Cooperative LBS for Secure Transport System

Andrea Tomatis, Politecnico di Torino – Electronic Department
Pasquale Cataldi, Politecnico di Torino – Electronic Department
Giovanni Pau, Computer Science Department – University of California
Paolo Mulassano, Istituto Superiore Mario Boella
Fabio Dovis, Politecnico di Torino – Electronic Department

BIOGRAPHY

Andrea Tomatis received his B.Sc. in Network Engineering in November 2003 and M.Sc. in Network Engineering in November 2005, both from Politecnico di Torino. Since January 2006 he has been attending the Ph.D. program in Electronics and Communications Engineering at the Politecnico di Torino funded by the Italian Space Agency (ASI). His research concerns the analysis of the weaknesses that afflict monitoring systems and the development of new algorithms for certification of position in transportation. Currently, he is a visiting scholar at the Network Research Lab (NRL) at UCLA where he is focused on the development of a Vehicular Test Bed which has been designed to test new protocols.

Pasquale Cataldi received both his B.Sc. and M.Sc. in Telecommunication Engineering in 2005, from Politecnico di Torino in 2003 and 2005, respectively. In January 2006 he started his Ph.D. program in Electronic and Communication Engineering at Image Processing Lab of the same University founded by Motorola. His research interests are in the field of data transmission over lossy networks. He has developed a novel scheme for sending multimedia contents using rateless codes. Since October 2007 he has been a visiting scholar NRL at UCLA, California. His main project is the study and development of a peer2peer system for vehicular networks.

Giovanni Pau is a Research Scientist at the UCLA computer Science Department. He received the Master Degree in Computer Science and the PhD in Computer Engineering from the University of Bologna in 1998 and 2003 respectively. His research interests include Peer-to-Peer networks, Wireless Multimedia, Distributed Systems and Ad Hoc Networks. He served as Consultant for international such the European Space Agency and the UNESCO. He is currently serving as secretary of the IEEE Multimedia Technical Committee and as Technical Program Committee member in several International Conferences.

Dr. Paolo Mulassano received his Masters Degree in Electronics Engineering (Summa Cum Laude) from Politecnico di Torino in December 1998, and a Ph.D. in Communications Engineering from the same University in December 2003. In 2000 he was one of the founders of the Navigation Signal Analysis and Simulation Group (NavSAS) under the coordination of Prof. Letizia Lo Presti particularly focused on navigation research activities. Since the end of 2003 he has been a senior researcher at Istituto Superiore Mario Boella where he is in charge of coordinating the Navigation Lab. He is also a member of several technical committees like the Galileo Signal Task Force and project manager for ISMB of different initiatives funded by national and European entities.

Dr. Fabio Dovis since 2001 is an assistant professor at the Information and Communication Technology Faculty of Politecnico di Torino, working in the Electronics Dept. as a member of the NavSAS group. His research interests cover many fields of navigation signal processing and communications. His research activities address also the theoretical study of hybrid algorithms based on raw NAV/COM measurements for the PVT computation, and signal processing techniques for multipath and interference identification and rejection.

ABSTRACT

An increasing number of applications have been developed around a GNSS receiver, such as automotive, marine and spacecraft navigation, surveying and mapping, precise time reference and marketing. A key factor that impacts the application’s effectiveness and performance is the precision and the trust of positioning. The main contribution of this paper is a novel approach for tracking loads using both GNSS positioning capabilities as well as network-supported location services. The use of these two methods allows us to have an independent cooperative evaluation of the current position of the tracked target.

To assure the security of the tracking and tracing application we propose a cooperative certification method
to evaluate the one-hop distance between the trucked target and all the cooperative nodes in the truck’s view. Since the control center knows the position of every cooperating node, it evaluates a Least Mean Square (LMS) trilateration. This triangulation compared with the position sent by the target allows the control center to make decision on the trucked vehicle.

As the results show, the availability of the certification strategy is directly connected to the distribution of the cooperatives nodes. In order to better understand this relationship an analysis has been performed on a scalable network simulator where different mobility scenarios have been considered.

