DOI: 10.21917/ijct.2011.0057

RESILIENT SCHEME AGAINST REDUCTION OF QUALITY (ROQ) DISTRIBUTED DENIAL OF SERVICE ATTACK IN MANET

S.A. Arunmozhi[1] and Y. Venkataramani[2]

Department of Electronics and Communication Engineering, Saranathan College of Engineering, Tamil Nadu, India

E-mail: [1]arunmozhisa@saranathan.ac.in and [2]diracads@saranathan.ac.in

Abstract

Defending against denial-of-service attacks (DoS) in a mobile ad hoc network (MANET) is challenging because of the dynamic network topology. Security primitives must be dynamically adjusted to cope with the network. The Reduction-of-Quality (RoQ) Distributed Denial of Service (DDoS) attack is one which throttles the tcp throughput heavily and reduces the quality-of-service (QoS) to end systems gradually rather than refusing the clients from the services completely. Supporting QoS in MANET is a challenging task, particularly in the presence of malicious users. In this paper, we propose a DoS resilient technique that uses a flow table to detect the attackers. The proposed defense mechanism identifies the attackers based on the congestion bit notification and asks the sending node to reduce the sending rate. Once the attackers are identified, all the packets from those nodes will be blocked. The throughput and delay performance of TCP or UDP flows are very sensitive to such RoQ attacks. Through extensive ns2 network simulations, we demonstrate the achievement of high throughput and low delay for a network under the RoQ attack.

Keywords:

MANET, Network Security, Distributed Denial of Service Attack, Reduction of Quality Attack

1. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. The mobile adhoc network does not provide the secure boundary to protect the network from some potentially dangerous network accesses. Lack of secure boundaries makes the mobile ad hoc network susceptible to the attacks.

A DDoS attack is a large-scale, coordinated attack on the availability of services at a victim system or network resource. The DDoS attack is launched by sending an extremely large volume of packets to a target machine through the simultaneous cooperation of a large number of hosts that are distributed throughout the network. The attack traffic consumes the bandwidth resources of the network or the computing resource at the target host, so that legitimate requests will be discarded. The only viable approach is to design defense mechanism that will detect the attack and respond to it by dropping the excess traffic. Generally it is easy to detect the abnormal behavior of attack near the victim. However, it is also often too late to detect the DDoS attack at the victim network. The attack should ideally be stopped as close to the sources as possible to save network resources and to reduce congestion. However, there are no common characteristics of DDoS streams that can be used to detect the attacks near the source. To balance this tradeoff, in this paper we try to detect the DDoS attacks in the intermediate network.

RoQ attacks are a new class of attacks that target adaptation mechanisms employed in current computing systems and networks. Denial of Service relies on overwhelming the victim with load that constantly exceeds its capacity. RoQ attacks, on the other hand, optimize the attack traffic to produce the maximum damage, while keeping a low profile to avoid detection. RoQ attacks are low rate TCP attacks in which the attacker sends periodic attack pulses to overflow a router’s buffer and force the legitimate TCP traffic flow to low throughput. The RoQ attack is shown in Fig.1.

We consider a RoQ attack comprising a burst of M packets (or bytes) transmitted at the rate of δ packets (or bytes) per second over a short period of time τ, where M = δτ. This process is repeated every T units of time. We call M the magnitude of the attack, δ the amplitude of the attack, τ the duration of the attack, and T the period of the attack. Typically τ should be much smaller than T. Thus the RoQ attack traffic, I(t), at time t is given by:

$$I(t)=\begin{cases}\delta, & t \bmod T \le \tau\\ 0 & \text{otherwise}\end{cases}$$

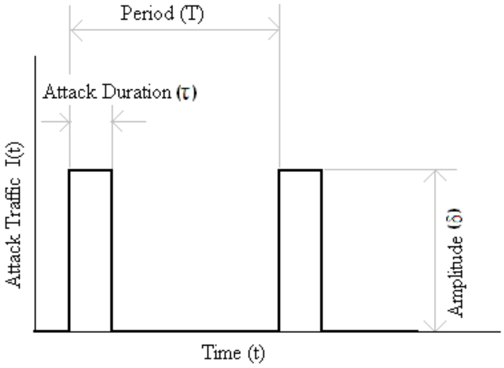

Fig.1. RoQ attack

By synchronizing the attacking period to the Retransmission Time Out (RTO) duration, the attacker can force TCP flows on congested link to frequently enter a time out state and leads to low throughput. Since the RoQ attack provides the freedom of varying attack parameters (δ, τ and T) causing different levels of damage and also it allows the zombies traffic to go unnoticed by having average attack traffic of M/ T that is much lower than the peak rate δ, the low rate attack traffic is more advantageous to an attacker.

