VEHICULAR 2013

The Second International Conference on Advances in Vehicular Systems, Technologies and Applications

ISBN: 978-1-61208-288-2

July 21 - 26, 2013

Nice, France

VEHICULAR 2013 Editors

Heung-Gyoon Ryu, Chungbuk National University, Republic of Korea

Pascal Lorenz, University of Haute Alsace, France

VEHICULAR 2013

Foreword

The Second International Conference on Advances in Vehicular Systems, Technologies and Applications (VEHICULAR 2013), held between July 21 and July 26, 2013 in Nice, France, was an inaugural event considering the state-of-the-art technologies for information dissemination in vehicle-to-vehicle and vehicle-to-infrastructure and focusing on advances in vehicular systems, technologies and applications.

Mobility brought new dimensions to communication and networking systems, making possible new applications and services in vehicular systems. Wireless networking and communication between vehicles and with infrastructure have specific characteristics from other conventional wireless networking systems and applications (rapidly-changing topology, specific road direction of vehicle movements, etc.). These led to specific constraints and optimizations techniques; for example, power efficiency is not as important for vehicle communications as it is for traditional ad hoc networking. Additionally, vehicle applications demand strict communications performance requirements that are not present in conventional wireless networks. Services can range from time-critical safety services, traffic management, to infotainment and local advertising services. They are introducing critical and subliminal information. Subliminally delivered information, unobtrusive techniques for driver’s state detection, and mitigation or regulation interfaces enlarge the spectrum of challenges in vehicular systems.

We take here the opportunity to warmly thank all the members of the VEHICULAR 2013 Technical Program Committee, as well as all of the reviewers. The creation of such a high quality conference program would not have been possible without their involvement. We also kindly thank all the authors who dedicated much of their time and efforts to contribute to VEHICULAR 2013. We truly believe that, thanks to all these efforts, the final conference program consisted of top quality contributions.

Also, this event could not have been a reality without the support of many individuals, organizations, and sponsors. We are grateful to the members of the VEHICULAR 2013 organizing committee for their help in handling the logistics and for their work to make this professional meeting a success.

We hope that VEHICULAR 2013 was a successful international forum for the exchange of ideas and results between academia and industry and for the promotion of progress in the field of vehicular systems.

We are convinced that the participants found the event useful and communications very open. We hope that Nice, France provided a pleasant environment during the conference and everyone saved some time to enjoy the charm of this city.

VEHICULAR 2013 Chairs:

Pascal Lorenz, University of Haute Alsace, France
Petre Dini, Concordia University, Canada / China Space Agency Center, China

VEHICULAR 2013

Committee

VEHICULAR 2013 Technical Program Committee

Aydin Akan, Istanbul University, Turkey
Waleed Alasmary, University of Toronto, Canada
Marica Amadeo, University of Reggio Calabria, Italy
Andrea Baiocchi, SAPIENZA University of Rome, Italy
Irina Balan, Ghent University - IBBT, Belgium
Monique Becker, Institut Mines Telecom, France
Luis Bernardo, Universidade Nova of Lisboa, Portugal
Yuanguo Bi, Northeastern University, China
Norbert Bissmeyer, Fraunhofer SIT, Germany
Pascal Bodin, Orange Labs, France
Mélanie Bouroche, Trinity College Dublin, Ireland
Robert Budde, TU Dortmund University, Germany
Chiara Buratti, DEIS, University of Bologna, Italy
Maria Calderon, University Carlos III of Madrid, Spain
Claudia Campolo, University of Reggio Calabria, Italy
Jean Pierre Cances, University of Limoges, France
Hongyang Chen, Fujitsu Labs. Ltd, Japan
Lien-Wu Chen, Feng Chia University - Taichung, Taiwan
Ray-Guang Cheng, National Taiwan University of Science and Technology - Taipei, Taiwan, R.O.C.
Yonggang Chi, Harbin Institute of Technology, China
Dong Ho Cho, Korea Advanced Institute of Science and Technology - Daejeon, Republic of Korea
Juan Antonio Cordero Fuertes, INRIA, France
Carl James Debono, University of Malta - Msida, Malta
Stefan Dietzel, University of Ulm, Germany
Trung Q. Duong, Blekinge Institute of Technology, Sweden
Weiwei Fang (方维维), Beijing Jiaotong University (BJTU) - Beijing, China
Michel Ferreira, University of Porto and Instituto de Telecomunicações, Portugal
Alois Ferscha, Institut für Pervasive Computing, Johannes Kepler Universität Linz, Austria
Malgorzata Gajewska, Gdansk University of Technology, Poland
Slawomir Gajewski, Gdansk University of Technology, Poland
Hassan Ghasemzadeh, University of California - Los Angeles, USA
Athanasios Gkelias, Imperial College London, UK
Javier Gozalvez, UWICORE Laboratory, University Miguel Hernandez of Elche, Spain
An He, Qualcomm, USA
Khelifa Hettak, Industry Canada / Communications Research Centre - Nepean, Canada
Daesik Hong, Yonsei University - Seoul, Korea
Daniel Jiang, Mercedes-Benz Research & Development North America, USA
Georgios Karagiannis, University of Twente, The Netherlands
Gunes Karabulut Kurt, Istanbul Technical University - Istanbul, Turkey

Frank Kargl, University of Ulm, Germany
Jungwoo Lee, Seoul National University, Korea
Jingli Li, Emerson Electric Co. - Louisville, USA
XiangYang Li, Illinois Institute of Technology - Chicago, USA
Qilian Liang, University of Texas at Arlington, USA
Kuang-Hao Lin, National Chin-Yi University of Technology, Taiwan
Thomas Little, Boston University, USA
Rongxing Lu, University of Waterloo, Canada
Johan Lukkien, Eindhoven University of Technology, The Netherlands
Barbara M. Masini, CNR - IEIIT, University of Bologna, Italy
Ingrid Moerman, Ghent University - IBBT, Belgium
Hidekazu Murata, Kyoto University, Japan
Shumao Ou, Oxford Brookes University, UK
Mohammad Patwary, Staffordshire University, UK
Matthias Uwe Pätzold, University of Agder - Grimstad, Norway
Adrian Popescu, Blekinge Institute of Technology - Karlskrona, Sweden
Ravi Prakash, University of Texas at Dallas, USA
M. Elena Renda, IIT - CNR - Pisa, Italy
Tapani Ristaniemi, University of Jyväskylä, Finland
Marco Roccetti, University of Bologna, Italy
Miguel Sepulcre, University Miguel Hernandez of Elche, Spain
Won-Yong Shin, Harvard University, USA
Marcin Sokól, Gdansk University of Technology, Poland
Hwangjun Song, POSTECH (Pohang Univ of Science and Technology) - Pohang, Korea
Kemal Ertugrul Tepe, University of Windsor, Canada
Necmi Taspinar, Erciyes University - Kayseri, Turkey
Olav Tirkkonen, Aalto University, Finland
Theodoros A. Tsiftsis, Technological Educational Institute of Lamia, Greece
Carlo Vallati, University of Pisa, Italy
Wenjing Wang, Blue Coat Systems, Inc., USA
You-Chiun Wang, National Sun Yat-Sen University, Taiwan
Andre Weimerskirch, ESCRYPT Inc., USA
Chih-Yu Wen, National Chung Hsing University - Taichung, Taiwan
Weidong Xiang, University of Michigan - Dearborn, USA
Jinyao Yan, Communication University of China, China
Zheng Yan, Aalto University - Espoo, Finland / Xidian University Xi'an, China
Wei Yuan, Huazhong University of Science and Technology - Wuhan, China
Peng Zhang, Xi`An University of Posts and Telecommunications (XUPT), China
Wensheng Zhang, Iowa State University, USA
Zhangbing Zhou, China University of Geosciences - Beijing, China & TELECOM SudParis, France
Haojin Zhu, Shanghai Jiao Tong University, China
Yanmin Zhu, Shanghai Jiao Tong University, China

Copyright Information

Table of Contents

Leveraging In-Car Security by Combining Information Flow Monitoring Techniques

Alexandre Bouard*, Hendrik Schweppe*,†, Benjamin Weyl*, Claudia Eckert‡
*BMW Forschung und Technik GmbH, Munich, Germany
Email: {alexandre.bouard, hendrik.schweppe, benjamin.wey}@bmw.de
†EURECOM, Sophia-Antipolis, France
Email: schweppe@eurecom.fr
‡Technische Universität München, Munich, Germany
Email: claudia.eckert@sec.in.tum.de

***Abstract*—Modern automobiles are increasingly connected to the world and integrate always more electronic components managing simultaneously infotainment and safety functions. Much more than just a simple transportation mean, the car is now customizable and like current smartphones, it will soon allow to load and install third-party applications directly from the Internet, which raises some security issues. Until now, the car manufacturer has full control over the development process of the in-car software and in particular can perform any required security tests before the car production. The integration of untrusted pieces of code requires from now on new dynamic security mechanisms operating during the life time of the car. In this paper, we present the integration of data flow tracking tools in an automotive middleware allowing dynamic security monitoring of untrusted applications. We describe the implementation and integration of these mechanisms and provide their evaluation.**

***Index Terms*—automotive applications, security, privacy, information flow controls, data flow tracking**

I. Introduction

Today automotive applications are deployed on on-board electronic platforms before their delivery and in-car integration. They are usually designed and programmed specifically for a brand or even for a precise car model. The car manufacturer always knows the application developers, either because they directly belong to the company or are working for a subcontractor, and can therefore contractually set certain responsibilities and testing processes. This clear relationship allows to pinpoint potentially arising liability issues if the security is broken. However, this model does not necessarily protect from security weaknesses [1] and leaves very little room for a flexible deployment. In contrast to this aforementioned pre-assembly-line development, loadable and on-the-fly installable applications have revolutionized the mobile device world and are now coming into cars [2]. While being foreseen only for the infotainment domain, they bring a number of risks that can hardly be deemed. With access to Internet and to a wide range of on-board functions, these "apps" may secretly do more than they appear to do under the hood [3] and may lead to severe driver's privacy infringements or even worse to life-threatening issues. The architecture for deploying and running such "apps" needs to be secured accordingly.

Dynamic data flow tracking (DFT) has been successfully applied in various security domains: exploit detection [4], malware analysis [5] and system monitoring [6]. It allows to tag and track data of interest as they propagate within a running application. Our approach presents the combination of two information flow control (IFC) approaches in order to secure, with acceptable performance, the execution environment of original on-board applications and third-party applications (TPAs) against security exploits and privacy infringements. DFT is locally applied to monitor TPA and is integrated in a car-wide security framework enforcing a decentralized IFC model. The main contributions presented in this paper are:

- A new *authorization model* combining local DFT techniques and car-wide IFC mechanisms.
- A *prototype implementation* integrating an automotive and IP-based communication middleware, *Etch* [7] and a DFT tool, our customized version of *libdft* [8].

The rest of the paper proceeds as follows. After giving a brief overview in Section II about the on-board automotive architecture and related work, Section III introduces our model combining two different information flow control techniques. Then, Section IV presents the implementation and integration of the security tools in an automotive middleware. Section V provides the evaluation of our concepts and prototype and finally Section VI our conclusions.

II. Scope of this Work

This section summarizes background information on future automotive systems and related work about security & privacy. A threat model and relevant scenarios are provided as well.

A. Current and Future Automotive Architectures

The automotive on-board network includes up to 70 Electronic Control Units (ECUs). ECUs are organized in subnetworks around specific domains (e.g., power train, infotainment), interlinked by different communication buses, e.g., CAN, MOST. On-board applications are divided into elementary function blocks, which are distributed over several ECUs and use broadcast to exchange data. Due to plaintext on-board communication and a lack of input validation in the ECUs, cars have been shown weak against simple attacks [1].

Tomorrow, Ethernet/IP will be used as communication standard for the on-board network and will provide a larger bandwidth. It will allow comply with the future application requirements for driver assistance and infotainment, which require large volume of data to be processed at real time [9]. Secondly, secure and mature protocols from the Internet will be immediately applicable. Then, the use of engineering-driven middleware will greatly simplify the communication management. It will abstract and automate the network addressing and security enforcement [10]. Finally the centralization of most of the external communication interfaces (e.g., LTE, Wi-Fi) around a multi-platform antenna (called proxy here) will give to car makers the opportunity to design a single security gateway for all Car-to-X (C2X) communications [11].

B. Threat Model and Attack Scenarios

Securing today's and tomorrow's car is challenging. Automotive applications are rarely updated and involve more and more new connected features. Their functional behavior relies on complex software, not free from any security weaknesses [1] and processing a huge amount of sensitive data. An attacker could therefore leverage defects in the logic of an application or in a weak security mechanism. The car could therefore leak private information or industrial secrets, have its integrity threatened and endanger the life of its occupants.

Our scenario is depicted in Figure 1 and considers both internal and external communication partners. We take the example of a TPA running on the Head Unit (HU), which is connected to services of the Internet, a CE device and to several original on-board applications. We mainly focus on attack scenarios trying to bypass security policies and taking advantage of the TPA in order to 1) corrupt internal resources or 2) release sensitive data to an unauthorized external entity. We consider a TPA, which respects the internal API of the car. However, it may present some weaknesses that are exploitable by an attacker.

1) **Integrity attack scenario**: the TPA forwards malicious messages from an external malicious communication partner or gets compromised. As a result the TPA may send bogus packets on the on-board network or access/modify critical resources on the HU and may dangerously disturb the car functioning.
2) **Confidentiality attack scenario**: the TPA accesses private/secret information, like the driver's home address in the navigation system. The TPA, even without the authorization to share it, may still send it to the outside, either directly over the proxy or through an intermediate step, e.g., an on-board application communicating with the outside.

This work aims at enhancing the information security and tackling the threats related to unfair entities, on which the car manufacturer has no control, while still keeping the car's requirements for high robustness and low latency in mind.

Assumptions: Next-generation ECUs will be equipped with a security middleware allowing on-board communications over strong security protocols like IPsec [10]. In addition they will soon make use of secure hardware extensions providing secure boot and secure key storage [12]. As a consequence, we assume that the middleware and the hardware platform are flawless and cannot be compromised. Finally, we trust the ECUs to establish secure communication channel with each others and to enforce the expected security mechanisms. We do not consider denial-of-service attacks in this work.

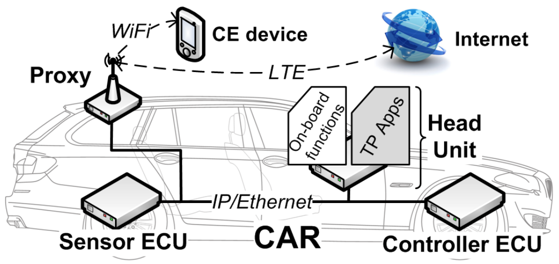


Fig. 1. Automotive scenario and considered communication channels. Solid right-angle lines represent the wired on-board network. The dashed arrows represent external communications over different wireless networks.

C. Related Work

DFT is not a new research topic, many DFT tools have already been implemented and tested for various security purposes, mostly for malicious code detection and information leakage. The main idea is to recognize data of interest according to predefined policies, to associate them with metadata called "taint tags" and to track their propagation within a running application or system. Two classes of tools can be distinguished: the single-process- and the cross-process-ones.

Single-process DFT tools [4], [8] instrument every machine instruction performed by a process. To do so, they generally make use of dynamic binary instrumentation (DBI) frameworks like Pin [13]. They usually suffer from significant decrease performance and need additional memory for taint propagation. They do not require source code modification or customized OS.

Cross-process DFT tools capture system-wide data flow and usually rely on modified runtime environments [6], emulators like QEMU [5] or hardware extensions [14]. They are usually heavyweight systems requiring an extensive maintenance. They instrument every instruction performed in the host and as a consequence impose a very significant overhead for the overall system. TaintDroid [6] alleviates the issue by regarding some libraries as "trusted", i.e., not monitored.

Solutions for **DFT in distributed systems** generally offer little reusability and require every peer to run the DFT tool, e.g., DBTaint [15], targeting data flow in data-bases, Neon [16] using a modified NFS server to track the taints of inbound/ outbound packets. Taint-Exchange [17] presents a generic framework based on libdft [8] allowing exchanges of taints over the network without proposing any concrete security model or policy enforcement. Another interesting automotive approach [18] proposes a security model using a DFT tool and network taint exchanges for every application running on the on-board network. While enhancing the security, we believe that such approaches will not meet the automotive latency requirements, if every on-board application is instrumented.

IFC is a general term. It usually designates a type of mandatory access control, allowing an entity, e.g., a person or a process, to access a resource depending on its clearance. IFC models have been already applied to secure distributed systems e.g., at the process level in customized OSes exchanging labeled messages through the network [19] or thanks to customized switches and a central synchronization server [20]. In opposition to DFT, these approaches provide better performance. They protect the information confidentiality and integrity, but do not protect against security vulnerabilities.

Outcome: Considering our requirements for low latency, we orient our approach towards efficient single-process DFT. The TPA is monitored, while trusted applications of the HU are not monitored. Potential misbehavior of the TPA is locally contained by the DFT tool. Communications between the TPA and other on-board applications are secured thanks to the enforcement of car-wide IFC policies.

III. A Combined Approach

The middleware is a software layer, common to every on-board application, including the TPA. Our approach makes use of the middleware to link the DFT tool and its local action to the security framework enforcing car-wide IFC policies. The rest of the section explains in more detail A) how the DFT tool works, B) how DFT tools and trusted on-board applications securely communicate, and C) how the DFT monitoring is integrated with a car-wide IFC framework.

A. Tracking and Controlling the Execution

DFT tools are characterized by three main elements: the taint sources, the intra-taint propagation and the taint sinks. For this subsection, we consider the pseudocode of Figure 2.

Taint sources: Taint sources are programs or memory locations, where data enter the monitored system after the invocation of a function or of a system call. If recognized as data of interest, they are tainted and tracked. Based on our scenarios, we identify all traditional I/O channels used by the TPA as sources : inter-process communication (e.g., pipe), filesystem and network socket. For instance, we monitor the functions “receiveBuffer()” (line 1) and “readBuffer()” (line 2) and tag the buffers “x” and “y” accordingly.

Intra-taint propagation: During runtime, tainted data are tracked while being copied and altered by the application execution, like in the function “processBuffers()” (line 3), which generates some data out of two tainted buffers that is tainted as well. The taint information is stored and dynamically propagated in a shadow memory mapped to the actual process memory. The taint expressiveness can be adapted depending on the needs. Originally DFT was used to protect software vulnerabilities from being exploited and a simple binary tainting was sufficient to track untrusted data (e.g., one bit tainting a byte of memory). But considering our goal to both protect the system integrity and the information sensitivity, we require more possible taint values with regard to the input sources. In practice, to limit the execution and communication overhead, we use four values: (3) for highly sensitive data of the car manufacturer (e.g., industrial secret) (2) for user’s very private data (e.g., location, routes), (1) for user’s private data (e.g., username, preferences) and (0) for nonsensitive data. This scale does not reflect data integrity, because by definition TPA cannot be trusted to produce data that are safe to directly process.

```
                                              | Shadow memory, taint of
                                              |    x      y      z
0:                                            |   (0)    (0)    (0)
1: buffer x = receiveBuffer(from_a_ECU);      |   (2)    (0)    (0)
2: buffer y = readBuffer(from_sensitive_file);|   (2)    (1)    (0)
3: buffer z = proccessBuffers(x, y);          |   (2)    (1)   (2,1)
4: write(z, in_output_file);                  |   (2)    (1)   (2,1)
5: sendBuffer(z, to_another ECU);             |   (2)    (1)   (2,1)
```

Fig. 2. On the left, an example of code with data dependencies (in bold, the data to taint). On the right the intra-taint propagation for the buffers x, y, z along the code execution.

Taint sinks: Like sources, taint sinks are function calls and memory locations, where the presence of a taint is checked in order to enforce a policy. The policies concern decision about transmitting data to a specific function, or using the data as program control data (e.g., return address). It determines whether the data can be written to a standard output (e.g., in a file, line 4) or sent over the network (line 5).

B. Middleware-based Taint Propagation

DFT tools allow to eliminate numerous attacks related to stack pointer overwriting, like buffer-overflow or format-string exploits. Other trusted automotive applications are not instrumented and directly communicate with the untrusted TPA. Thanks to the middleware and the exchange of security metadata, the DFT tool can share the intra-taints with other on-board applications.

Extra-taint propagation: Figure 3 shows the propagation of taints between a TPA and other on-board applications on other ECUs. The system calls, related to the network socket management (lines 2, 5 in Figure 2 and bullets 3, 4 in Figure 3) are intercepted by the *Injector*. For inbound messages (bullet 3), the *Injector* checks if the trusted applications is allowed to communicate with the TPA, extracts the taint of the payload from the middleware header and taints the received data in its shadow memory. For outbound messages (bullet 4), the *Injector* checks if the TPA is allowed to communicate with the addressee and adds the taints related to the message payload in the middleware header. Both sides of the communication establish a secure communication channel.This prevents any unauthorized taint manipulation or eavesdropping during the message exchange. After the message reception, the middleware of the receiving application extracts the taint values from the payload and enforces the related security policies.

Middleware enforcement: Unlike the DFT framework, the middleware of an on-board application enforces static policies and cannot be aware of each new TPA’s requirements and policies. The middleware therefore enforces a taint-based filtering involving generic rules for all TPAs. The middleware trusts the DFT framework to communicate accurate taint values. The

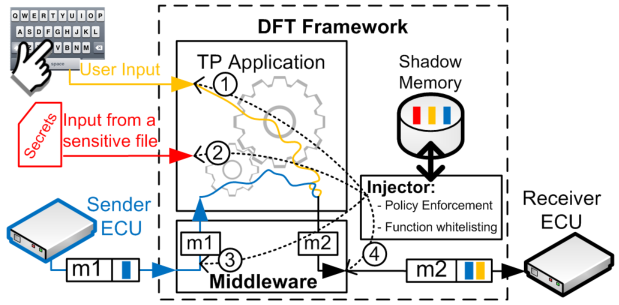


Fig. 3. Overview of the DFT framework. The solid lines show the input and output data of the TPA. The colors represent different levels of sensitivity, that are expressed by the taint values (i.e., blue/yellow/red and 1/2/3). These taints are injected using binary instrumentation (*Injector*). The *Injector* monitors the execution, especially system calls (dotted lines) and the propagation of memory and registers. $m1$ and $m2$ are tainted messages sent respectively to and from the TPA. The TPA output $m2$ shows a combination of the sources blue and yellow but not red and is therefore tainted accordingly.

taint values inform the middleware whether the data may be sensitive. The integrity of the data cannot be assessed, but TPA and middleware communicate through a dedicated channel. The middleware is therefore aware of the integrity risk. It first decides, whether it can process the payload depending on its version and its security level. and then evaluates, based on the taint values, which DFT/IFC rules of Section III-C to enforce.

Security policies: In order to control the data flows in the HU and over the network, we identify two types of policies: the first ones regulating the network exchanges and the DFT engine (middleware- & DFT-specific), the other ones locally enforced for a specific TPA (application-specific).

a) *Middleware- & DFT-specific policies*: Defined by the car manufacturer, these rules are static and defined during the design phase. They regulate the communication establishment between on board applications and specify the rules for IFC and for the interface DFT/IFC. Taint values and related source, propagation and sink tainting rules are statically set in the DFT engine by the car manufacturer

b) *Application-specific policies*: These policies only concern the TPA. When loaded on the ECU, the TPA is supplied with a customized rule set defining the associated permissions. These new rules are evaluated against the static ones and integrated in the DFT framework. Similar to the manifest provided by every Android application, the rule set provides more detailed policies and function whitelisting. For obvious security reasons, the rule set will have to be approved and signed by the car manufacturer after a testing process. In addition, other privacy-relevant policies may be specified directly by the user thanks to an on-board configuration interface.

C. Combining DFT & Car-wide IFC Enforcement

DFT provides efficient ways to control a TPA and to add/extract information from the in-band middleware protocol. However, because they monitor every single instruction of an application, they impose a significant overhead. As a consequence we chose to limit the taint information to four values. On-board applications are exchanging data which belong to different drivers or passengers and require different levels of integrity, e.g., to trigger a safety mechanism. Four taint values may lack some expressiveness. We therefore chose to couple the DFT mechanisms to a solution offering more flexibility: an automotive IFC framework.

Automotive IFC Framework: Our work about IFC in cars has been recently submitted [21] and makes use of a model inspired from Dstar [19]. We define as service, a group of on-board applications running on top of the same middleware and sharing the same security concerns in term of integrity (e.g., because they get access to the same safety mechanisms) and confidentiality (e.g., because they share data of same sensitivity). IFC is about controlling and monitoring which pieces of information are exchanged through the network between services. The goals of our framework are twofold. First it allows to control the access to on-board resources, e.g., service or file. The IFC framework makes sure that the access enquirer has a sufficient integrity level. Then it allows to prevent information leakage, caused by unintentional bugs and unfair external peers, like CE devices and online services.

Every service/user is assigned a label, i.e., a set of tags. Tags are unique values qualifying for each service/user either its integrity- or its confidentiality-concerns (i.e., the sensitivity of the information it processes). These labels form a lattice enforcing a form of mandatory access control, where information from a service can flow to a second one only if it fulfills certain conditions. Concretely, in order to send a message from A to B, the confidentiality tags of A have to be included in the label of B and the integrity tags of B in the label of A. When enforced, these conditions allow to preserve first the information confidentiality, i.e., A is sure that B is authorized to receive its message, and then the information integrity, i.e., B is sure that A provides a suitable integrity level and can therefore process the received information. Then depending on the use case, a service can "own" a tag, which means that for more flexibility it can chose to not enforce the condition linked to it. For example, the proxy owns several user confidentiality tags, i.e., reflecting the confidentiality concern of a user This allows the proxy to be able to receive information from several users of the car. A confidentiality tag of a user U in its label would constrain it to receive information only from U.

