
Securing Hybrid Wireless Mesh Protocol

Eng. Mohanad Al Akel*

Dr. Nawar Al-Awa

Dr. Moutasem Shafa amry

Abstract

Wireless Mesh Networking WMN is a promising concept to provide flexible, adaptive, and reconfigurable architecture while offering cost-effective solutions to service providers. Routing is the corner stone in Wireless Mesh Network, where most of the current solutions use Ad-Hoc routing protocols. A lot of known vulnerabilities can be exploited to attack routing messages, so it is important to provide secure routing protocol for WMN.

In this paper, we present a secure extension to Hybrid Wireless Mesh Protocol HWMP, the default routing for WMN. We considered Secure Ad-Hoc On-Demand Distance Vector SAODV specification with some modifications to secure HWMP. This work also includes extending NS-3 simulator to support SecHWMP Secure Hybrid Wireless Mesh Protocol. The simulation also includes comparison with some secure routing protocols within WMN. We found that the performance of our protocol is better than other protocols in most cases.

Keywords: WMN, Hybrid Wireless Mesh Protocol HWMP, SecHWMP

For the abstract in Arabic see pages (35-52).

* Department of Networking – Faculty of Information Technology Engineering, Damascus University