2. RELATED WORK

Fei Xing et al. [1] have proposed a model to characterize the evolution of node behaviors. They have analyzed the network survivability in the presence of node misbehaviours and failures. The impact of node behaviours was used as a guideline to design a survivable ad hoc network with the given predefined survivability preference. But in their proposed model, node misbehaviours may improve network performance in terms of end-to-end delays in some scenarios. Chia-Wei Chang et al. [4] proposed protection mechanism for defending against a low rate DDoS attack. Their proposed scheme identifies TCP victims by monitoring their drop rates and preferentially admits those packets from the victims with high drop rates to the output queue. This is to ensure that well-behaved TCP sessions can retain their bandwidth shares**.** The protection scheme can be readily deployable on top of existing router mechanisms. But, their proposed method focuses on protecting victims without explicitly identifying attackers. In the paper on Pulsing RoQ DDoS Attack [6] a detection scheme that monitors three MAC layer signals and a response scheme based on ECN marking are discussed. In this paper, the method of monitoring the sending rates of the nodes is not discussed. Hence identifying the attacking nodes becomes a problem. It may also result in increase of false positives and false negatives. Xiapu Luo et al. [7] have presented the important problem of detecting pulsing denial of service (PDoS) attacks which send a sequence of attack pulses to reduce TCP throughput. Their proposed detection method can detect polymorphic DoS (PMDoS) attacks which may exhibit various traffic patterns that cannot be easily detected.

Arunmozhi et al. [26] have proposed a defense scheme against RoQ attack in MANET using flow monitoring table. In their proposed scheme the flow details are continuously updated which leads to more overhead and increased average end to end delay. Their proposed scheme [26] focuses mainly on traditional flooding based RoQ attacks with zero attack intervals. In this paper, it is proposed to develop a resilient scheme using a flow table which is updated at the RTO period of each packet. This reduces the overhead information and the average end to end delay. This paper focuses on the RoQ attack with different attacking period. The impact of attack period is studied.

3. PROPOSED DEFENSE SCHEME

Security is essential for the widespread of MANET. However, the characteristics of MANET pose both challenges and opportunities in achieving the security goals, such as confidentiality, authentication, integrity, availability, access control, and nonrepudiation. A variety of security mechanisms have been invented to counter DDoS attacks. The conventional approaches such as authentication, access control, encryption, and digital signature provide a defense for wired and wireless networks. Since RoQ attacks are class of DDoS attack which produces the maximum damage in MANET, we have proposed a defense mechanism to detect such attacks.

In this paper, a resilient scheme against the RoQ attack is proposed. According to the resilient scheme, the flow details are maintained in a table called Flow Table (FT). The flow information includes flow ID, source ID, destination ID, the time at which the flow is updated, and packet sending rate. Sending rates are estimated for each flow in the intermediate nodes. The flow details are updated at every node at the estimated RTO of a packet. The updated flow information is sent to the destination along with each flow. When congestion is detected by intermediate node, it starts marking the Explicit Congestion Notification (ECN) in the IP header of the packet. When the destination node gets this congestion notification, it sends the ECN by setting the congestion bit to notify the sender nodes about the congestion. The sender nodes, upon seeing these packets with ECN marking, will then reduce their sending rate. If the sender nodes do not reduce their sending rate, it leads to severe congestion. The updated flow details of destination are used to find the source node which leads the congestion. The previous sending rate of a flow is checked with its current sending rate. When both the rates are same, the corresponding sender of the flow is considered as an attacker. This is because the sending node did not follow the rate control. Once the DDoS attackers are identified, all the packets from those nodes will be discarded. The ID of the attacking node is sent to all the nodes to inform all the nodes to completely remove the attacker from the network.

Every intermediate node is associated with an admission controller. The admission controller at the source node sends a probing request packet towards the destination node to assess the end to end bandwidth availability. This is a control packet that contains a bottleneck bandwidth field. Each intermediate node on the path between the source-destination pair that receives the probing request packet updates the bottleneck bandwidth field in the packet if the bandwidth availability at the node is less than the current value of the field. On receiving the probing request packet, the destination node sends a probing response packet back to the source node with the bottleneck field copied from the received probing request packet. After receiving the response message, the source node admits the traffic flow only if sufficient end to end bandwidth is available.

