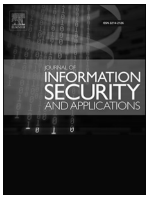
Journal of Information Security and Applications 39 (2018) 31–40

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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



Multirate DelPHI to secure multirate ad hoc networks against wormhole attacks

Shams Qazi[a,*], Raad Raad[b], Yi Mu[a], Willy Susilo[a]

[a] Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, University of Wollongong, NSW 2522, Australia
[b] School of Electrical, Computer and Telecommunications, Engineering University of Wollongong, NSW 2522, Australia

ARTICLE INFO

Article history:

Keywords:
Ad hoc networks
Wormhole attacks
DelPHI
AODV
Round trip time (RTT)

ABSTRACT

DelPHI [1] is a highly cited protocol that secures Ad hoc On Demand Distance Vector (AODV) routing protocol against wormhole attacks. DelPHI assumes that the underlying wireless transmission rate is constant. Under such an assumption it has a wormhole detection rate above 80%. In this work we show that DelPHI is unable to secure AODV in a multirate transmission environment because it does not take into account the variable bit rate nature of the wireless channel and assumes a constant bit rate leading to either false detection or no detection of wormhole attacks. We go on to propose an extension to DelPHI (M-DelPHI) that adapts it to the multirate 802.11 wireless channel. We propose three fundamental extensions: 1. Multirate channel, 2. Processing delay and 3. Neighbour monitoring. We provide 2 test cases that demonstrate our extension and simulate the new protocol in different environments. We show that M-DelPHI performs exceptionally well resulting in above 90% wormhole detection rate against inbound and out-of-band wormholes under the specified test conditions.

1. Introduction

A wireless ad hoc network is defined as a group of mobile nodes that do not rely on a pre existing infrastructure and allows all network functions to be performed by the nodes themselves. Broadcast is a fundamental operation in wireless ad hoc networks and the main reason is to propagate the data packets to all nodes in a collision free manner whilst incurring minimum latency [2]. The high mobility of nodes causes the routing information to change over time and the limited energy available across each node adds a further challenge to the network. Therefore, any node that runs out of energy reduces the network connectivity and makes the network disjoint which affects the overall network communications [3]. In ad hoc networks, it is important that a routing protocol satisfy bandwidth requirement for quality-of-service (QoS) constraints [4].

Ad Hoc networks are prone to a number of security attacks. These attacks could involve message tampering, identity spoofing due to physical security [5], jamming attack [6], eavesdropping, wormhole attacks [7], the rushing attack [8]. In [9], the authors discussed wifi channel-related and node-based attacks in mobile ad hoc networks.

A study of wormhole attacks in [10–12] reveals that this type of attack allows an intruder to capture data packets at one point and to tunnel them to other intruders further away in the network, who then broadcast them locally [13]. There are a number of ways of creating wormhole tunnels such as through packet encapsulation (inbound) or through an out-of-band channel between intruders (wired or wireless link), thus enabling the tunnelled data packets to reach their destination either earlier and/or with fewer hops compared to normal routes. By appearing to be a single hop neighbour, the transmitter is deceived into believing that the two distant points of the tunnel are very close. As shown in Fig. 1, the node S believes that the node D is its direct neighbour because of the hidden tunnel created by M_1M_2. This tunnel is used by the intruders to attract data traffic to pass through them so that various attacks can be launched. These attacks can cause disruptions such as: preventing two nodes from discovering legitimate routes greater than two hops away and thus disrupt network functionality, affecting data aggregation and clustering protocols and location-based wireless security systems. It is critical to realize that a wormhole attack does not require any legitimate node to be compromised nor does it require knowledge of the security system e.g. public/private keys, encryption/decryption etc. [10,11].

DelPHI [1] is a well known protocol that provides security to AODV against wormhole attacks. It has been widely cited in recent research against wormhole attacks in wireless ad hoc networks. A major drawback of DelPHI is that it assumes that the end-to-end

* Corresponding author.
E-mail addresses: shams@uow.edu.au (S. Qazi), raad@uow.edu.au (R. Raad), ymu@uow.edu.au (Y. Mu), wsusilo@uow.edu.au (W. Susilo).

https://doi.org/10.1016/j.jisa.2018.01.005
2214-2126/© 2018 Published by Elsevier Ltd.

