International Journal of Engineering & Technology
CENTRE OF PROFESSIONAL RESEARCH PUBLICATIONS
ISSN 2049-3444

International Journal of Engineering and Technology Volume 2 No. 8, August, 2012

CARD (Continuous and Random Dropping) based DRDOS Attack Detection and Prevention Techniques in MANET

Rupa Rani, A.K. Vatsa
Shobhit University, Meerut, UP, India

ABSTRACT

The DDOS is "distributed-denial-of-service" meaning many "zombies or daemons" computers performing a DOS (Denial of Service) attack on one computer, usually directed by one "master". In MANETs, DOS attacks not only consume the scarce system resources, such as bandwidth, battery energy, or CPU cycles, but also isolate legitimate users from a network. The DOS attacks may impact the network connectivity seriously and may further undermine the networking functions. In DRDOS attacks, the victim is bombarded by reflected response packets from legitimate communicating nodes, and thus it is difficult to distinguish attack packets from legitimate packets. In this paper, we propose a defense mechanism based on CARD based DRDOS attack detection and prevention techniques in MANET. The proposed rate limiting scheme will penalize the different attackers based on their rate limits and server load. The victim end defense system decrease the rate limit exponentially & increase it linearly based on the attack traffic rate. Finally this approach is discussed in three phases as detection, control and prevention which is explained in CARD detection architecture.

Keywords: *MANET(Mobile ad-hoc Network), Distributed denial of service (DDOS) attack, Rate Limiting, Packet Dropping, Flooding, CARD(continuous and random dropping).*

1. INTRODUCTION

Now-a-days, mobile ad-hoc network (MANET)[1] is one of the recent active fields and has received marvelous attention because of their self-configuration & self-maintenance capabilities. While early research effort assumed a friendly and cooperative environment and focused on problems such as wireless channel access in multi-hop routing, security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment. Recently because of rising popularity of multimedia applications and potential commercial usage of MANET [2], QoS (Quality of service) support in MANETs has become an unavoidable task. A lot of work has been done in supporting QoS [3] in the internet, but unfortunately none of them can be directly used in MANETs because of the bandwidth constraints and dynamic network topology of MANETs.

The main aim of a DOS attack [4] is the interruption of services by attempting to limit access to a machine or service instead of subverting the service itself. This kind of attack aims at rendering a network incapable of providing normal service by targeting either the networks bandwidth or its connectivity. These attacks achieve their goal by sending at a victim a stream of packets that swamps his network or processing capacity denying access to his regular clients. In the not so distant past, there have been some large - scale attacks targeting high profile Internet sites [5].

A Distributed Denial of Service (DDOS) attack uses many computers to launch a coordinated DOS attack against one or more targets. Using client/server technology, the perpetrator is able to multiply the effectiveness of the Denial of Service significantly by harnessing the resources of multiple unwitting accomplice computers which serve as attack platforms. Typically a DDOS master program is installed on one computer using a stolen account. The master program, at a designated time, then communicates to any number of "agent" programs, installed on computers anywhere on the internet. The agents, when they receive the command, initiate the attack. Using client/server technology, the master program can initiate hundreds or even thousands of agent programs within seconds. Here Master and Agents are password protected.

When a victim detects a DOS attack, a widely used solution is tracing the DOS attack back towards its origin, and then stopping the attacker at the source. As attackers usually use IP spoofing to conceal their real location, several IP traceback mechanisms have been proposed for the Internet, such as link testing [6], ingress filtering [7], probabilistic packet marking (PPM) [8], and ICMP traceback (ITrace) [9], to trace the true sources of attackers. These traceback approaches cannot be directly applied to MANET due to the following reasons that are related to two aspects: efficiency and effectivity. (1) Nodes in MANETs can move arbitrarily, which makes attack paths change frequently. Therefore, additional constraints are placed on tracing approaches for locating the attack sources in time. Therefore, the traceback approaches used in MANETS should be more effective than that in the Internet (2) Traceback approaches in the Internet always consume a lot of bandwidth,

computational resources, and battery power. However, in MANETs, nodes are typically devices with limited bandwidth, computational resources, and battery power. These limitations require that the traceback approaches in MANETs should be more efficient than that in the Internet.

