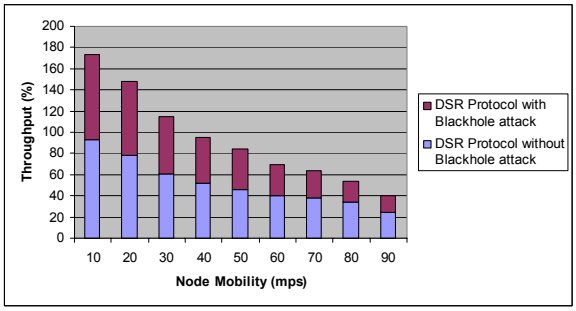

Fig 4: Impact of Black hole attack on Network Throughput

It is observed from the figure 4 that, the impact of the Black hole attack to the Networks throughput. The throughput of the network also decreases due to black hole effect as compared to without the effect of black hole attack. We vary the speed of the node and take the result to the different node speed.

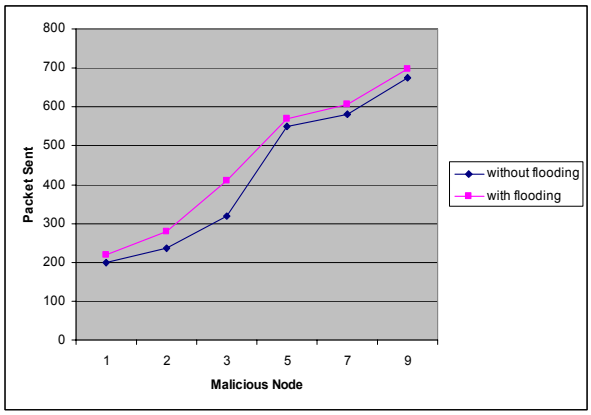

Fig 5: Data Analysis of RREQ Packet Sent

In the above figure we compare the performance of original DSR protocol in presence of malicious node and the performance of proposed technique in presence of malicious node. To evaluate the performance of the system, we used total number of RREQ sent and RREQ received in the network as a performance matrix.

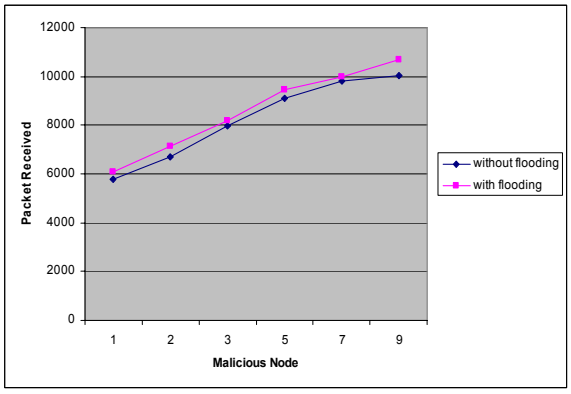

Fig 6: Data Analysis of RREQ Packet Received

The figure 6 shows the graph of total RREQ sent/receives versus malicious node with mobility speed 5 m/s and pause time zero (0). It is clear from the graph that total number of RREQ packet in the network increases with malicious node because malicious node floods the RREQ packet in the network.

V. CONCLUSION AND FUTURE WORK

In this paper, the issue of different attack and its affect on the DSR-based routing protocol has been discussed. We have make a simulation of certain attacks like blackhole, flooding. To resulting from our work we had specificities of the ad hoc mobile networks, the problems of security of routing protocols in these networks. Our preliminary results show that the impact of most types of attacks increases if additional attacking nodes are present. However, particular attack types (e.g. flooding) already achieve (more or less) their highest level of effectiveness when a single attacker is present.

We plan to extend our work by comparing and analyzing other routing attack viz, wormhole attack, selfish attack etc for some of the very popular on-demand and even secure routing protocols and compare them and also implementing and evaluating our proposed solution mechanism for the same.

ACKNOWLEDGMENT

We would like to express our sincere thanks to Prof. K Hemachandran, HOD, Dept. of Computer Science, Assam University, Silchar for his continued support and guidance towards the concept. His continuous feedback has always been the strongest motivation behind this work.

REFERENCE

[1] Wiley John, Security for Wireless Ad Hoc Networks. Ey- rolles 2007, pages 247.

[2] Curtmola Reza, Security of Routing Protocols in Ad Hoc Wireless Networks. 600.647 - Advanced Topics in Wireless Networks, February 2007, pages 26.

[3] A.Rajaram, Dr. S. Palaniswami, The Trust-Based MAC-Layer Security Protocol for Mobile Ad hoc Networks.. (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 02, 2010, 400-408. Anna University Coimbatore, India, March 2010, pages 9.

[4] Xue Xiaoyun. Security mechanisms for ad hoc routing protocols. Com- puter Science and Network Department, ENST, thesis September 2006, pages 234.

