International Journal of Cloud Applications and Computing
Volume 6 • Issue 2 • April-June 2016

Detection and Ignoring of Blackhole Attack in Vanets Networks

Chaima Bensaid, EEDIS Laboratory Computer Science Department, Djillali Liabes University at Sidi Bel Abbes, Sidi Bel Abbes, Algeria

Sofiane Boukli Hacene, EEDIS Laboratory Computer Science Department, Djillali Liabes University at Sidi Bel Abbes, Sidi Bel Abbes, Algeria

Kamel Mohamed Faraoun, EEDIS Laboratory Computer Science Department, Djillali Liabes University at Sidi Bel Abbes, Sidi Bel Abbes, Algeria

ABSTRACT

Vehicular networks or VANET announce as the communication networks of the future, where the mobility is the main idea. These networks should be able to interconnect vehicles. The optimal goal is that these networks will contribute to safer roads and more effective in the future by providing timely information to drivers and concerned authorities. They are therefore vulnerable to many types of attacks among them the black hole attack. In this attack, a malicious node disseminates spurious replies for any route discovery in order to monopolize all data communication and deteriorate network performance. Many studies have focused on detecting and isolating malicious nodes in VANET. In this paper, the authors present two mechanisms to detect this attack. The main goal is detecting as well as bypass cooperative black hole attack. The authors' approaches have been evaluated by the detailed simulation study with NS2 and the simulation results shows an improvement of protocol performance.

KEYWORDS

Ad Hoc, AODV, Black Hole, NS2, VANET

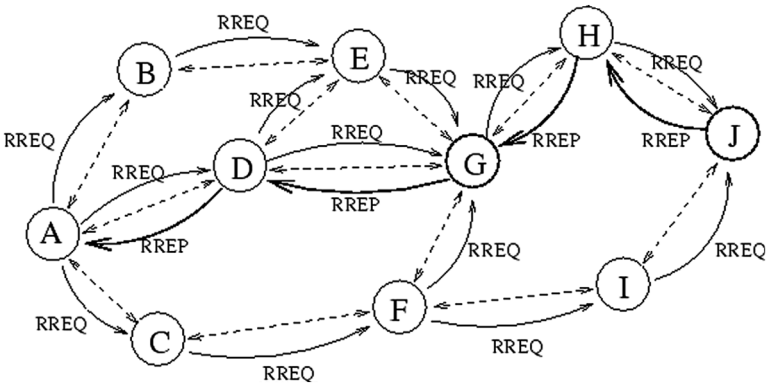
1. INTRODUCTION

Ad hoc networks consist of a set of self-organized of mobile nodes which cooperate using a routing protocol to facilitate the communication. They have become very popular in recent years due to their characteristics: easy deployment, lack of infrastructure, dynamic topology, mobility and minimum commissioning costs.

A VANET network is a subset of ad hoc networks where each mobile node is an intelligent vehicle equipped with communication resources (sensor). These networks have the same features as the ad hoc networks and can use the same routing protocols. However, the major problem of these networks is the security. Research studies indicate that wireless networks are more vulnerable than wired networks because of their characteristics as the dynamic topology, lack of infrastructure and the use of wireless links. A Black hole is a serious problem in VANETS, a malicious node exploits an existing vulnerability in a routing protocol such as in the Ad-hoc On Demand Distance Vector (AODV) by advertising a false information as the node having the shortest path to the destination and data packets are intercepted and dropped. In this paper, we proposed two solutions for detecting a Black Hole attack in VANET using as routing protocol the well-known AODV. The rest of the paper is structured as follows. In Section 2, we describe an overview of the AODV routing protocol. In Section 3, we discuss the black hole attack. In Section 4, we present a related work, in section 5,

DOI: 10.4018/IJCAC.2016040101

Figure 1. RREQ and RREP packets in AODV



we present our proposals. Finally, we preset the simulation results and performance analysis of black hole attacks and our proposals in section 6.

2. THE AODV ROUTING PROTOCOL

The AODV protocol is the most widely adopted and well known reactive routing protocol in which routes are created only when they are needed (Ochola EO & Eloff2011). The mobile devices or nodes in the network exchange the routing packets between them when they want to communicate with each other and maintain only these established routes (Ei Khin and Thandar 2014). The AODV routing protocol in an adaptation of the DSDV (Destination-Sequenced Distance Vector) protocol to get dynamic link conditions (E. Perkins & Elizabeth-Royer 2003). Whenever a node wants to send the data packet to another node, it checks its routing table. If it has a fresh route to the destination node, it uses that route to send the data packet. If it does not have a route or it is not fresh enough route, then the node starts the route discovery process. So, it broadcasts Route Request message (RREQ) to its neighbors. The intermediate nodes check whether it is the destination node or it has a fresh route to go to the destination node. If it is available, the intermediate node sends back Route Reply message (RREP) to the source node. Otherwise, it forwards the RREQ message to its neighbors by using flooding approach. This process is repeated until either the destination node or a node that has a fresh enough route to the destination is found. After finishing the route discovery process, the source and the destination node can be communicated and exchange packets between them. When any node detects a link break or failure, a Route Error (RERR) message is sent to all other nodes to notify the loss of link. Hello message is used for detecting and monitoring links to neighbors (Nital Mistry, Devesh.c 2010). Figure 1 illustrates the function of the routing protocol AODV.

External node can attack by following way (Mr. Ravi, Ms. Khushbu, 2005)(Y.-C. Hu, D.B. Johnson 2002).

3. THE BLACKHOLE ATTACK

Blackhole attack is one of the active DoS attacks possible in VANETs. In this attack, a malicious node sends a false RREP packet at the node that initiated the route discovery, in order to imposture itself as a destination node. In such a case, the source node would forward all of its data packets to the malicious node, which originally were intended for the genuine destination. The malicious node, eventually may never forward any of the data packets to the genuine destination. As a result, therefore, the source and the destination nodes became unable to communicate with each other (Ravi & Shah, 2005).