Available online at www.sciencedirect.com
ScienceDirect
Computer Networks 51 (2007) 3750–3772
Computer Networks
www.elsevier.com/locate/comnet

LiteWorp: Detection and isolation of the wormhole attack in static multihop wireless networks

Issa Khalil, Saurabh Bagchi *, Ness B. Shroff

Dependable Computing Systems Lab (DCSL), Center for Wireless Systems and Applications (CWSA), School of Electrical and Computer Engineering, Purdue University, 204-16 Airport Road, West Lafayette, IN 47906, United States

Received 12 October 2006; received in revised form 24 January 2007; accepted 5 April 2007
Available online 19 April 2007

Responsible Editor: J. Misic

Abstract

In multihop wireless systems, such as ad hoc and sensor networks, the need for cooperation among nodes to relay each other's packets exposes them to a wide range of security attacks. A particularly devastating attack is known as the wormhole attack, where a malicious node records control and data traffic at one location and tunnels it to a colluding node far away, which replays it locally. This can either disrupt route establishment or make routes pass through the malicious nodes. In this paper, we present a lightweight countermeasure for the wormhole attack, called LiteWorp, which relies on overhearing neighbor communication. LiteWorp is particularly suitable for resource-constrained multihop wireless networks, such as sensor networks. Our solution allows detection of the wormhole, followed by isolation of the malicious nodes. Simulation results show that every wormhole is detected and isolated within a very short period of time over a large range of scenarios. The results also show that the fraction of packets lost due to the wormhole when LiteWorp is applied is negligible compared to the loss in an unprotected network. Simulation results bring out the configuration where no framing is possible, while still having high detection rate. Analysis is done to show the low resource consumption of LiteWorp, the low detection latency, and the likelihood of framing by malicious nodes.

Keywords: Wireless sensor and ad hoc networks; Neighbor watch; Wormhole attack; Malicious node detection; Malicious node isolation

1. Introduction

Ad hoc and sensor networks are emerging as promising platforms for a variety of application areas in both military and civilian domains. These networks are especially attractive for scenarios where it is infeasible or expensive to deploy significant networking infrastructure. Initial research

* Corresponding author. Present address: 465 Northwestern Avenue, West Lafayette, IN 47907, USA. Tel.: +1 765 494 3362; fax: +1 765 494 2706.
E-mail addresses: ikhalil@purdue.edu (I. Khalil), sbagchi@purdue.edu (S. Bagchi), shroff@purdue.edu (N.B. Shroff).

1389-1286/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2007.04.001

efforts have focused on the realization and practical implementation of these networks by focusing on their functional attributes, such as data aggregation protocols and routing protocols. However, the open nature of the wireless communication channels, the lack of infrastructure, the fast deployment practices, and the hostile environments where they may be deployed, make them vulnerable to a wide range of security attacks. These attacks could involve eavesdropping, message tampering, or identity spoofing, which have been addressed by customized cryptographic primitives in the wired domain. Alternately, attacks may be targeted at control or data traffic in wireless networks, such as the blackhole attack [5] and the rushing attack [9]. Since many multihop wireless environments are resource-constrained (e.g., bandwidth, power, or processing), providing detection and countermeasures to such attacks often turn out to be more challenging than in their wired counterparts.

A particularly severe security attack, called the wormhole attack, has been introduced in the context of ad hoc networks [5,7,8,29]. During this attack, a malicious node captures packets from one location in the network, and "tunnels" them to another malicious node at a distant point, which replays them locally. The tunnel can be established in many different ways, e.g., through an out-of-band hidden channel (e.g., a wired link), packet encapsulation, or high powered transmission. This makes the tunneled packet arrive either sooner or with a lesser number of hops compared to the packets transmitted over normal multihop routes. This creates the illusion that the two end points of the tunnel are very close to each other. A wormhole tunnel can actually be useful if used for forwarding all the packets. However, in its malicious incarnation, it is used by attacking nodes to subvert the correct operation of ad hoc and sensor network routing protocols. The two malicious end points of the tunnel may use it to pass routing traffic to attract routes through them. They can then launch a variety of attacks against the data traffic flowing on the wormhole, such as selectively dropping the data packets. The wormhole attack can prevent two nodes from discovering legitimate routes greater than two hops away and thus disrupt network functionality. In addition, it may affect data aggregation and clustering protocols and location-based wireless security systems. Finally, it is worth noting that the wormhole attack can be launched even without having access to any cryptographic keys or compromising any legitimate node in the network [5,7].

In previous paper [28], we present a simple lightweight protocol, called LiteWorp, to detect and mitigate wormhole attacks in static ad hoc and sensor wireless networks. LiteWorp uses secure two-hop neighbor discovery and local monitoring of control traffic to detect nodes involved in the wormhole attack. It provides a countermeasure technique that isolates the malicious nodes from the network thereby removing their ability to cause future damage. We provide a novel taxonomy of the different ways in which wormhole attacks can be launched and show how LiteWorp can be used to handle all but one of these attack modes. LiteWorp has several features that make it especially suitable for resource-constrained wireless environments, such as sensor networks. LiteWorp does not require specialized hardware, such as directional antennas or fine granularity clocks. It does not require time synchronization between the nodes in the network. It does not increase the size of the network traffic, and incurs negligible bandwidth overhead, only at initialization and on detection of a wormhole. The lightweight feature of LiteWorp is in contrast to other countermeasures for wormhole attacks, which have requirements (e.g. directional antennas [8], highly accurate time measurement [21], specialized trusted nodes [29], and clock synchronization [7]) that often make them impractical for sensor networks and other classes of ad hoc networks. Finally, in LiteWorp, detection and isolation are done judiciously to minimize the possibility of victimizing innocent nodes due to false alarms caused by natural collisions in the wireless medium or due to malicious framing.

In this paper, we present a coverage analysis of LiteWorp and show the relation between the number of nodes required for local monitoring, called *guards*, and the probability of false or missed detection. Moreover, we present an analysis for the isolation latency and the framing probability with various parameters such as the number of malicious nodes. We build a simulation model for LiteWorp using the network simulator *ns-2* and perform a comparative evaluation of a network with and without the technique. The results show that with a large number of guards, LiteWorp can achieve 98.9% non-malicious routes, with 12% of the network nodes compromised. For this configuration, the possibility of false detection (due to natural collisions) or framing (due to malicious reporting) is