Available online at www.sciencedirect.com
ScienceDirect
Ad Hoc Networks 6 (2008) 32–46
Ad Hoc Networks
www.elsevier.com/locate/adhoc

A study of different types of attacks on multicast in mobile ad hoc networks ☆

Hoang Lan Nguyen *, Uyen Trang Nguyen

Department of Computer Science and Engineering, York University, Toronto, Ont., Canada M3J 1P3

Received 27 July 2006; accepted 31 July 2006
Available online 31 August 2006

Abstract

We present a simulation-based study of the impacts of different types of attacks on mesh-based multicast in mobile ad hoc networks (MANETs). We consider the most common types of attacks, namely rushing attack, blackhole attack, neighbor attack and jellyfish attack. Specifically, we study how the number of attackers and their positions affect the performance metrics of a multicast session such as packet delivery ratio, throughput, end-to-end delay, and delay jitter. We also examine rushing attackers' success rates of invading into the routing mesh when the number of attackers and their positions vary. The results enable us to suggest measures to minimize the impacts of the above types of attacks on multicast in MANETs.

Keywords: Multicast; Attack strategies; Security threats; Vulnerability analysis; Performance analysis

1. Introduction

A mobile ad hoc network is a self-organizing system of mobile nodes that communicate with each other via wireless links with no fixed infrastructure or centralized administration such as base stations or access points. Nodes in a MANET operate both as hosts as well as routers to forward packets for each other in a multi-hop fashion. MANETs are suitable for applications in which no infrastructure exists such as military battlefield, emergency rescue, vehicular communications and mining operations.

In these applications, communication and collaboration among a given group of nodes are necessary. Instead of using multiple unicast transmissions, it is advantageous to use multicast in order to save network bandwidth and resources, since a single message can be delivered to multiple receivers simultaneously. Existing multicast routing protocols in MANETs can be classified into two categories: tree-based and mesh-based. In a multicast routing tree, there is usually only one single path between a sender and a receiver, while in a routing mesh, there may be multiple paths between each sender–

☆ A preliminary version of this paper appeared in the Proceedings of 2006 IEEE International Conference on Networking (ICN 2006). This research was supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC) through a Discovery Grant.
* Corresponding author. Tel.: +1 416 739 1586.
E-mail addresses: lan@cs.yorku.ca (H.L. Nguyen), utn@cs.yorku.ca (U.T. Nguyen).

1570-8705/$ - see front matter
doi:10.1016/j.adhoc.2006.07.005

receiver pair. Routing meshes are thus more suitable than routing trees for systems with frequently changing topology such as MANETs due to the availability of multiple paths between a source and a destination. Multicast data may still be delivered to the destination on alternative paths even when the main route breaks. Example tree-based multicast routing protocols are MAODV [8], AMRIS [9], BEMRP [24] and ADMR [23]. Typical mesh-based multicast routing protocols are ODMRP [4], FGMP [22], CAMP [5], DCMP [6], and NSMP [7].

Among all the research issues, security is an essential requirement in MANET environments. Compared to wired networks, MANETs are more vulnerable to security attacks due to the lack of a trusted centralized authority, lack of trust relationships between mobile nodes, easy eavesdropping because of shared wireless medium, dynamic network topology, low bandwidth, and battery and memory constraints of mobile devices. The security issue of MANETs in group communications is even more challenging because of the involvement of multiple senders and multiple receivers. Although several types of security attacks in MANETs have been studied in the literature, the focus of earlier research is on unicast (point-to-point) applications [15–17]. The impacts of security attacks on multicast in MANETs have not yet been explored.

In this paper, we present a simulation-based study of the effects of different types of attacks on mesh-based multicast in MANETs. We consider the most common types of attacks, namely rushing attack, blackhole attack, neighbor attack and jellyfish attack.

- *Rushing attack*. Many demand-driven protocols such as ODMRP [4], MAODV [8], FGMP [22], and ADMR [23], which use some form of duplicate suppression in their operations, are vulnerable to rushing attacks. When source nodes flood the network with route discovery packets in order to find routes to the destinations, each intermediate node processes only the first non-duplicate packet and discards any duplicate packets that arrive at a later time. A rushing attacker exploits this duplicate suppression mechanism by quickly forwarding route discovery packets in order to gain access to the forwarding group. Rushing attacks were first introduced by Hu et al. [1].
- *Blackhole attack*. A blackhole attacker first needs to invade into the multicast forwarding group (e.g., by implementing rushing attack) in order to intercept data packets of the multicast session. It then drops some or all data packets it receives instead of forwarding them to the next node on the routing path. This type of attack often results in very low packet delivery ratio.
- *Neighbor attack*. Upon receiving a packet, an intermediate node records its ID in the packet before forwarding the packet to the next node. An attacker, however, simply forwards the packet without recording its ID in the packet to make two nodes that are not within the communication range of each other believe that they are neighbors (i.e., one-hop away from each other), resulting in a disrupted route.
- *Jellyfish attack*. A jellyfish attacker first needs to intrude into the multicast forwarding group. It then delays data packets unnecessarily for some amount of time before forwarding them. This results in significantly high end-to-end delay and thus degrades the performance of real-time applications. Jellyfish attacks in MANETs were first discussed by Aad et al. [2].

Using simulation, we study how the number of attackers and their positions affect the performance of a multicast session in terms of packet delivery ratio, throughput, end-to-end delay, and delay jitter. Our simulation results show that a large multicast group with a high number of senders and/or a high number of receivers can sustain good performance under these types of attacks due to several alternative paths in the routing mesh. The most damaging attack positions are those close to the senders and around the mesh center. We also examine rushing attackers' success rates of invading into the routing mesh. We find that in order to increase the likelihood of being selected into the routing group the attackers must gather themselves in a group and stay near the receivers or around the mesh center.

Our contributions are as follows. First, we present experimental results that show how a mesh-based multicast session performs under various attack scenarios. Second, we identify several unique behaviors of a multicast network under attack, which have not been seen in unicast environments. Third, the obtained results allow us to suggest some counter-attack measures (e.g., adding more senders and/or receivers to the multicast group to improve