INTRODUCTION

An increasing number of applications has been developed around a GNSS receiver, such as automotive, marine and spacecraft navigation, surveying and mapping, precise time reference and marketing. In addition, in the last few years the GNSS receivers have been used in vehicular networks to support routing (GPSR [1]) as well as a plethora of location based applications in several fields ranging from agriculture to homeland defense. A key factor that impacts the effectiveness and performance of the application is precision and the trust of positioning. For instance, in location aware marketing it is important to have a small localization error even in hostile environments such as urban canyon (i.e. New York City), while in tracking the distribution chain is essential to guarantee an anti-tamper positioning system. For advanced applications, such as those briefly depicted above, there is an urge to explore a novel area that falls between navigation and networking and leverages on the strength of both fields taking the GNSS technology far beyond the mere navigation purposes.

This paper focuses on the distribution-chain tracking. For example, let us consider a precious load that needs to be shipped across the nation, or a particularly hazardous material such as pollutants, or fuel. It is obviously important for the government to have the possibility to control in real time the position of such load in order to prevent possible hazards for the population or valuables losses. We present a novel approach to certifying the position of a target vehicle using both the GNSS positioning capabilities as well as network-supported location services. In addition, the applicative scenario is described and, as far as the strategy is concerned, the paper shows the simulations regarding the relationship between the cooperative nodes distribution and the availability of the certification service. In the following, we will consider the service available where the certification strategy can be performed.

COOPERATIVE CERTIFICATION

The scenario described in the introduction is definitely for fleet management systems, where vehicles have to be monitored to control their movements. In this application, the major requirement principally regards the capability of the NBMS to timely obtain position information in order to take the best decision. In case of dangerous or precious goods transport, additional and more demanding requirements are claimed, mainly concerning the availability of a guaranteed (that is, certified) position estimation.

Figure 1 shows the main elements composing a typical NBMS: the GNSS which generates the Signal In Space (SIS); the On Board Unit (OBU), which is the vehicle component in charge of managing GNSS SIS to perform ranging measurements; the Control Center (CC), which is the core of the NBMS in charge of evaluating the vehicle position; and the communication channel (Network), that connects the OBU with the CC.

In a generic NBMS, apart from the CC, all the components are intrinsically unsafe because they can be harmed by a lot of attacks[2]. Moreover, a weakness in a single NBMS component can affect the whole system, threatening its integrity and preventing position estimation certification.

Provide Certified Position

The use of GNSS positioning capabilities as well as network-supported location services allows us to have an independent cooperative evaluation of the current position of the tracked target.

Let us add further details about the previously described scenario. We suppose to have a truck transporting pollutant goods which has to move from the position A to the position B passing through the city. The track route has been mandated by the government in order to have the lowest level of danger for the populations. The truck is
equipped with a tamper-resistant client constituted by a GNSS receiver, a Wi-Fi and a cellular data channel. Moreover, it transmits its position to the government CC every second.

Figure 2 – Cooperative Certification schema

In addition, as Figure 2 shows, a certain number of wireless cooperatives nodes are present: some of them are access point (fixed node) while others are mobile nodes. The mobile nodes include police vehicles, firefighter trucks, parking enforcement cars that are already equipped with GNSS receiver and communication channels. The main reason that guides this choice is the limited cost of the needed infrastructure and the trust in secure vehicles.

In this scenario it is difficult to attack the vehicle-to-control center tracking chain (i.e., receiver, communication channel). In fact, the use of tamper resistance techniques at receiver-level defends the receiver from external modifications. In addition, all the communication channels (wireless and cellular networks) are trusted thanks to the presence of an asymmetric key encryption algorithm (i.e. AES, RSA) that permits confidentiality, authentication and non-repudiation.

Unfortunately these solution are not enough to assure a complete trust in the position sent by the tracked target. It is necessary to compare the position with a different trusted system. The solution proposed in this paper adopts a cooperative localization method to evaluate the one-hop distance between the trucked target and all the cooperative nodes in view of the truck. The idea is simple: the CC requests to all the cooperative nodes to certify the position of a particular vehicle. Each cooperative node that is in radio range with the target, evaluates its distance from the target and sends the result to the CC. Since the CC knows the position of every cooperating node it evaluates a Least Mean Square (LMS) trilateration.