In the Reputation scheme [10], the reputation of the nodes is assessed based on their past history of relaying packets, and are used by their neighbors to ensure that the packet will be relayed by the node. Instead of choosing the shortest path to the destination, the source node chooses a path whose next hop node has the highest reputation. As a result, the good nodes (nodes with higher reputations) become overloaded. Once the load on the good nodes is more than what the resources can manage , they start dropping packets and start loosing reputation. As a result, their incoming traffic is reduced to a level at which they can forward all the packets they receive for relaying. Also the number of route discoveries is more with increase in the average hop length.

A scheme [11] have extended the IDS model described in [12] to enhance the security in AODV (Ad-hoc on demand Distance Vector) routing protocol. Approach [13] proposes to monitor packet forwarding on top of source routing protocols like DSR but it has the limitations of relying on overhearing packet transmissions of neighboring nodes for detecting anomalies in packet forwarding. Reference [14] follows the concept of [15] but works with ADOV. Bal Krishnan [16] has proposed a way to detect packet dropping in ad-hoc networks. Trust features are used in [17, 18, 19, 20, 21, 22] existing trust-based routing schemes for MANET.

In this paper, we propose a simple and robust method to detect Distributed Reflective Denial of Service (DRDOS) attacks. In DRDOS attacks, the victim is bombarded by reflected response packets from legitimate communicating nodes, and thus it is difficult to distinguish attack packets from legitimate packets. We focus on a proposed defense mechanism for dropping based DDOS attack based on concept of rate limiting the attack traffic. The proposed rate limiting scheme will penalize the different attackers based on their rate limits and server load. The rate limit value for each attacker is calculated dynamically. The victim end defense system decrease the rate limit exponentially & increase it linearly based on the attack traffic rate. Finally our approach is displayed in three phases as detection, control and prevention which is explained in "continuous and random dropping detection architecture".

There are two major motivations for attacker to use randomly spoofed addresses. Firstly, To hide identity of Zombies; reduce risk of being traced back via Zombies. Secondly, Is to make it hard or impossible to filter this type of traffic without disturbing legitimate traffic. Packet filtering can be used to trace back the attacker [23, 24]. Compared to wired networks the rate control becomes complex in MANETs since the available bandwidth of the wireless channel is variable and unpredictable. The best effort traffic produces essential bandwidth required for real-time traffic and also it consumes the bandwidth which is not currently utilized by the real-time traffic at any particular moment. To avoid these, rate control mechanism is required. To maintain the total rate of all best effort and real-time traffic transported over each load shared media channel below an exacting threshold rate, unnecessary delays can be minimized [25].

The previous work [26] have proposed to design QoS architecture for Bandwidth Management and Rate Control in MANETs. But the Rate control and resource provisioning were not proper and effective. Therefore we have proposed a CARD based DRDOS attack detection and prevention techniques in MANET for smooth and high data rate communication over MANET.

This paper is organized into sections. The Section- 1, describe the introduction. Section-2, mentions background i.e. about related work studied together with proposed research for the quality of service and management of rate limiting under DRDOS attack. Section -3, explains the proposed work for CARD based DRDOS attack detection and prevention techniques in MANET. Section - 4 gives concluding remark under heads of Conclusion and finally, Section - 5 describes the future directions. All references used in this paper is mention in Section – 6 lead by Reference.

2. BACKGROUND

MANET, the nodes are required to watch their neighbors for misbehavior and this not only necessitates promiscuous modes of operation but also overloads the nodes. Watchdog and path rater [27] to detect and isolate the misbehaving nodes. In this approach; a node forwarding a packet checks if the next hop also forwards it. If not, a failure count is incremented and the upstream node is rated to be malicious if the count exceeds a certain threshold. The path rater module then utilizes this knowledge to avoid it in path selection. It improves the throughput of the network in the presence of malicious nodes.

A router-based approach to detect the stealthy law rate DOS and RoQ (Reduction of Quality) attacks [28] which uses IP address spoofing or botnets. This work addresses the IP address spoofing and botnet problem in the context of the law rate DOS and RoQ attacks, and proposes an effective and realizable solution to defend against RoQ attacks.

A novel defense scheme against RoQ[29] have explored the energy distributions of Internet traffic flows in frequency domain. Normal TCP traffic flows present some form of periodicity because of TCP protocol behavior. Their result reveal that normal TCP flows can be segregated from malicious flows using some energy distribution properties. They discover the spectral shifting of attack flows from that of normal flows. Combining flow-level spectral analysis with sequential hypothesis testing, they proposed a novel defense scheme against shrew DDOS or RoQ attacks.