Each node continuously estimates the locally available bandwidth. The MAC layer signals such as frequency of receiving RTS/CTS packets, frequency of sensing a busy channel and the number of RTS/DATA retransmissions are monitored by all the nodes. If the MAC layer signals exceed the threshold levels, the network is congested. When a node detects congestion or overload conditions, it starts marking the ECN bits in the IP header of the packets. If the destination receives a packet with ECN bits marked, it notifies the source using a regulate message. After receiving a regulate message, the source node initiates reestablishment of its session based on its original bandwidth requirements by sending a probe request packet to the destination. A source node terminates the session if the available end to end bandwidth cannot meet its bandwidth requirements. If the node detecting violations marks the ECN bits of all packets, then all sessions passing through this node are forced to reestablish their connections at the same instance.

ALGORITHM

1. Different flow requests are initiated from different sources to destinations.

2. Each node maintains a flow table which contains sender ID, destination ID, flow ID, flow update time and packet sending rate.
3. Each node updates the flow details from its one hop neighbors at RTO period of each packet.
4. Admission control is adopted by the source node.
5. Based on the admission control mechanism, the traffic flows are transmitted from the source nodes to the destinations.
6. MAC layer signals are checked with the threshold values for the occurrence of congestion.
7. If congestion occurs, ECN is marked and the source node is informed to apply the rate control mechanism.
8. From the updated flow details of the one hop neighbor, the source nodes are checked whether they follow the rate control or not.
9. The Normal Nodes follow the rate control whereas the node which does not follow the rate control is identified as the Attacker Node.
10. The ID of the Attacker Node is sent as the control message to all the nodes in the network for completely blocking the node.

4. SIMULATION

The network simulator ns2 is used to simulate the experiment. In simulation, the channel capacity of mobile nodes is set to the value of 2 Mbps. This section includes simulation parameters, simulation environment and simulation results.

4.1 SIMULATION PARAMETERS

The parameter settings for the simulations are: the radio propagation mode is TwoRay Ground, antenna type is omni antenna, interface queue length is 50 (packets), queue management scheme is Drop Tail, height of antenna is 1.5m, signal interference or sensing distance is 550m. Other simulation parameters are listed in Table.1.

Table.1. Simulation Parameters

No. of Nodes	100
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	300 sec
Traffic Source	CBR
Packet Size	512
Mobility Model	Random Way Point
Attackers	2,4,6 and 8
Pause time	10 sec
Routing Protocol	AODV

4.2 SIMULATION ENVIRONMENT

The UDP traffic flows are established in the network. All the source nodes negotiate a rate of 100 kbps for traffic flow and begin sending packets on flow at a rate of 100 kbps at time t = 1.0 sec. The attacking flow is set at a rate of 600 kbps. The RoQ attack flow is established with an attack rate (δ) of 600kb over the short period of time (τ) 0.1sec and the period of the attack (T) is 1.0 sec. The capacity of the link is set to 1 Mbps. Each simulation run lasts for 300 s in order to allow the network to experience some levels of congestion.

4.3 SIMULATION RESULTS

The simulation is carried out in 2 scenarios. In the first scenario, three traffic flows are established in the network. The number of attacking flow is initially set as 2 and the attack period of the attack is varied from 1 sec to 5 secs. The packet delivery ratio at the destination node is obtained and then the number of attacking flows is varied and the throughput and Average End to End Delay are obtained.