Many techniques can be used for the estimation of the one-hop distance. Common methods are based on Time-of-Arrival (ToA)[4], Time Difference Of Arrival (TDOA) [6] or Received Signal Strength (RSSI)[5]. The paper investigates and implements only the RSSI technique because the signal strength is available in the majority of the wireless card. Instead the other methods required ad hoc hardware that has to be developed.

PRELIMINARY ANALYSIS

Analyzing the proposed strategy it is clear that the quantity of the trusted nodes is the key point in the availability of the service. Since the Cooperative certification adopts LMS trilateration to evaluate a position, the minimum number of cooperative nodes in view should be at least three. Nonetheless, a number of techniques (i.e., map matching) can be used to relax this constrain[7]. This reduces the minimum number of cooperative nodes to two. In general, the bigger the number of cooperative node, the better the performance.

Another key point in the feasibility of the cooperative certification is the analysis of the Dilution Of Precision (DOP) that affects the position evaluated by the trilateration positioning process. In fact, since the trusted nodes are moving within roads, the value of the DOP could be large. As a result, the error in the position could impair the precision of the strategy. Fortunately in a monitoring system, the precision of the positioning is not a strict requirement as the capability of discovering an attack.

The network overhead required by the cooperative certification is small. In fact the beaconing data are normally transmitted by the network devices in order to enumerate the neighbors. From an implementation point of view, there is no cost for the cooperative nodes. In addition, the OBU has only to save measurements about the tracked targets. Finally, the computational burden undertaken by the CC is limited since it has to execute a LMS algorithm for each target.

SIMULATIONS AND RESULTS

In order to better understand the relationship between the distribution of cooperative nodes and the availability of the service, an analysis has been performed on a scalable network simulator – QualNet[8] – where different mobility scenarios have been considered. The whole system has been developed by means of ANSI C routines and connected to the simulator. Such simulations have been run with different cooperative nodes distributions and movement models in order to show the availability of the service.
In these simulations, errors due to the position or distance evaluation have not been considered because the goal of this research has been focused on the availability of the service, i.e. the number of cooperative nodes that are seen on average that allows to perform the certification strategy. Moreover, different scenarios have been experienced. The scenarios differ in mobility model, environment and distribution of the nodes. The analyzed scenarios are:

- Random Way Point (RWP)
- Rural
- Urban
- City

The RWP scenario is the most widely used and studied mobility model ([9], [10]). In this scenario nodes can move freely within a given area. According to random waypoint, a host randomly chooses a destination called waypoint and moves towards it in a straight line with a constant velocity which is selected randomly from some given range. After it reaches the waypoint, it pauses for some time and then repeats the procedure. Within this model, nodes are primarily distributed in the middle of the designed area [11].

The Rural scenario is based on a real map which is composed by major streets and a few intersections. In this scenario the mobility has been generated with Generic Mobility Simulation Framework (GMSF) [11]. The generator makes use of car following and traffic light models to describe the movements of the nodes. In the Rural scenario the nodes are mainly distributed on the major streets [11].

The Urban scenario is also based on a real map. Here there are major and secondary streets and a medium number of intersections. The mobility has been generated with GMSF. In this scenario the distribution of nodes is mainly concentrated on the major streets and in proximity of traffic lights [11].

The City scenario is based on a real map which is composed by major, secondary and minor streets, as the previous two. In addition there is a large number of intersections. The mobility has been made with GMSF. In this case the distribution of nodes is almost uniform with peaks in proximity of traffic lights [11].

Each simulation performed on the paper has been set with general parameters that are available Table 1.

### Analysis of the average number of cooperative nodes in a RWP scenario with mobile or fixed nodes

These simulations have been conducted in order to analyze if it is better to use fixed or mobile cooperative nodes. The advantage of using fixed nodes is that the nodes can be placed on the side of a street. In addition, they do not need a GNSS receiver. On the other side, mobile nodes can be used in different part of the area and they do not need to be installed.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map Dimension</td>
<td>3000 x 3000 [m]</td>
</tr>
<tr>
<td>RWP Speed</td>
<td>10 to 20 [m/s]</td>
</tr>
<tr>
<td>RWP Pause Time</td>
<td>15 [s]</td>
</tr>
<tr>
<td>Simulation Time</td>
<td>900 [s]</td>
</tr>
<tr>
<td>Number of nodes</td>
<td>10 to 120</td>
</tr>
<tr>
<td>Seed</td>
<td>1 to 100</td>
</tr>
</tbody>
</table>

