Journal of Network and Computer Applications 34 (2011) 455–463

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Improving security in WMNs with reputation systems and self-organizing maps

Zorana Bankovic, David Fraga, José Manuel Moya *, Juan Carlos Vallejo, Pedro Malagón, Álvaro Araujo, Juan-Mariano de Goyeneche, Elena Romero, Javier Blesa, Daniel Villanueva, Octavio Nieto-Taladriz

Dpto. Ingeniería Electrónica, Universidad Politécnica de Madrid, ETSI Telecomunicación, Av. Complutense, 30, 28040 Madrid, Spain

ARTICLE INFO

Article history:
Received 15 October 2009
Received in revised form
14 January 2010
Accepted 25 March 2010
Available online 7 April 2010

Keywords:
Wireless mesh networks
Security
Reputation system
Self-organizing maps
Sybil attack
Countermeasure
Security framework

ABSTRACT

One of the most important problems of WMNs, that is even preventing them from being used in many sensitive applications, is the lack of security. To ensure security of WMNs, two strategies need to be adopted: embedding security mechanisms into the network protocols, and developing efficient intrusion detection and reaction systems. To date, many secure protocols have been proposed, but their role of defending attacks is very limited.

We present a framework for intrusion detection in WMNs that is orthogonal to the network protocols. It is based on a reputation system, that allows to isolate ill-behaved nodes by rating their reputation as low, and distributed agents based on unsupervised learning algorithms (self-organizing maps), that are able to detect deviations from the normal behavior. An additional advantage of this approach is that it is quite independent of the attacks, and therefore it can detect and confine new, previously unknown, attacks. Unlike previous approaches, and due to the inherent insecurity of WMN nodes, we assume that confidentiality and integrity cannot be preserved for any single node.

© 2010 Elsevier Ltd. All rights reserved.

1. Introduction

Wireless mesh networks (WMNs) are dynamically self-organized and self-configured, with the nodes in the network automatically establishing an ad hoc network and maintaining the mesh connectivity. WMNs are comprised of two types of nodes: mesh routers and mesh clients. Other than the routing capability for gateway/bridge functions as in a conventional wireless router, a mesh router contains additional routing functions to support mesh networking. Through multi-hop communications, the same coverage can be achieved by a mesh router with much lower transmission power.

Mesh routers have minimal mobility and form the mesh backbone for mesh clients. Thus, although mesh clients can also work as a router for mesh networking, the hardware platform and software for them can be much simpler than those for mesh routers. For example, communication protocols for mesh clients can be light-weight, gateway or bridge functions do not exist in mesh clients, only a single wireless interface is needed in a mesh client, and so on.

In addition to mesh networking among mesh routers and mesh clients, the gateway/bridge functionality in mesh routers enable the integration of WMNs with various other networks. Consequently, instead of being another type of ad-hoc networking, WMNs diversify the capabilities of ad-hoc networks. This feature brings many advantages to WMNs, such as low up-front cost, easy network maintenance, robustness, reliable service coverage, etc.

The main characteristics of WMNs are outlined below, where the hybrid architecture is considered for WMNs, since it comprises all the advantages of WMNs:

- WMNs support ad hoc networking, and have the capability of self-forming, self-healing, and self-organization.
- WMNs are multi-hop wireless networks, but with a wireless infrastructure/backbone provided by mesh routers.
- Mesh routers have minimal mobility and perform dedicated routing and configuration, which significantly decreases the load of mesh clients and other end nodes.
- Mobility of end nodes is supported easily through the wireless infrastructure.
- Mesh routers integrate heterogeneous networks, including both wired and wireless. Thus, multiple types of network access exist in WMNs.

* Corresponding author. Tel.: +34 915495700; fax: +34 913367323.
E-mail addresses: zorana@die.upm.es (Z. Bankovic), dfraga@die.upm.es (D. Fraga), josem@die.upm.es (J. Manuel Moya), jcvallejo@die.upm.es (J. Carlos Vallejo), malagon@die.upm.es (P. Malagón), araujo@die.upm.es (Á. Araujo), goyeneche@die.upm.es (J.-M. de Goyeneche), elena@die.upm.es (E. Romero), jblesa@die.upm.es (J. Blesa), danielvg@die.upm.es (D. Villanueva), nieto@die.upm.es (O. Nieto-Taladriz).

1084-8045/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2010.03.023