Abstract

Mobile ad-hoc networks (MANETs) are composed of autonomous nodes that are self-managed, dynamically deployed without any pre-existing infrastructure. Gray hole attacks are an active type of attack, which leads to dropping of messages, attacking node first agrees to forward packets and then fails to do so. For this we are using an AODV routing protocol to
discover route. Initially the Malicious node behaves correctly and a reply sends true Route Reply (RREP) messages to nodes that initiate Route request (RREQ) messages. We use an intrusion detection system (IDS) to monitors the network or system activities for malicious activities or policy violation and produces reports to a Management Station. It takes over the sending packets. Afterwards, the node just drops the packets to launch a (DoS) denial of service attack. If neighbors nodes that try to send packets over attacking nodes lose the connection to destination then they may want to discover a route again and broadcasting Route Request (RREQ) messages. In Network Simulation-2 (NS-2) scenario the simulation result has shown that the throughput packet delivery is improved rather than traditional Gray hole attack.

Reference

- K Fall and K. Varadhan, "The NS Manual" , November 18, 2005, 
Grayhole Attack and Prevention in Mobile Adhoc Network

- R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.
- Electronic Publication: Digital Object Identifiers (DOIs): Article in a journal:
- Article in a conference proceedings:

Index Terms

Computer Science
Network Security

Key words

Gray hole Packet dropping malicious node
Routing
MANET
AODV