A Flow Monitoring based Distributed Defense Technique for Reduction of Quality Attacks in MANET

S.Venkatasubramanian
Department of Computer Science,
Saranathan college of Engineering,
Trichy, India

N.P.Gopalan
Department of Computer Applications,
National Institute of Technology,
Trichy, India

ABSTRACT
Reduction of Quality (ROQ) attack is one of the Denial of Service (DoS) attacks which affect the MANETs. Instead of refusing the clients from the services completely, these RoQ attacks throttle the TCP throughput heavily and reduce the QoS to end systems. To mitigate this RoQ attack in MANET, we propose to design a distributed defense technique in this paper. Initially, a mechanism for monitor node selection is designed such that the monitoring nodes should cover the entire network. These monitoring nodes estimate the short-lived flows to observe the sudden increase in the traffic load in a short time. When the total traffic load of such flow exceeds a threshold value, an attack is detected and the corresponding node is added into a local blacklist. The local blacklist from all the monitoring nodes is sent to a master node from which it evaluates the attacker. The attacker will be notified by the master node to all the monitoring nodes so that all the nodes become aware of the attacker. By simulation results, we show that the proposed technique improves the throughput with reduced packet drops.

General Terms
Wireless Ad hoc networks, QoS

Keywords
DDT, RoQ, MANET, DoS, short-lived flows.

1. INTRODUCTION
A group of wireless nodes which extends a network without the exploitation of existing network infrastructure is known as the mobile ad hoc network. When nodes collaborate to forward packets with each other, a node communicates through multi-hop with them. Impulsive topology changes are frequently caused in MANETs which makes the design of Quality of Service (QoS) routing protocol difficult than the conventional networks [1]. Researches under MANETs are in progress. The infrastructure-less network provides support to various services. The main aim of designing MANETs is for emergency services like natural disasters, military conflicts, medical facilities etc. But recently multimedia communications has been supported by MANETs widely. In the existence of dynamic network topology, maintaining real-time media traffics such as audio and video becomes difficult which is due to high rate requirements and severe delay constraints[2].

1.1 Problem Identification
Compared to wired networks the rate control becomes complex in MANETs since the available bandwidth of the wireless channel is variable and unpredictable. Rate measurements from aggregated real-time traffic is used as a feedback for source-based admission control mechanism and so the per-hop MAC delay measurements from packet transmissions are used as feedback for a rate control mechanism. In order to meet the bandwidth and delay requirements of real-time UDP traffic, rate control of TCP and UDP best effort traffic is performed in a fully distributed and decentralized manner at each and every mobile node. 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 this, rate control mechanism is designed. On maintaining 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. [3].

In our previous work[4] we have proposed to design QoS architecture for Bandwidth Management and Rate Control in MANETs. In our QoS architecture, each node will continuously estimate its available bandwidth. The bandwidth information will then be used for QoS capable routing protocols to provide support to admission control. The traffic is balanced and the network capacity is improved as the weight value assists the routing protocol to evade routing traffic through congested area. Rate control and resource provisioning is done in this approach. But this design can be affected badly by any one of the above discussed attacks. It is not designed to overcome such type of DoS attacks.

So, as an extension to this work, we propose a new defense technique to mitigate the some of the DoS attacks and thereby achieving an efficient QoS provisioning.

1.2 DoS Attacks
There are different types of DoS attacks

- *Pulsing Attack*: A single attacking node sends packets to a randomly selected victim node, with a random sending period and a random packet size.
- *Round Robin Attack*: Multiple randomly selected attacking nodes send packets in sequence in a round robin manner to randomly selected victim nodes, with a random sending period and a random packet size.1
- *Self-Whisper Attack*: Two randomly selected nodes send packets to each other with a random sending period and a random packet size.
- *Flooding Attack*: The purpose of the attack is to force the victim node to decrease its communication with other nodes and eventually enter into a DoS status. [5].
- *Reduction-of Quality*: Instead of refusing the clients from the services completely, these RoQ attacks throttle the TCP throughput heavily and reduce the QoS to end systems gradually.
- *SYN flood*: The attackers use half-open connections to cause the server exhaust its resource to keep the information describing all pending connections. The result would be system crash or system inoperative.

