RESEARCH ARTICLE

Defending against Flood Attacks in Disruption Tolerant Networks using Blowfish Algorithm

S. Pushpa[1], B. Mani Megalai[2], A. Wisy Shantha[3]

[1]PG Scholar of CSE Department& Anna University, India
[2]Mater of Computer Applications & Anna Universities, India
[3]PG Scholar of CSE Department &Department & University, India
Pushpaj85@gmail.com; mani17mca@gmail.com; Wisyabraham22@gmail.com

Abstract— Disruption Tolerant Networks (DTNs) utilize the mobility of nodes and the opportunistic contacts among nodes for data communications. Due to the limitation in network resources such as contact opportunity and buffer space, DTNs are vulnerable to flood attacks in which attackers send as many packets or packet replicas as possible to the network, in order to deplete or overuse the limited network resources. In this paper, we employ rate limiting to defend against flood attacks in DTNs, such that each node has a limit over the number of packets that it can generate in each time interval and a limit over the number of replicas that it can generate for each packet. We propose a distributed scheme to detect if a node has violated its rate limits. To address the challenge that it is difficult to count all the packets or replicas sent by a node due to lack of communication infrastructure, our detection adopts claim-carry-and-check: each node itself counts the number of packets or replicas that it has sent and claims the count to other nodes; the receiving nodes carry the claims when they move, and cross-check if their carried claims are inconsistent when they contact. The claim structure uses the pigeonhole principle to guarantee that an attacker will make inconsistent claims which may lead to detection. We provide rigorous analysis on the probability of detection, and evaluate the effectiveness and efficiency of our scheme with extensive trace-driven simulations.

Keywords— DTN; security; flood attack; detection

Full Text: http://www.ijcsmc.com/docs/papers/March2014/V3I3201499b24.pdf