RESEARCH PROPOSAL

SECURITY SERVICES IN GROUP COMMUNICATIONS OVER MOBILE AD- HOC AND WIRELESS SENSOR NETWORKS USING PERFORMANCE ANALYSIS OF ALGORITHMS

RAMKUMAR. R,
austinramkumar736@gmail.com

Abstract

Group communications in wireless networks has been facilitating many emerging applications that require packet delivery from one or more sender(s) to multiple receivers. Due to insecure wireless channels, group communications are susceptible to various kinds of attacks. Although a number of proposals have been reported to secure group communications using Group management key (GMK), provisioning security in group communications in wireless networks remains a critical and challenging issue. This article presents a survey of recent advances in security requirements and services in group communications in three types of wireless networks, and discusses challenges in designing secure group communications in these networks: wireless infrastructure networks, mobile ad hoc networks, and wireless sensor networks. This article presents a survey of recent advances in security requirements and services in group communications in three types of wireless networks, and discusses challenges in designing secure group communications in these networks: wireless infrastructure networks, mobile ad hoc networks, and wireless sensor networks.

Introduction

any Wireless Sensor Networks (WSNs) are being en-visage in military, emergency and surveillance applications today, where sensor nodes need to send sensed data to the sink. In many applications under hostile environment, sensor nodes cannot be deployed deterministically and thus are randomly deployed into the field. An important requirement in network management of many mission critical applications is to secure end to end sensor networks data from being eavesdropped by the attacker. While there have been many works devoted to hop by hop secure communications in WSNs, the issue of end to end secure communications is largely ignored. This is mainly due to the fact that there exist two intuitive approaches to provide a high

degree of end to end secure communications. Mobile ad hoc networks are formed by a collection of, potentially mobile, wireless nodes; communication links form and disappear as nodes come into and go out of each other's communication range. Wireless networking has received a boost from the development of standards such as IEEE 802.11 and Bluetooth. Much of this activity has focused on the design of routing and medium access control protocols, since efficiency of these protocols can have a significant impact on performance.

Review of literature

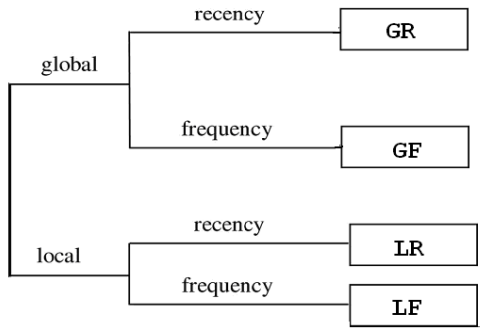
A group communication service forms an important building block for applications in dynamic distributed systems and is useful in many applications that involve collaborations among a group of people. The key features of a group communication service are:
(1) Maintaining information regarding group membership.
(2) Letting nodes within a group communicate with each other in an ordered manner.
There has been significant research activity on group communication in traditional wired networks. The vast body of this research is an indicator of the significance of the group communication service paradigm.

Objective of the proposal:

The aim of the proposed system is "Distributed Token Ring circulation in mobile Ad-hoc Networks", to measure the performance of the local and global connectivity between the nodes. This research will present recent advances in security requirements and services in group communications in three types of wireless networks, and will discusses challenges in designing secure group communications in these networks: wireless infrastructure networks, mobile ad hoc networks and wireless sensor networks.

Research Design

Mobile Ad - Hoc and Wireless Sensor Networks & Distributed Token Ring circulation in mobile Ad-hoc Networks. The researcher follows experimental Design for the research.



Materials & Method

SOFTWARE REQUIREMENTS

Platform	: JDK 1.5
Program Language	: JAVA
Tool	**:** NETBEANS 5.5
Operating System	: Microsoft Windows NT 4.0 or Windows 2000 or XP

HARDWARE REQUIREMENTS

Processor	: 733 MHz Pentium III Processor
RAM	: 128 MB
Hard Drive	: 10GB
Monitor	: 14” VGA COLOR MONITOR
Keyboard	: 104 Keys
Floppy Drive	: 1.44 MB

Mouse : Logitech Serial Mouse

Disk Space : 1 GB

Expected Outcome:

Tokens Carrying Messages

The research will result with an alternative approach to store the messages in the token itself – since the token visits all nodes in a virtual ring, the messages will eventually reach all the nodes, the order in which messages are added to the token determining the order in which they are delivered to the nodes. Both these approaches depend on the existence of a virtual ring in the network. But the prior work has not sufficiently addressed the issue of determining efficient embeddings of rings in networks with dynamically changing topology. The expected result of the research is to create Security Services in group communications over Mobile Ad- Hoc and wireless sensor networks using performance analysis of algorithms.

References

[1] S. K. S. Gupta and S. Cherukuri, "An Adaptive Protocol for Efficient and Secure Multicasting in IEEE 802.11 Based Wireless LANs," Proc. IEEE WCNC 2003, vol. 3, Mar. 2003, pp. 2021–26

[2] A. Wadaa et al., "On Providing Anonymity in
Wireless Sensor Networks," Proc. 10th Int'l. Conf. Parallel and Distrib. Syst., July 2004, pp. 411–18.

[3] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Elsevier's Ad Hoc Networks J., Special ssueI on Sensor Network Applications Protocols, vol. 1, no. 2–3, Sep. 2002, pp. 293–315.

[4] R. Maheshwari, J. Gao, and S. R. Das, "Detecting
Wormhole Attacks in Wireless Networks Using Connectivity Information," Proc. IEEE INFOCOM '07, Mar.2007.