The enforcement of the IFC policies is performed in the middleware of each service each time a message is received or sent. The security logic is isolated from the application logic. Because a service is not necessarily aware of the label used by another service, the middleware of the sender adds some metadata to the message payload describing the label, on which the receiving middleware has to enforce the IFC policy. The tags in a service label are static and defined by the car manufacturer at design time. Only user tags can be generated by the proxy during runtime, e.g., when a new user get logs into the car. In this case, the proxy can grant the ownership of the new tag to some services like the HU. It allows these services to securely handle the data of the user and the communications with the TPAs (see next paragraph "IFC/DFT Interface"). Labels and tags are only for an on-board usage and we only trust on-board services to enforce the IFC rules. External communication partners and TPAs do not enforce any of them. Messages to and from the outside are filtered by the proxy based on IFC rules. Messages to and from a TPA are filtered and linked to IFC rules by services authorized to communicate with it. In comparison to DFT, the IFC framework controls the data flows at a coarser level and provides better performance, a necessary requirement when dealing with time-critical mechanisms.

IFC/DFT Interface: This interface concerns the services allowed to communicate with the TPA. The applications of the concerned services are not aware of this interface. Their middleware links IFC labels to DFT taints. The TPA is not assigned any label like a service, but a user identity is linked to it. Along with the taint field, an identity field is added to the header of each messages from and to the TPA.

Every authorized service can send data to the TPA without constrain. The service middleware makes sure to taint the message header with (3), if the data are sensitive for the car manufacturer. For the driver's private data, the service taints the message as (2) or (1) depending on the information sensitivity. The middleware adds the identity field of the user whose information are private and the DFT framework makes sure that this identity is the same as the one the TPA has been assigned to, otherwise it ignores the message.

For every tainted message coming from the TPA, the middleware adapts its processing based on the received taint:

- a taint (3) forces the middleware to make sure that the data do not leave the car. The proxy will not forward such data to the outside. A service, whose applications send information out (i.e., with a user tag in their label), will not process them.
- the taint (2) and (1) impose the middleware to own the user confidentiality tag or have it in its label, in order to pass the data to its applications. The difference between (1) and (2) allows the proxy to forward data with taint (2) only to very trusted external peer, e.g., the user's CE device and (1) to less trusted ones, e.g., Facebook.
- a taint (0) does not impose any constrain, the service can freely use the data in any way, it wants.

Traditional IFC [19], [21] classifies every output of a TPA, which receives sensitive information, as necessarily containing sensitive information as well. DFT allows us to follow the exact processing of the sensitive data, so that not all outputs of the TPA need to be considered highly classified. But DFT does not consider data integrity. All output of the TPA can be potentially dangerous. Only middleware layers performing input validation should be authorized to process these outputs.

IV. Implementation

This Section describes the integration of a DFT tool with our IP-based automotive middleware.

Middleware: For the implementation, we chose the middleware Etch, an open-source software project under the Apache 2.0 license. Etch proposes a modular and extensible architecture providing an efficient serialization and is considered as a serious candidate for the automotive purpose [22]. We used its C-binding and extended the header for our 2 middleware versions: with a field of 8 bytes for the IFC version (4 for the integrity tags, 4 for the confidentiality ones) and with a identity field of 4 bytes and a taint field of 4 bits for the DFT version (each bit expressing the presence of a taint). Label serialization/extraction and enforcement is performed in the software logic of the middleware.

Then we developed an Etch proxy in C, similar to the one in [11]. The proxy provides two secure communication interfaces: external over SSL/TLS and internal over IPsec. Internal and external communication partners communicate over a mirror-service, making the communication decoupling completely transparent. The proxy is application-unaware. Either it extracts the label/taint field (depending on the message target) from the payload of an outbound message and enforces the required policy, or it adds a label/taint field (depending on the message source) to the inbound message. User tags and identity for DFT are based on the name provided by the client certificate of the SSL/TLS connection.

The DFT Tool: We use the DFT framework libdft [8]. libdft relies on the Intel's Pin [13] for DBI, i.e., in order to inject custom code into an unmodified binary during runtime. libdft allows to instrument machine instructions, system calls to track data flows between registers and memory locations. It can also raise a warning or stop the runtime in case of unauthorized behavior. This tool provides good performance in comparison of other frameworks [18] and a well-defined API for a customizable security enforcement.

More than just using libdft, we extended its expressiveness to the four taints mentioned in Section III-A, one byte of process memory being tagged by two bits of the shadow memory. We limited ourselves to four taints, in order to keep the size of the shadow memory reasonable and to provide an efficient taint propagation and management, locally for the DFT tool and for the other services. We extended libdft with the possibility to taint differently a user input (i.e., input from the keyboard) from a file input. The framework manages the access to files present on the HU thanks to a white-list specifying for each TPA how to taint information read from a file and how data should be tainted in order to be written in a file. The framework monitors system calls related to network inputs and outputs. It allows us to taint data of the ingress traffic depending on the received taint value. For outbound messages, the framework automatically determines the taints of the payload and injects them in the header.

Testing environment: We performed the implementation and experiments of Section V-A on computers interlinked with Gigabit Ethernet and running standard 32-bit Fedora Linux on an Intel Atom N270 (1,6 GHz) with 1GB RAM. This configuration is comparable to current unix-based HUs, which operate at 1,3 GHz [23]. Besides, we did not do extensive modifications of the Etch middleware mechanisms, which already provides suitable performances when tested on a microcontroller [22]. Therefore we believe that the addition of a simple IFC/DFT access control layer should not significantly slow down the middleware. This needs, however, to be verified for a more rigorous validation.

V. Evaluation

In order to evaluate our system, in this Section we quantify the overhead of our implementation and discuss its security.

A. *Performance Evaluation*

We measure the middleware throughput (in call/sec) between a CE device and an on-board TPA, running on the HU, in order to demonstrate the overhead of our DFT/IFC framework. Benchmarks are run on three separate machines running Etch services: a CE device, a proxy and the HU. The CE device sends a simple Etch message containing an integer to the TPA. The TPA retrieves a series of integers from a file on the HU. Based on the received numbers and information read from the file, it computes an answer and sends it back. We vary the size of the returned buffer to stress the middleware and taint propagation mechanisms. The TPA plays the role of a server, providing infotainment content to the CE device (e.g. music, picture). The messages go first through the proxy, then through a trusted HU service and finally to the TPA. IFC rules are enforced between proxy and HU service. Our results, in Figure 4, present the throughput performances of this scenario for various security levels and buffer sizes. We first measured them without any security feature enabled as reference (1). We then performed the same tests when adding the communication encryption (2) (SSL on the link CE device–Proxy and IPsec for the link Proxy–HU) and the enforcement of IFC rules (3), in order to determine a lower bound overhead imposed by the security framework without DFT. We finally repeated the measurements, while adding the DFT-based monitoring of the TPA (4) and evaluated its impact.

Discussion: We realized that, when normalized, the performances with the different enabled security features are proportionally the same regardless of the buffer size. We present the normalized results in Table I. It shows that the encryption is responsible for the most significant part of the system overhead (∼43%). The impact of the IFC framework between proxy and HU service stays minor in comparison (∼4%). The DFT monitoring decreases the system performance by 22%. This penalty is mostly due to the instrumentation of the sockets and the taint propagation. With DFT enabled, the use of bigger buffer is more suitable and achieves a relatively large bandwidth (up to 1,23 Mbit/sec). The use of DFT and IFC can therefore be suitable for infotainment use cases involving a CE device and requiring moderate bandwidth. Our example makes use of a communication between proxy and HU, in order to show the impact of using IFC and DFT simultaneously. Direct communications CE device–TPA over the proxy reach a bandwidth of 2,17 Mbit/sec with DFT and encryption.

However, our evaluation is mostly focused on our middleware in a small 3-node network for a specific scenario involving a simple TP application. Tests performed with libdft for bigger applications like a web-browser [8] or a MP3-player [18] have shown more significant latency. For optimal performances, the TPAs should remain small and simple and maximize the use of "trusted", i.e., non monitored, libraries. Additional investigations in larger network producing more traffic are recommended for further validation.

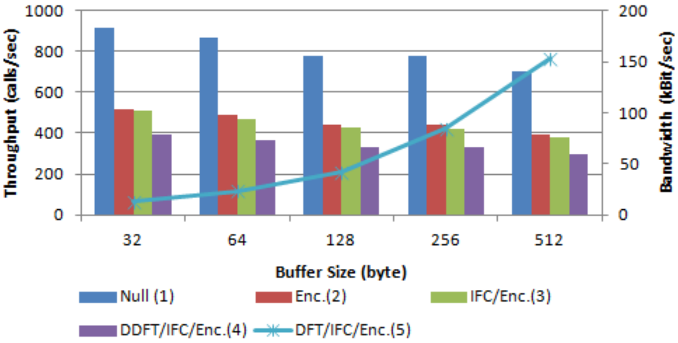


Fig. 4. Middleware throughput (1-4) and bandwidth (5) average for various buffer sizes and security features enabled (Enc.: The communications are encrypted, IFC: IFC rules are enforced, DFT: the TPA is monitored).

TABLE I
NORMALIZED PERFORMANCE OF THE SCENARIO IN SECTION V-A.
FACTOR (I) AND (II) TAKE RESPECTIVELY (1) AND (3) AS REFERENCE.

	Null (1)	Enc. (2)	IFC/Enc. (3)	DFT/IFC/Enc. (4)
Factor (i)	1	0.57	0.55	0.43
Factor (ii)	-	-	1	0.78

B. *Security Discussion*

For this section we describe how our system would react to the attack scenarios of Section II-B. Both scenarios feature an attacker taking control of the TPA, e.g., through a buffer overflow vulnerability. The DFT framework is designed and configured to detect attacks involving the overwriting of stack pointers and can stop the application. As a result an attacker cannot compromise the integrity of the TPA.

About the integrity scenario: This scenario considers an unauthorized access to car resources that may disturb the car functionality, e.g., access to a process, file of the HU or to critical services on other ECUs. The DFT is configured to block every system call involving the access of shared memory, filesystem and inter-process communications and restricts the ones concerning the access to HU files and network sockets. The TPA is therefore constrained to write in the files that have been whitelisted by the rule set provided by the car manufacturer. In a same way, the TPA is able to communicate only with services that have been authorized and therefore never gets access to highly critical services, e.g., brake controller. The TPA cannot directly get access to a HU service, except through a socket, but it has to be authorized to do so. Besides, in case of an unsuitable rule set, the contacted middleware can still ignore the message if it considers it does not provide the necessary security mechanism, e.g., input validation. However, this system does not protect against denial-of-service attacks.

About the confidentiality scenario: This scenario mostly considers the release of sensitive information to the outside. As said earlier, the TPA is constrained to whitelisted files, its capacity to write and read are controlled as well. Every data read from a file or received from another service are tainted with a value related to the sensitivity of the file or to the values present in the message header. This taint is propagated during runtime. In order to release data, the TPA either write the data into a file, whose access is whitelisted, or send them through the network to another authorized service. We do not consider information leakage through a file here and focus on the network exchanges heading out, i.e., through the proxy. The TPA may directly contact the proxy. The proxy, based on the taint of the message header, decides whether it may forward to the outside. The TPA may decide to choose an indirect way to reach the proxy: through another service, which communicates with the outside. When receiving a message from the TPA, the service middleware decides whether it can process the data or not. Having a user tags in its label generally means a high chance to forward data to the outside, so the middleware should refuse data tainted with (3). On the other hand, services with internal service tags, are not likely to have their information sent to the outside. However the tag-ownership concept may still allow such information to be sent out, therefore the decision to process (3)-tainted depends on the use-cases the ECU is involved in and is set by the car manufacturer. As for (2)- and (1)-tainted data, they can be processed only by services owning or labeled with the user tags related the user identity contained in the message header. This allows to share private information to services respecting the user's privacy. However this does not allow to maintain the difference between the 2 types of sensitivity.

Unlike OSes like Android, which controls applications with a limited set of coarse permissions, DFT allows a very fine granular security customization and enforcement. A main advantage of the DFT concerns the application flexibility. Even if the TPA receives sensitive data, the DFT framework determines and shares whether the outputs have to be considered as sensitive, or not. In addition, the coupling of IFC and DFT provides an efficient enforcement to secure internal information exchanges, while monitoring untrusted TPAs in contact with the outside world.

System limitation: We assumed in Section II-B that the integrity of the OS, the middleware and the DFT framework were ensured by a secure boot. However these mechanisms do not protect against runtime attacks, which could be significantly harmful when being performed on critical entities like the proxy or the HU. They may be detected by host-based intrusion detection tools performing scans and recognition of instruction patterns within a running platform [24]. Though these solutions might significantly degrade the system performance and should be used in a carefully selected manner.

VI. Conclusion

In this paper, we presented a security architecture, leveraging DFT engines to secure the on-board integration of automotive TPAs. Locally, the DFT framework controls and monitors the TPA against exploitation of security vulnerabilities. Regarding the network communications, the middleware-based exchange of taint information allows the DFT tool and the trusted services to preserve the data confidentiality and system integrity. Interface rules between labels and taints allow an efficient and simultaneous integration of the local DFT and the car-wide IFC. However while enhancing the car security, DFT/IFC tools have shown their limits in term of performance and can not be used for time-critical applications without further optimization but are suitable for an infotainment usage. Full virtualization solutions may be an efficient and secure alternative, that we intend to investigate.

References

[1] K. Koscher et al, "Experimental security analysis of a modern automobile", in proc. of the 31st IEEE S&P, 2010, pp. 447–462.

[2] Z. Lutz, "Renault debuts r-link", Engadget and Renault press release at leweb'11, December 2011 (retrieved 2013).

[3] E. Slivka, "Apple pulls russian sms spam app from app store", http://www.macrumors.com/2012/07/05/apple-pulls-russian-sms-spam-app-from-app-store/, 2012 (retrieved May 2013).

[4] F. Qin, C. Wang, Z. Li, H. Kim, Y. Zhou and Y. Wu, "Lift: a low-overhead practical information flow tracking system for detecting security attacks", in proc. of MICRO–39, 2006, pp. 135–148.

[5] H. Yin, D. Song, M. Egele, C. Kruegel and E. Kirda, "Panorama: capturing systemwide information flow for malware detection and analysis", in proc. of the 14th CCS, 2007, pp. 116–127.

[6] W. Enck et al, "Taintdroid: an information-flow tracking system for realtime privacy", in proc. of the 9th OSDI, 2010, pp. 393–407.

[7] Etch homepage. http://incubator.apache.org/etch/ (retrieved May 2013).

[8] V. Kemerlis, G. Portokalidis, K. Jee and A. Keromytis, "libdft: practical dynamic data flow tracking for commodity systems", in proc. of the 8th ACM SIGPLAN/SIGOPS VEE, 2012, pp. 121–132.

[9] A. Maier, "Ethernet - the standard for in-car communication", in 2nd Ethernet & IP @ Automotive Technology Day, 2012.

[10] A. Bouard et al, "Driving automotive middleware towards a secure ip-based future", in proc. of the 10st ESCAR, 2012.

[11] A. Bouard, J. Schanda, D. Herrscher, C. Eckert, "Automotive proxy-based security architecture for ce device integration", in proc. of 5th MobileWare 2012, Springer, 2012, pp. 62–76.

[12] Fujitsu Semiconductor Europe, "Fujitsu announces powerful mcu with secure hardware extension (SHE) for automotive instrument clusters", In Fujitsu Press Release at www.fujitsu.com, 2012 (retrieved May 2013).

[13] Intel's Pin homepage.http://www.pintool.org/ (retrieved May 2013).

[14] M. Dalton, H. Kannan and C. Kozyrakis, "Real-world buffer overflow protection for userspace & kernelspace", in proc. of the 17th USENIX SEC, 2008, pp. 395–410.

[15] B. Davis and H. Chen, "Dbtaint: cross-application information flow tracking via databases", in proc. of the 1st USENIX WebApps, 2010.

[16] Q. Zhang et al, "Neon: system support for derived data management", in proc. of the 6th SIGPLAN/SIGOPS VEE, 2010, pp. 63–74.

[17] A. Zavou, G. Portokalidis and A. Keromyitis, "Taint-Exchange: a generic system for cross-process and cross-host taint tracking", in proc. of the 6th IWSEC, 2011, pp. 113–128.

[18] H. Schweppe and Y. Roudier, "Security and privacy for in-vehicle networks", in proc. of the 1st IEEE VCSC, 2012.

[19] N. Zeldovich, S. Boyd-Wickizer, and D. Mazières, "Securing distributed systems with information flow control", in Proc. of the 5th USENIX NSDI, 2008, pp. 293–308.

[20] A. Ramachandran, Y. Mundada, M. Tariq and N. Feamster, "Securing enterprise networks using traffic tainting", in Special Interest Group on Data Communication, 2008.

[21] A. Bouard, B. Weyl and C. Eckert, "Practical information-flow aware middleware for in-car communication", submitted to CyCar'13, 2013.

[22] K. Weckemann, F. Satzger, L. Stolz, D. Herrscher and C. Linnhoff-Popien, "Lessons from a minimal middleware for ip-based in-car communication" in proc. of the IEEE IV'12, 2012, pp. 686–691.

[23] BMW AG. Navigation System Professional, http://www.bmw.com/com/en/insights/technology/technology_guide/articles/navigation_system.html (retrieved May 2013)

[24] T. Garfinkel and M. Rosenblum, "A virtual machine introspection based architecture for intrusion detection", in proc. of NDSS symposium 2003, Internet Society, 2003.

Simulation of a Security Function Based on Vehicle-to-X Communication and Automotive Lighting

Peter Knapik
Volkswagen AG
Wolfsburg, Germany
Email: peter.knapik@volkswagen.de

Elmar Schoch
Audi AG
Ingolstadt, Germany
Email: elmar.schoch@audi.de

Frank Kargl
University of Twente
Enschede, The Netherlands
Email: f.kargl@utwente.nl

***Abstract*—Crime and feeling of security are pervasive occurrences and can be influenced by lighting conditions. However, lighting improvements are generally concentrated on street lighting. Meanwhile, a vast variety of new technologies, including innovative lighting systems and connected mobility, are entering into the automotive field. Hence, opportunities are not limited only to provide traffic improvements, entertainment features or safety functions but also measures to tackle (vehicle related) crime and to increase the feeling of security. In this paper, we present an idea for a function which has the potential to tackle crime and increase drivers' feeling of security. Moreover, we explain our approach to measure the effectiveness of the function based on a proprietary simulation environment.**

***Index Terms*—security function, V2X-communication, simulation.**

I. Introduction

Advanced driver assistance systems (ADAS) and Vehicle-to-X (V2X) communication are on the advance. Meanwhile, a vast diversity of ADAS exists, where systems drawing on vehicle lighting are one part. ADAS like dynamic cornering lights, which light into corners, or adaptive high beam assistants, which detect oncoming traffic and adjust beams accordingly, actively intervene with the vehicle's lighting system. Additionally, lighting systems underlie a steady development so that incandescent systems are continuously replaced by LED systems, partly in combination with xenon lights [1]. Also, the penetration of mobile devices is increasing so that they have largely become our daily companion. Thus, connected mobility, which brings these new technologies together, has become a part of our life. In the last decades, there has been a lot of research on the influence of lighting, especially street lighting, on crime and the fear of crime [2]–[5]. A positive effect of lighting on fear of crime has been mostly assumed, whereas the research on the effect on crime has provided equivocal results.

We elaborate on a security function that makes use of vehicles' advanced lighting opportunities and vehicle-to-vehicle (V2V) communication to combat crime and mainly to increase drivers' feeling of security.

The rest of the paper is structured as follows. In Section II, we provide a short overview of automotive lighting systems followed by an explanation of our function's basic idea in Section III. In order to measure the effectiveness of our function, we are implementing a simulation environment, which is presented in Section IV. Then, we briefly show our implementation approach of the simulation in Section V before concluding our paper and providing an outlook on future work.

II. Lighting Systems

Dependent on the equipment level, vehicles, usually, posses at least the mandatory lighting systems for outside illumination. To avoid dazzling oncoming traffic, manual level adjustment exists besides the more sophisticated static and even dynamic automatic leveling. The static leveling system automatically adjusts the level dependent on vehicle loading. Dynamic systems additionally take into account vehicle's acceleration and deacceleration to adjust the tilt angle dynamically.

A further lighting feature, cornering light, occurs in a static and dynamic variant. The static cornering light usually turns on one of the front fog lamps to light into the according direction while turning. The static cornering light is intended to be used at lower speeds in urban areas. In contrast, the dynamic system is designed to be used in rural areas or on highways while driving through corners at higher speed. Low and high beams are actively moved horizontally into the corner with a maximum angle of commonly 15 degrees. Beams are usually controlled via electromotive actuators.

III. (Cooperative) Extended Coming / Leaving Home Function

Most OEMs provide a so called coming / leaving home function (CHF / LHF). Of course, the functionality differs by OEM specific adjustments but the basic idea is similar. When leaving the car, i.e., coming home (CHF), low beams, taillights and other available light sources keep on lighting (during darkness) for a specified period of time in order to light the driver the way "home". The duration can generally be adjusted by the vehicle owner. Referring to the LHF, the aforementioned light sources start lighting as soon as the driver remotely opens the vehicle.

This described functionality has the drawback to be static. The lighting duration can only be adjusted in the vehicle and it is independent of the drivers position. That means, if the duration is to short, the illumination turns off before the driver even reaches the vehicle and vice versa respectively. Furthermore, the vehicle turns on all light sources although some light sources are probably unnecessary since the driver approaches the vehicle from one direction.

Our idea is to extend the existing CHF / LHF by the opportunities of advanced sensors, sophisticated light systems and V2X communication. We suggest to use the opportunity that low beams can be swiveled vertically and horizontally to light the driver's direct route to the vehicle, of course within the mechanical limits of the beams. Additionally, only light sources are turned on which directly influence the illumination of the route so that energy consumption is reduced.

To realize the extended CHF / LHF (ECHF / ELHF), a bidirectional communication between the vehicle and a sophisticated key fob is assumed. The key fob is a smart device, such as a smartkey or smartphone, and must be in possession of the driver. Since the key only communicates with the own vehicle, the common IEEE 802.11a/b/g [6] standard is suitable for communication. Furthermore, position estimation of the key relatively to the vehicle is necessary. This challenge can be faced by localization based on ultra-wideband (UWB) technology [7]. Thereby, it is irrelevant whether the position is calculated by the key or by the vehicle since position data is continuously synchronized between both participating partners via bidirectional communication.

The ELHF is activated as soon as the doors are remotely unlocked. Both, the two-way communication between the key and the vehicle as well as the location estimation of the key are triggered. The position of the key is updated at regular intervals so that the vehicle can evaluate the position. Movable low beams are aligned in the direction of the driver. Other non-moveable light sources are only turned on when they illuminate the direct path of the driver. Since the driver of the vehicle is moving, the direct route to the vehicle is constantly changing. Therefore, low beams are continuously adjusted. Turned off light sources are turned on when they become relevant for the direct path of the driver to the vehicle. In return, turned on light sources are turned off when they lose relevance for illuminating the direct path. Further, there is no need to consider the time to turn off lighting because it is turned off with reaching and entering the vehicle or even after having closed the door. Nonetheless, a specific run-time can be defined as fallback option.

When exiting the vehicle (ECHF), the driver's path is illuminated analogously to the ELHF. The duration of illumination can be determined by a defined delay time. However, there is also the possibility to deactivate the illumination after the driver has left a certain radius around the vehicle. An irregular surface around the vehicle is also possible since the effectiveness of involved light sources is different. The function can be disabled with the key as well.

Due to the physical and mechanical constraints, the own vehicle is not always in a position to illuminate the direct path of the driver. Therefore, the ECHF / ELHF can use vehicle-to-vehicle (V2V) communications to be enhanced to a cooperative function (CECHF / CELHF). Vehicles in the surrounding environment are included to illuminate the driver's path. The own vehicle broadcasts a request to ask for lighting help. Surrounding vehicles being willing to support in lighting reply by providing their pose (position and heading) as well as lighting capabilities. This way, our vehicle is able to create a local map of participating vehicles with the aforementioned information. Since our vehicle is continuously aware of the driver's position, it continuously requests participating vehicles to light specific areas.

To realize inter-vehicle communication, we suggest to consider standardization provided by IEEE [6] and ETSI [8]. Thereby, V2V communication is based on IEEE 802.11p [6]. This way, designated communication and security mechanism are used. Further, positions of vehicles are either estimated in the traditional way with the help of GPS and compass or by making use of UWB technology, which is also suitable for indoor use, e.g., for parking garages. Research projects, such as AIM [9] or V-Charge [10], also partly address localization challenges to estimate vehicle positions within parking facilities.

IV. Simulation Environment

Our goal is to model diverse parking constellations of vehicles and diverse routes the driver goes to or from the vehicle. This way, we aim to compare the effectiveness of the different forms of (CHF / LHF) under different constellations. Our effectiveness criteria is the driver's duration in a lighted area when approaching or leaving the vehicle. Additionally, referring to the cooperative form of the (CHF / LHF), we want to investigate several equipment rates of vehicles being able to participate in V2V communication and see which penetration rates are necessary to achieve a gapless lighting of the driver's route. A further criteria is energy consumption. Under certain circumstances, it is not necessary to involve all V2V communication capable vehicles to light the route since several vehicles are eventually able to light the same area.