[5] Ramaswamy Sanjay, Fu Huirong, Sreekantaradhya Manohar, Dixon John and Nygard Kendall: Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks, Department of Computer Science, IACC 258 North Dakota State University, Fargo, ND 58105, March 2003, pages 7.

[6] Hesiri Weerasinghe and Huirong Fu, Preventing

Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation; International Journal of Software Engineering and Its Application Vol. 2, No. 3. Oakland University Rochester MI 48309 USA, June 2008, page 16.

[7] Hu Yih-Chun, Perrig Adrian, Johnson David B.: Packet Leashes, A Defense against Wormhole Attacks in Wireless Networks, INFOCOM 2003, pages 11

[8] Emmanouil A. Panaousis, Levon Nazaryan, Christos Politis, Securing AODV Against Wormhole Attacks in Emergency MANET Multimedia Communications, Wireless Multimedia and Networking (WMN) Research Group Kingston University London. Jully 2009, pages 7.

[9] Debdutta Barman Roy, Rituparna Chaki, Nabendu Chaki, A new cluster-based wormhole intrusion detection algorithm for mobile ad-hoc networks. International Journal of Network Security and Its Applications (IJNSA), Vol 1, No 1, West Bengal University of Technology, Kolkata 700064, India. April 2009, pages 9.

[10] Michiardi Pietro and Molva Refik, CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks. European Wireless Conference, Nonvember 2003, pages 15.

[11] Buttyan Levente and Hubaux Jean-Pierre, Nuglets: a virtual Currency to Stimule Cooperation in Self-Organized Mobile Ad Hoc Networks. Institute for Computer Communications and Applications Department of Communication Systems Swiss Federal Institute of Technology Lausanne, 18 January 2001, pages 15.

[12] Getsy S Sara, Neelavathy Pari. S, Sridharan. D, Energy Efficient Ad Hoc On Demand Multipath Distance Vector Routing Protocol, International Journal of Recent Trends in Engineering, Vol 2, No. 3. Department of Electronics and Communication Engineering, CEG Campus, Anna University Chennai, India November 2009, pages 3.

[13] Mads Dar Kristensen and Niels Olof Bouvin, Energy Efficient MANET Routing Using a Combination of Span and BECA/AFECA. Journal of Networks, Vol. 3, No. 3, New York, USA, March 2008, pages 8.

[14] S Arvind, Dr. T. Adilakshmi, Power Aware Routing for Mobile Agent in Ad-Hoc Networks. Journal of Theoretical and Applied Information Technology. Department of Computer Science Engineering, Vasavi College of Engineering, Hyderabad-500031. May 2009, pages 7

[15] Idoudi Hanen, Akkari Wafa, Belghith Abdelfatteh, Molnar Miklos, Alternance synchrone pour la conservation d'energie dans les rseaux mobiles ad hoc. IRISA, Centre Universitaire de Beaulieu-35042 Rennes CEDEX-France, Novembre 2006, pages 46.

[16] Choi Heesook, McDaniel Patrick, La Porta Thomas F, Privacy Preserv- ing Communication in MANETs. Department of Computer Science and Engineering the Pennsylvania State University, March 2007, pages 10.

[17] Yi Ping, Dai Zhoulin, Zhang Shiyong, Zhong Yiping, A New Routing Attack in Mobile Ad Hoc Network. Department of Computing and Information Technology, Fudan University, Shanghai, 200433, China, June 2005, pages 12.

[18] Revathi Venkataraman, M. Pushpalatha, and T. Rama Rao, Performance Analysis of Flooding Attack Prevention Algorithm in MANETs. World Academy of Science, Engineering and Technology 56, September 2009, pages 4.

[19] Aad Imad, Hubaux Jean-Pierre, Knightly Edward W, Impact of Denial of Service Attacks on Ad Hoc Networks. DoCoMo Euro-Labs EPFL Rice University Munich, Germany Lausanne, Switzerland Houston, TX, July 2007, pages 14.

[20] Network Simulator Official Site for Package Distribution, web reference, http://www.isi.edu/nsnam/ns.

Authors Biography

Bipul Syam Purkayastha received his B.Sc. degree from NEHU, Shillong, in 1982. He received his M.Sc., M. Phil. And Ph.D. degrees from NEHU, Shillong in 1985, 1987 and 1997 respectively. He is currently working as a Professor in the Department of Computer Science, Assam University, Silchar. His research interests include soft computing, combinatorial optimization and Computer Network. He has published lots of paper in National & International Journal.

Rajib Das received his MCA degree from IGNOU, New Delhi, M.Phil degree from Annamalai University, Chidambaram, T.N. and pursuing Ph.D from Assam University, Silchar in the field of Ad Hoc Network. His research interests are Mobile Computing and Image Processing. He is a member of IEEE Computer Society, ACM and IACSIT.