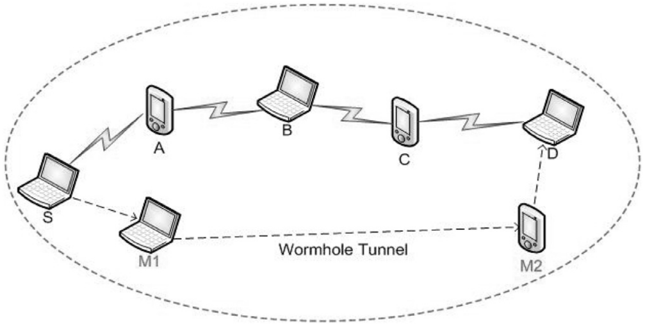


Fig. 1. Wormhole Attack - out-of-band tunnel.

multihop connection has a constant average bit rate and works well under such assumptions. In this paper, our proposed protocol M-DelPHI which extends DelPHI in 3 critical areas:

1. Multirate Wireless Environment
2. Reduced Processing Delays
3. Added Neighbour monitoring

DelPHI detects wormholes based on the measured round trip time (RTT) between source and destination when a new route is requested in AODV. The protocol obtains the packet delay at each node and the hop count information between source and destination. DelPHI assumes that a wormhole route has a significantly higher round trip time (RTT) than one without a wormhole. In addition, DelPHI does not address the problem of packet processing delay at different nodes which in fact could be higher than the transmission time. Also, processing and queueing delays exhibit a high variance depending on network load. But the critical factor that is overlooked by the protocol is multirate transmission in ad hoc networks without which detection of wormhole attacks based upon RTT calculations is not realistic. It is quite possible in some cases that higher RTT is the result of a lower transmission rate between two nodes without having any wormhole tunnel in that route but DelPHI declares such routes suspicious and discards them from the routing table hence resulting in a false positive.

This problem of only assuming a fixed end to end transmission rate is not unique to DelPHI but at present, most of the secure wireless routing protocols of which [14,15] are examples only provide security against wormhole attacks in a fixed transmission environment. This however is inadequate in preventing such attacks in an environment with different transmission rates between nodes which would be the norm. In this paper, we address this issue and provide one potential solution. Hence the proposed extension to DelPHI can be used with other protocols that rely on *RTT*.

Section 2 reviews the current literature regarding wormhole detection. In Section 3, we present two test cases to show how DelPHI fails in a multirate transmission against wormhole attacks. In Section 4, we present the M-DelPHI protocol including a protocol run, attack model and examples. In Section 5, we discuss the performance and simulation results of M-DelPHI and Section 6 presents the conclusion.

2. Related work

Existing approaches for detecting wormhole attacks can be classified into three main categories: topological analysis, special hardware/software based or delay calculation (RTT) based solutions.

In topological analysis based solutions, neighbourhood information is analysed with the help of graph theory to combat wormhole attacks. Specialized solutions use special hardware devices such as GPS, where usually strict time synchronization or special software or a specialist network protocol is used to secure against wormhole attacks. In RTT based approaches, no special (hardware/software) or topological analysis is required. The RTT is calculated between neighbours and if the RTT between two nodes is considerably higher than average then an alarm is generated for further checking.

Our solution is based on RTT calculation in multirate transmission which is not covered by any existing solution that we are aware of.

2.1. Topological based solutions

In [16], the authors proposed a wormhole detection algorithm that looks for a forbidden substructure in the connectivity graph that should not be present as compared to a legal connectivity graph. For the given node distribution and communication model, the authors first try to find the forbidden parameter f_k, which is the number of independent common k-hop neighbours between two non-neighbouring nodes. If f_k or more independent k-hop neighbours are found between any two non-neighbouring nodes, a wormhole attack is detected. However, when the wormhole detection scheme is evaluated, it is unclear how the neighbourhood discovery (ND) scheme would perform and the authors point out that the algorithm may reject valid links.

Prasannajit et al. [17] introduces an algorithm named WRTTGDD which works by calculating the RTT and geographic distance. This algorithm uses a two step operation. In the first step, hop counting and round trip time between consecutive nodes is used. In addition, every node must collect its neighbours hop counts and also use the Dijkstra algorithm to find the shortest route for every node pair based on the RTTs and hop count. In the second step, a local map is constructed by using multi-dimensional scaling (MDS). Any distortions in the local map are detected using a diameter feature. The authors considered that RTTs of all normal links are nearly the same whereas, a fake link created by attackers results in a higher value. Although, this protocol detects wormhole attacks, it fails to isolate malicious nodes to avoid any future attacks.

2.2. Special hardware/software based solutions

In [10], Hu et al. conceptualized the use of geographical and temporal leashes. Geographical leashes ensure that the distance between sender and receiver is within certain limits. While temporal leashes ensure that all packets have an upper limit on their lifetime, restricting the maximum travel distance for detecting wormhole attacks. They proposed that each node should be aware of its location and have tightly synchronized clocks. The authors assume that delays in packet processing and queueing are negligible. Further, use of this solution requires a considerably large amount of storage at each node as they use a hash tree based authentication scheme (Merkle hash trees)[18].

In [19], Garcia and Robert presented a modified version of the Split Multipath Routing (SMR) protocol [20] which allows intermediate nodes to forward repeated copies of a RREQ message, provided their hop counts are smaller than the hop counts of already received copies. The destination is able to build a list of available paths from the source as it receives numerous copies of the RREQ message, thereby providing it with a partial view of the network. This information is used by the WIM-DSR protocol to discover possible wormhole attacks. In WIM-DSR protocol, a chosen path is broadcast to the source by the destination. The intermediate nodes rebroadcast only one copy of a given message allowing them to validate the information.