- *TCP reset*: On listening to the TCP connections to the victim, the attacker sends a fake TCP RESET packet to the victim. Then it causes the victim to inadvertently terminate its TCP connection.
- *ICMP attack*: These attacks lead large amounts of ICMP echo reply packets being sent from an intermediary site to a victim, accordingly cause network congestion or outages.
- *UDP storm*: When a connection is established between two UDP services, each of which produces a very high number of packets, thus cause an attack.
- *DNS request*: In this attack scenario, the attack sends a large number of UDP-based DNS requests to a name server using a spoofed source IP address. Then the name server, acting as an intermediate party in the attack, responds by sending back to the spoofed IP address as the victim destination.
- *CGI request*. By simply sending multiple CGI request to the target server, the attacker consumes the CPU resource of the victim. Then the server is forced to terminate its services.
- *Mail bomb*. A huge amount of mail may simply fill up the recipient's disk space on the server or, in some cases, may be too much for a server to handle and may cause the server to stop functioning. [6]
- *Algorithmic Complexity Attacks*: It's a class of low-bandwidth DoS attacks that exploit algorithmic deficiencies in the worst case performance of algorithms used in many mainstream applications. .
- *Over reservation attack:* An over reservation attack does not consume the resources of the network, but locks out legitimate sources that could make use of the unused bandwidth that has been reserved by the attacker.
- *State table exhaustion attack*: The attacker causes the state table to be exhausted by issuing a large number of reservation requests to the victim node. [7].

1.3 Reduction of Quality (RoQ) Attacks

Reduction of Quality attack is an important DOS attack in Wireless Networks. The DDoS flooding attacks are characterized by the high rate or high volume. Recently a new attack called the shrew attacks or Reduction-of- Quality (RoQ) attacks has been identified. RoQ attacks gradually reduces QoS to end systems by strangling the TCP throughput heavily instead of entirely refusing the clients form the services.
Instead of limiting its steady state capacity, RoQ attacks targets the systems adaptive behavior. Source and destination IP spoofing are used by RoQ attacks. Due to the absence of dissimilar periodicity, the packets are not filtered accurately. RoQ attacks are commenced through multiple zombies and spoof header packet information so that they can escape from trace back techniques. In fact it is necessary to control the frequency domain characteristics of attacking flows. The attacking period has to be close to the Retransmission Time Out (RTO) so that TCP flows are efficiently strangled. Though the source IP addresses of the packet header are falsified, the malicious flow detection mechanisms are relinquished by energy distribution pattern using traffic spectrum. [8].

To mitigate this RoQ attack in MANET, we propose to design a detection algorithm in this paper.

2. RELATED WORK

Wei Ren, Dit-Yan Yeung, Dit-Yan Yeung and Mei Yang [5] have proposed a defense scheme that includes both the detection and response mechanisms. The detection signals include the frequency of receiving RTS/CTS packets, frequency of sensing a busy channel (signal interference), and number of RTS/DATA retransmissions.

Jatinder Singh, Dr. Savita Gupta, and Dr. Lakhwinder Kaur [8] have designed the MAC layer based defense architecture for RoQ attacks in Wireless LAN which includes the detection and response stages. The attackers are detected by checking the RTS/CTS packets from the MAC layer and the corresponding attack flows are blocked or rejected. It includes the detection and response stages. Detection makes use of three status values that can be obtained from the MAC layer: frequency of receiving RTS/CTS packets, frequency of sensing a busy channel, and the number of RTS/DATA retransmissions.

Zhu Lina, and Zhu Dongzhao [9] have proposed a router-based approach to detect the stealthy low rate DoS and RoQ attacks which use IP address spoofing or botnets. This work addresses the IP address spoofing and botnet problem in the context of the low rate DoS and RoQ attacks, and proposes an effective and realizable solution to defend against RoQ attacks.

Yu Chen and Kai Hwang [10] have proposed a novel defense scheme against RoQ. They 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 results 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 (reduction-of-service) attacks.