To the best of our knowledge, there is no simulation environment supporting a simulation of our security function. Consequently, we decided to implement a proprietary simulation environment, which is schematically illustrated in Figure 1.

A. Parking Constellations

The number of parking constellations is infinite since the driver's route can be manifoldly modeled and vehicles can be positioned in different ways. Nevertheless, we demand both, to freely position vehicles and to model driver's route. Further, a lot of possibilities exist how a vehicle is equipped. Consequently, we will have to pick out wisely "typical" constellations to be simulated and evaluated. Actual equipment rates of advanced lighting systems can be used to determine penetration rates for the simulation. Additionally, we think

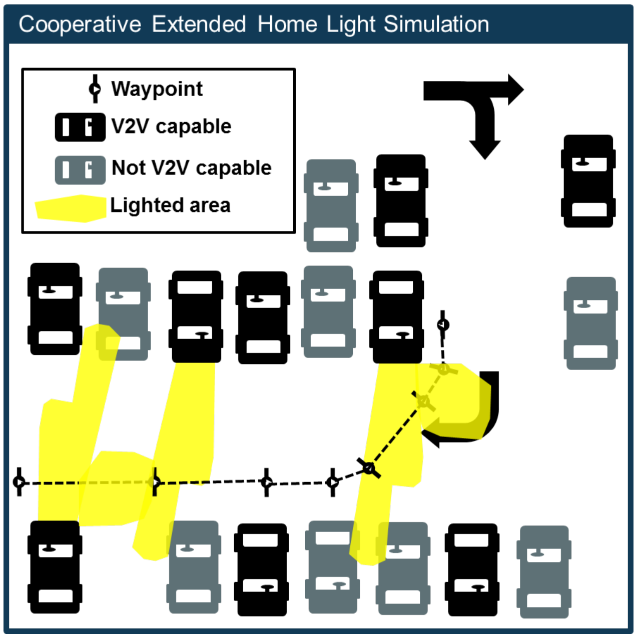


Fig. 1. Simplified schematic and dimensionless illustration of the simulation environment

that regarding an area of 100m around the host vehicle is a good approach since typical remote keys and low beams work nearly up to this distance.

B. Vehicles

Each vehicle has a set of light sources which can be used to light the environment. Light sources are not limited to low and high beams. We also consider fog beams, rear lights, license plate illumination and lighting elements integrated into exterior mirrors. Each vehicle is configured separately, so that vehicles with different equipment levels can be simulated. For reasons of simplification, we limit the lighted area of each light source in the first approach to one specific area. This way, we would not consider different light technologies, which consequently implies different lighted areas, especially regarding low beams. But, we keep the opportunity to model different lighted areas for each vehicle, as will be seen in section V-A. Furthermore, in reality, there is a fluent transition from a lighted to a non-lighted area due to effects of scattered light. However, we will approximate lighted areas by polygons so that lighted areas end abruptly. Vehicles supporting dynamic low beams, have also an adjustable yaw and pitch angle. Additionally, each light source has a predefined energy consumption parameter so that consumed energy is calculated within the simulation.

C. Driver's Route

Driver's route is modeled via linear interpolation of a chain of points, hereafter referred to as waypoints. A polynomial interpolation was discarded due the tendency for oscillation [11]. Furthermore, the driver's walking speed is adjustable so that the covered distance is calculated dependent on the discrete simulation steps.

D. Communication

The propagation of electromagnetic waves highly varies affected by many influencing factors. For example, Kwoczek et al. [12] investigated the influence of roof curvature, roof racks and panorama glass roofs on the antenna gain in the reserved V2V communication frequency band and found inter alia a high loss of gain caused by glass roof. Hence, it is highly challenging to consider and simulate all influencing factors.

We choose the Friis propagation model [13], which models a deterministic path loss over the distance from sender to receiver, in order to simulate propagation aspects of wireless communication. Since we don't have moving vehicles in our environment, we discard fading models accounting for non-deterministic effects of moving objects. When making our decision, we took into consideration available models benchmarked by [14] and implemented in the most widely used network simulator NS-3 [15]. However, we keep the propagation model exchangeable in our simulation to have the opportunity to use another loss model.

V. Implementation

A. Coordinate Systems

Our parking environment is represented by a coordinate system called environmental frame (e-frame), which could be mapped when needed to the World Geodetic System 1984 (WGS84) or a system related to a parking facility. Further, each vehicle has a coordinate system (v-frame), which is attached to the center of the vehicle. Each lighted area, which is generated by light sources, is represented by a polygon whose points refer to a coordinate system called a-frame. Consequently, several a-frames are attached to a vehicle depending on the vehicle's configuration. To represent the driver, we also decided to use a Cartesian coordinate system (d-frame) instead of a point in order to have the opportunity to model driver's orientation. Since we have two-dimensional (2D) right-handed Cartesian coordinate systems, rotations happen in the plane around the z-axis, which is directed out of the plane. All aforementioned frames are illustrated in Figure 2.

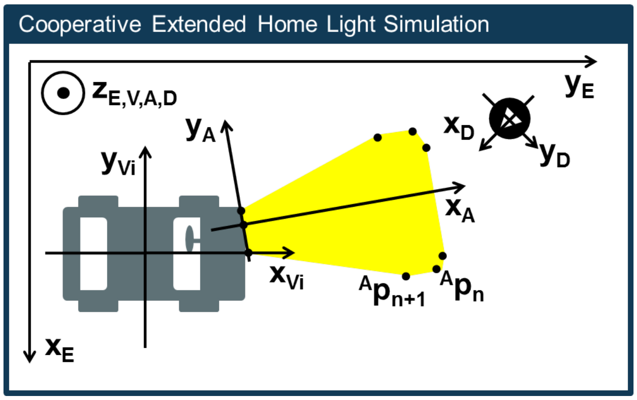


Fig. 2. Schematic illustration of frames involved in the simulation

B. Coordinate System Transformations

We use homogeneous coordinates [16] to calculate transformations between as well as within our frames. Since we have different frames of reference, we precede vectors with a superscript to show the related system. Transformation matrices are followed by a subscript to show the source frame and preceded by a superscript to show the target frame. For example, to calculate a point ${}^{V}\mathbf{p} = \left({}^{V}x,{}^{V}y,1\right)$, which refers to a v-frame, i.e., a vehicle, into coordinates related to the e-frame, i.e., the environment, we use the following equation

$${}^{E}\mathbf{p} = \begin{pmatrix} {}^{E}x_p \\ {}^{E}y_p \\ 1 \end{pmatrix} = {}^{E}\mathbf{H}_V * {}^{V}\mathbf{p} = {}^{E}\mathbf{H}_V * \begin{pmatrix} {}^{V}x_p \\ {}^{V}y_p \\ 1 \end{pmatrix} \qquad (1)$$

with the transformation matrix

$${}^{E}\mathbf{H}_V = \begin{pmatrix} \cos\left({}^{E}\alpha_V\right) & -\sin\left({}^{E}\alpha_V\right) & {}^{E}a_V \\ \sin\left({}^{E}\alpha_V\right) & \cos\left({}^{E}\alpha_V\right) & {}^{E}b_V \\ 0 & 0 & 1 \end{pmatrix}$$

where ${}^{E}\left(a,b\right)_V$ is the position of the v-frame related to the e-frame and ${}^{E}\alpha_V$ the according orientation, respectively.

Due to the use of homogeneous coordinates, a combination of transformations is achieved by multiplying according matrices as shown in (2) where a point is transformed from the a-frame via a v-frame into the e-frame.

$${}^{E}\mathbf{p} = {}^{E}\mathbf{H}_V * {}^{V}\mathbf{H}_A *{}^{A}\mathbf{p} \qquad (2)$$

C. Beam Movement

To simulate a low beam's horizontal rotation, the according a-frame is rotated with reference to its v-frame. To simulate a low beam's vertical movement, we directionally scale the lighted area on the x-axis of its according a-frame. Hence, a movement downwards will shrink and a movement upwards will enlarge the lighted area [17]. So, each point of the polygon representing the lighted area has to be multiplied with the scaling matrix $\mathbf{S}$ as shown in (3) where s_x is the scaling factor. A scaling factor $s_x < 1$ means a beam movement down and $s_x > 1$ up, respectively. The interested reader can find further information regarding the installation of lighting and light-signalling devices in the vehicle regulations [18] provided by the United Nations Economic Commission for Europe (UNECE).

$${}^{A}\tilde{\mathbf{p}} = \begin{pmatrix} {}^{A}\tilde{x} \\ {}^{A}\tilde{y} \\ 1 \end{pmatrix} = \mathbf{S} *{}^{A}\mathbf{p} = \begin{pmatrix} s_x & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} * \begin{pmatrix} {}^{A}x \\ {}^{A}y \\ 1 \end{pmatrix} \qquad (3)$$

D. Message Propagation

We estimate whether a vehicle takes part in communication or not using the Friis propagation model shown in (4). R is the distance between the transmitting and the receiving vehicle and λ the wavelength, which is calculated from the frequency used for V2V communication. Further, each vehicle has a transmission power (P_t), a threshold for receiving power (P_r) as well as antenna gain (G_t and G_r).

$$\frac{P_r}{P_t} = G_t G_r \left(\frac{\lambda}{4\pi R}\right)^2 \qquad (4)$$

VI. Conclusion and Future Work

The main goal of this work was to present an idea for a security function making use of new lighting opportunities as well as V2X communication and to show our approach to verify the effectiveness of our function.

In our future work, we will focus on finishing the implementation of the simulation environment and evaluating different parking scenarios. Besides, we will continuously extend our simulation environment by slipping in new ideas and improvements. Furthermore, we will elaborate on a more detailed realization of the V2X communication and an according protocol based on the latest standardization provided by the European Telecommunications Standards Institute (ETSI).

References

[1] A. Vollmer, "Der Weg zum pilotierten Fahren," *Automobil Elektronik*, vol. 4, pp. 38–39, Aug. 2012.

[2] M. Ramsay and R. Newton, "The effect of better street lighting on crime and fear: A review," Home Office Police Department, London, Crime Prevention Unit Papers 29, 1991.

[3] K. Pease, "A review of street lighting evaluations: Crime reduction effects," in *Surveillance of Public Space: CCTV, Street Lighting and Crime Prevention*, ser. Crime Prevention Studies, K. Painter and N. Tilley, Eds. Criminal Justice Press, 1999, vol. 10, pp. 47–76.

[4] D. P. Farrington and B. C. Welsh, "Effects of improved street lighting on crime: a systematic review," Home Office Research - Development and Statistics Directorate, London, Home Office Research Study 251, Aug. 2002.

[5] B. C. Welsh and D. P. Farrington, "Improved street lighting and crime prevention: A systematic review," The Swedish National Council for Crime Prevention, Stockholm, Tech. Rep., 2007.

[6] Institute of Electrical and Electronics Engineers (IEEE). [Online]. Available: http://www.ieee.org

[7] G. Shen, "Localization of active nodes within distributed ultra-wideband sensor networks in multipath environments," Ph.D. dissertation, University of Technology Ilmenau, Jul. 2012.

[8] European Telecommunications Standards Institute (ETSI). [Online]. Available: http://www.etsi.org

[9] Application Platform for Intelligent Mobility (AIM). DLR - Institute of Transportation Systems. [Online]. Available: http://www.dlr.de/fs/en/

[10] Automated Valet Parking and Charging for e-Mobility (V-Charge). [Online]. Available: http://www.v-charge.eu/

[11] H. R. Schwarz and N. Köckler, *Numerische Mathematik*, 8th ed., U. Schmickler-Hirzebruch and B. Gerlach, Eds. Wiesbaden: Vieweg und Teubner, 2011.

[12] A. Kwoczek, Z. Raida, J. Lacik, M. Pokorny, J. Puskely, and P. Vagner, "Influence of car panorama glass roofs on car2car communication (poster)," in *Vehicular Networking Conference (VNC), 2011 IEEE*, Nov. 2011, pp. 246–251.

[13] H. T. Friis, "A note on a simple transmission formula," *Proceedings of the IRE*, vol. 34, no. 5, pp. 254–256, May 1946.

[14] M. Stoffers and G. Riley, "Comparing the ns3 propagation models," in *Modeling, Analysis & Simulation of Computer and Telecommunication Systems (MASCOTS), 2012 IEEE 20th International Symposium on*, Aug. 2012, pp. 61–67.

[15] Network Simulator 3 (ns3). [Online]. Available: http://www.nsnam.org

[16] D. Salomon, *The Computer Graphics Manual*, D. Gries and F. B. Schneider, Eds. Springer, 2011.

[17] K. Reif, *Automobilelektronik - Eine Einführung für Ingenieure*, E. Schmitt and E. Lange, Eds. Wiesbaden: Vieweg und Teubner, 2012, vol. 4.

[18] *Uniform provisions concerning the approval of vehicles with regard to the installation of lighting and light-signalling devices*, United Nations Economic Commission for Europe Std. 48, Rev. 9, Jan. 2013.

Automatic Estimation of Moving Targets By MUSIC Algorithm Considering Doppler Effect

Xin Wang
Department of Electronic Engineering
Chungbuk National University
Cheongju, Korea 361-763
wxzf007@naver.com

Heung-Gyoon Ryu
Department of Electronic Engineering
Chungbuk National University
Cheongju, Korea 361-763
ecomm@cbu.ac.kr

Abstract — **For the multiple users communication or multiple target detection, it is important to separate multiple targets or users that are included in the same communication or radar antenna beam. In this paper, a combined OFDM (orthogonal frequency division multiplexing) system and bandpass sampling method using MUSIC (multiple signal classification) algorithm for automatic AOA (angle of arrival) tracking is discussed. Also, we propose a new method of the time division multiplexing with bandpass sampling at the same time to avoid the interference due to the imperfect RF (radio frequency) filter characteristics. The main purpose of our proposed structure is to avoid the interference generated from the multi-band signals processing. Next, we consider the Doppler effect caused by the target movement in mobile environment. After compensating the Doppler effect with valid range, the system performance is improved. Computer simulation results show the performances of MUSIC spectrum for AOA in various conditions and demonstrate the accuracy of AOA estimations.**

Keywords-MUSIC; AOA; Bandpass sampling; OFDM; Doppler effect

I. INTRODUCTION

Smart antenna is one of the possible solutions to increase the channel capacity due to an increase in the number of mobile units and the need for high-speed digital communication in mobile communication. Smart antenna utilizes the beamforming technique to spatially direct the electromagnetic power to an intended mobile unit while spatially null the signal power along other mobile units. The system needs the process of angle of arrival estimation to locate the mobile units before beamforming can be performed. Angle of arrival estimation technology play an important role in enhancing the performance of adaptive arrays for mobile wireless communications [1]. A number of angle of arrival estimation algorithms have been developed. The most recent ones are MUSIC [2] and ESPRIT (estimation of signal parameters via rotational invariance techniques) [3] algorithms; both utilize subspace-based exploitation of the Eigen structure of the input covariance matrix and thus require higher computation efforts. Although the ESPRIT needs less computation, the MUSIC algorithm is found to be more stable and accurate [4]. In this paper, we use the MUSIC algorithm combined with the OFDM bandpass sampling signal model to perform the antennas sensing for allowing the accurate azimuth. The accuracy of the estimation in azimuth increases proportionally to the number of antenna elements.

Bandpass sampling can be used for direct down conversion without analog mixers. In practice, the required sampling rate for ADC (analog to digital converter) can be too high to be achieved if the Nyquist sampling theorem is considered [5]. So, we want to use bandpass sampling which samples the signals with smaller sampling rate than Nyquist sampling rate to relax the demand for ADC. After down-sampling about over two band signals using the bandpass sampling, the signals are digitized. Then, two band signals can be received [6].

In the case of the conventional bandpass sampling receiver architecture, which we also refer to it as RF bandpass front-end receiver architecture, the SDR (software defined radio) receiver design has been widely treated in the literature. In particular, in [7] and [8], RF bandpass sampling frontend for SDR is designed to place analog-to-digital converter as near the antenna as possible. From the point of view of receiver design, due to previous system [9], although over two signals can be down-sampling without interference between signals, it is possible to generate interference due to RF filter characteristics. RF filter cannot cut adjacent band signals so the remaining adjacent band signals (undesired signals) can affect desired signals. So, when the existing receiver architecture try to receiver the multi-band signals, it inevitably generates interference among the multi band signals, which can seriously damage the performance of the communication system.

In this paper, we propose a novel TDM (time division multiplexing) [10] based on the bandpass sampling RF(radio frequency) front-end receiver structure [5], and we compare it with the state-of-the-art systems. Our proposed structure can avoid the interference generated when doing the multi-band signals processing. The main motivation of our proposed structure is that we can reduce the complexity of the operation by using the TDM structure comparing with the existing structure.

This paper is organized as follows. In Section II, the system model is introduced. In Section III, we consider the Doppler effect of the system and compensation. Section IV describes the existing structure as well as our proposed

ISBN: 978-1-61208-288-2

structure. Section V gives the simulation results, which show the performances of MUSIC spectrum for AOA in various conditions and demonstrate the accuracy of AOA estimations. In the end, Section VI gives the conclusions.

II. SYSTEM MODEL

A. OFDM Signal and Multi-Antenna Receiver

In this paper, we consider two signals that have different center frequencies. Transmitted signals are based on OFDM. Eq. (1) is the signal in time domain. Let us assume that there are two received bands and there are both transmitted signals. Each band has different signals from each transmitter and $X_{k,m}^{A}$ and $X_{k,m}^{B}$ are the transmitted signals, respectively. After an IFFT (inverse fast Fourier transform) processing, each band is represented in time domain as $x_A(t)$ and $x_B(t)$ and has center frequencies of f_A and f_B.

$$x(t)=\begin{cases}\dfrac{1}{\sqrt{N}}\displaystyle\sum_{k=0}^{N-1}X_{k,m}^{A}e^{j(\frac{2\pi k}{N}+f_A)t}, x_A(t)\\[2ex] \dfrac{1}{\sqrt{N}}\displaystyle\sum_{k=0}^{N-1}X_{k,m}^{B}e^{j(\frac{2\pi k}{N}+f_B)t}, x_B(t)\end{cases} \tag{1}$$

The receiver is equipped with ULA (uniform linear array) of M elements located along a straight line. The system can be viewed as the multiplication of each received ray by a steering vector considering the direction of arrival of each multipath. Assume that there are P (P <M) uncorrelated narrowband signals $x_p(t)$ received by ULA from different direction θ_p, corrupted by AWGN (additive white Gaussian noise), where p=1,2… P. The observation is given as

$$X(t)=\sum_{p=1}^{P}a(\theta_p)*x_p(t)+n(t) \tag{2}$$

where $a(\theta)$ is the array steering vector given by

$$a(\theta)=[1\ \ \mathrm{e}^{-j2\pi d\sin\theta/\lambda}\cdots\mathrm{e}^{-j2\pi d\sin\theta(M-1)/\lambda}]^T \tag{3}$$

where d is the inter-element spacing, λ is the signal wavelength. When we take a snapshot at time k=1,2…K, we can get

$$X(k)=\sum_{p=1}^{P}a(\theta_p)*x_p(k)+n(k) \tag{4}$$

where noise $n(k)$ is assumed to be both temporally and spatially white, and uncorrelated with signal $s_p(k)$.

In Figure 1, two signals are received through multi-antenna receiver. After amplification of received signals in low-noise amplifier (LNA), each signal passes through RF filter. After band pass filter (BPF), each signal is sampled in time. The sampling frequency is smaller than Nyquist rate but larger than signal bandwidth of twice shown in Figure 1. TDM and bandpass sampling are processed at the same time. The digital oscillator is processed in the digital part; so, there are no problems that are generated by analog oscillator. After ADC and removing the cyclic prefix (CP), signals are processed through the MUSIC algorithm and the frequency domain equalization.

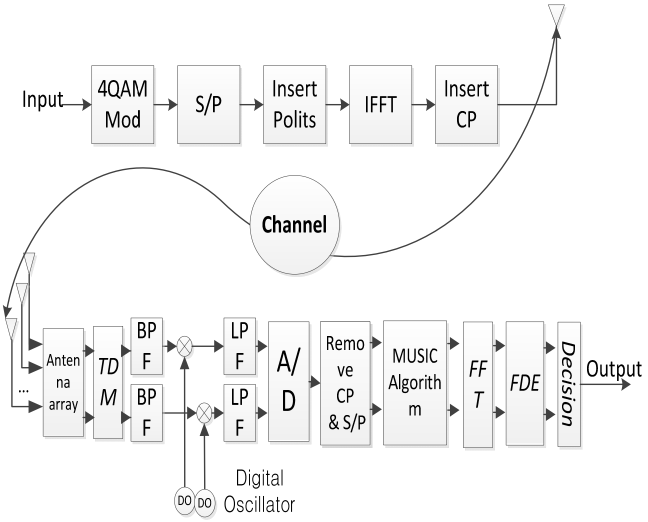


Figure 1. System Model.

B. Angle of Arrival Estimation using MUSIC Algorithm

MUSIC stands for MUltiple SIgnal Classification. The covariance matrix, R, is the collected data for each of the array receivers in the time domain. The correlation matrix is given as [6]

$$R=E\left[XX^H\right]=AR_sA^H+\sigma^2 I \tag{5}$$

where R_s is the $P\times P$ signal correlation matrix. σ^2 is the white noise power. The noise subspace E_N used in MUSIC can be obtained from eigenvalue decomposition of R, and the spatial spectrum of MUSIC is given by

$$P(\theta)=\frac{1}{a(\theta)^H E_N E_N^H a(\theta)} \tag{6}$$

III. DOPPLER EFFECT AND COMPENSATION

The orthogonality among the subcarriers is often destroyed by the carrier frequency offset due to the mismatching of oscillators between transmitters and receivers. Therefore, the Doppler effect is generated and degrades the communication performance. Doppler effect results in the frequency shift in frequency domain and is represented phase rotation in time domain. The signal x(t) is similar to Eq.(7) due to Doppler effect.

$$y_n=\sum_{k=0}^{N-1}H_k\cdot X_k\cdot e^{i2\pi\frac{k+\varepsilon}{N}}+z_n \tag{7}$$

The signal x(t) is like (8) due to Doppler effect in time domain.

Channel H is represented as product of X. Doppler effect is represented as phase rotation in frequency domain. In Eq. (7), k, n, ε are sub-carrier, symbol, and the normalized Doppler frequency, respectively.

$$Y_p = \sum_{m=0}^{N-1} \sum_{k=0}^{N-1} H_{k,m} \cdot X_{k,m} \cdot e^{i2\pi\frac{(k+\varepsilon)}{N}} \cdot e^{-i2\pi\frac{m}{N}} + Z_p$$
$$= H_p \cdot X_p \; e^{i2\pi\varepsilon p} + \sum_{\substack{m=0\\m\neq k}}^{N-1} \sum_{k=0}^{N-1} H_{k,m} \cdot X_{k,m} \cdot e^{i2\pi\frac{(k-m)}{N}} \cdot e^{i2\pi\frac{\varepsilon}{N}} + Z_p \tag{8}$$

In (8), the first stage is phase rotation and the second stage is inter carrier interference (ICI), where p is symbol in frequency domain and k, m are sub-carrier before IFFT in transmitter and sample before FFT in receiver. Phase rotation of Doppler is different per symbol and ICI is generated when one sub-carrier affects other sub-carriers.

The normalized offset value is found by division with the carrier spacing. We consider the direction of the receiver to be heading towards the transmitter.

$$\varepsilon = \frac{f_d}{carrier\ spacing}\ ,\ f_d = \frac{v \cdot f_c}{c} \tag{9}$$

In this system, we compensate those problems with synchronization signal and block type pilot and it is assumed that the receiver speed is constant. fd, c, v are Doppler frequency, the velocity of light, and the speed of receiver, respectively.

The problem of Doppler effect is compensated with block type pilot. The phase rotation is estimated by doing interpolation between pilots, because the receiver speed is not dramatically changed.

$$Y_p = H_p \cdot X_p \; e^{i2\pi\varepsilon p} + Z_p \tag{10}$$

The phase rotation is estimated by using the received pilot signals.

$$P(i) = \sum_{i=1}^{N} mean\left\{ \sum_{n=1}^{64} \ Block\_Pilot(i+n-1) \right\} \tag{11}$$

$$\frac{angle\{P(i)\} - angle\{P(i+1)\}}{pilot\_interval} \cdot ([1: pilot\_interval - 1])$$
$$i = 1, 2, \ldots \tag{12}$$

P is average of block type pilot. Eq. (12) represents linear interpolation using P. So, the symbols that have no pilots are estimated. But, if there is too long pilot interval or Doppler frequency, it is difficult to compensate the effect.

IV. Proposed Bandpass Sampling Method

A. Existing Structure

The existing multi-band system with bandpass sampling finds sampling frequency that does not overlap signals between multi-band signals according to (7). But, to select multi-band signals, RF filter is used. Although RF filter has good Q value, the RF filter cannot remove all adjacent signals. So, the remaining adjacent signal is able to be overlap when multi-band signals are converted at low frequency band. Bandpass sampling about multi-band of over 2 bands meet condition like (13) [9]. To convert the two signals in low frequency band without interference between signals, $F_{IF,A}$ and $F_{IF,B}$ have to meet (13).