This approach [30] suggest that despite the fact that advantageous for individual nodes not to cooperate. They propose a protocol, called CONFIDANT, which aims at

detecting and isolating misbehaving nodes, thus making misbehavior unattractive. Here misbehaving nodes are excluded from forwarding routes. It includes a trust manager to evaluate the level of trust of alert reports. But it is not clear how fast the trust level can be adjusted for compromised node especially if it has a high trust level initially [31].

Trust Evaluation method [32] provides an effective security mechanism based on data protection and secure routing. But it relies on global information and hence the reaction time is more. It would be preferable to reduce the reaction time.

Multipath Routing Single path transmission (MARS) scheme [33] to mitigate adverse effects of misbehavior combines multipath routing and single path data transmission with end-to-end feedback mechanism to provide more comprehensive protection against misbehavior from individual or cooperating misbehaving nodes.

The new mechanism called Packet Conservation Monitoring Algorithm (PCMA) [34] to detect selfish nodes in the presence of partial dropping when the selfish node does not drop all packets but sends some of them and drops other in MANET.

Much of research on security policies focuses on policy representation and evaluation [35, 36] or building security mechanisms based on specific policies [37] without addressing policy enforcement.

3. PROPOSED WORK

The proposed works are discussed as follows in Section 3.1 and Section 3.2.

3.1 Architecture of DRDOS attacks and it's Working Principles

The proposed architecture illustrated in figure 3.1. MANET is network where real attacker sends packets to master. Attacker can instruct all its **"Zombies or Daemons"** to send bogus data to one particular destination and causes problem with useless traffic. Attack daemon agents (agent program) are usually deployed in host computers. These affect both victim and host computers. The task of deploying these attack daemons requires the attacker to gain access and infiltrate the host computer. Sophisticated tools to gain root access to other people's machines are freely available on the internet. A **MAL (Manet Attack Launcher)** is an indirect attack in that intermediary node known as attack launchers.

In MANET, there may be three types of spoofing such as TTL (time to live) field spoofing, TOS (type of service) field spoofing and source address (SA) spoofing but in this approach, attacker uses the source address spoofing and TTL field spoofing. Spoofing a packet's TTL field means that the attacker will set the packet's initial TTL to a value different than the default TTL value used by the operating system of the attack machine. Most modern operating systems use only a few selected initial TTL values, 30, 32, 60, 64, 128, and 255. [37]. Master send packets with spoofed address of victim as a source address without realizing that packets are actually address-spoofed, then the MAL return response packets to victim. Here we consider two term packet dropping and threshold rate.

