Visvesvaraya Technological University

Belgaum

A

PROJECT REPORT
ON

"SECURE MULTICASTING IN WIRELESS NETWORK TO RESISTS THE VARIOUS ATTACKS"

Submitted in partial fulfillment of requirements for the award of degree of Bachelor of Engineering in Computer Science and Engineering from Visvesvaraya Technological University, Belgaum, Karnataka

Project Associates:

SHIVPRASAD.L.M	**3PG09CS404**
DEEPAK.D.G	**3PG09CS401**
ARJUN.H	**3PG08CS003**
MANI BHUSHAN	**3PG06CS020**

Under the guidance of

Prof. Malatesh.K M.Tech

Dept. of CS&E
PDIT, HOSPET

Bellary V.V. Sangha's
PROUDHADEVARAYA INSTITUTE OF TECHNOLOGY
T.B.DAM, HOSPET-583225

2011-2012

ABSTRACT

Multihop wireless networks rely on node cooperation to provide multicast services. The multihop communication offers increased coverage for such services but also makes them more vulnerable to insider (or Byzantine) attacks coming from compromised nodes that behave arbitrarily to disrupt the network. In this work, we identify vulnerabilities of on-demand multicast routing protocols for multihop wireless networks and discuss the challenges encountered in designing mechanisms to defend against them. We propose BSMR, a novel secure multicast routing protocol designed to withstand insider attacks from colluding adversaries. Our protocol is a software-based solution and does not require additional or specialized hardware. We present simulation results that demonstrate that BSMR effectively mitigates the identified attacks.

MULTICAST routing protocols deliver data from a source to multiple destinations organized in a multicast group. In the last few years, several protocols were proposed to provide multicast services for multihop wireless networks. A major challenge in designing protocols for wireless networks is ensuring robustness to failures and resilience to attacks. Wireless network provide a less robust communication than wired networks due to frequent broken links and a higher error rate. Security is also more challenging in multihop wireless networks because the open medium is more susceptible to outside attacks and the multihop communication makes services more vulnerable to insider attacks coming from compromised nodes. Although an effective mechanism against outside attacks, authentication is not sufficient to protect against insider attacks because an adversary that compromised a node also gained access to the node's cryptographic keys. Insider attacks are also known as Byzantine attacks and protocols able to provide service in their presence are referred to as Byzantine-resilient protocols.