Chapter 3
An Inter-Domain Agent Based Secure Authorization and Communication for Mobile Clients in Wireless Ad Hoc Networks

Neeraj Kumar
SMVD University, India

R. B. Patel
MM University, India

ABSTRACT

Wireless mobile ad hoc network (MANET) is a dynamic network. Nodes in a MANET have high degree of mobility from one domain to another in a particular time interval. In such a dynamic network, security is a major concern. In this paper, the authors propose an inter domain agent based secure authorization and communication for mobile clients/nodes (MCs) in MANET. Mobile agents (MAs) are software programs that support the mobility of clients in different domain and provide necessary resources to the clients for safe execution. It also shares the key with MCs in different domains. An algorithm for secure authorization and communication between MCs having mobility in different domains is proposed. The scheme is evaluated on ns-2 w.r.t. metrics such as overall cost in terms of overhead generated, admission and traceability cost, and itinerary chosen by MAs w.r.t. mobility of MCs.

DOI: 10.4018/978-1-4666-0119-2.ch003
# 1. INTRODUCTION

Security is a paramount concern in MANET because a MANET is much more vulnerable to malicious exploits than a wired (traditional) network. The use of wireless links renders the network susceptible to attacks ranging from passive eavesdropping to active interfering. Unlike wired networks where an adversary must gain physical access to the network wires or pass through several lines of defense at firewalls and gateways, attacks on a wireless network can come from all directions and target at any MC. Damages can include leaking secret information, message contamination, and node impersonation, i.e., a MANET did not have a clear line of defense, and every node must be prepared for encounters with an adversary directly or indirectly. Also MCs are autonomous units that are capable of roaming independently, i.e., MCs with inadequate physical protection are receptive to being captured, compromised, and hijacked. Since tracking down a particular MC in large scale MANET may not be easily done, attacks by a compromised node from within the network are far more damaging and much harder to detect. Therefore, MCs and the infrastructure must be prepared to operate in a mode that trusts no peer. The lack of centralized authority (CA) means that the adversaries can exploit this vulnerability for new types of attacks designed to break the cooperative algorithms.

The security of MANETs is often predicated on the availability of efficient key management techniques. However, the usual features like lack of a CA and dynamic nature of MANETs, represent major obstacles to providing secure, effective and efficient key management. What further complicates the issue is that, in many applications (such as secure routing (Hu et al., 2002; Papadimitratos & Haas, 2002) cryptographic keys need to be established prior to communication. As a result, standard key exchange solutions, e.g., Station-to-Station protocol (Menezes et al., 1997), are not appropriate because they require the nodes to interact and rely on some form of a Public Key Infrastructure (PKI) which is not usually available in MANETs.

To meet the above challenges, this paper proposes Inter domain MA based secure authorization and communication for MCs in MANET. Initially MC is registered in its home domain monitored by home agent (HA). Whenever MC roam into another domain, its services are provided and monitored by Foreign Agent (FA).

We have chosen Mobile Agents Technology (MAT) in which MAs will perform all the tasks. It is a software program that can migrate under its own or host control from one node to another in a heterogeneous network or it is a software programs that can halt execution from a host, travel across the network, and continue execution at another host, without human interruption. In other words, the program running at a host can suspend its execution at an arbitrary point, transfer itself to another host, (or request the host to transfer it to its next destination) and resume execution from the point of suspension is called Mobile Agent (Patel & Garg, 2001). After being dispatched, the MAs become independent of the creating host and can operate asynchronously and autonomously (Patel & Garg, 2004). They can be created and dispatched by individual nodes in the group for their specific purposes. They can also be owned by the system and shared by all the other nodes.

Rest of the paper is organized as follows: Section 2 discusses the related work, Section 3 describes the advantages of using agents, Section 4 describes the proposed approach in detail, Section 5 provides simulation and results obtained, and finally section 6 concludes the article.

# 2. RELATED WORK

MANETs are, by their nature, vulnerable to many types of attacks. (Zhou & Haas, 1999) proposed to distribute CA service among several nodes of the network. Their approach is hierarchical: only
Related Content

Reducing Power and Energy Overhead in Instruction Prefetching for Embedded Processor Systems
www.igi-global.com/article/reducing-power-energy-overhead-instruction/59872?camid=4v1a

2-clickAuth: Optical Challenge-Response Authentication Using Mobile Handsets
www.igi-global.com/article/clickauth-optical-challenge-response-authentication/55081?camid=4v1a

Mobile Commerce Applications and Adoption
www.igi-global.com/chapter/mobile-commerce-applications-adoption/26609?camid=4v1a

A Secure Architecture for Nomadic User in IMS Network
www.igi-global.com/article/secure-architecture-nomadic-user-ims/63047?camid=4v1a