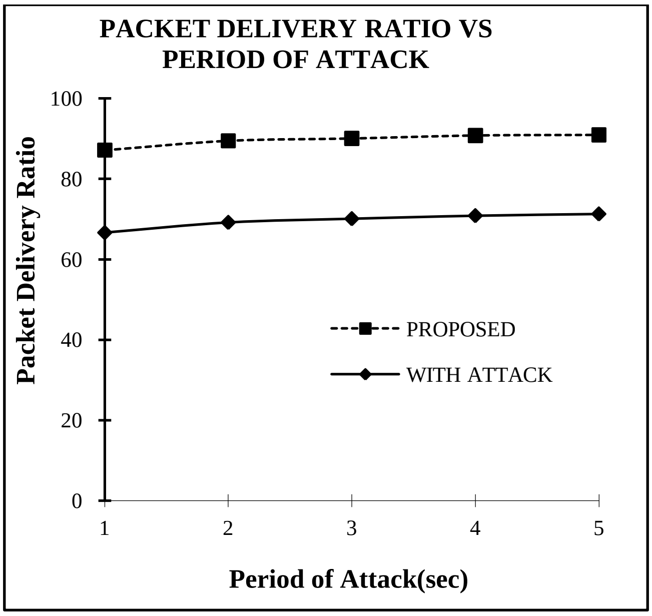

Fig.2. Packet Delivery Ratio with different Period of Attack

From the simulation results of Fig.2, it is observed that if the attacking period of the RoQ attack is increased, the packet delivery ratio can be increased. The packet delivery ratio is the ratio of the number of packets received successfully to the total number of packets sent. For the attacking period of 1 sec, 87.14% of packet delivery ratio is achieved. If the attacking period is increased to 5 secs, the packet delivery ratio is increased to 90.92%. This reveals that if the burst of attack occurs with a smaller value of T, the attack traffic occurs more often than with the case of greater value of T. As the attack traffic is increased, the packet delivery ratio is reduced.

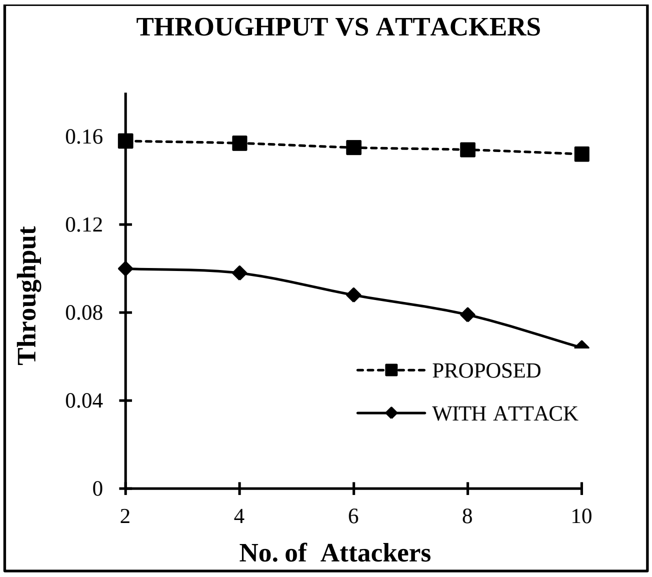

Fig.3. Average Throughput with different attacking flow

Fig.3 shows that when the number of attacking flows is increased the average throughput is reduced. The throughput is the volume of data successfully received by the receiver in Mbps. Since the proposed scheme is able to detect the attacker, effectively based on the flow details and is able to block the attacking flow. We are able to achieve up to 95.5% of throughput for 10 attacking flows as against 40.2% in normal network scenario.

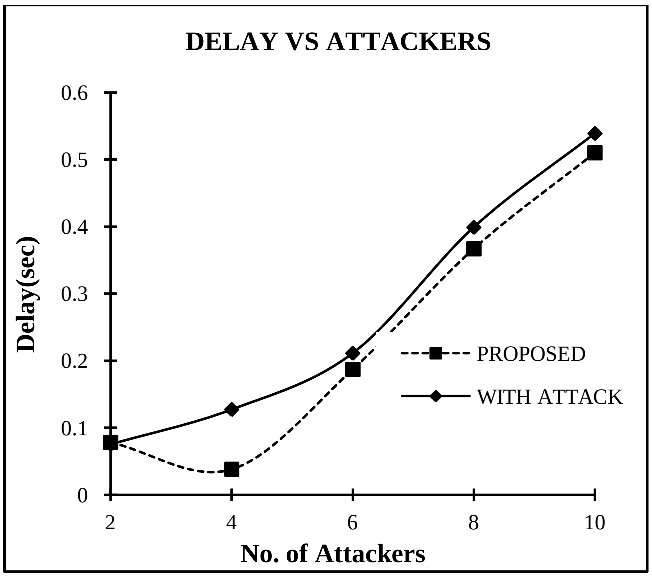

Fig.4. Average End to End Delay Vs Attackers

Fig.4 shows that when the number of attacking flows is increased, the average end to end delay incurred is increased. The average end to end delay calculates the delay of all the packets which have been successfully transmitted from source to the destination. It includes all possible delays caused by buffering during route discovery latency, queuing in the interface queue, retransmission delays at the MAC, propagation and transfer times. Since the attacking flows are rejected in the proposed scheme based on the flow state information at every node, we are able to achieve the lower value of average end to end delay. It is observed that with the proposed scheme we are able to achieve the delay increment of 22.17% for 10 attacking flows without which 36.47% of delay could be achieved.

