Chapter 1
Security Management for Mobile Ad Hoc Network of Networks (MANoN)

Ali H. Al-Bayatti
De Montfort University, UK

Hussein Zedan
De Montfort University, UK

Antoniuo Cau
De Montfort University, UK

François Siewe
De Montfort Universtiy, UK

ABSTRACT

Many military research efforts have concentrated on how to allow war-fighters to take advantage of all available information within the battlefield in a rapid and flexible manner. As a result, the development of the Global Information Grid (GIG) was the key enabler for this process; hence, adding to the development of the mobile networking part of the GIG, the concept of the Mobile Ad hoc Network of Networks (MANoN) is introduced. This article proposes a novel security management algorithm achieving the three management essentials: Security Administration; Prevention and Detection; and Containment and Recovery; based on the International Telecommunication Union's recommendation M.3400 to manage securely the future of military Network-Centric Warfare (NCW). The authors will employ Interval Temporal Logic (ITL) as a method of handling both sequential and parallel composition in flexible timely constrains, in addition, this technique will be evaluated using the Network Simulator (NS-2) to provide and check whether security requirements are met in a comprehensive manner.

DOI: 10.4018/978-1-4666-0119-2.ch001

INTRODUCTION

In the early part of the 21st century, the focus of many military research efforts was on how to allow war-fighters to take advantage of all available information within the battlefield in a rapid and flexible manner. As a result, the development of the Global Information Grid (GIG) was the key enabler of this process (Stotts, Seidel, Krout, & Kolodzy, 2008). GIG is a United States (US) Department of Defense (DoD) communication project; its target is to provide agile, responsive, robust and global networking forces, sensors, users, platforms, and applications, which are used as a first step to accomplish NCW operations. NCW is a new military doctrine that seeks to translate information advantage into a competitive warfighting advantage through the robust networking of forces distributed in large-scale conflict areas (Predd, Pfleeger, Hunker, & Bulford, 2008). In order to add to the development of the mobile networking part of the GIG, we introduced the concept of MANoN. MANoNs have various defining characteristics that differentiate them from other wired, wireless and even other ad hoc networks. MANoN is a combination of both the Mobile Ad hoc Network (MANET) (Toh, 2007) and a Network of Networks (NoN) (Spencer & Ironside, 2007; Cau, 2009), which are several nodes interconnected by wireless connections in a dynamic topology that lacks any infrastructure. Basically, each node is an ad hoc network in itself, with its own management and rules. In addition, MANoNs have the capability of operating under partial information, which makes them more flexible yet more configurable (evolvable) over time to networks joining and disconnecting, without affecting the main system. Figure 1 shows a vague idea of the GIG, consisting of different MANETs from different backgrounds and resources communicating with each other. These unique characteristics will raise non-trivial challenges for MANoNs, such as security, routing, scalability, availability, deployment considerations, media access, and Quality of Service (QoS) (Murthy & Manoj, 2004; Ilyas, 2003), in addition to conflicts which might occur because of conflicting policies (e.g. nodes following their own network policies and at the same time obeying different policies the new MANoN system might enforce) adopted by different entities in the MANoNs.

As a result, providing the components of a security management (e.g. prevention and detection) as defined by the International Telecommunication Union (2000a), is essential in order to overcome the security threats (ex. Denial of Service (DoS), host impersonation and information disclosure) our MANoN might encounter.

In this article we propose a novel, efficient, security management framework for our MANoN.

Figure 1. Global information grid showing the mobile part MANoN