P. Varalakshmi, S.Thamarai Selvi, S. Monica and G. Akilesh [11] have proposed a three-tier architecture consisting of Service Providers, Brokers and Regional Resource Administrators is proposed. This architecture is secured by building a mechanism to detect and counter Distributed Denial of Service (DDoS) Attacks. Consumers submit service requests and policy constraints to the RRA. Each entity has a trust value associated with them which is computed based on their behavior. The three-tier architecture ensures trustworthy resource selection in a grid environment. The DDoS defense consists of sensory registers that capture and analyze the traffic characteristics, short-term memory for local detection of DDoS attacks and a long-term memory for collaboration.

3. PROPOSED DEFENSE TECHNIQUE

3.1 Monitor Node Selection

For the selection of monitor nodes, the node weight is introduced. The weight metric(W), assigns a cost to the nodes in the network. The weight W combines the link quality Lq, channel quality C_{occ} and the average delay D_{avg} , and residual energy E_i to select monitoring node. For an intermediate node *i* with established transmission with several of its neighbors, the W for the link from node i to a particular neighboring node is given by

$$W = \lceil\lceil (Lq + Cocc) / \ Davg \rceil\rceil Ei$$

By using the above formula the weight for each node is calculated and exchanged with the neighbors. The node with

maximum weight is selected as monitor node and the same is intimated to the neighbors. The same procedure is repeated throughout the network to select monitoring nodes for a set of nodes. The information about the monitoring nodes are sent to the master node(MS). The master node then create the key pair and send the private keys to the monitoring nodes while keeping the public key.

3.2 Detection of RoQ Attacks

The mechanism for the detection of the RoQ attacks is done using the following detection logic.

The low rate DoS and RoQ attack flows that use IP address spoofing are similar to legitimate short-lived flows in terms of the number of packets per flow. By the Internet traffic characteristic, we know that short-lived flows occupy less percentage of the total traffic passing through a link

Assuming that the attacker uses the source IP address and the destination IP address spoofing, we propose to detect the sudden increase in the traffic load of all the short-lived flows. We calculate the flows formed and ended within a second to observe the sudden increase in the traffic load in a short time.

Let CrTime and LaTime be the created and last accessed times of individual monitored flows, by the monitoring nodes. Let CurTime the current time. Let {SF} be the set of all the short-lived flows. Let the number of packets in each flow be m and the L be the link capacity and the Ps be the minimum packet size.

Algorithm

For all f in {SF}
If (LaTime-CrTime) = CurTime -1 , then

$$\text{Tot} = \sum_{F=1}^{N} load$$

where load is the total load of each flow.
End if
If Tot > Th , *Where Th is a threshold value*, then
The attack may be Low rate DoS or RoQ
Add the node into the local blacklist.
End if
End For

3.3 Blacklisting of the Nodes

The nodes having the attack are set into the blacklist using the monitoring node. Nodes set into the blacklist are involved only in the data forwarding and is not able to perform any other operations.

- Transmission security is based on *digital signature method* [12] in which each node uses private key to sign the blacklist.
- The signed blacklist list is transmitted to the master node (MS) by each monitoring node.
- MS integrates all blacklisted nodes collected from the monitoring nodes.
- The node which is placed in more than a certain number of local blacklists is considered as an attacker.
- The attacker will be notified by the MS through the Notification message to all the monitoring nodes.
- All the monitoring nodes become aware of the attacker and block that node from further transmissions.

Thus we can reduce the RoQ attack effectively using this mechanism.

For example, suppose that there are four monitoring nodes MN1, MN2, MN3, and MN4 with private keys pr1,pr2,pr3 and pr4 which will send the Local blacklists to their master node MS. The set of transmissions that occur between the monitoring nodes and the master node are given below:

1. MN1 ---- $Sign_{pr1}$ [blacklist] ---- > MS

   MN2 ---- $Sign_{pr2}$ [blacklist] ---- > MS

   MN3 ---- $Sign_{pr3}$ [blacklist] ---- > MS

   MN4 ---- $Sign_{pr4}$ [blacklist] ---- > MS

2. MS Check Blacklist and create Notification message

3. MS ------- Notification message --------- > MN1

   MS ------ Notification message ---------- > MN2

   MS ------- Notification message---------- > MN3

   MS -------- Notification message------- > MN4

4. SIMULATION RESULTS

4.1 Simulation Model and Parameters

The Network Simulator (NS2) [13], is used to simulate the proposed architecture. In the simulation, The distributed coordination function (DCF) of IEEE 802.11 is used for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 250 meters. In our simulation, the speed is 10 m/s and pause time is 5 sec. The simulated traffic is Constant Bit Rate (CBR). The simulation settings and parameters are summarized in table.