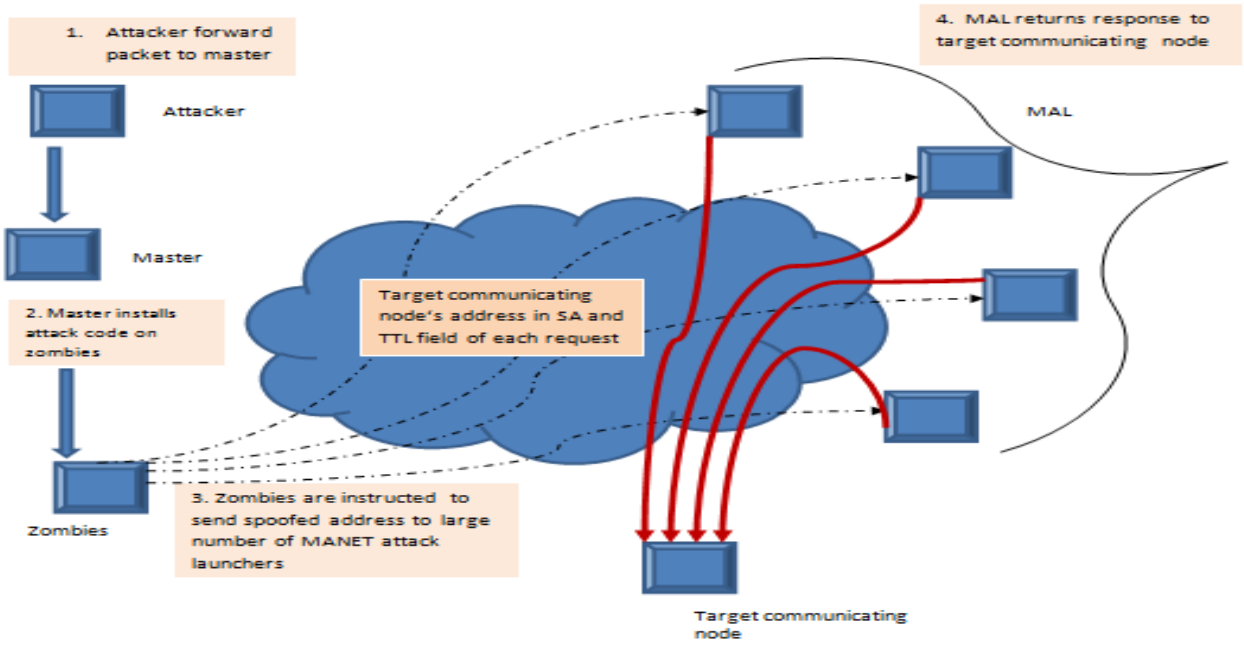

Figure 3.1: DRDOS (Distributed Reflector Denial of Service) based Scenario

Continuous and Random dropping(CARD) Detection is an advanced queue method, that drops packets from the queue with a certain probability, which increases with the exponential moving average queue length .So queue is not filled by only one flow. Packets drop requires several configuration Parameters such as Buffer capacity, Lower threshold (min), Upper threshold (max) and Average queue length. No packets are discarded if average is smaller than min threshold and if average is between lower and upper thresholds by dropping packet with a drop probability that is linearly proportional to the exponential moving average queue size. These probabilistic drops are called close drops. If the exponential moving average queues size is larger than min. Each coming packet is compared with a randomly selected packet, called the drop candidate packet. If both packets flow Ids are same then both dropped else choose packet randomly.

