MAODV: A Defense against Sybil Attacks in Wireless Networks

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 135
Number 12

Year of Publication: 2016

Authors:
Manish Kumar Suman, Sini Shibu

Abstract

Wireless networks are gaining popularity to its peak today, as the users want wireless connectivity irrespective of their geographic position. An ad-hoc wireless network is a collection of nodes that come together to dynamically create a network, with no fixed infrastructure or centralized administration. In mobile ad-hoc networks, data transmission is performed within an untrusted wireless environment. The lack of centralized infrastructure in ad-hoc network makes it vulnerable to various attacks. Sybil attack is one of the serious attacks, which form a serious threat in the networks, especially against many ad hoc wireless routing protocols, and location based wireless security system.

In the Sybil attack incorporates a malicious device with the ability to illegitimately take on several identities in the same network. The forged identity from a malicious device is called a Sybil node. A malicious device can obtain an identity for a Sybil node in two different ways; (a) generating a new identity; or (b) taking the identity from an existing node (with the cooperation of the node or by developing a spoofing attack). We identify two types of Sybil attacks.
first type, malicious nodes do not take part in finding routes, meaning that, legitimate nodes do not know their existence. In the second type, malicious nodes do create route advertisements and legitimate nodes are aware of the existence of malicious nodes, just do not know they are malicious. Some of the researchers have proposed many solutions for Sybil attack.

In this paper, an efficient method to detect a Sybil attack called modified Sybil detection AODV protocol has been proposed. Detection of Sybil attack is performed using number of hops in different paths from source to destination and delay of each node in different paths from source to destination. The destination is able to detect both kinds of Sybil attacks. The performance of modified Sybil detection AODV protocol is justified by simulations.

References


Index Terms

Computer Science  Wireless

Keywords