Table 2 – Parameters of the analysis of the average number of cooperative nodes in a RWP scenario with mobile and fixed nodes

The simulations have been performed with the parameters in Table 2. A node, Node 1, moves through the area with a RWP mobility (the parameters are in Table 2). In the first series of simulations each node except for Node 1 is fixed while in the second series the nodes move following a RWP mobility. During the simulations the Node 1 collects data from the link layer saving the number of nodes in radio coverage.

Figure 3 shows the average number of cooperative nodes in the simulated area for mobile and fixed scenario. Both the curves have linear trend, i.e. increasing the number of nodes, the number of cooperative nodes seen by Node 1 increases linearly. In addition Figure 3 shows that the curve related to the mobile scenario is higher than the one related to the fixed scenario.

The cause is that some of the nodes may follow almost the same direction during the movement. This would result in a longer connection time, i.e. the nodes are in radio coverage. A second reason could be the intrinsic characteristic of the RWP model. In fact, most of the nodes are distributed in the middle of the area. Since the simulations does not highlight the component due to RWP mobility, more study needs to be done with realistic mobility patterns.
Figure 3 – Average number of cooperative nodes as a function of the total number of nodes in a RWP scenario.

**Analysis of the average number of cooperative nodes as a function of the percentage of cooperative nodes in different scenarios**

The aim of these simulations is to narrow the availability of the proposed certification strategy to different scenarios analyzing the average number of cooperative nodes.

**Parameter** | **Value**
--- | ---
Map Dimension | 3000 x 3000 [m]
RWP Speed | 10 to 20 [m/s]
RWP Pause Time | 15 [s]
Simulation Time | 600 [s]
Total number of nodes | 10 to 120
Cooperative Nodes | 4 to 50 %
Seed | 1 to 100

Table 3 – Parameters of the analysis of the average number of cooperative nodes in function of the percentage of cooperative nodes in different scenarios.

The simulations have been performed with the parameters available in Table 3. In these simulations the number of cooperative nodes has been changed from a minimum of five percent to a maximum of forty percent of the total number of nodes available in the area. During the simulation each node collects data from the link layer saving the number of nodes in radio coverage.

Figure 4 shows the average number of cooperative nodes in the simulated scenarios. All the scenarios have linear trend, i.e. increasing the number of nodes the number of cooperative nodes increases linearly. In addition, the RWP scenario represents the lower bound of all simulations. In fact, since the RWP mobility does not have street constraints, nodes are placed uniformly in the area. It follows that, in general, it is lower the probability to meet a node.

Moreover, the Rural scenario presents a better average number of cooperative nodes. The reason of this result is connected with the number of streets contained in the map. In general it is possible to assume that more the number of streets, lower is the average number of nodes. Finally, Figure 4 shows that City and Urban scenarios get almost the same average values. The cause has to be searched in the pattern of the chosen maps. In fact, even if Urban map contains less secondary streets compared to City map, the two scenarios do not differ too much.

**CONCLUSIONS**

This paper focuses on the essential problem of providing certified tracking information to an agency controlling dangerous goods transportation.

In the paper the weaknesses of a NBMS has been addressed. Then some solutions for the weaknesses have been investigated. Unfortunately, these solutions are not enough to achieve the required trust in the position, so a novel approach that uses cooperative nodes to certify the position has been proposed.

From a preliminary analysis, the issues concerning the distribution of nodes have been analyzed. The paper presents the results of the simulations that have been conducted to understand the feasibility of the proposed cooperative certification strategy.

Future effort is devoted to analyze the impact of the DOP in the different scenarios. In addition, the impact of the position of the antenna on the performances of the system has to be investigated. Finally, the analysis of the RSSI precision has to be compared with government constraints.
ACKNOWLEDGMENTS

Andrea Tomatis wish to thank the Italian Space Agency (ASI – www.asi.it) that supports the research.

REFERENCES