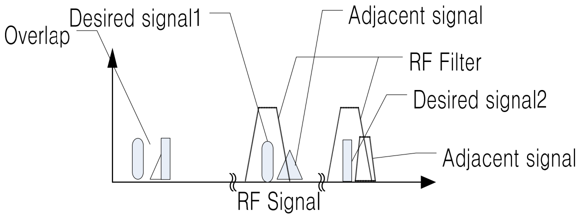


Figure 2. The problem when signals are sub-sampled from RF band.

$$0 < F_{IF,A} - BW_A/2, \quad F_S > F_{IF,A} - BW_A/2$$
$$0 < F_{IF,B} - BW_B/2, \quad F_S > F_{IF,B} - BW_B/2$$
$$if\ F_{IF,B} > F_{IF,A}$$
$$F_{IF,B} - BW_B/2 > F_{IF,A} + BW_A/2$$
$$if\ \ F_{IF,A} > F_{IF,B}$$
$$F_{IF,A} - BW_A/2 > F_{IF,B} + BW_B/2 \tag{13}$$

At first, the signals that are converted into low frequency band are larger than 0 and smaller than Fs/2, respectively. Secondly, the low frequency part of $F_{IF,A}$ is larger than the high frequency part of $F_{IF,B}$ ($F_{IF,B}$ <$F_{IF,A}$) or, the low frequency part of $F_{IF,B}$ ($F_{IF,A}$ >$F_{IF,A}$) is larger than the high frequency part of $F_{IF,A}$ ($F_{IF,B}$ >$F_{IF,A}$).

B. Proposed Structure

We propose a method that adds TDM method into the bandpass sampling system.

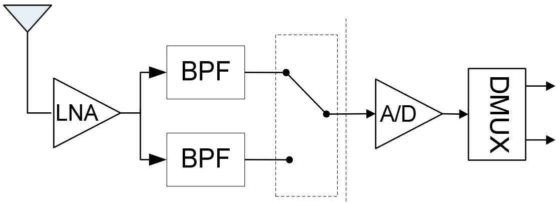


Figure 3. A multi-band receiver structure with bandpass sampling and TDM method.

The proposed structure is shown in Fig.3.

$$0 < F_{IF,A} - BW_A/2, \quad F_S > F_{IF,A} - BW_A/2$$
$$0 < F_{IF,B} - BW_B/2, \quad F_S > F_{IF,B} - BW_B/2 \tag{14}$$

Multi-band signals are received with antennas and the signals pass through LNA. Afterward, the multi-band signals are divided into two signals by filter. Each signal is sampled two times faster than the existing bandpass sampling frequency. After sampling processing in front of the ADC, TDM and bandpass sampling are performed at the same time. The signals that are received by TDM have no interference between the receiving signals because the signals are divided in time. Therefore, the converted signals just satisfy Eq. (14) instead of Eq. (13). So, it is possible to give an low sampling frequency.

Owing to our proposed algorithm, which adds TDM method using bandpass sampling in Eq.(14), we can reduce the complexity of operation by using the TDM structure comparing with the existing structure. Secondly, while by reducing the complexity of operation comparing Eq. (13) and Eq. (14), the system will relax its burden of hardware requirement and provide a faster processing speed than the existing structure.

V. Simulation and Discussion

Table 1 shows the simulation parameters. OFDM signals using 4-QAM modulation are used in the simulation. The number of OFDM subcarrier is 64 and the number of antenna is 8.

TABLE I. SIMULATION PARAMETERS

OFDM system	
The number of Subcarriers	64
Bandwidth	20MHz
Symbol Period	4us
Subcarrier Spacing	312.5KHz
CP Length	0.8us
Modulation	4-QAM
Channel	AWGN
Antenna Number	8
Antenna Type	ULA
Target A azimuth	10°
Target B azimuth	50°

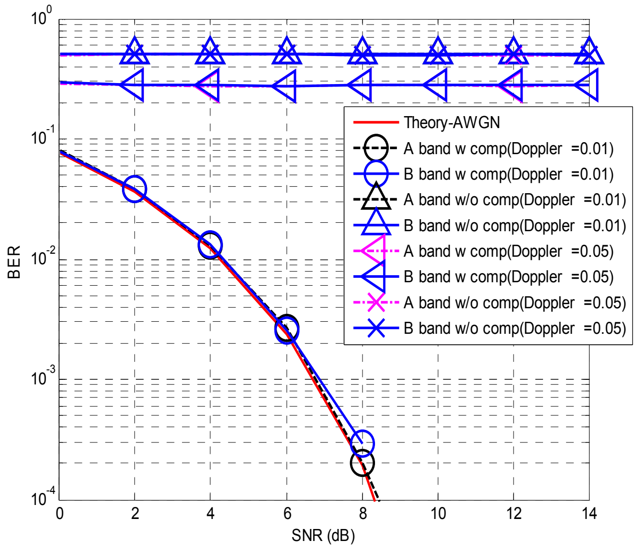


Figure 4. BER performance with Doppler effect.

Fig. 4 shows the BER performance under the Doppler effect with two different normalized offset values 0.01 and 0.05. Due to our proposed system, TDM can divide the multi-band signals into time one and time two then we can see performance according to only one band at a time. For the situation of normalized offset value given as 0.01 according to both band A and B without compensation, we cannot communicate because of the heavily damaged phase rotation. Then, after compensating the phase rotation, our proposed system shows that comparing with the theory curve, the degradation is very small, which is caused by remaining ICI. So, we can recover the communication performance. When the normalized offset value is 0.05, the pilot signal is of block type and the linear interpolation is performed. It is difficult to estimate fast phase rotation. We cannot communicate well when both band A and B are too much seriously damaged in the phase rotation.

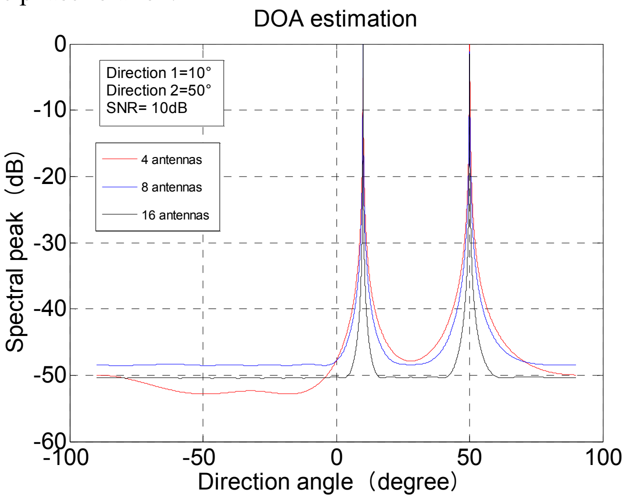


Figure 5. AOA estimation with array antenna numbers at SNR=10dB.

Fig. 5 and Fig. 6 show the MUSIC AOA performance with the different array antenna numbers under the same SNR environment. We can see that, the larger the array antenna number is, the more accurately the system can separate the signals. The better performance shows the sharper shape.

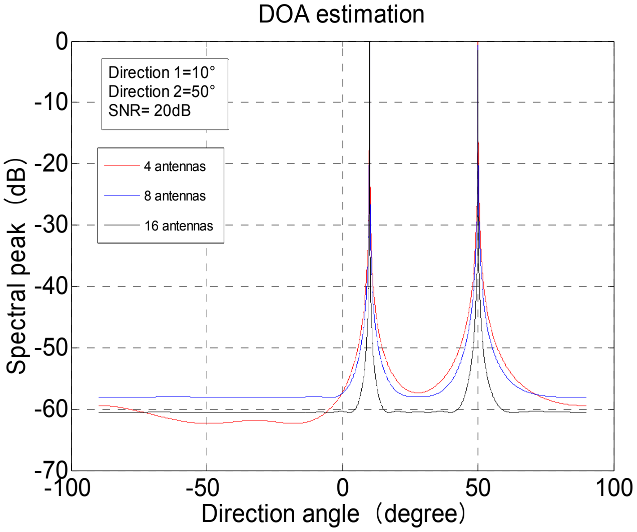


Figure 6. AOA estimation with array antenna numbers at SNR=20dB.

We evaluate the AOA estimations for two scenarios. One is to estimate the two mobile targets in a low speed environment, while the other considers the fast speed environment. The parameters of both cases are shown in Table 2 and Table 3.

TABLE II. PARAMETERS OF TARGETS IN LOW SPEED ENVIRONMENT

Target No	Power(dB)	AOA(degree)	Velocity(m/s)
Target 1	20	25°	20 （72km/H）
Target 2	15	24°	18 （64.8km/H）

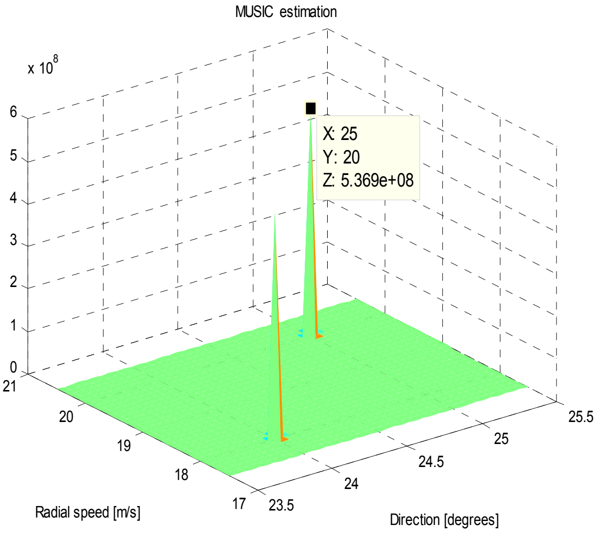


Figure 7. Estimation of Target 1 by MUSIC algorithm in low speed.

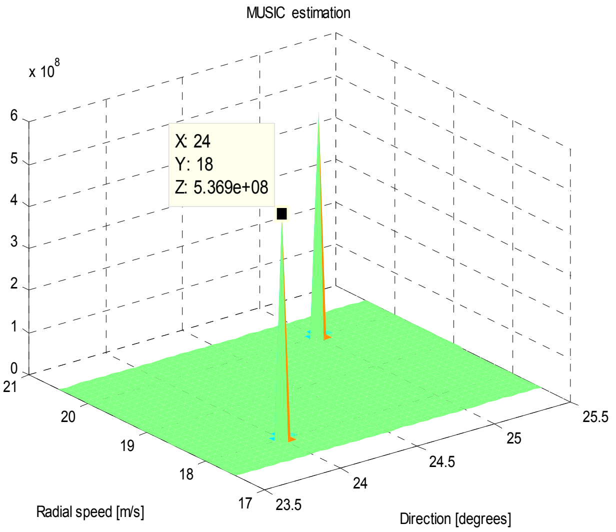


Figure 8. Estimation of Target 2 by MUSIC algorithm in low speed.

Fig. 7 and Fig. 8 show the estimation performances of two targets in low speed environment. And we can see that both the two targets are estimated by MUSIC algorithm which indicates their DOAs and velocities in the labels.

Fig. 9 and Fig. 10 show the estimation performances of two targets in the fast speed environment. We can see that both the two targets are estimated by MUSIC algorithm, which indicates their DOAs and velocities in the labels.

TABLE III. PARAMETERS OF TARGETS IN FAST SPEED ENVIRONMENT

Target No	Power(dB)	AOA(degree)	Velocity(m/s)
Target 1	20	35°	41.6 （150km/H）
Target 2	15	30°	44.4 （160km/H）

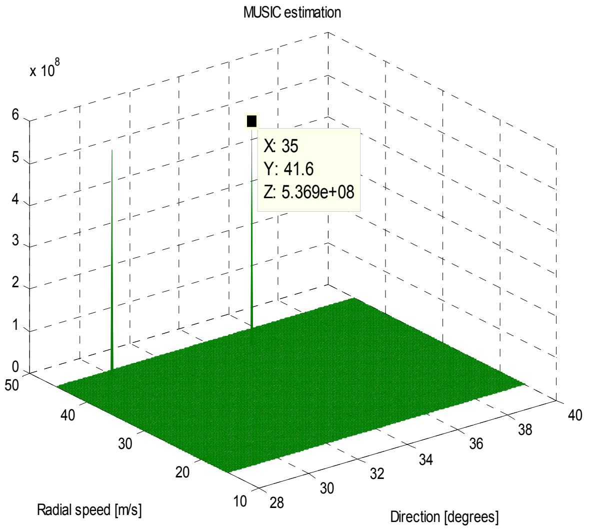


Figure 9. Estimation of Target 1 by MUSIC algorithm in high speed.

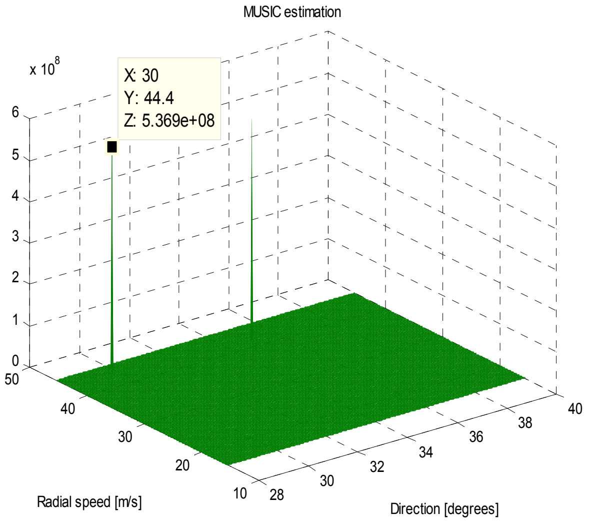


Figure 10. Estimation of Target 2 by MUSIC algorithm in high speed.

VI. CONCLUSIONS AND FUTURE WORK

In this paper, we proposed a new TDM based bandpass sampling method for the mobile targets tracking using MUSIC algorithm. The proposal consists of time division multiplexing with bandpass sampling at the same time to avoid the interference due to the imperfect RF filter characteristics in the receiver side. The main motivation of our proposed structure is that it can reduce the complexity of operation by using the TDM structure comparing with the existing structure. By using MUSIC algorithm, we can estimate the AOA of the targets in both low speed environment and fast speed environment. When we consider the Doppler effect, the system using the proposed method improves the communication performances by compensating the Doppler effect. Finally, computer simulations show that MUSIC algorithm can accurately estimate the AOA of the two targets under different conditions.

There are several directions that need to be investigated in the future. One of the directions is to improve the computational efficiency for covariance matrix of the conventional MUSIC algorithm. Other possible direction we want to explore is to improve the accuracy of the AOA estimation in the more complicated situation by considering other domain-related beamforming technology.

ACKNOWLEDGEMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. 2012017339)

REFERENCES

[1] R. Schmidt, “Multiple emitter location and signal parameter estimation,” IEEE Transactions on Antennas and Propagation, vol. 34, no. 3, pp. 276– 280, Mar. 1986.

[2] A. Paulraj, R. Roy, and T. Kailath, “A subspace rotation approach to signal parameter estimation,” Proceedings of the IEEE, vol. 74, no. 7, pp. 1044 – 1046, July 1986.

[3] T. Lavate, V. Kokate, and A. Sapkal, “Performance analysis of MUSIC and ESPRIT DoA estimation algorithms for adaptive array smart antenna in mobile communication,” International Journal of Computer Networks (IJCN), vol. 2, no. 3, pp. 152 – 172, July 2010.

[4] R. H. Walden, “Performance trends for analog-to-digital converters,” IEEE Commun. Mag., vol. 37, no. 2, pp. 96-101, Feb. 1999.

[5] D. M. Akos, M. Stockmaster, J. B. Y. Tsui, and J. Caschera, “Direct bandpass sampling of multiple distinct RF signals,” IEEE Trans. on Commun., vol. 47, no. 7, pp. 983-988, July 1999.

[6] J. Wang,Y.J. Zhao, and Z.G. Wang. “A MUSIC like DOA estimation method for signals with low SNR,” GSSM 2008, pp.321-324, April 2008.

[7] R. Barrak, A. Ghazel, F. Ghannouchi, “Optimized Multistandard RF Subsampling Receiver Architecture,” IEEE Trans. on Wireless Commun, vol. 8, no. 6, pp.2901-2909, June 2009.

[8] H. J. Kim, J. U. Kim, J. H. Kim, H. M. Wang, I. S. Lee, “The Design Method and Performance Analysis of RF Subsampling Frontend for SDR/CR Receivers,” IEEE on Industrial Eletronics, vol. 57, no. 5, pp.1518-1525, Oct. 2009.

[9] Ching-Hsiang Tseng and Sun-Chung Chou, “Direct Downconversion of Multiband RF Signals Using Bandpass Sampling,” IEEE Trans. on Commun, vol. 5, no.1, pp.72-76, Jan. 2006.

[10] Xin Wang and Heung-Gyoon Ryu,” Design of multi-band receiver with pre-FFT beamformer for wireless communications,” 2013 15th International Conference on Advanced Communication Technology (ICACT), pp.227-232, Jan. 2013.

An Opportunistic Dissemination Model for Traffic Congestion Management in Vehicular Networks

Zhangyin Qian, Yue Wu
National Engineering Laboratory of Information Content Analysis
Shanghai Jiao Tong University
Shanghai, China
{william324, wuyue}@sjtu.edu.cn

***Abstract*—Road congestion has troubled hundreds of thousands of drivers for a long time. In recent years, an application named Dynamic Routing, in which vehicles reroute themselves around congested areas with road information received, is proposed to deal with traffic jam. However, due to the high mobility of the topology of vehicular networks, conventional Ad-Hoc routing is not suitable in Dynamic Routing. As a result, the opportunistic routing might play an important role in this field due to its disruption-tolerant nature. In this paper, we propose a geo-based opportunistic information dissemination model tailored for Dynamic Routing. Instead of the assumption that vehicles participate in message exchanging unconditionally or stand alone completely, we think that a considerable proportion of vehicles in real life belong to certain groups and take the willingness to make contributions to their own groups' driving conditions as a rational cooperation incentive. We evaluate the performance of our model and its effect on saving trip-time in a realistic scenario on an integrated simulation platform. The experimental results show that our dissemination model decreases forwarding overhead dramatically while still delivering as many useful messages into right vehicles as conventional broadcast algorithm does. We also evaluate the performance of different groups in terms of forwarding efficiency and trip-time improvement.**

***Keywords*—Dynamic Routing; geo-based; opportunistic network; TraCI.**

I. Introduction

Traffic congestion has long been a hot topic in the study of Intelligent Transport System (ITS). One solution to this problem is Dynamic Routing, in which vehicles equipped with Short-Range Devices (SRD) may re-compute their path with local digital maps and congestion warning (CW) messages received to route around congested streets.

The dissemination of CW messages based on infrastructure seems to be a feasible solution, but the prohibitive expense makes it hard to be deployed globally. On the other hand, researches on opportunistic routing mechanism provide an alternative to exploit inter-vehicle communication to disseminate messages in an opportunistic manner.

Geo-based opportunistic routing is one of the main branches of opportunistic routing researches. In geo-based opportunistic routing, the holder of a message tries to find a neighbor node that is "closer" to the target under a certain distance definition. Since many vehicles are already equipped with GPS devices, position information is now readily available. This leads to a great potential for geo-based opportunistic routing.

Many researches have been done, aiming to establish a general information dissemination framework. However, each algorithm needs to be tailored for user applications before it is put into use, especially the metric they apply in next relay selection process. More specifically, in Dynamic Routing, the originator of a CW message knows neither IDs nor locations of potential receivers. Consequently, the distance to the target cannot be calculated. Dynamic Routing needs a geo-cast featured information dissemination model, and some researches reveal that candidates' vehicle information will be of great help in relay selection [6][7].

Rational selfishness has also been regarded as a vehicle's nature. Vehicles may not bother to originate and forward CW messages to enhance other vehicles' driving condition. However, vehicles of the same group, such as taxis of a single company, would like to help divert their partners away from congested roads. How this partial cooperation would affect message dissemination and vehicles' trip-time improvement also needs to be investigated further.

In this paper, we propose a new geo-based information dissemination model, named Direction-Assisted Geographic Relay (DAGR) for Dynamic Routing. The model takes relay candidate's moving direction and route into consideration while still leaving carry-CW-or-not decision for relay candidates to make. We evaluate the performance of our model on an integrated simulation platform proposed by A. Wegener *et al.* [12]. The results help us understand the impact of grouping of vehicles on dissemination and how trip-time improvements are distributed in a real city scenario.

The remainder of this paper is organized as follows. We start by describing the existing related works in Section II, and then illustrate DAGR's mechanism in Section III. In Section IV, we present our simulation setup and discuss some experimental results. Finally, Section V concludes the paper.

II. Related work

Vehicular network is conventionally modeled as a planar graph where nodes are junctions and links are road segments. A vehicle may have a chance to forward a message as it approaches a junction [1][2].

In Geographic Delay-Tolerant Network (GeoDTN) Routing, Cheng *et al.* [3] summarized and categorized geo-based routing algorithms in vehicular networks. The routing process is divided into greedy mode, perimeter mode and DTN mode. Vehicles are classified into 4 categories by the deterministic of their destinations and routes. Different distance metrics are defined for each category to guide the switch between routing modes and next relay selection.

Lee *et al.* studied vehicles' behavior at junctions in a micro perspective in [4]. Instead of choosing a farthest 1-hop neighbor as next relay, they proposed an augmented beacon to collect topology information within 2-hop area, and argued that this may help select a relay closer to the target in the situation that routes might be blocked by street topology. Ma *et al.* [5] used angle of vehicles' motion vectors as a metric in relay selection and suggested that the bus system can be a communication backbone in geo-based opportunistic delivery service because of its high punctuality and deterministic of its route and destination.

All these geo-based algorithms require that applications know targets' positions or IDs in advance. While in Dynamic Routing, the originator and forwarders of a message have no idea who may need it and where they are. To disseminate road information in the network quickly and widely, Wischhof *et al.* proposed a simple message dissemination algorithm in [6], which broadcasts messages road by road firstly. Then, through measuring some road condition parameters such as car density and average speed, forwarders may adjust the broadcast interval to decrease communication overhead.

Yang *et al.* evaluated the effectiveness of Dynamic Routing and the feasibility of broadcast interval adjustment through simulation in [7]. Meanwhile they also found that relay candidates' vehicle information can be very useful in selecting a good relay. Similar results also appeared in [8].

From another perspective, Leontiadis *et al.* argued that there is no need to broadcast all cached congestion warning messages in a junction. Applying gossip algorithm, the Computer-Assisted Traveling Environment (CATE) model they proposed defines a utility function and selectively broadcasts a sample of messages [9]. The simulation results show that it still achieves a notable trip-time improvement.

III. Direction-assisted geographic relay model

A. *Assumptions and Proposed Model*

The urban map is modeled as a weighted graph in Dynamic Routing. Each road segment is associated with a travel time as a weight. The default value is computed dividing the segment's length by the speed limit. Once a vehicle's time spent in a road segment surpasses a travel delay threshold, a CW message consisting of road ID and travel delay will be originated and broadcast. This message would be spread into the network, ether in an Ad Hoc or in an opportunistic mode. Upon receiving the message, receivers update their local weighted graphs and apply Shortest Path Algorithms (mostly Dijkstra) to re-compute new routes. Discussions in previous researches have revealed that in the process of selecting a relay, motion information of candidates, e.g., position, direction and route, may improve final trip-time dramatically. Since drivers might regard routes and directions as privacy, advertising this information might not be plausible.

We propose a new geo-based dissemination model for Dynamic Routing, named Direction-Assisted Geographic Relay (DAGR). In this model, the holder of a message just simply broadcasts it in certain conditions and every vehicle v_o that overhears the message decides whether to carry it or not. The decision-making process depends on v_o's direction and its relative position with the message originator v_a.

In our scenario, vehicles are categorized into 4 types.

1) *Non-equipped vehicle:* Vehicles that are NOT equipped with SRDs and do NO rerouting.

2) *Public vehicle:* Vehicles that ALWAYS originate and forward CW messages selflessly when necessary and do rerouting with them, e.g., police cars, buses.

3) *Private vehicle:* Vehicles that NEITHER originate nor forward CW messages. But they DO rerouting with messages overheard from others.

4) *Group vehicle:* Vehicles that originate and forward messages ONLY when there are vehicles of the same group in vicinity, e.g., cars of the same taxi company.

As to the adversary model, faking congestion warning to divert traffic to other areas is studied in [9], and it turned out that it required a significant size of misbehaving nodes (>22% of the total vehicles) to collaborate to make vehicles' trip-time deteriorate notably. So, in our model, the selfishness of vehicles is regarded as the passive attitude in message exchanging instead of broadcasting malicious messages. To inform 1-hop neighbors of their existences, Public and Group vehicles broadcast short HELLO beacons constantly, while Private vehicles always keep silent and just reroute with CW messages overheard from others. So, they are just free-riders.

B. *Dissemination Performance Metric*

The design goal of our dissemination model is to enhance the forward efficiency of CW messages. This means that vehicles in the scenario should only carry and forward messages most likely to make contribution to traffic-jam avoidance, instead of simply forwarding every message they overheard. In fact, most CW messages are of no use to a given vehicle if it contains no roads that consist of the vehicle's route. So, we need a new metric rather than simple delivery ratio when evaluating dissemination performance in Dynamic Routing. Before any further discussion, Table I lists some symbols we may encounter in the rest of this paper.

TABLE I. SYMBOL CONVENTIONS

v	vehicle, v_a denotes a vehicle with ID a.
G	group of vehicles, G_b is a group with ID b.
l	road segment, a one-way road between two adjacent junctions. l_k is a road segment with ID k.
R	route, a sequence consisting of continuous and non-repeating road segments.
p_v^t	v's GPS position at time t.
cl_v	the road segment that v is currently in.
CR_v	the current route of v.
$group(v)$	the group that v belongs to.
$ind(l,R)$	the index of l in R.
$jf_v^{(i)}$	the GPS position of the i'th junction ahead of v along CR_v.
jb_v	the GPS position of the first junction behind v along CR_v. In another word, it is the entrance of cl_v.

Vehicle v_o may benefit from a message only if the message informs it of a congested road segment downstream along its current route.

Definition 1: effective hit (eff-hit) — A CW message causes an effective hit to a vehicle v_o, if and only if the road segment described by the message, denoting l_k, is in v_o's route CR_{v_o} and $ind(cl_{v_o}, CR_{v_o}) < ind(l_k, CR_{v_o})$.

Definition 2: CW message format: $CW = \{a, t, p_{v_a}^t, k, \tau\}$. a is the ID of originator v_a; t is a time stamp; k is the congested road ID and τ is the travel delay corresponding to l_k.

A message is further encapsulated in a bundle.

Definition 3: bundle format: $bundle = \{f, CW, hc\}$. f is the ID of the forwarder v_f; hc is the hop count of the CW.

C. Carry Strategy

Assuming that v_o overhears a $bundle = \{f, CW, hc\}$ at t_{now}, in which $CW = \{a, t, p_{v_a}^t, k, \tau\}$, the vehicle's Carry Decision is made by Procedure 1 shown in Fig. 1.

Firstly, the Carry Decision Procedure verifies whether the message expires by the value of $k \cdot \lambda^{\Delta t}$. λ is a time decay factor and k is a constant. After that, v_o's action depends on its position.

```
Procedure 1 Carry Decision Procedure
IF  $k \cdot \lambda^{t_{now}-t} > eff\_thresh$
    IF  $\angle(\overrightarrow{jb_{v_a} jf_{v_a}^{(1)}}, \overrightarrow{jb_{v_a} p_{v_o}^{t_{now}}}) < \phi$
        IF  $hc == 0$
            Put $(CW, hc)$ in Cache
        END IF
    ELSE
        IF  $\angle(\overrightarrow{jb_{v_a} p_{v_o}^{t_{now}}}, \overrightarrow{p_{v_o}^{t_{now}} jf_{v_o}^{(2)}}) < \varphi$
            Put $(CW, hc)$ in Cache
        END IF
    END IF
END IF
```

Figure 1. Pseudo code of DAGR's Carry Strategy.

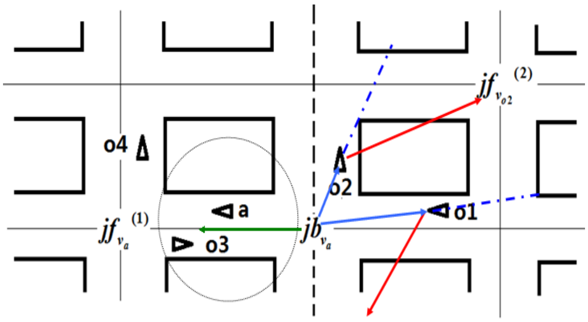


Figure 2. Illustration of Carry Decision Procedure.

As illustrated in Fig. 2, supposing v_a is the CW originator, vehicles on the left side of the dotted line, e.g., v_{o3} and v_{o4}, cannot be effective-hit by this CW because they are not bound for the congested road segment l_k. The procedure may still choose v_{o3} as a relay since it's a 1-hop neighbor of v_a traveling in the opposite direction. The relative position of v_o is measured by the angle between vector $\overrightarrow{jb_{v_a} jf_{v_a}^{(1)}}$ (direction of l_k, green arrow) and vector $\overrightarrow{jb_{v_a} p_{v_a}^{t_{now}}}$ (blue arrow). ϕ is the position angle threshold to determine that v_o is on the left part or the right one. If v_o is on the right side (v_{o1} and v_{o2}), its direction need to be taken into consideration. We adopt the definition of direction in [5], which is a vector from the current location to the 2nd junction downstream v_o's route, denoting $\overrightarrow{p_{v_o}^{t_{now}} jf_{v_o}^{(2)}}$. Abstractly, CW messages are disseminated radially from v_a. If the angle between $\overrightarrow{jb_{v_a} p_{v_o}^{t_{now}}}$ (blue dotted line) and $\overrightarrow{p_{v_o}^{t_{now}} jf_{v_o}^{(2)}}$ (red arrow) is greater than the direction angle threshold φ, it is not necessary to carry the message because v_o is moving toward congested road's entrance jb_{v_a} and vehicles it's about to encounter are likely to have received the message. Otherwise, v_o should carry the message when it is moving away from jb_{v_a}. The angle α between vector $\vec{A}$ and vector $\vec{B}$ is given by

$$\alpha = \arccos\left(\frac{\vec{A} \cdot \vec{B}}{|\vec{A}| \cdot |\vec{B}|}\right) \tag{1}$$

D. Broadcast Strategy

As approaching current road's exit $jf_{v_o}^{(1)}$, v_o processes CW messages it has cached by the Procedure 2 shown in Fig. 3. Denoting $t_{cl_{v_o}}$ the time when v_o entered cl_{v_o}; N_{v_o} is v_o's 1-hop neighbor set. Each element of N_{v_o} has a structure of (u, t_u), where u is the neighbor's ID and t_u is the time when u entered N_{v_o}.

```
Procedure 2 Broadcast Procedure
FOR EACH $(CW, hc)$ in $Cache$
    IF  $k \cdot \lambda^{t_{now}-t} > eff\_thresh$
        FOR EACH $(u, t_u)$ in $N_{v_o}$
            IF  $group(u) == group(v_o)$ AND $t_u > t_{cl_{v_o}}$
                Broadcast $bundle = \{o, CW, hc+1\}$
                BREAK
            END IF
        END FOR
    ELSE
        Drop $(CW, hc)$ from $Cache$
    END IF
END FOR
```

Figure 3. Pseudo code of DAGR's Broadcast Strategy.

The Broadcast Procedure takes vehicle's rational selfishness into consideration. After verifying that the cached CW does not expire, v_o iterates its 1-hop neighbor set to check whether there is any vehicle from the same group in vicinity (the first condition at line 4, Public vehicles bypass this step). If the test is positive, a broadcast attempt is initiated.

The second condition $t_u > t_{cl_{v_o}}$ is to avoid the situation where v_o and u might have kept their 1-hop neighbor relationship for a long time and v_o could broadcast one message repeatedly for u even though u has received it successfully before.

The contention-based broadcasting mode described in [10] is further introduced in case that several vehicles holding the same CW messages might do the broadcasting repeatedly at one junction. Under such circumstance, vehicles would suppress their broadcast attempt if the CW message it was going to broadcast is just overheard.

IV. EVALUATION

Mobility decision and message dissemination are influenced by each other in Dynamic Routing. To study the CW dissemination performance and its impact on vehicles' trip-time, we evaluate DAGR on an integrated simulation platform consisting of traffic simulator *sumo* [11] and network simulator *ns2*, which two are coupled through *TraCI* protocol.

A. Simulation Tools

Fig. 4 shows the simulator architecture. To achieve synchronization between two simulators, *ns2* which acts as a *TraCI* client, sends SIMSTEP commands constantly to trigger the simulation process of *sumo* from step k-1 to step k. Then *sumo* sends back all equipped vehicles' Cartesian coordinates to *ns2*. The latter updates all *ns* nodes' destination positions and start the network simulation process of step k. *sumo* keeps the map between vehicle's *sumo* node ID and *ns* node ID [12].

B. Simulation Setup

The simulation is focused on two aspects: 1. DAGR's forwarding efficiency. 2. Vehicles overall trip-time improvements.

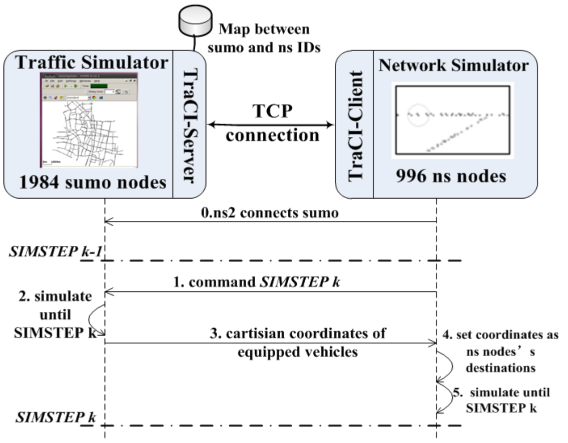


Figure 4. Architecture of *TraCI* simulation environment [12].

The scenario is based on the map of Nanjing, Jiangsu province, China, from *OpenStreetMap* project [13]. It covers 8500m×9500m downtown area of the city, containing 267 junctions and 731 road segments. The speed limit of each road segment is greater than 40km/h. 996 out of the total 1984 vehicles are equipped with SRDs. These equipped vehicles are divided into 1 Private vehicle group, 1 Public vehicle group and 2 Group vehicle groups. DAGR and Convention strategies are tested respectively in the same scenario to compare their performance on the effective-hit numbers and forwarding overheads.

1) Convention Strategy: All equipped vehicles will carry every message they overheard and broadcast them at every junction before these messages expire. It's a brutal but classic strategy, adopted by many researches (like [1][2][6]) to achieve a high delivery ratio. In the simulation, this strategy gives an upper bound in terms of effective hit number.

2) DAGR Strategy: As described in Section III, Private vehicles carry and forward nothing and only do rerouting with CWs overheard; Public and Group vehicles apply Procedure 1 and 2 in their Carry and Broadcast processes.

Before the simulation starts, departure and destination of each vehicle are generated randomly. The straight line distance between two points must larger than 4000m. This guarantees enough traffic crossing the city. The departure time of vehicles is set between 1—200s uniformly, which means there are about 10 vehicles depart per second. Road travel delay threshold is set to 150s, about 3 times of the traffic light duration, which means that if one fails to pass a road segment in two green-light periods, a conclusion can be drawn that congestion happened. Taking the scenario map size and road segment length into consideration, for simplicity the usual ns2 802.11b (with TwoRayGround propagation model) is used. The receiving threshold is adapted to achieve a transmission distance of 300m. As to the message expiration, time decay factor is set to 0.98 and threshold is set to 0.05 to keep the life time of a message at about 150s, which is the travel delay threshold. Other simulation parameters are listed in Table II.

TABLE II. SIMULATION PARAMETERS

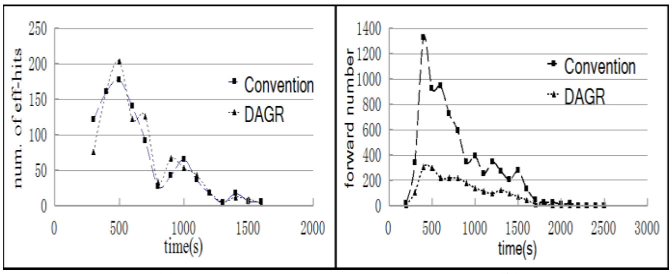
Parameter name	Value
OS version	ubuntu 10.04
sumo version	0.12.3
ns2 version	2.34
Vehicle number	1984
Non-equipped vehicle number	988
Private vehicle (G0) number	575
Public vehicle (G1) number	131 (Including 35 route-fixed buses)
Group vehicle (G2) number	194
Group vehicle (G3) number	96
Traffic light duration	45s
Position angle threshold	90 degree
Direction angle threshold	90 degree

ISBN: 978-1-61208-288-2

C. Dissemination Efficiency

In Fig. 5, we plot the number of effective hits and forwarding attempts for Convention and DAGR, respectively. As we see, DAGR achieves almost the same number of effective hits as that of Convention with only 31.5% of its forwarding overhead. In total, DAGR got 912 effective hits with 2276 forwards while Convention got 936 effective hits with 7210 forwards. Furthermore, if we define Forwarding Efficiency (FE) of a vehicle group G as the average number of effective hits caused by a single forward that vehicles of G make.

$$FE = \frac{num.\ of\ effhitscausedby\ G}{num.\ of\ \ fwds\ G\ has\ made} \qquad (2)$$



(a) (b)

Figure 5. Effective hits and forward numbers of Convention and DAGR: (a) number of effective hits.(b)number of forwards

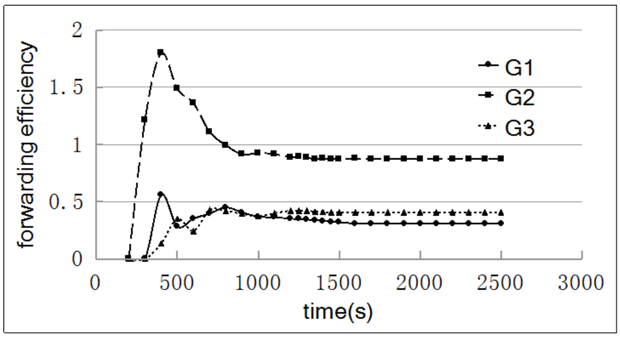


Figure 6. Forward Efficiency of vehicle groups in DAGR

Fig. 6 shows how each group's forward efficiency changes with time. We note that the most influential factor of the forward efficiency is group size instead of vehicle groups' different carrying and broadcasting strategies. Public vehicles in group G1 broadcast CW messages in every road segment before they expire, while vehicles in group G3 broadcast only when there are partners from the same group in vicinity. Yet, such a selfish strategy in broadcasting does not diminish forwarding efficiency. More specifically, each forward of vehicles in G1 result in 0.31 effective hit, in G3 result in 0.4 effective hit and in G2 result in 0.87 effective hit.

As discussed before, vehicles may use messages overheard from other groups. We call this spillover effect. To understand how broadcasting strategy influence spillover effect, we define spillover ratio as:

$$spilloverratioof\ G = \frac{effhitcausedby\ G - G's\ effhitcausedby\ G}{effhitcausedby\ G}. \qquad (3)$$

The spillover ratio of G1, G2 and G3 is 11.5, 3.08 and 5.38 respectively. This means among every 12.5 effective hits caused by G1 vehicles, 11.5 hits are contributed to vehicles of other groups. It seems that Public vehicles do more for public welfare. However, if we look each group's FE again, the largest group G2 with a 0.87, still contributes 0.87×3.08/(1+3.08)=0.66 effective hit to other groups per forward, higher than G1's 0.23 and G3's 0.34.

D. Trip-Time Improvement

We evaluate the trip-time gain/loss of our model with metrics named Trip-Time Decrease/Increase Ratio, defined in CATE [9]. Fig. 7 shows the comparison between CATE and DAGR. *oldtime* refers to vehicle's trip-time when Dynamic Routing is not used and *newtime* refers to the one when Dynamic Routing is adopted. The Decrease Ratio is defined as ratio=*oldtime/newtime*. Obviously, the greater this ratio is, the more time Dynamic Routing saved. Similarly, Increase Ratio is defined as ratio=*newtime/oldtime*. If the variation of this ratio is within ±10% trip-time, we think the vehicle is not affected in terms of trip-time.

The trip-time saving effect of Dynamic Routing is not as significant as we used to expect. As we may see, most vehicles in both models get either a slight improvement (33% in CATE and 16% in DAGR, ratio less than 1.25) or no improvement (23% in CATE and 45% in DAGR, not drawn in histograms). CATE's performance seems to be slightly better than DAGR and their distribution are roughly consistent. One point that should be kept in mind is that, since CATE adopts a replica-based forwarding mechanism while DAGR is a geo-based algorithm, they are two orthogonal techniques and may be combined to achieve a better performance.

V. CONCLUSION AND FUTURE WORK

A. Conclusion

Through discussion and simulation above, we can conclude that in Dynamic Routing, Direction-Assisted Geographic Relay can decrease forwarding overhead dramatically without sacrificing dissemination performance compared with Convention forwarding strategy. In addition, we also find that the group size is the most influential factor of forwarding efficiency despite of different forwarding strategies of vehicle groups. Even if we take spillover effect into consideration, vehicles from large-size groups still make more contributions to the total effective hit gain. As to the trip-time improvement, nearly 25% of vehicles notably benefit from Dynamic Routing while the trip-time of the rest remains almost unchanged (±25% trip-time).

B. Future Work

The DAGR model in this paper is specially tailored for Dynamic Routing and may not support other vehicular network applications, especially those requiring a high real-time performance and cooperation between vehicles, such as traffic safety applications. To build a general dissemination model is a very challenging and meaningful task and certainly a lot of factors about performance, security and privacy need to be taken into consideration.

During the simulation, we set two DAGR's angle thresholds to an intuitive value $\phi = \varphi = 90^o$. Whether it is an optimal choice still needs to be investigated, both theoretically and experimentally. Furthermore, the urban scenario still needs more improvements and different ratios of vehicles will be evaluated to figure out how these parameters influence the system performance.

Last but not least, messages from other groups may not be trusted completely in real life for security considerations. Trust management between different vehicles is still an unsolved problem. Some trust models for vehicular network have been proposed, but they still need to be tailored for specific applications and their effectiveness yet need to be evaluated in realistic scenarios.

ACKNOWLEDGMENT

This work was supported in part by International Researcher Exchange Project of National Science Foundation of China and the French Centre National de la Recherche Scientifique (NSFC-CNRS) under the Grant No 61211130104 and National Science Foundation of China under Grants No 60932003, 61271220.

REFERENCES

[1] B. Karp and H. T. Kung, “GPSR: Greedy Perimeter Stateless Routing for Wireless Networks,” Proc. of MobiCom’00, ACM Press, Aug. 2000, pp. 243-254, doi:10.1145/345910.345953.

[2] C. Lochert, M. Mauve, H. Füßler, and H. Hartenstein, “Geographic Routing in City Scenarios,” ACM SIGMOBILE Mobile Computing and Communications Review, vol. 9, no. 1, Jan. 2005, pp. 69–72, doi:10.1145/1055959.1055970.

[3] P. C. Cheng, K. C. Lee, M. Gerla, and J. Härri, “GeoDTN+Nav: Geographic DTN Routing with Navigator Prediction for Urban Vehicular Environments,” Mobile Networks and Applications, Springer, vol. 15, Feb. 2010, pp. 61-82, doi:10.1007/s11036-009-0181-6

[4] K. Lee, U. Lee, and M. Gerla, “Geo-Opportunistic Routing for Vehicular Networks,” IEEE Communications Magazine, vol. 48, no. 5, May 2010, pp. 164-170, doi:10.1109/MCOM.2010.5458378.

[5] G. Ma, D. Wang, G. Zhao, and M. Huang, “A geographical opportunistic dissemination protocol via bus networks,” Proc. of Intelligent Sensors, Sensor Networks and Information Processing International Conference (ISSNIP 2008), IEEE Press, Dec. 2008, pp. 499-504, doi:10.1109/ISSNIP.2008.4762038.

[6] L. Wischhof, A. Ebner and H. Rohling, “Information dissemination in self-organizing intervehicle networks,” IEEE Transections on Intelligent Transportation Systems, vol. 6, no. 1, Mar. 2005, pp.90-101, doi:10.1109/TITS.2004.842407.

[7] Y. Yang and R. Bagrodia, “Evaluation of VANET-based advanced intelligent transportation systems,” Proc. of the 6th ACM international workshop on VehiculAr InterNETworking (VANET ’09), ACM Press, Sep. 2009, pp. 3-12, doi:10.1145/1614269.1614273.

[8] I. Leontiadis and C. Mascolo, “Opportunistic spatio-temporal dissemination system for vehicular networks,” Proc. of the 1st international Mobisys Workshop on Mobile Opportunistic Networking (MobiOpp ’07), ACM Press, Jun. 2007, pp. 39-46, doi:10.1145/1247694.1247702.

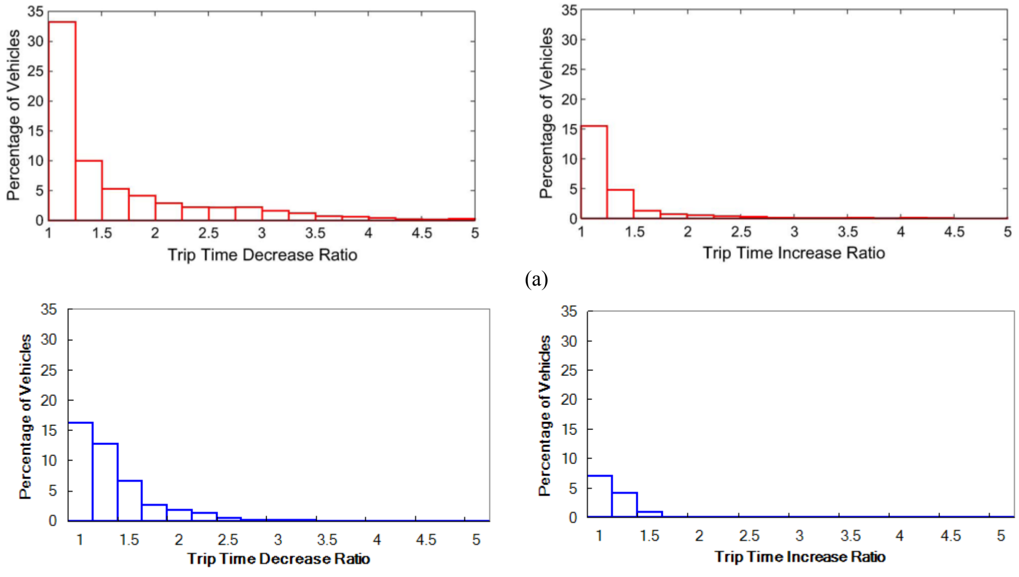
[9] I. Leontiadis, G. Marfia, D. Mack, G. Pau, C. Mascolo, and M. Gerla, “On the Effectiveness of an Opportunistic Traffic Management System for Vehicular Networks,” IEEE Transactions on Intelligent Transportation Systems, vol. 12, no. 4, Dec. 2011, pp. 1537-1548, doi:10.1109/TITS.2011.2161469.

[10] H. Füßle, H. Hartenstein, J. Widmer, M. Mauve, and W. Effelsberg, “Contention-based Forwarding for Street Scenarios,” in the 1st International Workshop in Intelligent Transportation (WIT ’04), Hamburg, Germany, Mar. 2004, pp. 155-160.

[11] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, “Sumo - simulation of urban mobility: An overview,” in the 3rd International Conference on Advances in System Simulation (SIMUL 2011), Barcelona, Spain, Oct. 2011, pp. 63-68.

[12] A. Wegener, M. Piórkowski, M. Raya, H. Hellbrück, S. Fischer and J.-P. Hubaux, “Traci: An interface for coupling road traffic and network simulators,” Proc. of the 11th Communications and Networking Simulation Symposium (CNS'08), ACM Press, Apr. 2008, pp. 155-163, doi:10.1145/1400713.1400740.

[13] M. Haklay and P. Weber, “OpenStreetMap: User-Generated Street Maps,” IEEE Pervasive Computing, vol. 7, no. 4, Oct. 2008, pp. 12-18, doi:10.1109/MPRV.2008.80.



(a)

(b)

Figure 7. Trip-time improvement of CATE [9]and DAGR:
(a) Histogram of CATE’s trip-time gain/loss. (b) Histogram of DAGR’s trip-time gain/loss

The Charge Collector System

A New NFC and Smartphone-based Toll Collection System

João R. Dias, Arnaldo S. R. Oliveira, João Nuno Matos
Departamento de Electrónica, Telecomunicações e Informática, Universidade de Aveiro
Instituto de Telecomunicações
Aveiro, Portugal
(jmrd@ua.pt, arnaldo.oliveira@ua.pt, matos@ua.pt)

***Abstract* — This paper proposes a new system to collect tolls on open road tolling (ORT) infrastructures. The actual Electronic Toll Collection (ETC) systems do not fulfill fundamental user requirements, such as interoperability and portability between systems and road operators (in the same or different countries), as well as advanced toll logging and reporting (capabilities ensuring user privacy, an interesting feature in car rental or sharing use cases). The C2S is a work in progress project that will provide some features, such as flexible payment options, recording of incurred tolls and make them available to the end user and management entities, exploring a synergy of technologies in ETC scenario, namely Dedicated Short Range Communication (DSRC), Global Navigation Satellite System (GNSS), Near Field Communication (NFC) and smartphone-based mobile applications. This system is also an approach to interoperable European ETC solutions, in a way that uses DSRC and GNSS-based solutions together.**

Keywords— Electronic toll collection; EETS; DSRC; GNSS; multitechnology OBU.

I. Introduction

Since the 60's, the Electronic Toll Collection (ETC) is used around the world and, on last decade, it is becoming more and more pervasive [1]. The benefits of ETC associated to free flow systems are well known and the actual trends point to the creation of Open Road Tolling (ORT) infrastructures, i.e., roads where tolls are entirely electronic with little or no impact on traffic flow. The two main technologies used on ORT are based on:

- Dedicated Short Range Communication (DSRC) transponders [2], using 5.8 GHz microwave technology;
- Global Navigation Satellite System (GNSS) with Global System for Mobile Communications (GSM) [3], i.e., satellite positioning coupled with mobile communications.

Besides its advantages, the current ORT systems do not address conveniently the following issues:

- The flexibility of the bank account that can be used for toll payment, i.e., currently, users have always to pay by the same bank account, which can be an issue in some cases;
- The payment information/receipts or toll logs are not readily available to the user or management entities. In some cases, such as rent-a-car or car sharing companies, there is a need to know if costumers used tolls and payment has been done. In some systems, the information or toll receipt takes 48 hours to be available [4];
- The lack of an On-Board Unit (OBU) user interface that could provide road information and support for implementing Dynamic Road User Charging (DRUC) [5] systems. On current systems it is impossible to apply different prices on several users in real-time because there is no user interface to say how much he/she has to pay [6];
- The problems related to interoperability between different systems. If a user travels abroad, she/he cannot use ETC automatically without buying the local OBU [7];
- In case of GNSS-GSM based infrastructures, the toll companies have to use GSM so they are dependent of mobile operators [8].