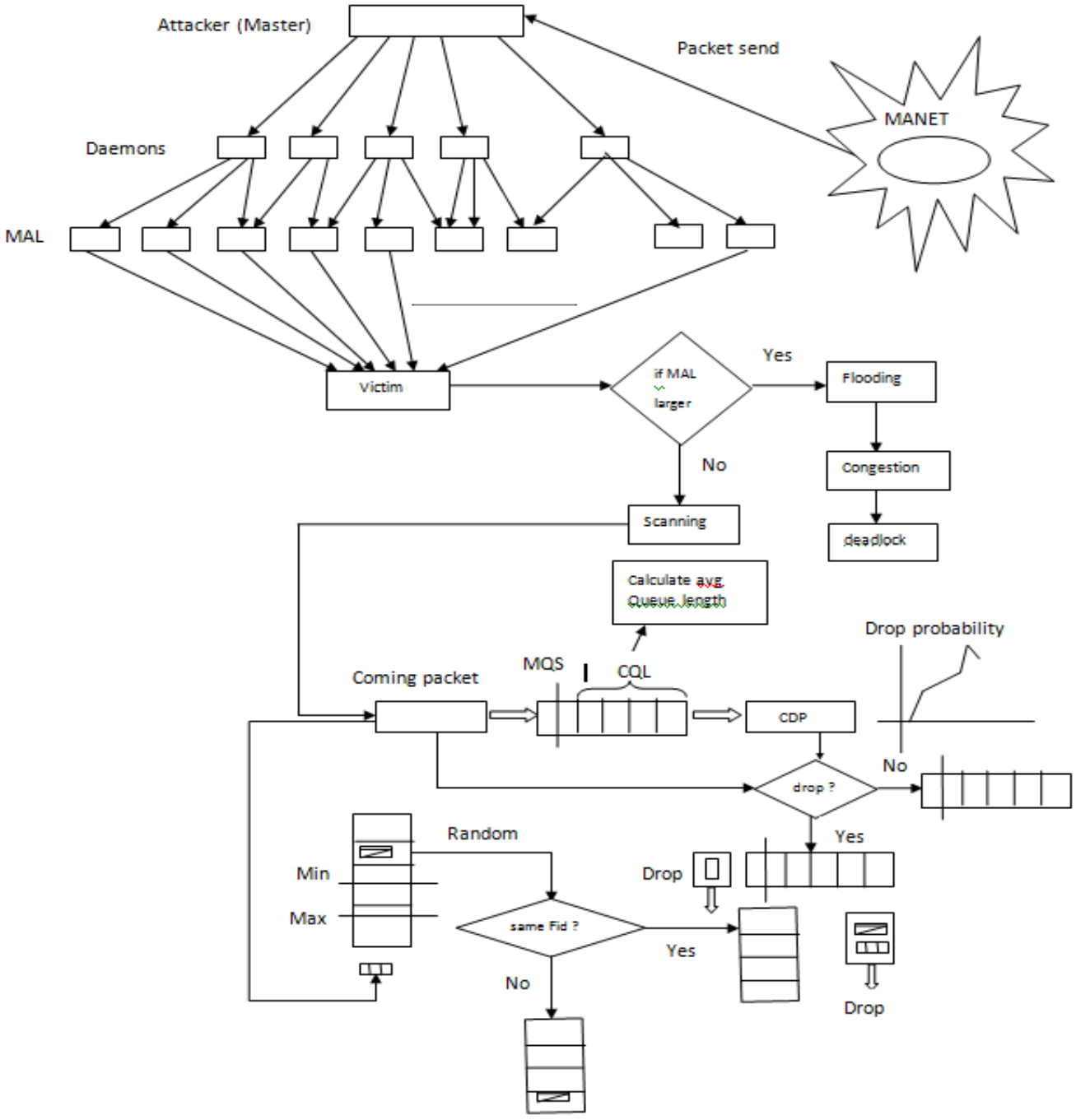

Figure 3.2: Architecture of Continuous and Random Dropping (CARD) Detection

Where MQS= maximum queue size, CQL= current queue length, CDP= calculate drop probability, Fid=flow id, MAL= MANET attack launcher

3.2 Mechanism of CARD based DRDOS Attack Detection and Prevention Techniques

The proposed mechanism is discussed as follows in three phases.

Phase -I: Rate and Bandwidth based DRDOS attack mechanism

RBDRDOS_attack ( )
{
Step1: Real attacker forward packets to Cluster Head (CH) in MANET.
Step2: forwarded message format is shown as below:

Source address	Destination address	Source port	Destination port	Flow size	Packet count	TTL value	TOS field

Step3: once a node is cracked, it is turned into a "Zombies or Daemons" under the control of one master.
Step4: attacker instruct all its Daemons to send a bogus data to one particular Destination via MANET attack launchers (MAL).
Step5: now MAL return response to victim with spoofed address (not realize actual address)
Step6: In a MAL based DDOS attack, agents must put the victim's address in the source address field. The spoofed addresses can be addresses of either existing or non-existing communicating nodes.
Step7: If(No. of MAL Node >> Victim's Node or Communicating Node)
then flooding occurs & network become Congestion and deadlock occurs.
Else if (SA==DA && SP==DP &&TTL<= default number)
then route is valid
else Evaluate route via continuous and random dropping
(CARD) scheme i.e. Scanned procedure
Else if (CARD is SUCCESSFUL or True)
then perform rate limiting
Step8: finally , MAL return response to victim and it maintain a table that contain malicious nodes and legitimate nodes list and is used for detection phase.
}

Phase II: Detection of RBDRDOS

RBDRDOS_detection ( )
{
Step1: Let us consider two type of packets i.e. coming packet and random packet for detection.
Step2: For coming packets, calculate current queue length and average queue length and then check drop probability.
Step3: For random packets, check flow ID as in algorithm.
Step4: If packet dropping does not occur
Then perform rate limiting by setting the threshold value
else enqueue remaining packets
}

Phase III: Prevention of RBDRDOS (i.e. CARD scheme)

RBDRDOS_prevention ( )
{
Step1: Check queue length.
Step2: If (Qlength <min)
A new packet can enter the queue.
Step3: If (Min < Qlength < Max)
Check (Rpacket, Cpacket) same ID?
Step4: If (Yes)
Drop (Rpacket);
Drop (cpackets);
Step5: If (no)
Enqueue (Cpacket);
Step6: calculate threshold value of enqueue coming packets
Step7: To keep server load within specified load limit[Ls, Us]
whenever rate limiting is in effect
Step8: If server load > Us (specified upper value).
Then Traffic decrease
Step9: Calculate traffic rate decrease factor.
Step10:If server load < Ls (lower load limit)
Then Calculate traffic rate increase factor
Step11:For each individual router, Calculate a separate rate limit
value by considering current traffic at victim end & traffic
rate at source end.
Step12:If (Max < Qlength < Qcapacity)
Do (check process) three times

```
Step13:if  (not all random packets have same Id as the coming
        packet)
            Enqueue (Cpackets)
Step14:if (Qlength+1 > Qcapacity)
            Do (check process) three times
            Drop(Cpackets)
}
```

In above mechanism, SA= source address, DA= destination address, SP= source port, DP= destination port, Qlength= queue length, Rpacket= random packet, Cpacket= coming packet and Qcapacity= queue capacity.