In the second scenario, the number of UDP flows are varied, the Packet Delivery Ratio & Average End to End Delay is obtained. The offered load could be varied by changing the CBR packet size, the number of CBR flows or the CBR packet rate. Fig. 5 shows that as the number of flows is increased, the packet delivery ratio gets reduced. As the offered load is increased, the packet delivery ratio is reduced due to the network congestion. Since distributed rate control is applied in the proposed scheme, we are able to achieve the packet delivery ratio of 70.38% for 7 CBR traffic flows. It is observed that without the proposed scheme we are able to achieve only 29.22% of packet delivery ratio. Fig. 6 shows that as the number of UDP flows is increased the average end to end delay is also increased due to the same reason. However with the proposed system we are able to achieve less delay.

In addition, the proposed scheme works well along with different routing protocols. Since mobility causes frequent network topology changes, routing is difficult in MANET. When the nodes move, the established paths may break and the routing protocols must dynamically search for other feasible routes. Hence, the proposed method is experimented with both proactive and reactive protocols. Ad hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR) are the reactive protocols which use an on-demand approach for finding routes. In reactive protocols, route is established only when it is required by a source node for transmitting data packets. Destination Sequenced Distance Vector (DSDV) is one of the proactive routing protocols which maintain routes to all destinations, regardless of whether or not these routes are needed. Fig. 7 shows the compatibility of working the proposed scheme with different routing protocols such as AODV, DSDV and DSR.

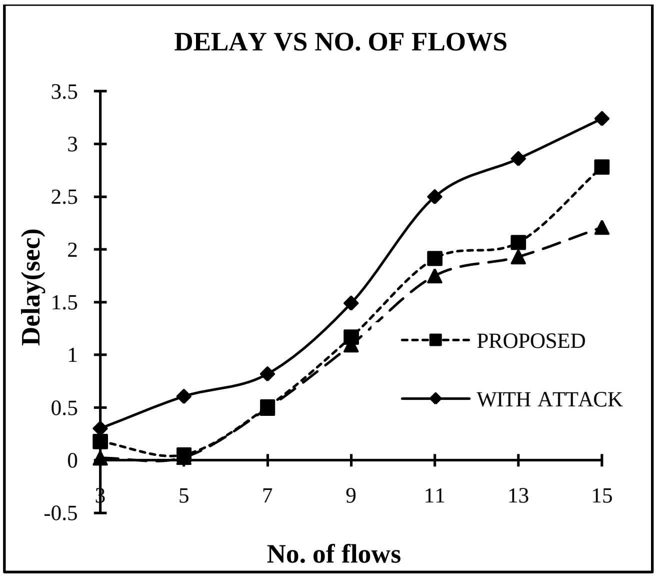

Fig.5. Average End to End Delay with variable number of UDP flows

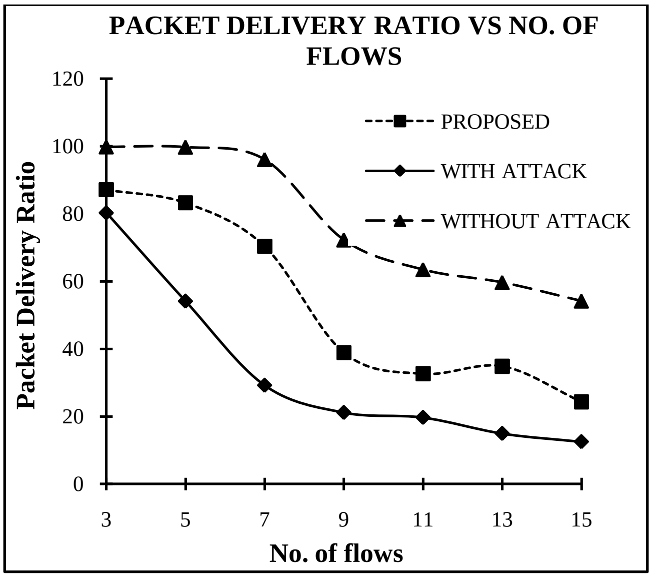

Fig.6. Packet Delivery Ratio with variable number of UDP flows

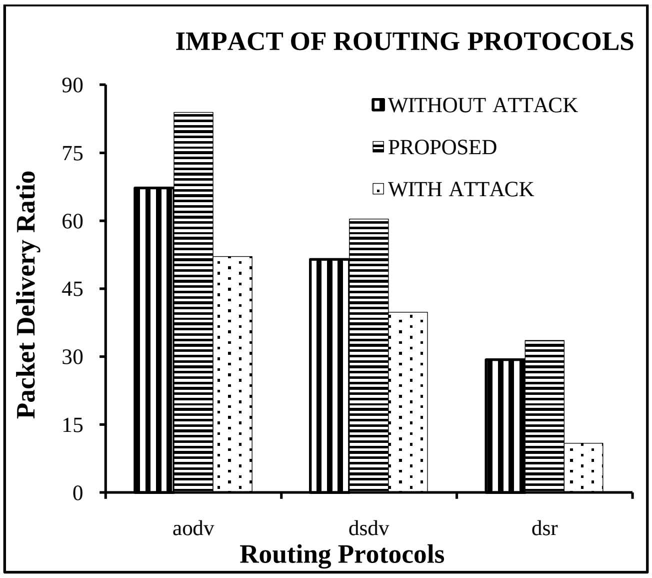

Fig.7. Compatibility with different routing protocols

5. CONCLUSION

In this paper an effective resilient scheme against RoQ DDoS attack in MANET is developed. The proposed scheme detects the attacker based on the flow information updated at the RTO period of packets and the congestion bit information. Once the attackers are identified, all the packets from the attacking nodes will be discarded. The network resources are made available to the legitimate users. The RoQ attack is analyzed for different attack periods. Network simulation experiment on RoQ attack shows that greater throughput and packet delivery ratio can be achieved with the proposed scheme. Increase in delay and decrease in throughput can be observed especially when large number of attacks occurs. The proposed scheme also shows the compatibility of working with different routing protocols.

REFERENCES

[1] Fei Xing and Wenye Wang, “On the Survivability of Wireless Ad Hoc Networks with Node Misbehaviors and Failures”, *IEEE Transactions on Dependable and Secure Computing*, Vol. 7, No. 3, pp. 284-299, 2010.

[2] Haibo Hu and Jianliang Xu, “2PASS: Bandwidth-Optimized Location Cloaking for Anonymous Location-Based Services”, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 21, No. 10, pp. 1458-1472, 2010.

[3] Mina Guirguis Azer Bestavros Ibrahim Matta, “Exploiting the Transients of Adaptation for RoQ Attacks on Internet Resources”, in *Proceedings of 12th IEEE International Conference on Network Protocols*, 2004.

[4] Chia-Wei Chang, Seungjoon Lee, Bill Lin, Jia Wang, “The Taming of The Shrew: Mitigating Low-Rate TCP-Targeted Attack”, *IEEE Transactions on Network Service Management*, Vol. 7, No. 1,pp. 1-13, 2010.

[5] Jian-Hua Song1, 2, Fan Hong1, Yu Zhang1, “Effective Filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks”, in *Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies*, 2006.

[6] Wei Ren, Dit-Yan Yeung, Hai Jin and Mei Yang, “Pulsing RoQ DDoS Attack and Defense Scheme in Mobile Ad Hoc Networks”, *International Journal of Network Security*, Vol. 4, No. 2, pp. 227-234, 2007.

[7] Xiapu Luo, Edmond W.W.Chan and Rocky K.C.Chang, “Detecting Pulsing Denial-of-Service Attacks with Nondeterministic Attack Intervals”, *EURASIP Journal on Advances in Signal Processing*, 2009.

[8] Ping Yi, Zhoulin Dai, Shiyong Zhang and Yiping Zhong, “A New Routing Attack in Mobile Ad Hoc Networks”, *International Journal of Information Technology*, Vol. 11, No. 2, pp. 83-94, 2005.

[9] John Haggerty, Qi Shi and Madjid Merabti, “Statistical Signatures for Early Detection of Flooding Denial-Of service Attacks”, *Springer*, Vol. 181, pp. 327-341, 2005.