Table 1 : Simulation parameters

No. of Nodes	50
Area Size	1000 m X 1000 m
Mac	802.11
Radio Range	250m
Simulation Time	100 sec
Traffic Source	CBR
Packet Size	512
Speed	10m/s
Attackers	2,4,6,8 and 10
Rate	0.5,1.0,1.5,2.0 and 2.5Mb

4.2 Performance Metrics

The proposed Distributed Defense Technique (DDT) is compared with the normal scenario without any detection technique. The performance is evaluated mainly, according to the following metrics.

i. Aggregated Throughput: We measure aggregated throughput in terms of Mbit/second.
ii. Packet Loss: We measure the packet loss, which is the number of packets lost per unit time.

4.3. Results

4.3.1 Based on Attackers

In the initial experiment, we vary the RoQ attackers as 2,4,6,8 and 10.

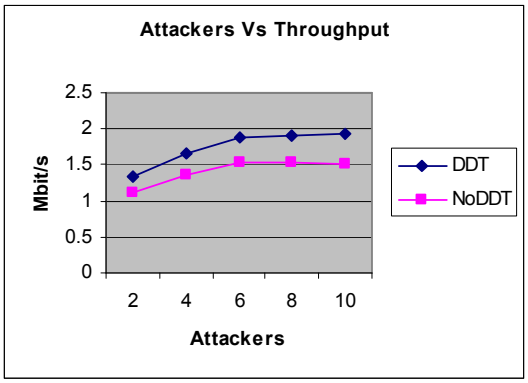

Fig 1: Attackers Vs Throughput

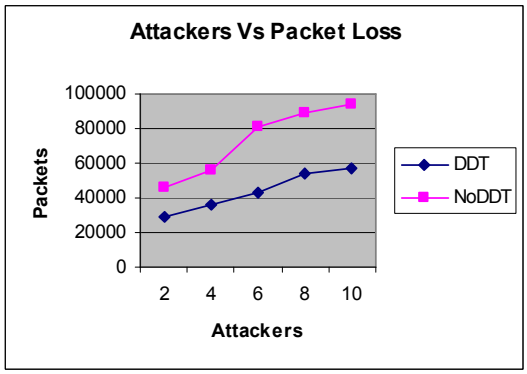

Fig 2: Attackers Vs Packet Loss

Figure 1 shows the results of throughput for the increasing misbehaving nodes. Clearly our DDT technique achieves more throughput than without DDT.

Figure 2 shows the results of packet loss the increasing misbehaving nodes. From the results, we can see that DDT technique has less packets drops when compared with the NoDDT scheme.

4.3.2 Based on Attack Traffic Rate

In the second experiment, we vary the attack traffic rate from 0.5Mb to 2.5Mb.

