Chapter 5.21
Security Across Disparate Management Domains in Coalition MANETs

Mudhakar Srivatsa
IBM T.J. Watson Research Center, USA

Dakshi Agrawal
IBM T.J. Watson Research Center, USA

Andrew D. McDonald
Roke Manor Research Ltd, UK

ABSTRACT

Designing a coalition network for chaotic environments (e.g., responding to a large catastrophe) is challenging because such systems cannot rely on availability of a fixed communication or a security infrastructure. In such situations, a coalition may use Mobile Ad-hoc NETworks (MANETs) to communicate and to extend its operational reach and tempo. In this scenario, bootstrapping security and networking protocols requires that networking protocols cannot assume full existence of operational security protocols and vice-versa. In this chapter, the authors outline a realistic bounded resource adversary model and examine bootstrapping problems in the physical & link layer and the routing layer with the goal of identifying new research challenges and novel solution methodologies. In particular, (i) the authors examine secure link key set up protocols at the physical & link layer that neither use computationally intensive PKI mechanisms nor assume pre-configured shared keys between nodes that belong to different coalition partners, (ii) identify new security issues owing to power saving intra-domain routing protocols that use sophisticated packet matching and forwarding mechanisms; in a coalition setting they also examine inter-domain routing protocols that preserve domain autonomy and yet permits scalable network monitoring and misbehavior detection, (iii) examine identity management issues in MANETs and outline a wireless fingerprinting approach to condone a malicious node from spoofing and forging one or more identities on the network.

DOI: 10.4018/978-1-61350-101-6.ch521

INTRODUCTION

Large corporations are slowly being transformed from monolithic, vertically integrated entities, into globally disaggregated value networks, where each member focuses on its core competencies and relies on partners and suppliers to develop and deliver goods and service. The ability of multiple partners to come together, share sensitive business information and coordinate activities to rapidly respond to business opportunities, is fast becoming a key driver for success.

The defense sector too has similar dynamic information sharing needs. The decentralized, dynamic and distributed threat of global terrorism has created a need for information sharing between intelligence agencies of different countries and between multiple security and law-enforcement agencies within a country. Furthermore, traditional wars between armies of nation-states are being replaced by highly dynamic missions where teams of soldiers, strategists, logisticians, and support staff, drawn from a coalition of military organizations as well as local (military and civilian) authorities, fight against elusive enemies that easily blend into the civilian population (Roberts et. al., 2007). Securely disseminating mission critical tactical intelligence to the pertinent people in a timely manner will be a critical factor in a mission's success.

Mobile ad hoc networks (MANETs) have been developed to support communication in tactical missions wherein, the availability of a fixed communication infrastructure cannot be assumed. Many such situations require resources from a coalition wherein multiple groups and organizations come together, communicate, and collaborate, all within a short period of time; for example, in a disaster recovery operation, the local police force, fire-fighters, military forces, medical crews, and other organizations may all coordinate their activities. Such situations call for a *coalition MANET* – interconnect of several MANETs governed by different administrative domains – to enable end-to-end communication. However, most approaches to date have considered MANETs from an intra-domain perspective with a flat network under a single administrative entity. In order to allow inter-operation among heterogeneous network domains operated by different organizations, inter-domain routing approaches such as IDRM (Inter-Domain Routing Protocol for MANETs) (Chau et. al., 2008) are now being considered.

This chapter explores issues in bootstrapping networking and security protocols in a coalition MANET. The key challenge in bootstrapping a coalition MANET is the establishment a secure and reliable end-to-end packet delivery service starting from a point where nodes belonging to different organizations are placed in a field *without* any pre-configured coordination of either the networking or the security protocols amongst the members of a coalition. In this scenario, bootstrapping security and networking protocols requires that networking protocols cannot assume full existence of operational security protocols and vice-versa.

In this chapter, we examine how to enable secure communication at the lower layers (physical and data link layer) as well as at the network layer leading to secure end-to-end packet delivery service in a coalition MANET. We start with the challenges in establishing physical layer communication including discovery of other nodes and secure configuration of physical & link layer parameters. We illustrate bootstrapping issues by considering two cases: in the first case, nodes use a wireless communication protocol similar to the family of IEEE 802.11 standards that are vulnerable to jamming attacks, and in the second case, nodes use a low probability of interception and detection (LPI/LPD) wireless communication protocol from the military grade wideband waveform that are resilient to jamming attacks, but require pre-configuration (e.g., shared spreading code, hopping pattern, etc.). Using these consid-