[10] Sugata Sanyal, Ajith Abraham, Dhaval Gada, Rajat Gogri, Punit Rathod, Zalak Dedhia and Nirali Mody, “Security Scheme for Distributed DoS in Mobile Ad Hoc Networks”, *ACM, USA*, 2004.

[11] Xiaoxin Wu and David K. Y. Yau, “Mitigating Denial-of-Service Attacks in MANET by Distributed Packet Filtering: A Game-theoretic Approach”, in *Proceedings of the 2nd ACM symposium on Information, computer and communication security*, pp. 365- 367, 2006.

[12] Amey Shevtekar and Nirwan Ansari, “A router-based technique to mitigate Reduction Of quality (RoQ) attacks”, *Computer Networks: The international Journal of Computer & Telecommunication Networking*, Vol. 52, No. 5, pp.957-970, 2008.

[13] Zhiqiang Gao and Zhiqiang, “Differentiating Malicious DDoS Attack Traffic from Normal TCP Flows by Proactive Tests”, *IEEE Communications Letters*, Vol. 10, No. 11, pp. 793-795, 2006.

[14] P.Ebinger and M.Parsons,“Measuring the Impact of Attacks on the Performance of Mobile Ad hoc Networks”, in *Proceedings of the 6th ACM International Symposium on*

Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks, 2009.

[15] Xin Jin, Yaoxue Zhang, Yi Pan and Yuezhi Zhou, “ZSBT: A Novel Algorithm for Tracing DoS Attackers in MANETs”, *EURASIP Journal on Wireless Communications and Networking,* pp. 1-9, 2006.

[16] Marek Hejmo, Brian L. Mark, Charikleia Zouridaki, and Roshan K. Thomas, “A Denial-of-Service Resistant Quality-of-Service Signaling Protocol for Mobile Ad Hoc Networks”, in *Proceedings of Second International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks*, pp.32, 2005.

[17] Wei Ren, Hai Jin and Tenghong Liu, “Congestion Targeted Reduction of Quality of Service DDoS Attacking and Defense Scheme in Mobile Ad Hoc Networks”, in *Proceedings of 7th IEEE International Symposium on Multimedia*, 2005.

[18] Qi Liao, David A. Cieslak, Aaron D. Striegel and Nitesh V. Chawla, “Using selective, short-term memory to improve resilience against DDoS exhaustion attack”, *Security and Communication Networks*, Vol. 1, pp. 287-299, 2008.

[19] T.Peng, C.Leckie and K.Ramamohanarao, “Protection from distributed denial of service attack using history-based ip filtering”, in *Proceedings of IEEE International Conference on Communication*, Vol. 1, pp. 482-486, 2003.

[20] H.Wang, D.Zhang and K.Shin, “Detecting SYN flooding attacks”, in *Proceedings of IEEE INFOCOM*, 2002.

[21] A.Hussain, J.Heidemann and C.Papadopoulos, “A Framework for Classifying Denial of Service Attacks”, in *Proceedings of ACM SIGCOMM*, pp. 99-110, 2003.

[22] C.Jin, H.Wang and K.Shin, “Hop-count filtering: an effective defense against spoofed DoS traffic”, in *Proceedings of the 10th ACM Conference on Computer and Communications Security*, pp. 30-41, 2003.

[23] M.Guirguis, A.Bestavros, I.Matta and Y.Zhang, “Reduction of quality (RoQ) attacks on dynamic load balancers: Vulnerability assessment and design tradeoffs”, *in Proceedings of the IEEE International Conference on Computer Communication*, pp. 857–865, 2007.

[24] Abraham Yaar, Adrian Perrig and Dawn Song, “SIFF: a stateless internet flow filter to mitigate DDoS flooding attacks”, in *Proceedings of IEEE Symposium on Security and Privacy*, pp. 130–143, 2004.

[25] Wei Lu and I.Traore, ”An unsupervised approach for detecting DDoS attacks based on traffic-based metrics”, in *Proceedings of IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*, pp. 462–465, 2005.

[26] Arunmozhi S.A, Venkataramani Y., “A Flow Monitoring scheme to Defend Reduction-of-Quality (RoQ) Attacks in Mobile Ad-hoc Networks”, *Information Security Journal: A Global Perspective*, Vol. 19, No. 5, pp. 263–272, 2010.