4. CONCLUSION

MANET [38, 39, 40, 41] has no clear line of defense, thus, it is accessible to both legitimate network users and malicious nodes. In this paper, the proposed work developed a CARD (continuous and random dropping) detection mechanism which reduces deficiency of the reduction of Quality (RoQ) to the mobile nodes. The proposed rate limiting scheme will penalize the different attackers based on their rate limits and server load. The victim end defense system decrease the rate limit exponentially and increase it linearly based on the attack traffic rate. The rate control and resource provisioning were not proper and effective in previous papers. Therefore the proposed a CARD based DRDOS attack detection and prevention techniques [42, 43] in MANET for smooth and high data rate communication over MANET. If the nodes packet dropping value falls below a threshold value, the corresponding to the intermediate node is marked as malicious node which is caused by means of DRDOS attack. The value of short-lived flows and observed the sudden increase in the traffic load in a short time. When the total traffic load exceeds the threshold, an attack is detected. Finally this approach is discussed in three phases as detection, control and prevention which is explained in CARD detection architecture.

5. FUTURE SCOPE

The proposed architecture and mechanism for CARD (continuous and random dropping) based DRDOS attack detection and prevention techniques for smooth and high data rate communication over MANET. But when communicating node start scanning then that may be of two types i.e. port scanning & network scanning, we consider port scanning if spoofed addressed packets and actual addressed packets are coming at same port no. then conflict occur. Node can solve these problems in future and can differentiate both type of packets based on flow ID & packet ID together.

REFERENCES

[1] S.B. Anieth Kumar, S. Allwin Devraj, J. Arun Kumar, ”Efficient Detection of DOS attack in MANET”, International Journal of Advance Research in Computer Science and Software Engineering, Volume 2, Issue 5, pp. 470-476, May 2012.

[2] S.Venkatasubramanian, N.P.Gopalan, “A Flow Monitoring based Distributed Defense Technique for Reduction of Quality Attacks in MANET” International Journal of Computer Applications, Volume 21, Issue 1, pp. 0975 – 8887, May 2011.

[3] Raman Singh, Amandeep Verma, “A Dynamic Bandwidth Assignment Approach Under DDoS Flood Attack”, Journal Of Advances In Information Technology, Volume 3, Issue 2, pp. 120-129 May 2012.

[4] Mr. Nallamala Sri Hari, Dr. N. Srinivas Rao, Dr. N. Satyanarayana, “A Novel Routing attack In Mobile Ad Hoc Networks”, Indian Journal Of Computer Science And Engineering, Volume 1, Issue 4, pp. 382-391, 2010.

[5] Douligeris and A. Mitrokotsa, “DOS attacks and defense mechanisms: classification and state-of-the-art”, The International Journal of Computer and Telecommunications Networking, Volume 44, Issue 5, pp. 643-666, April 2004.

[6] R. Stone, “CenterTrack: an IP overlay network for tracking DOS floods”, 9th conference on USENIX Security Symposium, Volume 9, Issue 15, pp. 199–212, August 2000.

[7] P. Ferguson and D. Senie, “Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing”, RFC, Jan 1998.

[8] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, “Practical network support for IP traceback,” ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, Volume 30, Issue 4, pp 295–306, October 2000.

[9] S. Bellovin, M. Leech, and T. Taylor, “ICMP Traceback Messages,” IETF Internet Draft, Version 4, Volume 9, Issue 1, February 2003.

[10] Prashant Dewan, Partha Dasgupta,Amiya Bhattacharya “Reputation in Adhoc network to counter malicious nodes Proceeding of Parallel and distributed system”, 10th International Conference on the Parallel and Distributed Systems, pp 665 – 672, July 2004.

[11] Bhargava, S.; Agrawal, D.P. , "Security enhancements in AODV protocol for wireless ad hoc networks ," Vehicular Technology Conference, Volume 4, pp.2143-2147, 2001

[12] Zhanfei Ma; Xuefeng Zheng; , "Cooperation modeling for intrusion detection system based on Multi-SoftMan," 3rd International Conference on Anti-counterfeiting, Security,

and Identification in Communication, pp.493-496, Aug. 2009.

