Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 48 (2015) 472 – 479

Procedia Computer Science

International Conference on Intelligent Computing, Communication & Convergence

(ICCC-2015)

Conference Organized by Interscience Institute of Management and Technology,

Bhubaneswar, Odisha, India

An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network

Vimal Kumar [a] **, Rakesh Kumar** [b]

[a,b]Department of Computer Science & Engineering, Madan Mohan Malaviya University of Technology

Gorakhpur, 273010, U.P. , India

{vimalmnnit16@gmail.com, rkiitr@gmail.com}

Abstract: Security is an essential component for mobile ad hoc network (MANET). In order to provide security against attacker, researchers are working specifically on the security challenges in MANETs, and many techniques are proposed for secure routing protocols within the networks. Our proposed work presents a more efficient solution for detecting a black hole attack with less communication cost in the MANET, which is particularly vulnerable compared to infrastructure-based networks due to its mobility and shared broadcast nature. As an adversary can successfully deploy black hole attack in the network. It can be seen that proposed work is more secure than the existing solutions. We also compared its performance to standard AODV routing protocol. The experimental results show that the proposed approach is better than standard AODV.

Keywords: Black hole attack, Secure AODV, Mobile Ad hoc network

1. Introduction

Mobile ad hoc network is a collection of nodes that do not depend on any infrastructure to maintain the network connection. They may act as a source, destination or as a router. It also avoids a single point of failure due to its nature of dynamic topology. The routing protocol in a mobile ad hoc network (MANET) can be categorized into three categories, namely, table-driven/proactive, on-demand/reactive and hybrid one. They provide various

1877-0509 © 2015 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).
Peer-review under responsibility of scientific committee of International Conference on Computer, Communication and Convergence (ICCC 2015)
doi:10.1016/j.procs.2015.04.122

applications that includes, military application, disaster relief, collaborative and distributed computing, wireless sensor network (WSN), networks of visitors at airport, health and business. Development of a security protocol in ad hoc network is not an easy task due to its unique characteristics of ad hoc wireless network, namely, shared broadcast channel, insecure operational environment, lack of central administration, lack of association between nodes, limited availability of resource and physical vulnerability. An attacker can easily deploy the security attacks due to security breaches in the network [1, 2, 3, 4]. This paper is organized in the following four sections. Section 2 presents an overview of AODV routing protocol and blackhole attack. In sections 3, we discuss related work in the area. In Section 4, we propose the detection scheme for a black hole attack. In Section 5, we describe the performance evaluation. Finally, we conclude our proposed work in Section 6.

2. Background

2.1 AODV Overview: AODV is an on-demand/reactive routing protocol. In AODV, when a route to new destination needed, a source node broadcast a route request (RREQ) packet to find a route to the destination node. A valid route can discover when a RREQ reaches a destination node either itself, or an intermediate node with a fresh route to the destination node. A fresh route is a valid route entry for the destination node whose associated sequence number is greater than sequence number of RREQ packet. A route is made available by unicast a route reply (RREP) packet to a source node. A RREP packet is unicast by a destination or an intermediate node. When a link break in a route is detected, a route error (RERR) packet is used to notify other participating nodes [5].

2.2 Blackhole Attack: A malicious node uses the routing protocol (such as AODV) to advertise itself as having the shortest path to the destination node whose packets it wants to discard/replay packets. When an attacker receives RREQ packet, then they create a reply where an extremely short route is advertised. If the malicious reply reaches to a source node before the reply from a legitimate node, a forged route has been created. Once the attacker has been able to insert itself between source and destination node, it is able to do discard/replay packets passing between them [6]

دریافت فوری ← متن کامل مقاله

ISIArticles
مرجع مقالات تخصصی ایران

✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
✓ امکان دانلود نسخه ترجمه شده مقالات
✓ پذیرش سفارش ترجمه تخصصی
✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
✓ دانلود فوری مقاله پس از پرداخت آنلاین
✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات