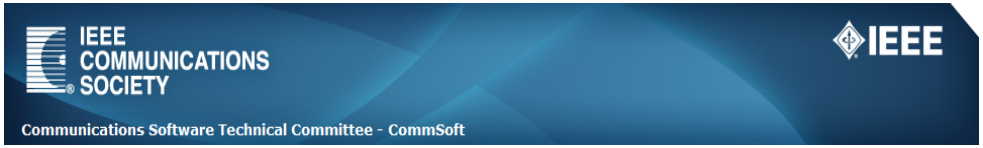
Communications Software Technical Committee – CommSoft




*http://committees.comsoc.org/commsoft/policies.html*

# IEEE CommSoft E-Letters

Vol. 4, No. 1, May 2015

## CONTENTS

# MESSAGE FROM COMMSOFT TC CHAIR

The Technical Committee on Communications Software (TC-COMMSOFT) examines methods and techniques devoted to advancement of the formal methods and tools, use of system analysis and design, methodology for development of communications protocols as well as application of general Software Engineering approaches for the purpose of development of communications applications. The issues addressed by the TC-COMMSOFT include domain-specific languages and practices of using them. Developing of "middleware" between networks and applications and the usefulness and usability of it is also a topic.
In this volume, we have selected 3 papers on three various subjects: wireless sensor networks for smart cities, routing protocols for mobile AdHoc networks and cloud computing.

# Sybil Attack Detection Survey in VANETs

Marwane AYAIDA
CReSTIC,
University of Reims Champagne-Ardenne,
Reims, France
Email: marwane.ayaida@univ-reims.fr

**Abstract:** Vehicular ad hoc networks (VANETs) are expected to play an important role in our lives. They will improve the traffic safety and bring about a revolution on the driving experience. However, these benefits are counterbalanced by possible attacks that threaten not only the vehicle's security, but also passengers' lives. One of the most common ones is the Sybil attack, which is even more dangerous than others because it could be the starting point of many other attacks in VANETs.
This paper proposes a survey of Sybil attacks' detection. The key idea here is that each vehicle will monitor its neighborhood in order to detect an eventual Sybil attack.

**Keywords:** ITS, VANETs, Sybil attack, CAM, Ad Hoc Network.

## 1. Introduction

The new mobility challenges of vehicles in Smart Cities need the enhancement of Intelligent Transportation Systems (ITS) that helps to reduce congestions, accidents, fuel consumption, etc. Thus, Vehicular Ad Hoc Networks (VANETs), which are a major component of ITS, has been a subject of some intensive research and experimental applications in these last two decades. In such networks, vehicles on the road will communicate with each others to exchange information about their directions, their speeds, their positions, the state of road, etc. Currently, the automotive industry is working to equip new vehicles with Wireless Access Vehicular Environment (WAVE) devices [1]. WAVE protocols are based on the IEEE 802.11p standard and provide the basic radio standard for dedicated short-range communication (DSRC). Intelligent Transportation Systems.

Since a successful attack could have dramatic consequences, security of Vehicular Ad Hoc Networks becomes an important issue. A well-known attack is 15 the Sybil one. This attack is considered as one of the most dangerous and the basis of many other attacks [2]. In Sybil attack, malicious node may assume multiple identities. The least harmful objective of such attack is to create an illusion of traffic congestion in order to reroute other vehicles from the road that the attacker will take. At the other end, the attacker could push a specific vehicle to take a particular route in order to trap it or, even, guide it straight to a crash in an accident. Therefore, detecting such attack is very sensitive for several safety, privacy and security reasons.

The paper is organized as follows: the section 2 presents a categorization of the Sybil attack detection mechanisms. The section 3 shows some challenges in the design of such mechanisms. Finally, section 4 concludes the paper and gives some perspectives for our future works.

## 2. Overview of Sybil Attacks detection

### a. Resource testing

Many mechanisms that aim to detect Sybil attacks have been proposed. Among them, we can cite those based on resource testing [3] (i.e. computing ability, storage ability, communication bandwidth, etc.). The idea here is that each vehicle broadcasts to all its neighbors a request that needs some physical resources to be computed. Thus, since attackers have to reply simultaneously for them and for the created fake nodes, they will not be able to reply in the given interval time and only honest vehicles will be trusted. However, this approach wastes a lot of computing resources and bandwidth for these tests. Moreover, attackers equipped with powerful computing devices can bypass these tests.

### b. Public Key Infrastructure

Another common used solutions for defending against Sybil attacks are based on Public Key Infrastructure (PKI). Since the vehicle can be authenticated with its unique public key and certificate managed by the Root Authority (RA), an attacker can be detected at any time. Traditional PKI-based certificates include only key information and do not include any unique physical information related to the vehicle. This makes such approach potentially vulnerable to impersonation attack because any stolen valid key pair and certificate can be used by another malicious vehicle to create fake nodes with valid certificates. In multi-factor authentication scheme [4], the certificate contains not only the public key information but also a set of physical attribute values about the vehicle (i.e. the radio frequency fingerprint, etc.) recorded by the Certificate Authority (CA). Nevertheless, establishing such Public Key Infrastructure for individual vehicles [5, 6] takes a long time. The use of a long-term key pairs and certificates can also make the tracking and the collecting of vehicles behaviors easier. PKI-based approaches are complex and expensive to be implemented in terms of equipments that have to be deployed. For example, we have to deploy a Root Authority (RA), a Long-Term Certificate Authority (LTCA) and a Pseudonym Certificate Authority (PCA), knowing that the PCA has to be reached by the vehicles in order to download new Pseudonym Certificates (PCs). Therefore, vehicles have to

access to the PCA through the Road Side Units (RSUs). The deployment of these RSUs is estimated to end by 2026 with a cost of 660 M€[7]. Another alternative is to take advantage from the existing cellular networks to download certificates. However, drivers have to pay this access. Moreover, vehicles will overload the cellular network if they use this media since it was not initially sized to manage this task. Moreover, even if a vehicle with a valid Long-Term Certificate (LTC) is corrupted, but not yet identified as it is, it can continue to download PCs as needed. Therefore, the PKI protection stills available for new vehicles but not really for already involved corrupted vehicles. Since all the nodes are perceived as honest by each others, this makes the detection of Sybil attacks very difficult and subsequently more difficult the defense against them [9].

#### c. Other approaches

Zhou et al. proposed a privacy preserving method to detect Sybil attacks using trustable roadside units and pseudonyms [9]. A pool of pseudonyms is assigned to each vehicle from the Department of Motor Vehicles (DMV). The latter are used to generate traffic messages instead of the real identities in order to ensure the privacy. This technique avoids also that vehicles abuse on the usage of those pseudonyms to conduct Sybil attacks since the pseudonym belonging to a vehicle is hashed to a unique value. Even though the suggested scheme which guarantees the vehicles privacy can fight against Sybil attacks, it is still need the registration of vehicles by trusted authorities such as in PKI-based approaches.

Guette and Bryce suggested a secure hardware-based method built on the trusted Platform Module (TPM) [10]. Secure information and related protocols are stored in shielded locations within the module, where any data access or changing is impossible since the platform credentials are trusted by car manufacturers. Therefore, the communication between vehicles are protected from Sybil attacks. However, as the TPM is an improved variation of a certificate, it still needing trusted authorities that can take the responsibility of managing individual vehicles. Moreover, each vehicle has to be equipped with an additional hardware (i.e. TPM), which increases the cost of such approach.

Another well-known approach to detect Sybil attacks, without a major modification of the system, is to benefit from the Received Signal Strength (RSS) [11, 12, 13] to detect if multiple messages with different identities are sent out by the same physical device. Guette et al. [10] analyzed the effectiveness of the Sybil attack in various assumptions of transmission signal tuning and antenna, and then showed the limitation of RSS based Sybil detection in VANETs.

## 3. Challenges

To tackle some limitations of the overviewed approaches, it is needed to design new Sybil attack detection mechanisms. The challenges that have to be overtaken are numerous. They will be presented in this section.

#### a. Secured

The mechanisms have to protect well the vehicles. It has not to threaten their security. The objective is to detect attackers while ensuring their safety.

#### b. Anonymous

Detection mechanisms should keep secret the identity of the drivers in order to preserve they identities. Their objectives are principally the detection of attacks and the identification of the attackers and the fake nodes. However, they have to preserve the identities of honest nodes.

#### c. Distributed

The mechanisms used for the detection have to be distributed. In fact, a centralized solution like the PKI presents a bottleneck that have to be avoided. Moreover, it is not an efficient one since vehicles have to be connected continuously to some specific servers to download certificates for example.

#### d. Easy to be implemented

These mechanisms have to be also easy to be implemented. This will make such solutions rapid and energy efficient also.

## 4. Conclusion

In this paper, we proposed a survey of the mechanisms used for the detection of the Sybil attacks in vehicular networks. There are principally three types of Sybil attacks detection algorithms. The first one is the resource testing. Every vehicle has to do some works in order to detect the fake nodes. The second category is the approaches that use the Public Key Infrastructure, where vehicles have their own certificates. Attackers cannot use their certificates for fake nodes. Many other approaches were also proposed. We decided to gather them in one category.
For our future work, we intend to study the flow traffic model in the Sybil attack detection. Knowing how the vehicles have to move could help us to detect if there is an orchestrated attack or not

**References**

[1] Al-Sultan S, Al-Doori MM, Al-Bayatti AH, Zedan H. A comprehensive survey on vehicular Ad Hoc network,J Netw Comput Appl 2014 Jan 31; 37:380-92.

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[3] J. Newsome, E. Shi, D. Song, and A. Perrig, The Sybil Attack in Sensor Networks: Analysis Defenses. Proc. of International symposium on information processing in sensor networks, pp 259268, 2004.

[4] S. Pal, AK. Mukhopadhyay and PP. Bhattacharya, Defending Mechanisms Against Sybil Attack in Next Generation Mobile Ad Hoc Networks, IETE Technical Review, vol 25, no 4, pp. 209-214, 2008.

[5] M. Raya and JP. Hubaux, Securing Vehicular Ad Hoc Networks, Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks, vol. 15, no. 1, pp. 3968, 2007.

[6] M. Raya, P. Papadimitratos, and JP. Hubaux, Securing Vehicular Communications, IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, vol. 13, no. 5, pp. 815, 2006.

[7] Study on the Deployment of C-ITS in Europe: Final Report, Website available at: https://ec.europa.eu/transport/sites/transport/files/2016-c-its-deployment-study-final-report.pdf.

[8] T. Zhou, R.R. Choudhury, P. Ning and K. Chakrabarty, Privacy-Preserving Detection of Sybil Attacks in Vehicular Ad Hoc Networks, Proc. of International Conference on MobiQuitous 2007, pp. 1-8, 2007 .

[9] G. Guette and C. Bryce, Using TPMs to Secure Vehicular Ad-Hoc Networks (VANETs), Proc. of WISTP 08, LNCS 5019, pp. 106-116, 2008.

[10] M. Demirbas and Y. Song, An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks, Proc. of International Symposium on World of Wireless, Mobile and Multimedia Networks, pp. 564 570, 2006 .

[11] S. Lv, X. Wang, X Zhao and X Zhou, Detecting the Sybil Attack Cooperatively in Wireless Sensor Networks, Proc. of International Conference on Computational Intelligence and Security (CIS '08), pp. 442-446, 2008.

[12] B. Xiao, Bo Yu and C Gao, Detection and Localization of Sybil Nodes in VANETs, Proc. of the 2006 workshop on Dependability issues in wireless adhoc networks and sensor networks, pp. 1-, 2006.

**Biographies**

**Marwane Ayaida** studied at E.N.S.E.A (High National School in Electronics and their Applications) in Cergy-Pontoise France, where he took his Engineering Diploma in Electronics of Embedded Systems in 2009. The same year he got his Master Degree in Electronics of Autonomous Systems at the University of Cergy-Pontoise in France. Marwane holds his PhD at the University of Reims Champagne-Ardennes in France on 2012. His research interests are on the interoperability modeling for embedded systems in the field of transportation. Also, his work focuses on Vehicular Communications (V2V and V2I). Specifically, he studies the routing protocols in Vehicular Ad-hoc Networks (VANETs). Currently, he is an associate professor at University of Reims since September 2013.

**- Special Interest Group on "Communication softwares for Vehicular AdHoc Networks"**
Coordinator : Prof. Hacene Fouchal, Hacene.Fouchal@univ-reims.fr

**- Special Interest Group on "NFV and SDN technologies"**
Coordinators: Dr. Adlen Ksentini, adlen.ksentini@eurecom.fr

**- Special Interest Group on "Security in Software Communication"**
Coordinators: Prof. Jalel Ben-Othman, Jalel Ben-Othman
Dr. Yessica Saavedra Yessica Saavedra
Address theoretical, conceptual and technological aspects of communication

**- Special Interest Group on "Big Data"**
Coordinator : Dr. Periklis Chatzimisios, peris@it.teithe.gr
Address new trend on Big Data and Communication software

**- Special Interest Group on "Designing Future Optical Wireless Communication Networks-DETERMINE"**
Coordinator: Dr. Scott Fowler, scott.fowler@liu.se

## TC OFFICERS AND NEWSLETTER EDITORS

**TC Officers**

| Names | Affiliation | Email |
|---|---|---|
| Lynda Mokdad | University of Paris-Est, Créteil | lynda.mokdad@u-pec.fr |
| Hacène Fouchal | Université de Reims Champagne-Ardenne | Hacene.Fouchal@univ-reims.fr |
| Adlen Ksentini | IRISA | Adlen.Ksentini@irisa.fr |

**Editor-In-Chief**

| Names | Affiliation | Email |
|---|---|---|
| Lynda Mokdad | University of Paris-Est, Créteil | Lynda/mokdad@u-pec.fr |
| Hacène Fouchal | Université de Reims Champagne-Ardenne | Hacene.Fouchal@univ-reims.fr |