These issues constitute a set of challenges that motivate the researching on new technologies and tolling mechanisms.

This paper starts with the motivation to this work, i.e., what is the problem that this solution solves. Next, the architecture and the utilization methods are described, as well as the OBU operation. Then, we show a first step in the development of the proof-of-concept, the technologies and challenges related to its implementation. Finally, two user cases are presented, one related to the interoperability between systems and the other targeted to a car sharing system.

II. Motivation

The C2S proposed in this paper is specially developed to ORT infrastructures and it consists of a new OBU that integrates the most used technologies on toll collection: DSRC and GNSS, with a smartphone mobile application, providing new features to the users, such as:

- A mobile application with a user-friendly interface, which provides several types of information (e.g. road prices, best routes, tolls to pay, selection of the payment method / bank account, etc.);
- A new payment method based in NFC, that many believe to be widely used in a near future – user simply touches the OBU with a smartphone and collects all the bills to pay.

Moreover, gathering the characteristic of this system proposal, there is an opportunity to establish a new mechanism of interoperability between the different technologies used on toll collection [7], since the C2S OBU proposal combine the two technologies used on most of the actual systems.

III. C2S OVERVIEW AND ARCHITECTURE

The idea to create this system arises from the expectable demand for mobile applications and NFC technology to pay bills. This system proposal breaks the current paradigms, introducing the possibility of flexible payment after incurring on tolls.

In most ORT infrastructures this system will follow the process illustrated in Figure 1: the C2S enabled vehicle acts as an OBU that is not recognized by the conventional DSRC tolling system. When it passes on tollbooths, the enforcement system is triggered and the Automatic License Plate Recognition (ALPR) takes a picture; however, the C2S OBU saved the toll and it provides the possibility to pay in a legal time period.

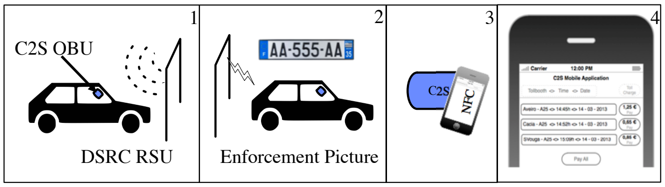

1
C2S OBU
DSRC RSU
2
AA-555-AA
Enforcement Picture
3
C2S
NFC
4
Carrier
12:00 PM
C2S Mobile Application
Tollbooth <> Time <> Date
Toll Charge
Aveiro - A25 <> 14:45h <> 14 - 03 - 2013
1,25 €
Cacia - A25 <> 14:52h <> 14 - 03 - 2013
0,65 €
SVouga - A25 <> 15:09h <> 14 - 03 - 2013
0,85 €
Pay
Pay All

Figure 1 – Utilization steps.

So, basically, there is an OBU, called C2S, that collects the tolls while the user is driving. After the travel, the user can transfer all the toll logs to a smartphone (with NFC) by a simple touch and pay the tolls via a mobile application, in a legal time period (e.g., one week).

Although it seems awkward, there are some niche markets interested in a log and post payment, as discussed bellow in use case scenarios.

A. *OBU Architecture*

The base of C2S is a new OBU composed of several blocks, as illustrated in Figure 2, and implemented on an embedded computer that provides General Purpose Input/Output (GPIO) and USB ports to connect with a GPS receiver, a DSRC Beacon Service Table (BST) detector and the NFC interface. The embedded computer runs several processes to control those peripherals. On the block diagram, in Figure 2, we also included a smartphone as an element of the system because it is where the user interface and a mobile application which communicates with the system OBU via NFC are implemented.

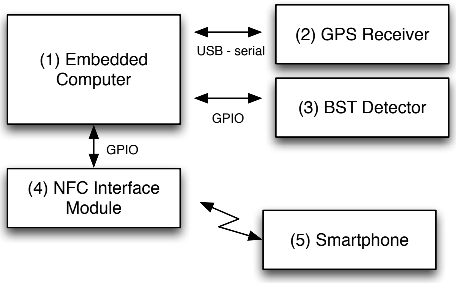


Figure 2 – Overall on-board system block diagram.

The main block is an (1) embedded computer that receives all information from a (2) GPS locator and a (3) BST detector. The GPS locator is responsible for tracking the vehicle and setting time/date when the OBU is turned on. The BST is the first message received from the Road Side Unit (RSU) in a DSRC toll system. Its detector is a small radio device that triggers a signal to the embedded computer when the vehicle passes in a toll. Finally, this OBU can establish communication with a smartphone (with a mobile application) via NFC.

B. *OBU Operation*

The OBU operation is divided into several steps, as illustrated in Figure 3:

- When the system starts, it sets the time and date via GPS and determines if the vehicle is on a DSRC or GNSS/GSM infrastructure;
- In case of a DSRC infrastructure, when a vehicle (with this OBU) passes in a toll, it detects a BST and saves its location via GPS receiver; If the vehicle is in a GNSS/GSM infrastructure, it will track the location and find the position of virtual tolls;
- If the toll is valid to pay, the system saves the information about date and tollbooth location;
- During the road trip, the user has only to touch his smartphone with the OBU and the data containing the tolls to pay is transmitted to the mobile. So the user can check via mobile application how much he has to pay for the tolls;

Finally, the user has to pay the tolls in a legal time period, via a web service.

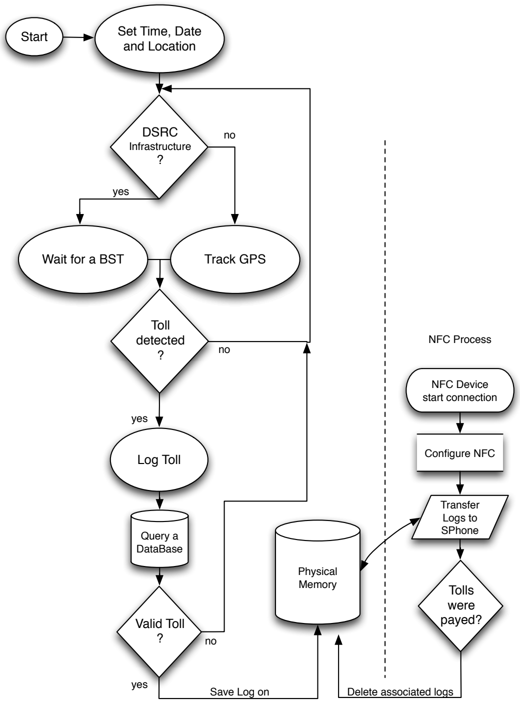


Figure 3 - Operational flow diagram.

ISBN: 978-1-61208-288-2

The web service component and mobile application are outside of the scope of this paper, but it is worth to mention that the ability to specify the payment method, the bank account and other options can be provided.

IV. Proof of Concept Implementation

To build a proof-of-concept prototype, in order to test the functionality of the system, we chose a cheap and widely used computer called Raspberry Pi (RPi) model B as host computer and a GPS receiver [9] attached via USB-Serial was employed, as illustrated in Figure 4.

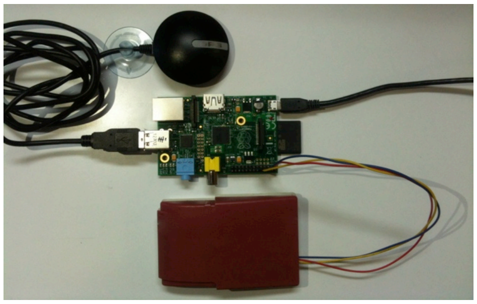


Figure 4 – Prototype - RPi, USB GPS Receiver and BST Detector.

Running on Raspberry Pi is the lightweight and flexible Arch Linux distribution. As already mentioned, there are three peripherals on the system: BST detector, NFC module and GPS receiver. The BST detector simply triggers an interrupt via GPIO pins. One possibility to connect the NFC module is via RPI UART (Universal Asynchronous Receiver/Transmitter). Finally, to communicate with the GPS receiver, it was used the GPS daemon (*gpsd*) service. It is a service that monitors the GPS receiver organizing the sensor data (like location or velocity) to be queried by a client session.

A. GNSS – GPS receiver

The *gpsd* service is widely used because it is easier to parse information compared with NMEA 0183 (National Marine Electronic Application specification) emitted by most GPSes [10]. On the other hand, it recognizes different sensors and it can sniff all the incoming data with zero configurations, it is almost plug and play.

Although the *gpsd* is an open-source project, it has quality and it is an audited code, which already won the Good Code Grant from the Alliance for Code Excellence [11].

Figure 5 illustrates the dataflow diagram. When the sensor receives a signal it fed the packet sniffer, which has the job to tell core library that contains payload to be interpreted. The driver determines the type of packet information. When the packet reaches the end, the data is sent to an exporter to be available to a client. The main exporter uses sockets where an object is generated in JSON and it is provided to all the clients that are watching the device. There is also the option to export data via Shared Memory or via D-Bus [12].

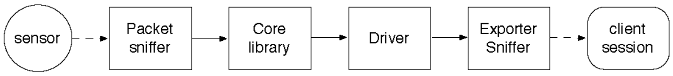


Figure 5- GPS dataflow [12].

The *gpsd* service includes a linkable C service library that encourages developers to use it on their applications. So, the objective is to implement a program, which launches a process that configures and creates a client session.

On GNSS/GSM infrastructure, the client session will track the GPS and compare its location with the fix locations of virtual tollbooth. Here, there is an implementation challenge. To increase the efficiency of the system it is important to define a strategy of how to determine if the vehicle incurred on tolls. One option is to use a data structure that sorts the location of tollbooths by route, i.e., tracking few points it determines in which route the vehicle is and predicts which is the location of the next tollbooth, as illustrated in Figure 6.

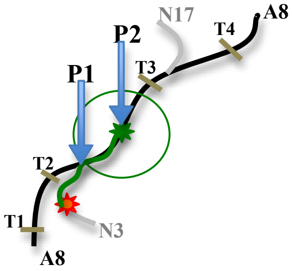


Figure 6 – Route Tollbooth.

The process has a cache memory where the recent positions are saved and compared to each other. For example, sampling two points: P1 and P2, illustrated in Figure 6, it is possible to define a path, to assign it to a route (A8) and then to predict the probable next tollbooth (T3). This approach is in progress and under study.

On DSRC infrastructures, we do not have this problem. Due to BST detector, a flag is raised when the vehicle passes on tollbooth. So, a process logs the position of tollbooth and subsequently compares this with a database of tollbooth locations, to infer the validity of the logging and offer other type of information to the user (price, etc.).

B. General purpose Input/Output pins

Using the GPIO and a simple electronic circuit to control a Radio Frequency module, it is possible to activate an interrupt a line of the host computer (Raspberry Pi).

Finally, the GPIO will be also used to connect to a NFC device via an UART to subsequently communicate with the smartphone mobile application. The goal is to implement a communication based on NFC, because it is a user-friendly technology and, at the same time, secure, as it implies that anyone who wants read, the data of the OBU, has to touch on it so she/he has to be inside of the vehicle.

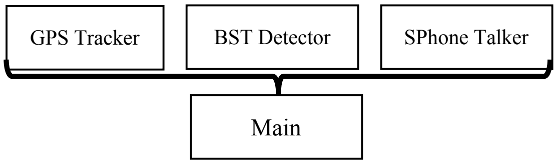


Figure 7 – Primary embedded computer processes.

Copyright (c) IARIA, 2013. ISBN: 978-1-61208-288-2

Briefly, there are several processes: GPS Tracker, BST Detector and Smartphone Talker. These support the main process, illustrated in Figure 7, and together implement the algorithm presented on operational diagram from Figure 3.

V. USE CASE SCENARIO

In some countries, there are user needs that are not satisfied on ORT infrastructures due to the limitations already mentioned. The two issues already listed are the lack of interoperability and a factual case related to car rental or car sharing.

A. Interoperability

One of the most unreasonable restrictions on ETC from the user perspective is the lack of interoperability between distinctive ETC systems of different countries, illustrated in Figure 8. For example, in Europe, there are systems based on same technology (DSRC) and there are countries that use different systems, like Germany that uses GNSS-GSM [13]. In both cases there is no evidence of interoperability between systems. If a driver wants to go from Nice to Aveiro he has to use the manual toll collection systems or travel on national routes, or in worst case, if he has to do it frequently, affix several DSRC electronic tags on his vehicle.

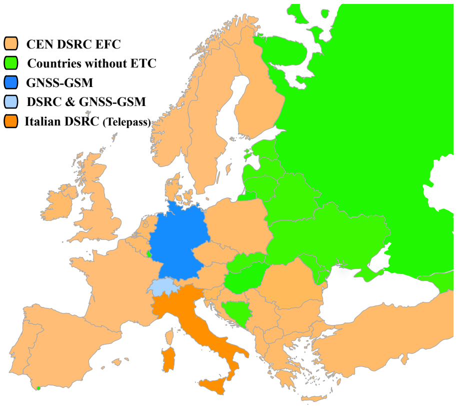


Figure 8 – Distribution of the systems in EU.

From the economical perspective, the road-networks are essential to support the competitiveness, sustainability and success of the markets between states that share long line land borders [7].

So, to address these issues, the European Commission decided to create a European Electronic Toll Service (EETS), launching the Directive 2004/52/EC and related Decision 2009/750/EC [7]. The main objectives are to establish interoperability and to reduce the proliferation of incompatible systems in European Union. The project takes into account technology already implemented and aims to create a road-usage declaration by means of a single OBU.

Following the directive, the C2S proposal constitutes a system technologically compatible with the existing systems. Moreover, the system conceptually ensures interoperability between systems. The user can drive on GNSS-GSM or DSRC infrastructures. The C2S saves the incurred tolls and makes them available for payment in real-time. The user has only to access to the pay web platform (which can be via mobile application), paying in the preferable method, in a legal time. This feature allows users to pay when they have a good and cheap Internet connection (e.g., WiFi) and it represents an advantage to the GNSS-GSM systems where the payment is made via GSM [3]. To implement this feature, it is only needed that each toll company of each country creates a web platform available to the user that receives all the toll payments.

B. Car Rent/Sharing

Another pitfall of the actual systems arises when a costumer rents a car or uses a car sharing service (in a vehicle without an OBU) and passes in an ORT tollbooth. The enforcement system is triggered and a picture is taken and the vehicle is identified via ALPR system. So some time later the rent car company receives the toll receipts to pay the expenses of some costumer. So usually the company sends the receipt to the costumer that probably already left the country, in case of tourism or business travels and then it charges the expenses on the credit card associated with the rent car contract [4]. Otherwise, if the costumer is still around, he can pay the tolls for example in central post office or in a pay shop.

In both cases, the current system causes troubles to costumers, which undeservedly do not understand the information and easily are driving on an ORT. It also causes problems to the hire firms that have to install OBUs on their vehicles and even then do not solve the problem, since the receipts are sent only 48 hours after the incurrence, so the costumer already left the country.

The C2S solves this problem with a simple feature of providing to the rent car company a toll declaration of each costumer. Using a simple and cheap OBU (C2S), it is possible to know if the vehicle incurred tolls just touching a smartphone or a NFC reader to the C2S OBU.

VI. CONCLUSION AND FUTURE WORK

The number of ORT infrastructures is increasing, based on their benefits for the user and the reduction of operational costs for toll companies.

However, these systems have some limitations and do not answer to the requirements of some users, such as rent-a-car costumers, car sharing users and foreign drivers.

The C2S will allow any road user to pay easily the incurred tolls in a friendly user interface.

For now, the system is a work in progress project with the main system blocks, interfaces and communication technologies already operating.

For the future work, we need to develop an application that transfers all the toll data to the toll provider, via mobile application, so it is essential to create an API (Application Programming Interface), in toll providers systems. Finally, to conclude the proof of concept, it is required to test this solution in real scenarios, across several countries in different systems.

REFERENCES

[1] K. Persad, C. Walton, and S. Hussain, “Toll Collection Technology and Best Practices Vehicle,” pp. 1–2, 2007.

[2] R. Zhengang and G. Yingbo, “Design of Electronic Toll Collection System in Expressway Based on RFID,” 2009 International Conference on Environmental Science and Information Application Technology, pp. 779–782, Jul. 2009.

[3] K. Persad, C. Walton, and S. Hussain, “Electronic vehicle identification: Industry standards, performance, and privacy issues,” pp. 1–3, 2007.

[4] “The News Online,” 2013. [Online, retrieved: July, 2013]. Available: http://www.theportugalnews.com/news/view/1147-1

[5] N. Velaga, K. Pangbourne, and K. Papangelis, “GNSS-based Dynamic Road User Charging System,” pp. 11–13, 2010.

[6] R. Sanchez, “Pricing Models in the Toll Road Business,” 2011.

[7] E. P. E. Council, “Directive 2004/52/EC interoperability of electronic road toll systems in the Community.” EUR-Lex. European Union, pp. 4–54, 2011.

[8] W. Beier and R. L. Rodriguez, “EG5 on GNSS technologies for EFC Open issues to enable the widespread introduction of GNSS-based EFC services in Europe Final report,” p. 15, 2005.

[9] “USGlobalsat BU 353,” 2012. [Online, retrieved: July, 2013]. Available: http://www.usglobalsat.com/p-62-bu-353-w.aspx#images/product/large/62.jpg.

[10] “National Marine Electronics Association (US).,” NMEA 0183--Standard for Interfacing Marine Electronic Devices, 2002.

[11] “CATB,” 2013. [Online, retrieved: July, 2013]. Available: http://catb.org/gpsd/.

[12] “GPSD,” 2013. [Online, retrieved: July, 2013]. Available: http://www.aosabook.org/en/gpsd.html.

[13] IBTTA, “State of the Art Analysis of European Toll Collection Systems,” 2004.

Low-power TPMS Data Transmission Technique Based on Optimal Tire Condition

Suk-seung Hwang
Dept. of Mechatronics Engineering,
Chosun University
Gwangju, Korea
hwangss@chosun.ac.kr

Seong-min Kim
Dept. of Advanced parts and
Materials Engineering
Chosun University
Gwangju, Korea
millionairek@naver.com

Jae-Young Pyun,
Goo-Rak Kwon
Dept. of Information and
Communication Engineering,
Chosun University
Gwangju, Korea
jypyun@chosun.ac.kr,
grkwon@chosun.ac.kr

Abstract—**Tire Pressure Monitoring System (TPMS), which is a type of wireless communication device used in vehicles, is a safety aid system designed to prevent tire-related accidents in advance by regularly checking tire pressure and temperature and notifying the driver about any abnormality through its display. TPMS sensor unit in a tire contains sensors to measure the temperature and pressure and transmits the measured data to the signal processing unit in a vehicle via wireless communication. For the conventional TPMS, there is unnecessary power consumption in the sensor unit because of continuous transmission of the measured data from the tire to the signal processing unit at a regular interval. In this paper, we propose the low-power TPMS communication technique in which the signal processing unit in the vehicle transmits optimal tire pressure and threshold values based on the road condition and external temperature to the sensor unit in the tire. The sensor unit compares the measured data value with the optimal tire pressure value received from the signal processing unit and it sends the measured tire pressure data to the signal processing unit only if the difference between the values exceeds the threshold value. When the difference between both values is smaller than the threshold value, the sensor unit recognizes it as normal mode and transmits a normal mode bit to the signal processing unit. The performance of the proposed low-power TPMS communication technique is verified through computer simulation example.**

Keywords-Tire Pressure Monitoring System (TPMS); Low-Power; Optimal Tire Pressure Value.

I. INTRODUCTION

Tire pressure may become lower or higher comparing with the standard condition, due to certain circumstances during vehicle operation, resulting in serious accidents. The majority of drivers may not be able to detect such risk in advance, which often leads to a major accident [1][2]. In order to prevent this problem, TPMS was developed and there have been active studies to develop high-performance TPMS. TPMS can be defined as a safety aid system that displays the information about temperature and pressure from the sensors attached to the tire wheel or valve to the driver so that the driver can check the tire condition in real time and thus prevent the tire-pressure related accident in advance [3][4][5][6][7]. Currently, many countries are promoting to mandate or have already mandated vehicles to be equipped with TPMS. A representative example that has led to mandating TPMS due to an accident in which some of the tires supplied by one of the world's largest tire manufactures had ruptured while driving due to lower air pressure, leading to many casualties. With this incident, the United States legislated about TPMS on vehicles in 2003 and has mandated to install TPMS on every vehicle since September 2007 [8][9]. In Korea, it is mandatory to install TPMS on all passenger cars and vans less than 3.5 tons to be manufactured after January 1, 2013.

Most of the currently TPMSs need to be replaced when the battery for the sensor unit is exhausted, making it an urgent need to develop the low-power TPMS. To solve this problem, we propose in this paper a low-power TPMS wireless communication scheme based on a duplex communication. In the proposed scheme, the signal processing unit in the vehicle saves the information of optimal tire pressure values for road conditions and external temperature in its database, measures the road conditions and the external temperature using sensors attached to the bottom of the vehicle, selects optimal tire pressure and threshold value from the database, and sends them to the sensor unit. Instead of transmitting data of the tire pressure and temperature at a certain interval (for example, per second) to the signal processing unit, the sensor unit sends the measured data only when the tire pressure is not normal that the difference between the measured pressure in sensor unit and the optimal pressure transmitted from signal processing unit is greater than the threshold for the instant external condition. As a result, the sensor unit attached to the tire may consume much less power than the conventional TPMS.

The rest of this paper is organized as follows. In Section II, the system model for the low-power TPMS wireless communication is presented. The data structure for the proposed system is described in Section III and a flow-chart for low-power TPMS wireless communications is presented in Section IV. In Section V, we provide computer simulation results to demonstrate the performance of the proposed system. Finally, conclusions are outlined in Section VI.

II. SYSTEM MODEL FOR LOW-POWER TPMS WIRELESS COMMUNICATION

In the low-power TPMS wireless communication scheme proposed in this section, the signal processing unit in a

ISBN: 978-1-61208-288-2

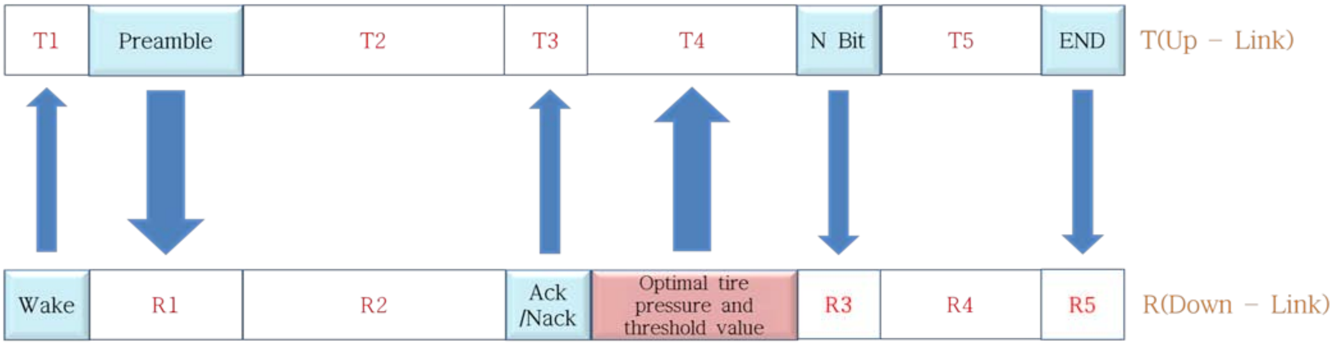


Figure 1. Data structure for low-power TPMS wireless communications based on duplex communications (Normal Mode).

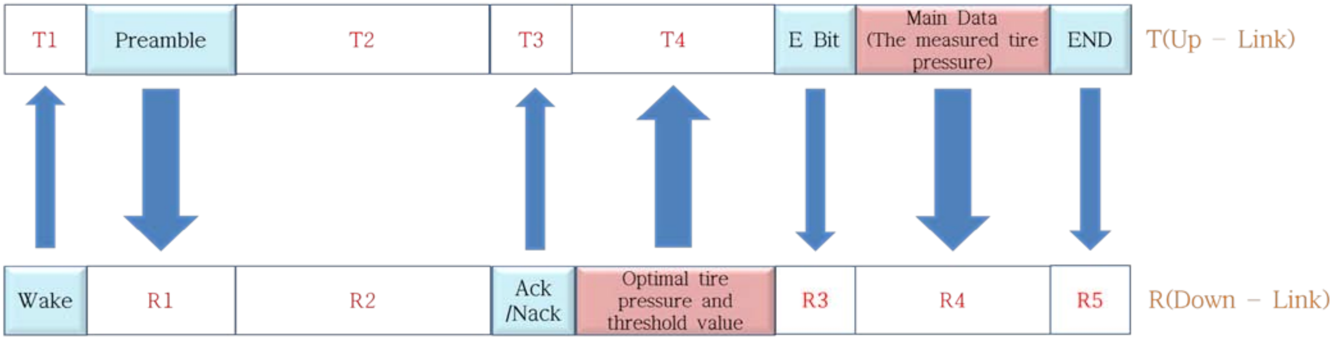

T1
Preamble
T2
T3
T4
E Bit
Main Data (The measured tire pressure)
END
T(Up − Link)
Wake
R1
R2
Ack /Nack
Optimal tire pressure and threshold value
R3
R4
R5
R(Down − Link)

Figure 2. Data structure for low-power TPMS wireless communications based on duplex communications (Emergency Mode).

vehicle transmits the tire pressure and threshold value suitable for the road condition and the external temperature to the sensor unit on the tire, and the sensor unit compares the measured data with the optimal tire pressure value received from the signal processing unit and sends the measured tire pressure data to the signal processing unit only if the difference is bigger than the threshold value. The sensor unit compares the measured tire pressure data with the optimal tire pressure and threshold value using (1)

$$|x-a_i| \gtrless \beta, \quad i=1,2,3,4 \qquad (1)$$

where, x is an optimal value for the tire pressure suitable for the road condition and external temperature, α_i means the tire pressure measured at the i th tire, and β is a threshold value.

For example, if the threshold value β to determine the tire condition is set to 3 and the optimal pressure x for road conditions and external temperature to 40Psi, and the actually measured tire pressure α_i is 35Psi, the difference between the optimal tire pressure and the measured tire pressure is 5, which exceeds the preset threshold value of 3. In this case, the sensor unit determines the tire condition as dangerous state and the sensor unit operates in the emergency mode to send the measured tire pressure to the signal processing unit at a regular interval (for example, every second). For another example, assuming that the preset threshold value β and the optimal tire pressure x for road conditions and external temperature are the same as in the first example, if the measured tire pressure α_i is 38Psi, the difference between the optimal tire pressure and the measured tire pressure would be 2. As it is smaller than the preset threshold value 3, the sensor unit determines that the tire pressure is in normal state. In this case, the sensor unit operates in the normal mode, and sends N bit for normal mode to the signal processing unit only when the optimal tire pressure and threshold value are received from the signal processing unit (e.g., per minute).

III. Data Structure for Low-Power TPMS Wireless Commiunication

In this section, data structures for the low-power TPMS wireless communications based on duplex communication are proposed. Fig. 1 and Fig. 2 show data structures for normal mode and emergency mode for the proposed low-power TPMS wireless communication technique, respectively. Most of the currently used TPMSs use simplex wireless communication mode, in which the data measured at the sensor is transmitted periodically (e.g., per second), resulting in unnecessary power consumption. The data structure proposed in this paper transmits the optimal tire pressure data periodically (e.g., per minute) from the signal processing unit to the sensor unit, and transmits the measured pressure data from the sensor unit to the signal processing unit. It switches to emergency mode only if the measured data is larger than the preset threshold value. This allows saving the power consumption of the battery installed in tires and thus the proposed TPMS communication technique is much more efficient than the conventional TPMS in terms of power management.

A. Data Structure for Normal Mode

Components of the low-power TPMS wireless communication data structure for normal mode are defined as follows:

- Wake: a bit for requesting the operation of the sensor unit.
- Preamble: data for channel estimation, signal-to-interference and noise ratio (SINR) estimation, synchronization, etc.
- Ack/Nack: Ack bit means that the transmitted data is effective and Nack bit means that the transmitted data is non-effective (for example, transmitting ‘1’ for Ack and transmitting ‘0’ for Nack).
- Optimal tire pressure and threshold value: optimal tire pressure and threshold value selected from the database of measured road conditions and external temperature sent to the sensor unit.
- N Bit: informing the normal state bit.
- END: information bit for the end of the transmission of the main data.
- T1: blank in the sensor unit for receiving Wake bit.
- T2: blank in the sensor unit for waiting the transmission of the preamble data for other tires.
- T3: blank in the sensor unit for receiving Ack/Nack bit from signal processing unit.
- T4: blank in the sensor unit for receiving data of the optimal tire pressure and threshold value.
- T5: blank in the sensor unit between transmitting N bit and transmitting END bit.
- R1 : blank in the signal processing unit for receiving the preamble data.
- R2 : blank in the signal processing unit for waiting the transmission of the preamble for other tires.
- R3 : blank in the signal processing unit for receiving N bit.
- R4 : blank in the signal processing unit between receiving END bit and receiving N bit.
- R5 : blank in the signal processing unit for receiving END bit.

B. Data Structure for Emergency Mode

Components of the low-power TPMS wireless communication data structure for emergency mode are defined as follows (terms already defined in the normal mode structure are omitted):

- E bit: informing the emergency state bit.
- R3: blank in the signal processing unit for receiving E bit.

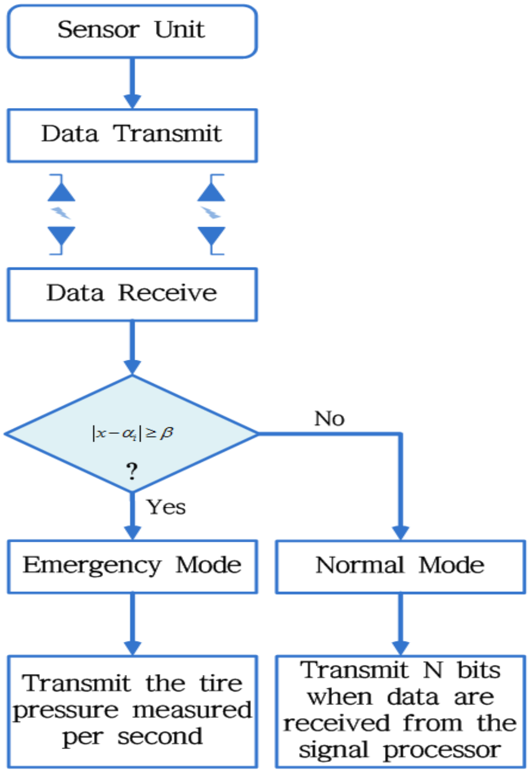

Sensor Unit
Data Transmit
Data Receive
$|x-\alpha_i| \geq \beta$
?
No
Yes
Emergency Mode
Normal Mode
Transmit the tire pressure measured per second
Transmit N bits when data are received from the signal processor

Figure 3. Flow-chart for low-power TPMS wireless communications based on duplex communications.

- R4 : blank in the signal processing unit for receiving the main data.

The proposed low-power TPMS wireless communication system based on duplex communications repeats transmitting /receiving the above-mentioned data between the sensor unit and the signal processing unit as needed.

IV. FLOW-CHART FOR LOW-POWER TPMS WIRELESS COMMUNICATIONS

This section presents a basic flow-chart for the proposed low-power TPMS wireless communication based on a two-way communication, as shown in Fig. 3. Based on the data received from the signal processing unit, if the left side of (1) is bigger than the preset threshold value, it is deemed dangerous condition, causing TPMS to operate in an emergency mode. In this case, the tire pressure data is transmitted to the signal processing unit every second the same as in one-way wireless communications, so that the tire pressure can be checked every second. On the other hand, if the left side of (1) is smaller than the preset threshold value, it is deemed normal condition, leaving TPMS to operate in normal mode. In this case, the sensor unit transmits N bit for normal condition to the signal processing unit, only when receiving the optimal tire pressure and threshold value data from the signal processing unit, instead of transmitting the tire pressure data every second.

V. COMPUTER SIMULATION

In this section, we present the results of computer simulation to demonstrate the performance of the low-power TPMS wireless communication technique based on duplex communications, comparing with the conventional one-way TPMS communication scheme. For the first simulation, we assume that the length of preamble and main data are 56 bits and main 32 bits, respectively, thus the total length of TPMS data frame is 88 bits. It is also assumed that the subject vehicle operates two hours a day in a 30 days period. For the conventional TPMS wireless communication scheme, it is assumed that the sensor unit transmits a data frame every second in consideration of emergency. For the proposed scheme, it is assumed that the signal processing unit transmits the optimal tire pressure and threshold value to the sensor unit once per minute. Fig. 4 shows the comparison of the total number of bits transmitted in the two systems when the tire condition was normal for the considered period. As shown in the figure, for the 30 days period, the total number of bits transmitted in the proposed system is much smaller than in the conventional one-way TPMS system. Fig. 5 shows the comparison of the total number of bits transmitted in the two systems, with the assumption that the systems operated in emergency mode for approximately 30 minutes as the tire fault was detected on the 15th day. As shown in the figure, although the number of bits transmitted in the proposed system is increased as it operated in emergency mode for 30 minutes on the 15th day, it is much smaller than the number of bits transmitted in the conventional one-way TPMS system.

Fig. 6 shows the comparison of power consumption in the two systems for 30 days, assuming the transmitted power per bit is 0.1μW and the tire condition is normal. As shown in the figure, the total power consumption for the sensor unit in the proposed system is significantly lower than the conventional system. Fig. 7 shows the comparison of power consumption in the two systems with the assumption that the transmitted power per bit is 0.1μW and the systems

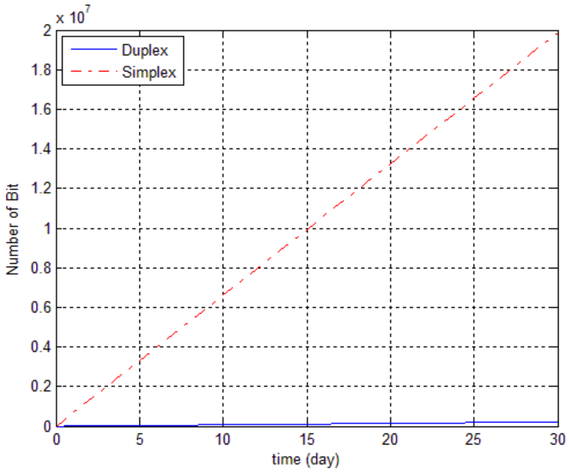


Figure 4. Number of bits versus duration for the proposed and conventional TPMS communiatoin tehcniques for normal mode

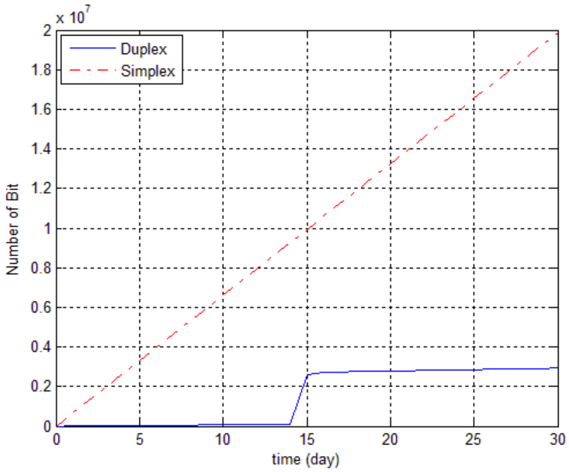


Figure 5. Number of bits versus duration for the proposed and conventional TPMS communiatoin tehcniques for considering the emergence mode

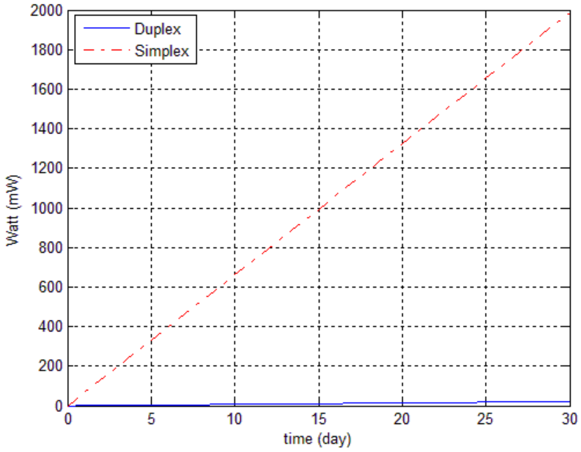


Figure 6. Power consumption versus duration for the propsed and convetional TPMS communications technues for normal mode.

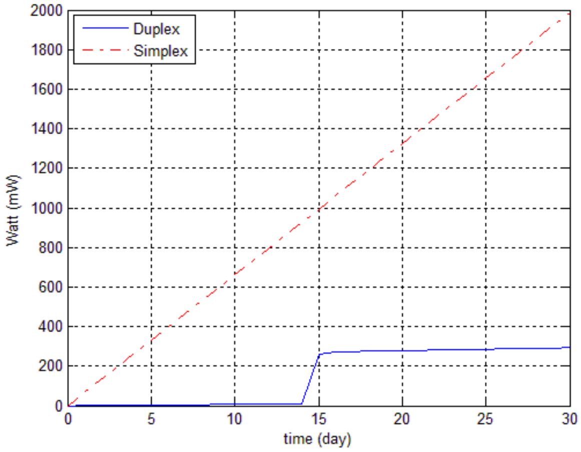


Figure 7. Power consumption versus duration for the proposed and conventional TPMS communiatoin tehcniques for considering the emergence mode

ISBN: 978-1-61208-288-2

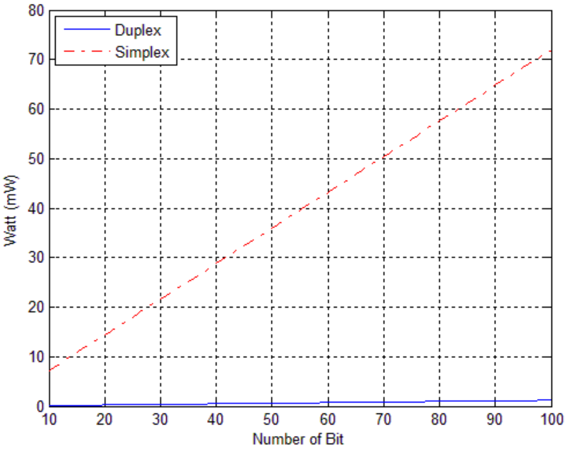


Figure 8. Power consumption versus number of bits for the proposed and conventional TPMS communiatoin tehcniques for normal mode

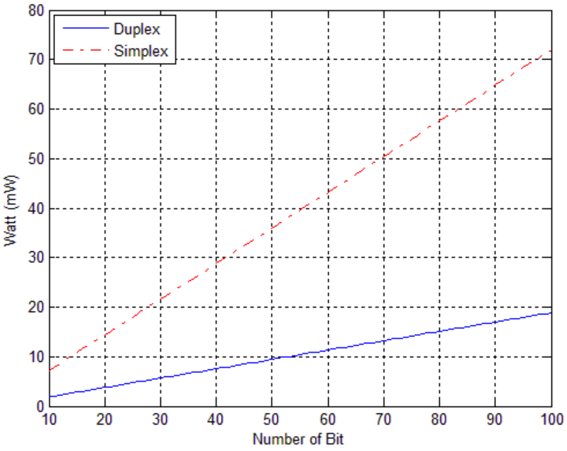


Figure 9. Power consumption versus number of bits for the proposed and conventional TPMS communiatoin tehcniques for considering the emergence mode

operated in emergency mode for 30 minutes as a tire fault was detected on the 15th day. The figure shows that, although the power consumption of the proposed system is increased as the system operated in emergency mode for 30 minutes on the 15th day, it is significantly lower than that of the conventional system for the considered duration.

Fig. 8 shows the comparison of power consumption versus the length of data frame transmitted from the sensor unit to the signal processing unit, in the two systems, while driving two hours, assuming that the transmitted power per bit is 0.1μW and the tire condition is normal. As shown in the figure, power consumption for the proposed method varies with the changing the length of the data frame (number of bits) and is significantly lower than the power consumption for the conventional method. Fig. 9 shows the result of the compared power consumption for the two systems depending on the changing length of the data frame. It is assumed that the transmitted power per bit is 0.1μW, the vehicle runs for two hours, and the vehicle has run in the emergency mode for 30 minutes. As shown in Fig. 9, while operating in the emergence mode for 30 minutes, the power consumption of the proposed system is increased compared with that in Fig 8., but it is significantly lower than the power consumption of the conventional one-way TPMS method. As verified through the simulation, we observe that it is more efficient to use the proposed system as it transmits significantly less data bits and thus significantly saves the power of the battery installed in the sensor unit, unless it always keeps operating in emergency mode. However, the proposed system requires significantly small power consumption comparing with the transmitted power for comparison of the difference value between the optimal and the measured pressure, and the threshold value.

VI. CONCLUSION AND FUTURE WORK

As the casualties caused by tire accidents increased, TPMS has attracted much attention worldwide. Since TPMS has the average life of seven years and when the battery life is over, the TPMS itself needs to be replaced, it is urgently needed to develop a low-power TPMS sensor unit with similar life-time to a vehicle. In this paper, in order to extend the battery life-time of the conventional TPMS, we proposed a new TPMS wireless communication technique, in which the sensor unit installed in a tire receives the optimal tire pressure and threshold value for road conditions and external temperature from the signal processing unit installed in the vehicle and transmits the measured tire pressure data to the signal processing unit only when it is needed. When the difference between the measured tire pressure and the optimal tire pressure is not greater than the threshold value, the sensor unit transmits one bit indicating normal condition to the signal processing unit, instead of periodically transmitting the measured pressure vale, which helps reduce the power consumption of the sensor unit. The performance for saving power consumption of the proposed system was illustrated through simulation examples. Currently, we are studying for the reduced interelement spacing of antennas for the TPMS beamformer.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (Nos. 2012-0008837 and 2011-0024811)

REFERENCES

[1] N. N. Hasan, A. Arif, M. Hassam, S. S. U. Husnain, and U. Pervez, "Implementation of Tire Pressure Monitoring System with Wireless Communication, " 2011 International Conference on, Communications, Computing and Control Applications(CCCA), Mar. 2011.

[2] M. Shao and W. Guo, "Tire Pressure Monitoring System," 2011 Second International Conference on, Mechanic Automation and Control Engineering(MACE), pp. 1840-1842, July 2011.

[3] J. Zhang, Q. Liu, and Y. Zhong, "A Tire Pressure Monitoring System Based on Wireless Sensor Networks Technology, "

International Conference on, Multimedia and Information Technology 2008, MMTT ’ 08, Dec. 2008, pp. 602-605.

[4] Q. Zhang, B. Liu, and G. Liu, “Design of Tire Pressure Monitoring System Based on Resonance Frequency Method,” IEEE/ASME International Conference on, Advanced Intelligent Mechatronics 2009, AIM 2009, July 2009, pp. 781-785.

[5] Y. Zhou, Y. Chai, Y. Lin, and K. Wang, “An application of multi-sensor information fusion in Tire Pressure Monitoring System,” 2010 International Conference on, Intelligent Systems and Knowledge Engineering (ISKE), Nov. 2010, pp. 187-190.

[6] X. Wang, Z. Wu, and S. Liu, “Modeling and Simulation of Thermal-mechanical Characteristics of the Packaging of Tire Pressure Monitoring System(TPMS) ,” 2005 6th International Conference on, Electronic Packaging Technology, Sept. 2005.

[7] M. Cheikh, H. Tartarin, J. David, S. Kessler, and A. Morin, “Transmission quality evaluation of Tire Pressure Monitoring System, ” 12th International IEEE Conference on, Intelligent Transportation System 2009, ITSC ’09, Oct. 2009.

[8] H. Grosinger, L. W. Mayer, C. F. Mecklenbrauker, and A. L. Scholtz, “ Determining the Dielectric Properties of a Car Tire for an Advanced Tire Monitoring System,” 2009 IEEE 70th Vehicular Technology Conference Fall(VTC 2009-Fall), Sept. 2009.

[9] L. Tan, S. Liu, H. Zahang, Z. Gan, and C. Chen, “Numerical Analysis of the Reliability of Tire Pressure Monitoring System Installed on Wheel Hub With Glue,” 7th International Conference on, Electronic Packaging Technology 2006, ICEPT ’ 06, Aug. 2006.

A Time-series Clustering Approach for Sybil Attack Detection in Vehicular Ad hoc Networks

Neelanjana Dutta
Department of Computer Science
Missouri University of
Science and Technology
Rolla, Missouri 65409
Email: nd2n8@mst.edu

Sriram Chellappan
Department of Computer Science
Missouri University of
Science and Technology
Rolla, Missouri 65409
Email: chellaps@mst.edu

***Abstract*—Sybil attack is a security threat wherein an attacker creates and uses multiple counterfeit identities risking trust and functionality of a peer-to-peer system. Sybil attack in vehicular ad hoc networks is an emergent threat to the services and security of the system. In the highly dynamic environment of vehicular ad hoc networks, due to mobility and density of nodes, it is challenging to detect the nodes that are launching Sybil attack. Existing techniques mostly use additional hardware or complex cryptographic solutions for Sybil attack detection in vehicular ad hoc networks. In this paper, we propose a fuzzy time-series clustering based approach that does not require any additional hardware or infrastructure support for Sybil attack detection in vehicular ad hoc networks. The proposed technique leverages the dispersion of vehicle platoons over time in a network and detects Sybil nodes as those which are traveling closely in a cluster for an unusually long time. Simulation results and analysis show that the approach is able to identify Sybil nodes with very low false positive and false negative rates even under varying intensity of attack.**

***Index Terms*—Sybil attack; vehicular ad hoc networks; platoon dispersion; fuzzy time series clustering.**

I. Introduction

Vehicular Ad hoc Network (VANET) is a type of ad hoc network that is comprised of vehicles and road transportation infrastructure. The application of VANETs in different emergency notification system, safety-related and infotainment purposes have increased over past few years, leading it to become the backbone of *Intelligent Transport System* (ITS). Alongside, new security threats in VANETs have been investigated as well [1], [2], [3]. In this paper a critical security problem, namely *Sybil attack*, has been addressed and a time-series clustering based approach is proposed for detection of nodes that are launching this attack in VANETs.

Sybil attack [4] is a security threat wherein an attacker creates and uses multiple counterfeit identities risking trust and functionality of a peer-to-peer system. Sybil attack in Vehicular Ad hoc Networks (VANET) is an emergent threat to the services and trust of the system. In the highly dynamic environment of a VANET, an attacker can easily create and use multiple fake identities, and exploit node mobility to exit the location of the attack. Consequently, detecting the presence of Sybil attack and identifying the Sybil nodes become a challenge considering the dynamic nature of vehicular networks, ephemeral neighborhood proximities and ad hoc mobility.

In this paper, we propose a fuzzy time-series technique to cluster mobile nodes' locations based on neighborhood proximity. The underlying principle behind our approach is as follows. As a Sybil node counterfeits multiple identities and presents them to the system, those *fake* vehicles (represented by the counterfeit identities) will generally be reported around the Sybil vehicle that uses the identities leading these vehicles to violate normal dispersion dynamics. The proposed technique leverages the dispersion of vehicle platoons over time in a network and detects Sybil nodes as those which are located closely in a cluster as they move for an unusually long time. Simulation results and analysis show that the approach is able to identify Sybil nodes with very low false positive and false negative rates even under varying intensity of attack.

A. Related Work

While Sybil attacks have been addressed in social networks, Wireless Sensor Networks and Mobile Ad Hoc Networks, solutions in these domains require long term observation, collaboration and verification which are not possible in ephemeral networks like VANETs, where associations are short and unlikely to repeat. However, there have been research for detection of Sybil attack and identification of Sybil nodes in VANETs as well. In [5], a physical signal characteristics based technique was discussed for Sybil node detection in VANETS. A pair of nodes could be distinguished from each other using estimate of relative node localization that gives an indication of the coherence of the received signal. A signal strength distribution based method for detection and localization of Sybil nodes is proposed in [6] too. In [7], authors propose to employ RSUs that issue temporally varying pseudonyms to vehicles near their vicinity. A cryptographic solution to the problem of Sybil attack detection is proposed in [8]. In [9], spatial and temporal correlation between vehicles and RSUs is used to detect Sybil nodes, exploiting the fact that two vehicles passing by multiple RSUs at exactly the same time is rare. In [10], the authors presented a general approach to validate the VANET data, even in the presence of a few Sybil nodes. Anomalies are detected by checking the validity of the VANET data with respect to the VANET model and adversarial model.

Existing techniques for Sybil detection in VANETs mostly require additional hardware and overhead, but they do not use the available network physics, physical infrastructure information and statistics. The Sybil node detection technique proposed in this paper does not need any external support or complex algorithms, but rather relies on leveraging a basic mobility feature of nodes in VANET - the dispersion of vehicle platoons over time, or platoon dispersion [11]. Platoon dispersion indicates that in normal conditions, vehicles in proximity of each other at a certain time are unlikely to sustain their proximity clustering over time, i.e., proximity clusters are ephemeral. Based on this premise, the proposed solution in this paper uses fuzzy time series clustering for detection of Sybil nodes. We incorporate data preprocessing and feature extraction phases to make the algorithm more efficient. We perform theoretical analysis and simulations to derive threshold parameters and demonstrate performance of the technique. We also take into consideration various intensities of attack, which the attacker can adopt by utilizing only a part of its available counterfeit identities at a time. Such a variation in attack model makes it all the more difficult to estimate consistent association of nodes with one another. Simulation results show that the proposed technique succeeds in identifying most of the Sybil nodes over a period of time under such conditions as well.

The rest of the paper is arranged as follows. In Section II, the problem addressed is formally defined. In Section III, our time-series clustering based solution is presented. Detailed discussion about data preprocessing and feature extraction phases, the clustering algorithm and theoretical analysis are parts of this section. Performance evaluation of the proposed method is presented in Section IV. Section V presents concluding remarks and future work.

II. Problem Definition

The network model, attack model and the problem addressed are defined in this section.

Network Model - The main components of the VANET are - vehicles, Road Side Units (RSUs) and Certification Authority (CA). Vehicles are alternatively referred to as “nodes” in this paper. Nodes in VANETs are equipped with On Board Units (OBUs) to communicate and compute messages. Nodes may also have sensors, navigation device or Global Positioning System (GPS), computing devices, display units, etc. Each node is aware of its own location and the map of the network area and usually communicates using short range wireless communication technology, such as Dedicated Short Range Communication (DSRC), bluetooth, etc. RSUs usually comprise of cheap embedded devices including sensors, smart traffic controllers, etc. RSUs store secure information such as its secure communication keys, traffic information, safety-related information etc. CA is a central authority, which authenticates vehicles and RSUs using the secure authentication infrastructure like public key infrastructure. Each node is given a unique identity or *ID* by the CA.