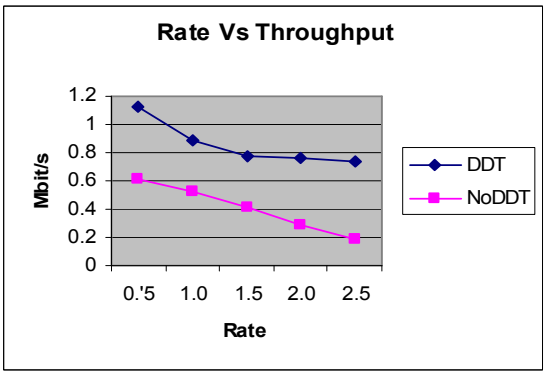

Fig 3: Rate Vs Throughput

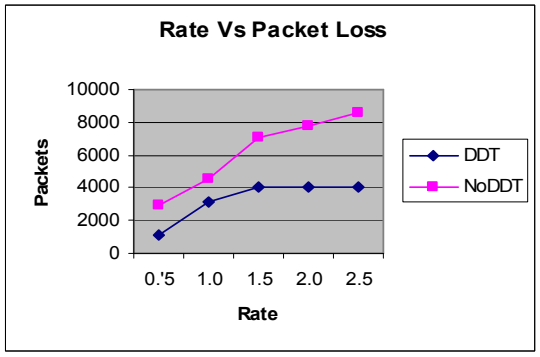

Fig 4: Rate Vs Packet Loss

Figure 3 shows the results of throughput for increasing attack traffic rate. Clearly our DDT technique achieves more throughput than the NoDDT.

Figure 4 shows the results of packets dropped for increasing attack traffic rate. From the results, we can see that DDT technique has less packet drops.

5. CONCLUSION

In this paper, we focus upon the Reduction of Quality (ROQ) attacks in MANETs. Instead of refusing the clients from the services completely, the RoQ attacks throttle the TCP throughput heavily and reduce the QoS to end systems gradually. The RoQ attacks may not filter the attack packets precisely. In order to avoid this, we have proposed a distributed defense technique. We also developed a mechanism for monitor node selection. which detects all affected packets as it selects the monitoring node so as to cover the entire network We have estimated the 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 and the attacker is added into a local blacklist. The monitoring nodes send the Blacklisted nodes to the master node and the attacker will be notified through the notification message so that all the nodes become aware of the attacker. By simulation results, show that the proposed technique improves the throughput with reduced packet drops.

6. REFERENCES

[1] Yuh-Shyan Chen, Shin-Jr Jan and Ming-Chin Chuang, "A Shoelace-Based QoS Routing Protocol for Mobile Ad Hoc Networks Using Directional Antenna", Wireless Personal Communications, SpringerLink, 2009.

[2] A.N. Al-Khwildi, S. Khan, K.K. Loo and H.S. Al-Raweshidy, "Adaptive Link-Weight Routing Protocol using Cross-Layer Communication for MANET", WSEAS Transactions on Communications, 2007.

[3] 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, 2002.

[4] S.Venkatasubramanian and N.P.Gopalan "A QoS Architecture for Resource Provisioning and Rate Control in Mobile Adhoc Networks" published in International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.1, No.3, September 2010, pp 106- 120

[5] 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, Mar. 2007.

[6] Yang Xiang, Wanlei Zhou and Morshed Chowdhury "A Survey of Active and Passive Defence Mechanisms against DDoS Attacks" 2004.

[7] Marek Hejmo, Brian L. Mark, Charikleia Zouridaki, and Roshan K. Thomas "Design and Analysis of a Denial-of-Service-Resistant Quality-of-Service Signaling Protocol for MANETs" IEEE transactions on vehicular technology, VOL. 55, NO. 3, MAY 2006.

[8] Jatinder Singh, Dr. Savita Gupta, and Dr. Lakhwinder Kaur "A MAC Layer Based Defense Architecture for Reduction-of-Quality (RoQ) Attacks in Wireless LAN" International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010.

[9] Zhu Lina, and Zhu Dongzhao "A Router-based Technique to Detect and Defend against Low-rate Denial of Service" 2009 International Symposium on Web Information Systems and Applications.

[10] Yu Chen and Kai Hwang "TCP Flow Analysis for Defense against Shrew DDoS Attacks" IEEE International Conference on Communications (ICC 2007).

[11] P. Varalakshmi, S.Thamarai Selvi, S. Monica and G. Akilesh "Securing Trustworthy Three-tier Grid Architecture with DDoS Attack Defense Mechanism" IC3–2008.

[12] Dhanant Subhadrabandhu, Saswati Sarkar, and Farooq Anjum "A Framework for Misuse Detection in Ad Hoc Networks—Part I" 2006 IEEE.

[13] Chetan N. Mathur and K. P. Subbalakshmi "Digital Signatures for Centralized DSA Networks" IEEE 2007.

[14] Network Simulator, http://www.isi.edu/nsnam/ns