[13] Chengqi Song, Qian Zang,"Suppressing selfish behavior in adhoc networks with one more hop" 5th International ICST Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, Volume 14, Issue 2, pp. 178-187, April 2009.

[14] Jiejun Kong; Petros, Z.; Haiyun Luo; Songwu Lu; Lixia Zhang; , "Providing robust and ubiquitous security support for mobile ad-hoc networks," Ninth International Conference, pp. 251-260, Nov. 2001.

[15] Balakrishnan, K.; Jing Deng; Varshney, V.K.; , "TWOACK: preventing selfishness in mobile ad hoc networks," Wireless Communications and Networking Conference, Volume4, Issue , pp. 2137- 2142, March 2005.

[16] Husain Shahnawaz, Gupta S.C., "Friend Features Extraction to Design Detection Engine for Intrusion Detection System in Mobile Adhoc Network", International Journal of Computer Science & Information Technology, Volume 2, Issue 4, pp 1569-1573, 2011.

[17] Razak, S.A., Furnell, S., Clarke, N. Brooke, P. Mehrotra, Sharad.Zeng, Daniel, Chen, Hsinchun. Thuraisingham, Bhavani. "A Two-Tier Intrusion Detection System for Mobile Ad Hoc Networks—A Friend Approach", Lecture Notes In Computer Science, volume 3975, pp. 590-595, 2006.

[18] Abusalah, L.; Khokhar, A.; Guizani, M.; , "NIS01-4: Trust Aware Routing in Mobile Ad Hoc Networks," Global Telecommunications Conference, pp.1-5, 2006.

[19] Pirzada, A. A and McDonald, C. "Establishing Trust in Pure Ad-Hoc Networks" 27th Australasian Computer Science Conference, Volume 26, pp. 47-54, 2004.

[20] Yan, Z., Zhang, P. and Virtanen, T. "Trust Evaluation Based Security Solution in Ad Hoc Networks", 7th Nordic Workshop on Secure IT Systems, pp. 1-14, 2003.

[21] Eschenauer, L. "On Trust Establishment in Mobile Ad-Hoc Networks," Master's Thesis, Department of Electrical and Computer Engineering, University of Maryland, 2002.

[22] Kui Ren, Tieyan Li, Zhiguo Wan, Feng Bao, Robert H. Deng, Kwangjo Kim, "Highly reliable trust establishment scheme in ad hoc networks", The International Journal of Computer and Telecommunications Networking, Volume 45 Issue 6, Pages 687 – 699, August 2004

[23] Kumar Sanjeev, " Smurf Based Distributed Denial of Service Attack Amplification in Internet", Second International Conference on Internet Monitoring and Protection IEEE pp. 25-29, July 2007.

[24] Gahng-Seop Ahn, Andrew T. Campbell, Andras Veres and Li-Hsiang Sun "Supporting Service Differentiation for Real-Time and Best-Effort Traffic in Stateless Wireless Ad Hoc Networks (SWAN)", IEEE Transactions on Mobile Computing, Volume 1, Issue 3, July-September 2002

[25] S.Venkatasubramanian and N.P.Gopalan "A QoS Architecture for Resource Provisioning and Rate Control in Mobile Adhoc Networks" International Journal of Ad hoc, Sensor & Ubiquitous Computing, Volume 1, Issue 3, pp 106- 120, September 2010.

[26] S.Marti,T.J.Giulli,K.Lai and M.Baker "mitigating routing misbehavior in mobile adhoc network Mobile computing and networking", ACM, Volume 4, pp. 255- 265, 2000.

[27] Zhu Lina, and Zhu Dongzhao "A Router based Technique to Detect and Defend against Law-rate Denial of Service" International Symposium on Web Information Systems and Applications, pp. 257-260, May 2009.

[28] Yu Chen and Kai Hwang "TCP flow Analysis fow Defence against Shew DDOS Attacks" IEEE International Conference on Communications, June 2007.

[29] S. Buchegger and J. Boudec, "Performance Analysis of the Confidant Protocol," Proc. Int'l Symp, Mobile Ad Hoc Networking and Computing, June 2002.

[30] Y.Huang and W.Lee "A cooperative IDS for adhoc network Security of adhoc and sensor networks", International Journal of Computer Applications, pp. 135-145, 2003.

