

SECURE NETWORK USING RECTIFIED PROBABILISTIC PACKET MARKING BASED ON TRACE BACK DEFENSE AGAINST DDOS FLOODING ATTACKS

ANIL V TURUKMANE¹ & S. K. YADAV²

¹Research Scholar, JJTU, Rajasthan, India

²JJTU, Rajasthan, India

ABSTRACT

The most significant merit of the RPPM algorithm is that when the algorithm terminates, the algorithm guarantees that the constructed attack graph is correct with a specified level of confidence. We carry out simulations on the RPPM algorithm and show that the RPPM algorithm can guarantee the correctness of the constructed attack graph under 1) different probabilities that a router marks the attack packets, and 2) different structures of the network graph. The RPPM algorithm provides an autonomous way for the original PPM algorithm to determine its termination, and it is a promising mean to enhance the reliability of the PPM algorithm. As attackers use automated methods to inflict widespread damage on vulnerable systems connected to the network, it has become painfully clear that traditional manual methods of protection do not suffice. This paper discusses an intrusion prevention approach, intrusion detection, response based on active networks that helps to provide rapid response to vulnerability advisories.

KEYWORDS: Structured Network, Secure Data Sharing, Secure Packets