AU J.T. 10(4): 215-224 (Apr. 2007)

Dynamic *K*-value for Belief-based Ad Hoc Sinkhole Detection

Piyakul Tillapart, Tapanan Yeophantong, Patra Vatanasak, and Sahapak Manopimok

Faculty of Science and Technology, Assumption University
Bangkok, Thailand

Abstract

Sinkhole detection is one of the challenging issues in the area of ad hoc network security, since a sinkhole attack disrupts communications in the entire network by attracting traffic to a malicious path of the network. However, transmission failure in the ad hoc network is caused not only by the sinkhole attack but also by weak signal strength which forms a communication link. In practice, ad hoc nodes are located in different places where their environmental conditions may be different. These environments affect nodes' signal strength which would affect success of packet transmission between nodes. If a node is located in a bad environment, the node maintains poor communication links with its neighboring nodes, causing high probability of packet loss. Consequently, this innocent node becomes less trusted by its neighbors and may eventually be classified as a sinkhole. In this research, we present an approach for sinkhole detection in ad hoc networks in poor environment.

Keywords: *Sinkhole detection, ad hoc network, belief-based detection mechanism, and dynamic network environment.*

1. Introduction

A mobile ad hoc network is an infrastructureless network which is temporarily formed up from a collection of two or more mobile nodes. The nodes are capable of transmitting data packets through wireless links. The network topology is not fixed since the nodes are free to move and are allowed to join and leave the network at any time. Due to the limited transmission range of wireless links, the nodes within each other's wireless transmission range can communicate directly while distant nodes located outside their transmission ranges have to relay messages through neighboring nodes. Therefore, each node operates not only as a host when receiving/sending data from/to other nodes but also as a router when being dynamically involved in the path set up between other nodes in order to transmit data packets to arbitrary destinations (Deng *et al*. 2002; Ramaswamy *et al*. 2003; Burg 2003).

Characterized by the dynamic nature of the network topology, open medium, absence of central support infrastructure, distributed cooperation, and constrained transmission capability, the ad hoc networks are more vulnerable to various types of attacks such as eavesdropping, injected bits, fake route reply, and malicious routing attacks. By attacking routing protocols, an attacker can introduce a malicious node into a routing path between a source-destination pair in the network. Consequently, the malicious node can later drop or alter attracted data packets and generate fake route replies.

In this paper, we emphasize on a sophisticated routing attack called sinkhole attack which is a challenging issue in ad hoc network security. A sinkhole attack is caused by a malicious node which lures traffic to a malicious path of the network. The malicious node exploits an ad hoc routing protocol and attracts its neighbors by answering each route request with a fake route reply claiming to have the best path to a given destination. Therefore,