ABSTRACT

A mobile ad hoc network (MANET) is a self configuring network of mobile devices connected by wireless links. Due to the dynamically changing topology, open environment and lack of centralized security infrastructure, MANET is vulnerable to the attacks by malicious nodes and also ad hoc routing attacks. The common type of security attack in MANET is denial of service attack. A Distributed Denial of Service (DDoS) attack is a distributed, large scale attempt by malicious users to flood the victim network with an enormous number of dummy packets. This exhausts the victim network of resources such as bandwidth, computing power, etc. We have analyzed two types of DDoS attacks viz; flooding attack and black hole attack and have proposed solutions for them. The malicious flooding attack is a fatal attack on existing on demand routing protocols. It is achieved either by forwarding many Route Request (RREQ) packets or by sending bogus data packets. Hence, they can be categorized into RREQ flooding attacks and data flooding attacks. A Defense scheme against RREQ flooding attack has been proposed. The proposed Modified Ad hoc On Demand Distance Vector (MAODV) protocol is based on binary exponential back off and RREQ_RATELIMIT. For resisting data flooding attack, a Flow Monitoring Scheme (FMON) was developed based on the flow information. The proposed FMON scheme employs distributed rate control to manage the bandwidth resources of the network effectively. The FMON protocol provides QoS for MANET routing protocol and employs mechanisms at the medium access control (MAC) layer for QoS provisioning and resistance to attacks. The attackers are effectively identified with the proposed scheme. We have presented a mathematical analysis for ad hoc network with DDoS flooding.
attack. The performance of the network with FMON scheme is evaluated by comparing theoretical results with the simulated results.

We have developed a detection scheme against flooding attack which uses load balancing method, along with active queue management technique. In FMON scheme, the source node periodically sends probe packet to the destination and waits for the probe reply packet to be sent back by the destination. Normally, the reply probe packet provides the available bandwidth for communication. Based on the available bandwidth, the source node adjusts its sending rate to avoid congestion. In the proposed load balancing based detection scheme (LBDS), the reply probe packet provides additional information, such as Channel Occupancy Time (COT) and interface queue size. Based on these load information, the source node could determine on which path it would send more data, and on which path it would send less. The proposed scheme successfully detects the misbehaving nodes.

We have also studied the black hole attacks that can be mounted against a MANET, and proposed a feasible solution for it on top of AODV protocol. A Neighborhood Route Monitoring Table (NRMT) based defense scheme for MANETs has been developed. It is resistant to the black hole attack. The scheme identifies the attacker based on timing information and destination sequence number. Hence secure routing is provided with the proposed solution. Simulation is carried out using NS2. The impact of the proposed defense schemes against the attacks were studied with varying number of nodes, varying number of flows and varying pause time. The performance metrics such as packet delivery ratio, average end to end delay, routing overhead were evaluated. Simulation results validate the effectiveness of our proposed schemes.

Comparisons of our proposed schemes are made with other existing protocols. MAODV protocol is compared with FSRFA. This FSRFA
scheme uses threshold values to detect the attack. In our scheme, we not only use threshold values to check the rate for detection of RREQ packet, but also take steps to bypass the attack traffic based on checking whether the nodes adopt binary exponential back off or not. The traffic is again checked for its legitimacy using threshold values. Hence, the proposed scheme improves the detection rate. Our FMON scheme is compared with SWAN as proposed by Ahn et al (2002) and SPA-ARA as proposed by Mehfuz & Doja (2008). According to our proposed defense scheme, Flow Monitoring Table (FMT) is maintained by each intermediate node. Hence attack packets do not get propagated to the entire network. The key MAC layer elements of the scheme consist of estimating the available wireless bandwidth and rate monitoring which are performed in a distributed manner in the network. The proposed LBDS scheme is compared with HHCC as proposed by Yi & Shakkottai (2007). In HHCC, congestion feedback is sent by a node to its one hop neighbor based on queue length. But, our scheme uses channel occupancy time along with queue length. Hence, LBDS performs better than HHCC. Our proposed NRMT scheme is compared with DPRAODV as proposed by Raj & Swadas (2009). It is observed that NRMT performs better than DPRAODV since it includes additional checking based on time of reply of a packet. Based on the comparisons, it is concluded that our proposed schemes perform better than the other schemes. The simulation results prove that the proposed solutions improve the network performance.