[31] Li Zhao and José G. Delgado-Frias, "MARS: Misbehavior Detection in Ad Hoc Networks", IEEE GLOBECOM, pp. 941-945, 2007.

[32] Zheng Yan and peng Zhang, Teemupekka Virtanen, "Trust Evalution based security solution in Adhoc network", *Volume* 4, Issue 2, pp.36-44, 2000.

[33] Tarag Fahad and Robert Askwith "A Node Misbehaviour Detection Mechanism for Mobile Ad-hoc Networks", 7th Annual Post Graduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting, June 2006.

[34] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management," Proc. IEEE Conf. Privacy and Security, pp. 164-173, 1996.

[35] M. Blaze, J. Feigenbaum, J. Ioannidis, and A.D. Keromytis, "The Keynote Trust-Management System, Version 2," RFC 2704, Sept. 1999.

[36] P. Dinsmore, D. Balenson, M. Heyman, P. Kruus, C. Scace, nd A.Sherman, "Policy-Based Security Management for Large Dynamic Groups: An Overview of the dccm Project", Proc. DARPA Information Survivability Conf. and Exposition , pp. 64-73, Jan. 2000.

[37] Haining Wang, Cheng Jin, Kang G. Shin, **"** Defense against spoofed IP traffic using hop-count filtering", IEEE/ACM Transactions on Networking**,** Volume 15, Issue 1, pp. 40 – 53, February 2007.

[38] G.S. Mamatha, Dr.S.C. Sharma, "A Highly Secured Approach against Attacks in MANETS", International Journal of Computer Theory and Engineering, Volume 2, Issue 5, pp. 1793-8201, October 2010.

[39] Prajeet Sharma , Niresh Sharma , Rajdeep Singh, "A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network", International Journal of Computer Applications , Volume 4, Issue 21, pp. 0975 – 8887, March 2012.

[40] Yogesh Chaba, Yudhvir Singh, Preeti Aneja, "Performance Analysis of Disable IP Broadcast Technique for Prevention of Flooding-Based DDoS Attack in MANET", Journal Of Networks, Volume 4, Issue 3, pp. 178-183, May 2009.

[41] Rachana Yogesh patil, Lata Ragha, "A Rate Limiting Mechanism for Defending Against Flooding Based Distributed Denial of Service Attack", World Congress on Information and Communication Technologies, pp. 182 – 186, Dec. 2011.

[42] Husain. Shahnawaz, Gupta S.C., Chand Mukesh, " Denial of Service Attack in AODV & Friend Features Extraction to Design Detection Engine for Intrusion Detection System in Mobile Adhoc Network", International Conference on Computer & Communication Technology, pp. 292-297, 2011.

[43] Nirbhay Ahlawat, Chetan Sharma, "Classification And Prevention Of Distributed Denial Of Service Attacks", International Journal Of Advanced Engineering Sciences And Technologies, Volume 3, Issue 1, pp. 052 – 060, 2011.

AUTHORS PROFILE

Rupa Rani is working as Assistant Professor in IIMT engineering college, Greater Noida (U.P.), INDIA. She obtained her M-Tech (Computer Engineering) from Shobhit University and MCA from IEC-CET (UPTU) Greater Noida (U.P.). She has worked as software engineer in software industry. She has been in teaching from more than one decade. She has been member of several academic and administrative bodies. Her paper is published in international journal. Her area of research includes MANET (Mobile Ad-Hoc network) and Network Security.

Avimanyou Kumar Vatsa is working as Assistant Professor and Coordinator - CSE at Shobhit University, Meerut, (U.P.), INDIA. He obtained his M-Tech (Computer Engineering) with Hons. from Shobhit University and B-Tech(I.T.) from V.B.S. Purvanchal University, Jaunpur (U.P.). He has worked as software engineer in software industry. He has been in teaching from more than one decade. During this short period of time, he has been supervised several dissertation of M.Tech. students. He is on the editorial board and reviewers of several international and national journals in networks and security field. He has been member of several academic and administrative bodies. During his teaching he has been coordinated many Technical fests and National Conferences at Institute and University Level. He has attended several seminars, workshops and conferences at various levels. His many papers are published in various national, international journals and conferences. His area of research includes MANET (Mobile Ad-Hoc network), Network Security, Congestion Control and VOIP-SIP (Voice over IP).