Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 113 (2017) 170–177

Procedia Computer Science

www.elsevier.com/locate/procedia

The 8th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2017)

Quality Control Chart for Detecting the Black Hole Attack in Vehicular Ad-hoc Networks

Badreddine Cherkaoui[a,*], Abderrahim Beni-Hssane[a], Mohammed Erritali[b]

[a]*LAROSERI Laboratory, Department of Computer Science, Faculty of Sciences, Chouaib Doukkali University, El Jadida, Morocco*
[b]*TIAD Laboratory, computer science department, Sciences and Technics Faculty, University of Sultan Moulay Slimane, Béni-Mellal, Morocco.*

Abstract

In recent years, a new network type has appeared as a wireless ad-hoc network to rely on between vehicles, it calls Vehicular Ad-hoc Network. The purposes of creating this type of communication network are handling traffic and ensure a safe driving by delivering some useful information to users. To guarantee this, we have to secure the communication by predicting serval security issues to handle them before setting up this network in the real life. One of these issues is the Black Hole Attack. In this paper, we propose a novel method to detect the black hole attack using a quality control chart. This method acts in real-time by monitoring the network activity using graphic representations to detect any abnormal behavior during the communication process.

Peer-review under responsibility of the Conference Program Chairs.

Keywords: Quality Control Chart, Vehicular Ad-hoc Networks, Black Hole Attack,

1. Introduction

Nowadays, communication between vehicles has become a major necessity to facilitate the conduct to drivers. This necessity has led researchers to think about a communication way for these vehicles[1]. Ad-hoc Networks are the best way to establish vehicular communication because it doesn't need a pre-existing infrastructure. This type of networks is called Vehicular Ad-hoc Networks (VANETs). VANETs are considered as a new sub-category of Mobile Ad-hoc Networks (MANETs) where vehicles communicate with each other. The main difference between MANETs and VANETs is the high speed of vehicles[2,3], which has a direct impact on the topology. The topology is permanently changing due to the high speed of vehicles which makes it difficult to manage. VANETs are used in

* Corresponding author.
E-mail address: b.cherkaoui@ucd.ac.ma

1877-0509
Peer-review under responsibility of the Conference Program Chairs.
10.1016/j.procs.2017.08.337

several applications, such as collision warning systems. This latter is used to notify other drivers to change direction to avoid congestion.

Any communication system has his vulnerabilities. VANETs vulnerabilities are not tolerable because any vulnerability can put people's lives in danger. Among these vulnerabilities, we find the black hole attack that already exists in MANETs, so it is necessarily replicated in VANETs. Security constraints in VANETs are very complex to manage in an ad hoc environment. These constraints are due to the permanent changing of the topology and the high-speed of vehicles.

The aim of this attack is that a malicious node forges the routing message to acquire a road. Then it intercepts and destroys all data that passes through it. The most discussed protocol in the literature is Ad-hoc On-demand Distance Vector (AODV). After receiving a route request (RREQ) from the source node[4], the attacker uses the weaknesses of AODV protocol to acquire the route illegally by forging the sequence number and the number of jumps in a route response (RREP) as shown in Fig. 1. Then, the malicious node intercepts data and drops them silently with transferring it to its destination node[5].

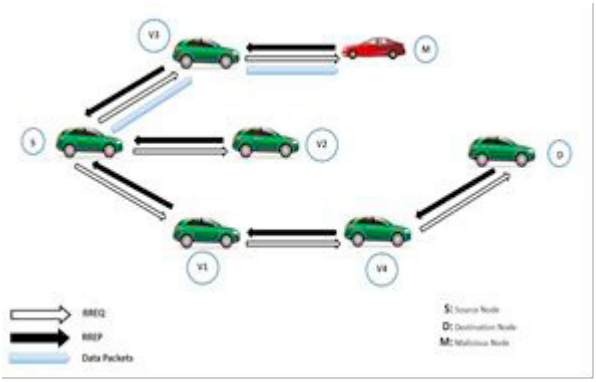

Fig. 1: The mechanism of the black hole attack

Our work is about initiating a novel method to detect the black hole attack in real-time. This method is based on a quality control chart that is widely used in industrial fields to monitor production lines. This chart is called the p-chart of fractional nonconforming.

This paper is composed of six sections with the introduction being the first. The second section discusses the works done to detect and handle the black hole attack. The third section presents the p-chart of fractional nonconforming that we mentioned earlier. The fourth section concerns the presentation of our novel detection method of black hole attack. The fifth section discusses the results of the so-called detection method. Finally, we conclude our work and offer a vision of our future works.

2. Related work

In this section, we present a general view of the works done in order to detect and eliminate the black hole attack. The most discussed protocol by researchers is AODV.

Ming-Yang Su[6] designed an anti-black hole mechanism by adopting some ids nodes to monitor a given area. Each ids node analyses the communication in his area and shares information's about any malicious behavior with the other ids nodes to isolate it from the network. This mechanism observes the difference between RREQs and RREPs diffused by a node. The nodes that are not within the IDS nodes range cannot be detected. Thus, the mechanism won't secure the uncovered areas. The widening of the geographical area means that the mechanism must increase the number of its IDS nodes to cover the entire geographical area. This can make the exchange of information much slower.