Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

RIPsec – Using reputation-based multilayer security to protect MANETs

T.H. Lacey, R.F. Mills, B.E. Mullins, R.A. Raines, M.E. Oxley, S.K. Rogers*

Air Force Institute of Technology, Department of Electrical and Computer Engineering, 2950 Hobson Way, Wright-Patterson AFB, OH 45433, United States

ARTICLE INFO

Article history:
Received 25 January 2011
Received in revised form
10 August 2011
Accepted 20 September 2011

Keywords:
MANET
Ad-hoc
IPsec
DSR
Multipath
Behavior grading
Reputation
Trust
PKI

ABSTRACT

This paper examines the theory, application, and results for a Reputation-Based Internet Protocol Security (RIPsec) framework that provides security for a Mobile Ad-hoc Network (MANET) operating in a hostile environment. While there has been significant research in MANET security, the research has tended to address subsets of the overall security challenge. RIPsec leverages existing technologies to provide an overarching layered security framework that provides a more comprehensive security solution than existing approaches. Protection from external threats is provided in the form of encrypted links and encryption-wrapped nodes while internal threats are mitigated by behavior grading that assigns reputations to nodes based on their demonstrated participation in the routing process. End-to-end message security using public and private certificates protects against both internal and external threats. Network availability is improved by behavior grading and round-robin multipath routing.

Simulation results showed that the number of routing errors sent in a MANET was reduced by an average of 52% when using RIPsec. The cost in network performance for the security provided by RIPsec was a reduction in throughput. However, the reduction was acceptable given the increase in security. The network load was also reduced, decreasing the overall traffic introduced into the MANET and permitting individual nodes to perform more work without overtaxing their limited resources.

The RIPsec framework was analyzed to demonstrate its robustness against a number of well-known attacks against ad-hoc networks. Of the four features incorporated into RIPsec (encryption, IPsec transport mode, behavior grading, and multipath routing), three other frameworks incorporated two of the features (encryption and behavior grading), and the remaining eight frameworks only incorporated one of the four security features. The incorporation of all four security features at multiple levels makes RIPsec very robust against attacks.

1. Introduction

Mobile Ad-hoc Networks (MANETs) are self-configuring networks of mobile routers connected by wireless links. When one node desires to communicate with another that is out of transmission range, intermediate nodes are used to relay messages (Carruthers and Nikolaidis, 2005). MANETs have received the attention of numerous agencies due to their

* *Corresponding author*. Tel.: +1 937 255 6565.
E-mail address: timothy.lacey.ctr@afit.edu (T.H. Lacey).
0167-4048/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2011.09.005

self-configuration and self-maintenance capabilities. Their many applications include military battlefields, disaster relief efforts, conferences, classrooms, taxicabs, sports stadiums, boats, and small aircraft (Sun, 2001).

In (Bellur et al., 2002), Unmanned Aerial Vehicles (UAVs) are organized into MANETs to facilitate intra-team communications. Additionally, Fig. 1 shows how teams of MANETs composed of several military components, to include UAVs, may be organized and deployed. Live surveillance video is increasingly in demand on the battlefield to achieve information dominance (Dai and Topiwala, 2008). To this end, unmanned vehicles are currently being formulated and fielded at a breathtaking pace, some of them no bigger than paper planes (Austin, 2010). State-of-the-art video compression and transmission technology will be needed to achieve secure, real-time transmission of data by on-board sensors.

Early MANET research efforts focused on functionality (Yang et al., 2004). Security has now become a priority since MANETs are being deployed in hostile environments. For a MANET to be secure, required services include authentication, confidentiality, integrity, availability, and non-repudiation. Traditional wired security solutions do not apply to MANETs due to their "open" network architecture (nearby nodes will often be capable of sending and receiving MANET protocol packets), shared wireless medium, resource constraints, and dynamic network topology.

For example, a unique characteristic of MANET security is the lack of a clear line of defense. Traditional fixed networks have dedicated infrastructure such as firewalls, routers, and Intrusion Detection Systems (IDS) to provide protection from outside threats. However, each MANET node functions as its own router and forwards packets to other peer nodes. The wireless channel used by a MANET is open to legitimate users, eavesdroppers, and malicious attackers. No well-defined place exists in a MANET where traffic can be monitored or access controls deployed. Therefore, there is no clear separation between the "inside" and "outside" network. Since there is no clear threat to defend against, typical MANET routing protocols assume a trusted and cooperative environment. A trust environment may enable malicious nodes to disrupt network operations by intentionally disobeying protocol specifications. Nodes may also misbehave unintentionally due to hardware failure or restriction of resources, such as limited battery power.

While there has been significant research in MANET security, the research has tended to address subsets of the overall security challenge (Yi and Kravets, 2003; Capkun et al., 2003; Yang et al., 2002; Ramrekha and Politis, 2009), and (Hu et al., 2003). This paper presents a holistic security framework called Reputation-based Internet Security (RIPsec) that leverages existing technologies to provide a more comprehensive security solution. This includes a combination of behavior grading, link and message encryption and multipath routing. The main contribution of this framework is a methodology that provides a MANET capable of supporting high bandwidth applications (e.g., video and imagery) protected from both internal and external threats.

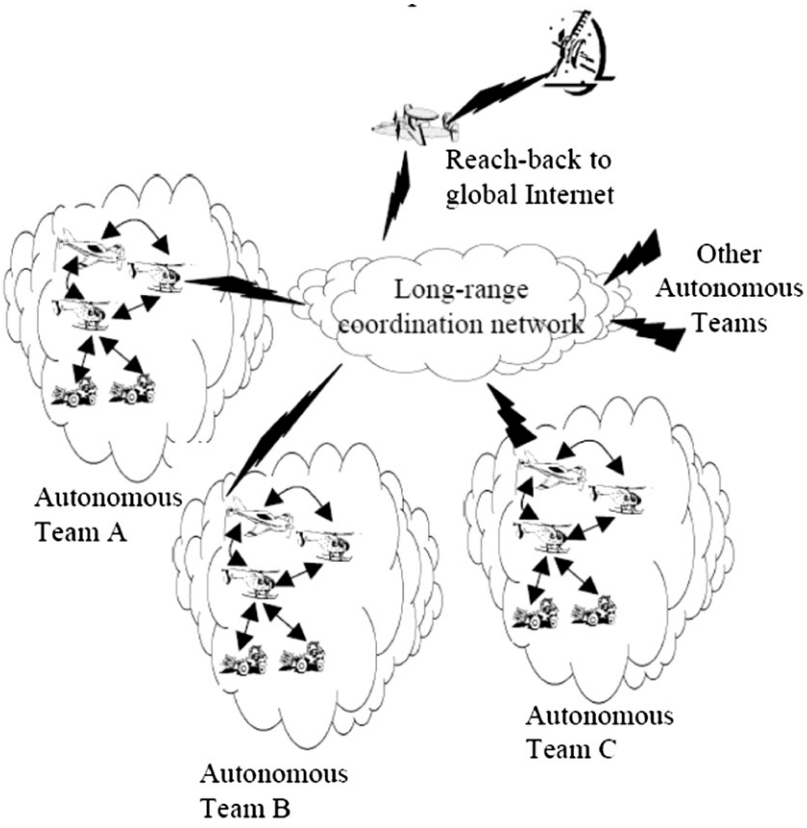

Fig. 1 – A Large-scale Deployment of Autonomous Teams in a MANET (Bellur et al., 2002).