Journal of Network and Computer Applications 34 (2011) 492–505

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Two secure and energy-saving spontaneous ad-hoc protocol for wireless mesh client networks

Raquel Lacuesta [a], Jaime Lloret [b,*], Miguel Garcia [b], Lourdes Peñalver [c]

[a] Computer Science and Systems Engineering, University of Zaragoza, Ciudad Escolar s/n, 44003 Teruel, Spain
[b] Integrated Management Coastal Research Institute, Polytechnic University of Valencia, C/ Paranif 1, 46730 Gandia, Spain
[c] Department of Systems Data Processing and Computers, Polytechnic University of Valencia, Camino Vera s/n, 46022 Valencia, Spain

ARTICLE INFO

Article history:
Received 16 November 2009
Received in revised form
29 January 2010
Accepted 25 March 2010
Available online 9 April 2010

Keywords:
Wireless mesh client network
Spontaneous network
Secure protocol
Energy-saving protocol

ABSTRACT

We can find many cases where a spontaneous wireless ad-hoc network must be built for a limited period of time in a wireless mesh network: meetings, conferences, etc. One of the main aspects in a spontaneous network is to provide security mechanisms to the users. Confidentially, integrity, authentication, availability and no-repudiation should be provided for all the users in the network and the information should travel ciphered through the network. This paper shows two secure spontaneous wireless ad-hoc network protocols for wireless mesh clients that are based on the computational costs: the weak and the strong one. They are based on the trust of the users and guarantee a secure protocol between the users and the mesh routers. Both protocols provide node authenticity, intermediate node authenticity, integrity checking, random checking, verification distribution and erroneous packets elimination (before they arrive to the destination). The protocol procedure, its messages and development are explained in detail. Finally, we will compare their energy consumption with other secure protocols. The comparison will prove their benefits.

1. Introduction

A wireless mesh network (WMN) is a communication network made up of radio nodes organized in a mesh topology. This kind of network lets the combination of wireless and wired technologies. It has two kinds of nodes: mesh clients and mesh routers. Mesh routers use to have minimal mobility (they are usually static), use to have several wireless interfaces, and according to their connections, there could be of different types. On the one hand, there are mesh routers that act as gateways and let WMN nodes access to Internet and they are connected to other mesh routers. On the other hand, there are mesh routers with gateway or bridge functionalities that connect wired clients, wireless clients and others wireless networks through the core of the network. All mesh routers are connected among themselves by self-configuring, self-healing links forming wireless mesh backbone. So, a mesh router has several types of interfaces built on different wired or wireless access technologies. Besides, with the same level of power, the area of coverage of a conventional wireless router is smaller than a mesh router due to multi-hop communications are possible in a mesh network (Ian et al., 2005). Mesh clients can be laptops, cell phones and other wireless devices. The main difference between a mesh router and mesh clients is that the last ones do not provide gateway or bridge functions, but they are able to route other clients.

A spontaneous ad-hoc network is a computer network that is set up for a limited period of time, the nodes could be mobile and join or leave the network at any time, and the information is transmitted in ad-hoc mode (Jidong and Martina, 2001). The network has to be set up without any dependence with a central administration or expert users. The spontaneous network features was introduced by Feeney et al. in (Laura Marie et al., 2001). They have many application areas: meetings, conferences, sensor networks, hostile environments, education, etc. Spontaneous networks and ad-hoc networks have many features in common such as dynamic topology, limited bandwidth, variable capacity, energy and computing limitations, but other features are different because spontaneous networks are based on human relations and they are set up to collaborate and perform a cooperative task and services integration. These limitations should be covered by automatic management mechanisms. Many of the security issues of ad-hoc networks (such as security routing, device and users authentication, key management, etc.) can be also applied to a spontaneous ad-hoc network. But, a spontaneous network has to pay more attention to the intrusion detection because of the devices dynamism and the required user level when they are setting up the network. Configuration, management and security issues have to be performed by the devices automatically.

* Corresponding author. Tel.: +34 609 549043; fax: +34 962849313.
E-mail address: jlloret@dcom.upv.es (J. Lloret).

1084-8045/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2010.03.024