# **Accepted Manuscript**

A game theory based multi layered intrusion detection framework for VANET

Basant Subba, Santosh Biswas, Sushanta Karmakar

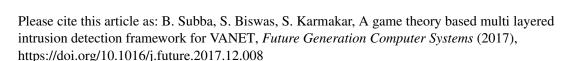
PII: S0167-739X(17)31448-6

DOI: https://doi.org/10.1016/j.future.2017.12.008

Reference: FUTURE 3846

To appear in: Future Generation Computer Systems

Received date: 30 June 2017 Revised date: 1 December 2017 Accepted date: 3 December 2017



This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.



### **ACCEPTED MANUSCRIPT**

## A game theory based multi layered intrusion detection framework for VANET

Basant Subba, Santosh Biswas, Sushanta Karmakar s.basant@iitg.ernet.in, santosh\_biswas@iitg.ernet.in, sushantak@iitg.ernet.in

Indian Institute of Technology, Guwahati India, Assam, 781039

Santosh Biswasa, IIT Guwahati\*

<sup>a</sup>Indian Institute of Technology, Guwahati

#### Abstract

Vehicular Ad-hoc Networks (VANETs) are vulnerable to various type of network attacks like Blackhole attack, Denial of Service (DoS), Sybil attack etc. Intrusion Detection Systems (IDSs) have been proposed in the literature to address these security threats. However, high vehicular mobility makes the process of formulating an IDS framework for VANET a difficult task. Moreover, VANETs operate in bandwidth constrained wireless radio spectrum. Therefore, IDS frameworks that introduce significant volume of IDS traffic are not suitable for VANETs. In addition, dynamic network topology, communication overhead and scalability to higher vehicular density are some other issues that needs to be addressed while developing an IDS framework for VANETs. This paper aims to address these issues by proposing a multi-layered game theory based intrusion detection framework and a novel clustering algorithm for VANET. The communication overhead of the IDS is reduced by using a set of specification rules and a lightweight neural network based classifier module for detecting malicious vehicles. The volume of IDS traffic is minimized by modeling the interaction between the IDS and the malicious vehicle as a two player non-cooperative game and adopting a probabilistic IDS monitoring strategy based on the Nash Equilibrium of the game. Finally, the proposed clustering algorithm maintains the stability of the IDS framework, which ensures that the framework scales up well to networks with higher vehicular densities. Simulation results show that the proposed framework achieves high accuracy and detection rate across wide range of attacks, while at the same time minimizes the overall volume of intrusion detection related traffic introduced into the vehicular network.

Keywords: Intrusion Detection System (IDS), Vehicular Ad-hoc Network (VANET), Game Theory

#### 1. Introduction

The concept of enabling vehicles with the capability to make transportation infrastructure more secure and efficient has received immense attention in recent years. This has lead to the emergence of Vehicular Ad-hoc Networks (VANETs), which are formed on the fly by a network of vehicles equipped with multiple sensors and On Board Units (OBUs). The OBUs enable vehicles to connect with Road Side Units (RSUs) through a wireless short-range direct communication link based on the IEEE 802.11p radio frequency channel. VANET uses various type of notification messages like Post Crash Notification (PCN), Road Hazard Condition Notification (RHCN), Stopped/Slow Vehicle Advisor (SVA) etc., to provide vehicular communication.

VANET uses 75 MHz of Dedicated Short Range Communications (DSRC) spectrum at 5.9 GHz to support IEEE 802.11p standard for communication among vehicles. DSRC provides a communication range of 300 to 1000 m with a data rate

VANETs use emergency broadcast messages for disseminating information about adverse road conditions and traffic accidents, which require communication between the member ve-

of more than 27 Mbps and supports a vehicular mobility as high as 200 Kmph [1]. The IEEE P1609 working group has

proposed DSRC as IEEE 802.11p standard for Wireless Ac-

cess in Vehicular Environment (WAVE) platform [2]. The

DSRC based WAVE architecture supports two different proto-

col stacks namely, the WAVE Share Message Protocol (WSMP)

and the traditional IPv6 protocol. Time sensitive and high

priority communication are achieved using the WSMP, while

the less demanding communication involving the UDP/TCP/IP

data frames are achieved using the IPv6 protocol. As shown in

the Fig. 1, the DSRC spectrum band is divided into seven chan-

nels of 10 MHz each [3]. Channel 178 is the Control Channel

(CCH), which is used for transmission of emergency messages.

The other six channels numbered 172, 174, 176, 180, 182 and

184 are Service Channels (SCHs), which are used for both both

safety and non-safety applications. If the CCH channel is ac-

tive, all vehicles are bound to stop their communication during

CCH time frame to receive and transmit emergency messages

on CCH channel.

Email address: santosh\_biswas@iitg.ernet.in(IIT Guwahati)
URL: http://www.iitg.ac.in/santosh\_biswas/(Santosh Biswas)

<sup>\*</sup>Corresponding author

# دريافت فورى ب متن كامل مقاله

# ISIArticles مرجع مقالات تخصصی ایران

- ✔ امكان دانلود نسخه تمام متن مقالات انگليسي
  - ✓ امكان دانلود نسخه ترجمه شده مقالات
    - ✓ پذیرش سفارش ترجمه تخصصی
- ✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
  - ✓ امكان دانلود رايگان 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