Attack Model - A Sybil node is defined to be one which uses multiple counterfeit identities to pretend to be some other node(s). As discussed in Section I, the benefits of the attacker in launching such attacks are multi-fold. A group of malicious nodes can subvert the trust and reputation system of the network if they conduct Sybil attack on the network for some time. Eventually this can deteriorate the overall performance of the system. In our model, we consider that a malicious vehicle, with original id V, has n different identities, V_n = V_0, V_1, ..., V_{n-1}. V can determine the intensity of attack by choosing to use only a certain percentage of the counterfeit identities at a time. Intuitively, using lesser number of ID’s at a time will lower its chance of getting detected, but at the same time it will mitigate the intensity of attack as well. In our model, V uses $x\%$ of these ids over a time duration Δt where $x \in [0, 100]$. It is assumed that V randomly selects i different ids from the set V_n such that $x = \frac{100i}{n}$ and uses them to communicate for the next Δt, and then again repeats the same process. We assume that the vehicles follow predefined speed limits on the roads.

In the very dynamic environment of a VANET, it is challenging to identify a Sybil node due to the high mobility and density of nodes. In other words, a node can escape one part of the network and reach another part very fast. The large number of nodes in a network makes it all the more difficult to identify malicious node(s). These challenges warrant the need of a lightweight and efficient approach to detect Sybil nodes in VANET. The objective of the paper is to propose an efficient method to detect Sybil nodes without using additional hardware or infrastructure support.

III. Proposed Solution

In this paper, a time-series clustering method called FSTS [12] is used to detect Sybil nodes in VANETs under varying attack intensity. Time-series clustering helps to identify the nodes that are moving in proximity of each other over a time period based on the location traces of the nodes. Because of the large number and density of nodes in a typical VANET, it is likely that a node can be part of multiple clusters at the same time, making fuzzy clustering algorithms suitable for the scenario. In this section we first discuss the location data collection method, followed by different steps of the proposed technique for Sybil node detection.

The key idea behind the proposed solution comes from a vehicular network phenomenon called *platoon dispersion* [11] as mentioned in Section I. A platoon is a group of vehicles traveling together. If all vehicles in an existing platoon maintain their speeds, a platoon will never disseminate. However, due to physical factors like road friction, vehicle characteristics and signaling, along with human factors like car following pattern, lane changes, fatigue, there is inherent randomness in driver behavior, and platoons tend to disperse over time. Intuitively, longer the travel time between points, greater is the dispersion, since there is more time for drivers to deviate from current speeds. We use this idea to derive a threshold probability P_{Th} of two vehicles being within a specified distance after a given time if their initial locations were same.

By the virtue of platoon dispersion, different vehicles in a network are not likely to travel together for very long. Towards this end, the threshold duration for which vehicles are likely to travel with each other can be estimated theoretically. If any two or more vehicles surpass this threshold duration, they are likely to be the same node faking identities as different nodes. The clustered time-series correspond to the identities of the vehicles which are likely to be Sybil nodes.

A. Location Data Collection by Peer Nodes

Standard DSRC communication allows vehicles to update its location and other physical parameters using periodic messages at a short, regular interval (usually 20 ms). However, in the scenario considered in this paper, any node can be a malicious Sybil node and it can also falsify its own location information to avoid detection. So, location data of vehicles over time is collected through peer vehicles through via messages or *report*. All nodes send *report* messages to the base station on a periodic basis in a fixed time interval. The purpose of *reports* is to inform the base station about the nodes which V_x has heard communicating in the last time interval. Because only a part of the nodes could be malicious, this collaborative process of reporting assures that the real location of a node is reported. For instance, if node V_x receives message from a node V_y at time t when V_x was at location l, it will incorporate this information in its next *report* to the base station. The location data of V_y collected by peers over time is represented in form of a time series $L_{V_y} = l_{V_y}(0), l_{V_y}(1), ..., l_{V_y}(t)$. It can be noted that the RSUs deployed along the road serve as local base stations that can execute the clustering algorithm and collaborate with each other as needed too.

B. Preprocessing Collected Data

After base station collects the location data from nodes in the network, all the following steps are executed by the base station for detection of Sybil nodes. Clustering algorithms are usually used for evenly distributed sampling for time-series, or can handle unevenly sampled data to some extant. But handling the ad hoc nature of data in VANET, specially when the Sybil node uses only a part of it's Sybil ID's at a time, becomes an orthogonal challenge. In simulation based experimentations it is feasible to collect data with regular sampling rates, but it is unlikely to do so in practical scenario. For instance, locations of V_x can be reported by peer nodes time instants t_0, t_1, t_5, t_9, t_{10} and t_{20} whereas locations of V_y can be reported by peer nodes time instants t_0, t_1, t_2, t_3, t_9, t_{11}, t_{12} and t_{15}. Clustering of these two time-series becomes due to the irregularity of sampling rate and size. In this paper, the effect of linear interpolation in time-series clustering of data is studied. Subsequently in Section III-D, a prediction technique is proposed to estimate locations of vehicles when no report is obtained. Although the time-series clustering algorithm used in this paper supports clustering of unevenly sampled time-series data, preprocessing of collected data is done for better results.

Linear Interpolation - Referring back to Section III-A, the time-series data for V_y can be represented as, $L_{V_y} = l_{V_y}(0), l_{V_y}(1), ..., l_{V_y}(t)$, where, $l_{V_y}(i) = (x_{V_y}(i), y_{V_y}(i))$. The linear interpolation between points $(x_{V_y}(i), y_{V_y}(i))$ and $(x_{V_y}(j), y_{V_y}(j)) \forall (i,j)$ and $(j-i) > 1$, can be given by,

$$y = y_{V_y}(i) + (x - x_{V_y}(i)) \frac{y_{V_y}(j) - y_{V_y}(i)}{x_{V_y}(j) - x_{V_y}(i)} \qquad (1)$$

The data points between $l_{V_y}(i)$ and $l_{V_y}(j)$ can be constructed on the line represented by Equation 1 at regular distances $\Delta d = \frac{||(l_{V_y}(i), l_{V_y}(j))||}{p-1}$, where $(j-i) = p$ and $||.||$ refer to Euclidean distance.

C. Estimation of Number of Sybil Nodes

Association rule mining is used as a basic feature extraction step in this paper, in order to have an idea about how many Sybil nodes are likely to be present in a part of network. Association Rule Learning mines relation between multiple attributes of an entity based on their frequency of co-occurrence in a dataset [13]. Let $I = i_1; i_2; i_3, ..., i_r$ be a set of r binary attributes called items. Let $\tau = \tau_1, \tau_2, \tau_3, ..., \tau_s$ be a set of s transactions called a database. Each transaction in τ contains a subset of the items in I. The problem here is to identify association rules in the database, which is an implication of the form $X \implies Y$, where $X, Y \in I$ and $X \bigcap Y = \emptyset$. Reverting back to Sybil detection, consider a Vehicle V_x that has communicated with peers over time. The dataset τ_x of V_x is a row of transactions with each time-stamped row consisting of vehicle ids with which V_x has communicated at that time. Recall from platoon dispersion that a group of vehicles is highly unlikely to be consistently associated geographically (i.e., as a platoon) over a long time period. When a consistent association of two or more vehicles is seen, those vehicles can be suspected to be Sybil. Using this technique, different peer nodes in a network can predict how many Sybil nodes are likely to be present in its vicinity and report to the base station. Also, the base station itself can use this technique to gauge which nodes could possibly be Sybil. However, it is not possible to draw a conclusion from their analysis when the Sybil node uses only a part of forged identities over time and changes them over next time period. This step is only useful for the base station to predict expected number of clusters, w_{ij}, which is an input to the clustering algorithm as discussed in Section IV-A.

D. Fuzzy Time-Series Clustering

Fuzzy time-series clustering involves fuzzy clustering of time-series data collected over time with even or uneven sampling rate. In this paper, *Fuzzy Short Time-Series* (FSTS) clustering of location traces of mobile nodes over a time period is used for Sybil attack detection. The proposed technique is based on the FSTS algorithm presented in [12]. It can be noted that the proposed short time-series based piecewise slope distance clustering seems intuitively appropriate for the application considered in this paper. The type of location data obtained from vehicles in a VANET can be enormous in size, but the Sybil detection technique deals with data over a comparatively shorter period of time. However, there are several differences in the two approaches. Firstly, in this paper, two-dimensional data (location) is considered for clustering over time. So, the time-series data considered is three dimensional unlike the two dimensional clustering performed in [12]. Besides, this technique is further extended in Section III-D to leverage the advantages of estimation techniques in the domain of time-series clustering.

Fuzzy short time-series (FSTS) technique proposed in [12] is a variation of fuzzy C-means clustering for time-series data. The basic idea is to perform a slope distance computation of time-series, which can be used for clustering the time-series in FSTS method. In this paper, the distance considered includes the three dimensional data (x and y coordinates of location and time) obtained from VANETs. For time-series of vehicle $l_{V_x} = l_{V_x}(0), l_{V_x}(1), ..., l_{V_x}(t_n)$, the linear function between $L_{V_x}(t)$ two consecutive time instants t_k and $t_{(k+1)}$ are defined as,

$$L_{V_x}(t) = m_k(t) + b_k, \tag{2}$$

where $t_k < t < t_{k+1}$, and

$$m_k = \frac{||l_{V_x}(k+1) - l_{V_x}(k)||}{t_(k+1) - t_k}, \tag{3}$$

$$b_k = \frac{t_(k+1) l_{V_x}(k+1) - t_k l_{V_x}(k)}{t_(k+1) - t_k} \tag{4}$$

Consequently, a set of equations can be derived as both x and y coordinate are separately considered in Equation 4. The short time-series distance between time-series vector of vehicle V_x and prototype vector V_y is computed as below -

$$d^2_{STS}(V_x, V_y) = \sum_{k=0}^{n_t - 1} \Bigg(\frac{V_y(k+1) - V_y(k)}{t_{k+1} - t_k} - \frac{V_x(k+1) - V_x(k)}{t_{k+1} - t_k})^2 \tag{5}$$

Rest of the FSTS algorithm is similar to fuzzy C-means algorithm . The cost function is defined as,

$$J(V_x, V_y, u) = \sum_{i=1}^{n_k} \sum_{i=1}^{n_v} u_{ij}^w d^2(V_x(j), V_y(i)), \tag{6}$$

where n_k is the number of clusters, n_v is the number of vehicles and w is the weight factor. All these values are user-defined. The value of u determines the membership value of the element in the cluster. Updating of the partition matrix is done in the same way as described in [12], where u_{ij}^w is updated as,

$$u_{ij}^w = \frac{1}{\sum_{q=1}^{n_k} (d_{STS_{ij}} / d_{STS_{qj}})^{\frac{1}{w-1}}} \tag{7}$$

Further details of this algorithm is abstracted in the current paper and can be found in [12].

E. Derivation of P_{Th}

In this section, the objective is to derive P_{Th}, the probability of two vehicles traveling in each other's vicinity so that the expected time of observation for Sybil node detection can be estimated. Towards this end, first theoretical analysis is performed to determine P_{Th} and then the outcome is tested using simulation studies.

Let us consider that two vehicles are moving on a straight road. They are initially (time $t = 0$) at a distance d_0 apart. In a time interval δt, the vehicles can move any distance within a range of D_H and D_L on the road. The range is represented as D_{range}. At every time instance the vehicles update their velocities based on past velocities and thus the distances to be covered (denoted by D_1 and D_2) in next time interval, δt. D_1 and D_2 are chosen from D_{range} using uniform distribution. Our initial objective is to figure out the probability that the two vehicles are within a distance α of each other after a time interval $n\delta t$.

As mentioned above, we assume uniform distribution for D_1 and D_2. For simplicity of computation, we assume d_0 = 0 throughout this derivation. Now, using normal approximation of uniform distribution, if $D_1 \sim Unif(D_H, D_L)$ and $D_2 \sim Unif(D_H, D_L)$, then $\sum_{i=1}^n D_{1i} \sim N(\frac{n(D_L+D_H)}{2}, \frac{n(D_H-D_L)^2}{12})$ and $\sum_{i=1}^n D_{2i} \sim N(\frac{n(D_L+D_H)}{2}, \frac{n(D_H-D_L)^2}{12})$.
So, $(\sum_{i=1}^n D_{1i} - \sum_{i=1}^n D_{2i}) \sim N(0, \frac{2n(D_H-D_L)^2}{12})$.

Now, the probability that the condition $|\sum_{i=1}^n D_{1i} - \sum_{i=1}^n D_{2i}| \leq \alpha$ holds true can be written as

$$P(|\sum_{i=1}^n D_{1i} - \sum_{i=1}^n D_{2i}|) \tag{8}$$

$$= P(-\alpha \leq \sum_{i=1}^n D_{1i} - \sum_{i=1}^n D_{2i} \leq \alpha)$$

$$= P(\frac{-\alpha - 0}{\sqrt{\frac{2n(D_H-D_L)^2}{12}}} \leq Z \leq \frac{\alpha - 0}{\sqrt{\frac{2n(D_H-D_L)^2}{12}}})$$

$$[where\ Z = \sum_{i=1}^n D_{1i} - \sum_{i=1}^n D_{2i}]$$

$$= P(-z \leq Z \leq z) \tag{9}$$

$$[where\ z = \frac{\alpha}{\sqrt{\frac{2n(D_H-D_L)^2}{12}}}]$$

Using standard normal distribution of Z, i.e., $\Phi(Z)$, it is evident that, $\Phi(Z)$ = $P(Z \leq z)$. So, our probability expression, (in equation 9) = 2 $\Phi(Z)$-1.

Using the standard normal CDF table, the probability for different values of D_H, D_L, n and α can be found out. From this derivation, it is straight forward to derive the expected time, t_{exp}, that two vehicles will take to reach a threshold probability P_{th} that they are traveling in each other's vicinity. It can be noted that in real life, based on several physical and human factors, any other distribution other than uniform distribution can be used to model vehicle's distance traveled over a time period. However, similar derivation can be done using other probability distributions too.

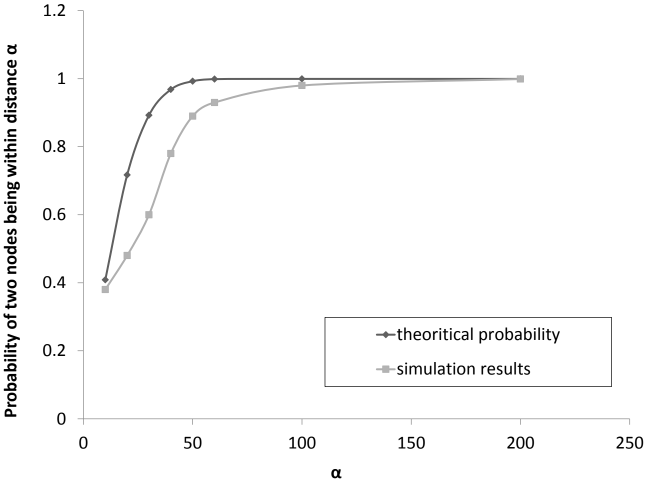


Fig. 1. Determination of Input Parameters where D_H = 50 m, D_L = 0 m, n = 10, δt = 1 s

A theoretical probability of two nodes moving within a given distance over a time period can be obtained by plugging in values of different input parameters into the expression derived above. In Figure 1, probability values derived through theoretical analysis and simulation results are plotted against different values of α where D_H = 50 m, D_L = 0 m, n = 10, δt = 1 s. This figure shows a case where simulation data is plotted along with theoretical results to show that the results match closely. Thus from this derivation, for a given time period, the probability of two vehicles being in a same cluster (or within a given distance) for a given time period can be obtained. For different experiments performed with different values of network parameters (like D_H, D_L etc.), we derived the probability threshold for which two nodes can be in a cluster for a given time duration. If the output of FSTS algorithm yielded a higher cluster membership than the probability threshold derived, the node in the cluster are detected as Sybil nodes. Derivation of threshold parameter through this process helped us differentiate among nodes traveling together for long time and malicious Sybil nodes.

IV. Performance Evaluation

In this section, the performance of the proposed technique is presented. Most of the work for this section is still on-going and only preliminary results are presented. So far, the main effort in this section has been in developing a customized simulator for data collection, interpolation and association rule mining based estimation, and FSTS clustering.

A. Experimental Setup

SUMO (Simulator of Urban Mobility) was used to generate mobility traces of nodes and this data was used as input to the network. A C++ simulator is developed to emulate the vehicular network where the nodes move following the mobility traces from SUMO, thereby mimicking real traffic patterns. The final clustering experiments are done using the C++ simulator. By default, there were 100 vehicles with an average speed of 50mph, and sources and destinations were randomly chosen for each vehicle. There were 10 Sybil nodes among them, and each had 10 identities. Each vehicle was assumed to report it's location once every second, and the transmission range was assumed to be 250 m. The simulation was run for 1000 seconds and the default clustering distance was 400 m. All simulations were conducted 10 times and results were averaged.

Different sets of experiments were run in different phases. First the collected time-series data is preprocessed using linear interpolation using Matlab and then association rule mining is used for feature extraction phase estimating expected number of clusters in the data using WEKA (Waikato Environment for Knowledge Analysis). For the first phase of the study with association rule mining, each Sybil node used all its counterfeit identities during query response. Later the cases were studied when only a smaller percentage of identities are used by a node during a time period.

Apriori algorithm implemented in WEKA tool was used as feature extraction technique to estimate number of abnormally repeating associations or clusters in the dataset of each vehicle. The success rate was 100% in Sybil vehicle detection without false positives. However when the percentage of ID's used by the Sybil node varied, only 60% of the Sybil nodes were detected and equal number non-Sybil nodes were detected as Sybil nodes. It means that the false positive and true positive rates were equal, which is not a desired performance. Clearly there is need of further analysis, which is conducted subsequently. However, several association rule experiments help get an *feel* or estimate of how many clusters to look for and the probable number of Sybil nodes in a set of nodes. For instance, in the case mentioned above, the results of feature extraction show that there are likely to be 12 clusters. In reality, there were 10 clusters that had Sybil nodes in them in that case. Hence in our experiment, we put the input number of clusters between 9 and 15, getting the best results when the number of clusters was 10. It can be noted that usually all clustering algorithm (including FSTS) require preprocessing and feature extraction of data or some sort of prior knowledge to estimate number of clusters. However, the results from association rule mining are not conclusive, warranting further experiments using the FSTS technique to determine the Sybil nodes from past location traces.

B. Clustering of Data

Recall from Section III-E, theoretical analysis can be used to derive P_{Th} for different input parameters and the output can be used to determine whether the concerned nodes are Sybil or not based on their cluster membership values determined using FSTS. In the clustering process, firstly the binary connection metric is clustered using the FSTS algorithm. Figure 2 shows the detected number of false positives and false negatives aver-

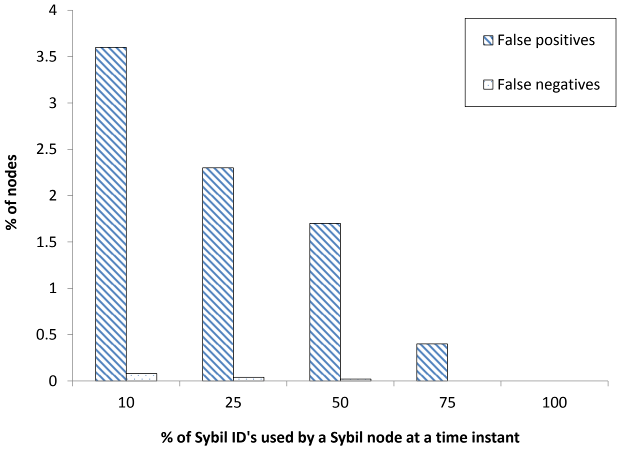


Fig. 2. False positive and false negative rate for varying percentage of Sybil ID's used by a Sybil node at a time instant

aged over 10 runs of simulation each. The X axis represents the percentage of available fake IDs that a Sybil node is using at a time instant. As mentioned earlier in this section, there were 10 Sybil nodes using 10 Sybil IDs each and there were 100 vehicles in total in the simulation setup. If all of the available IDs are used for transmission at every time instant, the false positive and false negative rates are both zero, indicating that all the Sybil nodes are identified. However, as the percentage decreases, both false positives and false negatives increase, although a major part of the Sybil nodes are detected over time. The reason behind the increase in false positives and false negatives is that with lesser number of counterfeit IDs being used at a time, it becomes increasingly difficult to cluster such IDs. This figure demonstrates the effectiveness of the proposed technique in detecting Sybil nodes in VANETs.

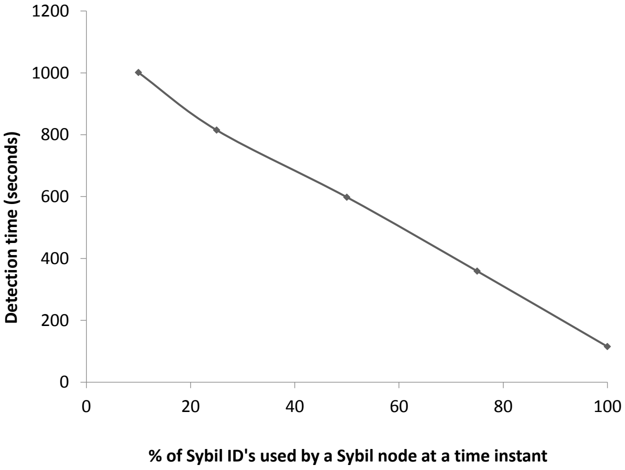


Fig. 3. Detection time in seconds for varying percentage of Sybil ID's used by a Sybil node at a time instant

Figure 3 plots the time required to reach 100% true positive rate (that is, detects all Sybil nodes) for varying percentage of ID's used by the Sybil nodes at a time instant. With increasing percentage of ID's used, the detection is faster. But as very less percentage of ID's are used by a Sybil node at a time instant, it still reaches 100% true positive rate in longer time. Clearly, this trend is exhibited due to the fact that with lesser number of counterfeit IDs being used at a time, clustering of such IDs become increasingly harder resulting in longer detection time.

V. Conclusions

This paper proposes a technique for Sybil attack detection in VANETs, based on fuzzy time-series clustering. The method leverages the principle of dispersion of vehicle platoons in a VANET and detects the nodes clustered with each other for longer than expected. Theoretical analysis has been conducted to derive input parameter to the algorithm and simulation results are presented to evaluate performance of the proposed method. The proposed method has achieved very low false positive and false negative rates even when the Sybil nodes use a small percentage of the counterfeit identities at a time instant. Future work involve derivation of threshold parameters considering different mobility models of vehicles and further investigation of platoon dispersion models to incorporate physical and human factors into the current analysis.

References

[1] J. T. Isaac, S. Zeadally, and J. Camara, "Security attacks and solutions for vehicular ad hoc networks," *Communications, IET*, vol. 4, no. 7, pp. 894–903, April 2010.

[2] L. Cheng and R. Shakya, "Vanet worm spreading from traffic modeling," in *IEEE Radio and Wireless Symposium (RWS)*, 2010, pp. 669–672.

[3] N. Dutta, R. Kotikalapudi, and M. Bhonsle, "A formal analysis of protocol-independent security threats in vanets," in *IEEE Students' Technology Symposium (TechSym)*, 2011.

[4] J. R. Douceur, "The sybil attack," in *Revised Papers from the First International Workshop on Peer-to-Peer Systems*, 2002, pp. 251–260.

[5] M. S. Bouassida, G. Guette, M. Shawky, and B. Ducourthial, "Sybil nodes detection based on received signal strength variations within vanet." *International Journal on Network Security*, vol. 9, no. 1, pp. 22–33, 2009.

[6] B. Xiao, B. Yu, and C. Gao, "Detection and localization of sybil nodes in vanets," in *Workshop on Dependability issues in Wireless Ad hoc Networks and Sensor Networks*, 2006, pp. 1–8.

[7] T. Zhou, R. Choudhury, P. Ning, and K. Chakrabarty, "P2DAP- Sybil Attacks Detection in Vehicular Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 582 – 594, 2011.

[8] M. Rahbari and M. Jamali, "Efficient detection of sybil attack based on cryptography in vanet," *International Journal of Network Security and Its Applications*, vol. 3, 2011.

[9] S. Park, B. Aslam, D. Turgut, and C. Zou, "Defense against sybil attack in vehicular ad hoc network based on roadside unit support," in *Military Communications Conference, 2009. MILCOM 2009. IEEE*, October 2009, pp. 1 – 7.

[10] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in vanets," in *Proceedings of the ACM First International Workshop on Vehicular Ad Hoc Networks*, 2004, pp. 29–37.

[11] R. Denney Jr, "Traffic platoon dispersion modeling," *Journal of transportation engineering*, vol. 115, pp. 193 – 207, 1989.

[12] C. Mller-Levet, F. Klawonn, K. Cho, and O. Wolkenhauer, "Fuzzy clustering of short time-series and unevenly distributed sampling points," *Advances in Intelligent Data Analysis V, Lecture Notes in Computer Science*, vol. 2810, pp. 330–340, 2003.

[13] R. Agrawal and T. Imielinski, "Association rules between sets of items in large databases," in *Proceedings of ACM SIGMOD*, 1993, pp. 207 –216.