UNIVERSITY CARLOS III OF MADRID

Department of Telematics Engineering

Master of Science Thesis

Speeding IPv6 Address Autoconfiguration for VANETs through Caching

Author: **Marco Gramaglia**
Dipl.Eng. in Telecommunications

Supervisors: **María Calderón Pastor, Ph.D.**
Carlos Jesús Bernardos Cano, Ph.D.

Leganés, September 2009

Abstract

GeoSAC is a mechanism that enables IPv6 address autoconfiguration in vehicular networks based on geographic routing. It is built using one of the most know networking stack in the field of VANET, the one proposed by the car-to-car consortium. GeoSAC adapts the existing IPv6 stateless address autoconfiguration protocol to VANETs. In this thesis we analytically model GeoSAC in order to evaluate its perfomance, especially in terms of configuration times. Then we propose an optimization for this protocol using router advertisement caching which has also been modeled. We validate both the model we proposed by means of simulation. Simulation results show that our optimization significantly improves the performance in terms of configuration time but also for signalling overhead.

Table of Contents

List of Figures

Chapter 1

Introduction

Vehicular networks are a solution for providing connectivity among vehicles travelling along roads. This connectivity can also be extended to an infrastructured network, such as the Internet, by placing fixed installations on road borders. A couple of years ago the term VANET (Vehicular ad hoc networks) was introduced, joining mobile ad hoc networks (MANETs) and Inter Vehicle Systems (IVC). Research efforts in this area are driven especially by the goal of improving safety and traffic efficiency. Therefore governments, car manufacturers and telecommunication players are working together towards the definition of a new communication standard that enables drivers to take advantage from the improved capabilities of their vehicles.

Hence, the most common considered applications are related to increasing traffic yields and safety, especially collision warning systems and intelligent vehicle navigation. These applications have the potential to make travel considerably more efficient, pleasant and safe. Although most efforts have been done to standardize these two categories of applications, a third one is increasing its importance inside VANETs sphere: infotainment. Infotainment applications will use an available global connectivity inside the vehicle to provide classical and new Internet applications. This will increase the adoption of vehicular communication systems by the users, because they will see an added value from the installation of such devices inside their vehicles. Enabling IP connectivity in VANETs means also make vehicles become an active part of the Internet, with the need to be compliant with all the protocols and the mechanism used in the core network.

An example of these functionalities is IP address autoconfiguration. As every vehicle will be an operative node in the network, a valid address assignation technique is needed in order to provide a good interconnection between VANETs and the Internet. At the current state of the art, the solution for this problem has not been reached yet. The lack of standard protocols in this field coming from mobile ad hoc networks is reflected and amplified in VANETs, where the possible high number of nodes and their quick mobility make applying existing solutions even more difficult.

GeoSAC, (Geographic scoped stateless address configuration) is a proposal by Baldessari et. al. [2] that tackles this problem, by bringing standardized IPv6 schemes into VANETs. It make use of geographical networking capabilities, which are currently provided in most of the VANET proposed architectures being standardized nowadays. In this particular case, GeoSAC was built on top of the stack provided by the Car-to-car communication consortium

(C2C-CC) [1]. In [2], GeoSAC performance was modelled assuming a high vehicular density and evaluated by deploying a testbed of four vehicles and two road infrastructure nodes.
In this thesis we provide an analytical model of GeoSAC and, based on analysis, we propose an improvement technique based on caching. Finally we prove our analytical evaluation by means of simulation and we show that our caching optimization significantly improves the performance of GeoSAC.
The rest of the thesis is structured as follows: in chapter 2 we present the state of the art regarding IP address autoconfiguration in VANETs, then in chapter 3 we focus on GeoSAC solution. In chapter 4 we present our analytical model of GeoSAC, then in chapter 5 we propose our improvement based on caching. We validate the proposed models and show simulation results in chapter 6, before concluding in chapter 7.

---

[1] `www.car-to-car.org`

Chapter 2

State of the Art

Despite IPv4 being the most deployed layer three protocol in the Internet, all the workgroups active in the VANET field (IEEE 1609 [1], ISO TC 204 *CALM* [2], the Car-to-Car Communication Consortium *C2C-CC* and the ETSI TC ITS [3]) decided to include IPv6 as network layer protocol in their stacks, due to its larger addressing space. Most of them developed a multi hop IPv6 based infrastructure, so it is expected that IPv6 role is becoming more and more relevant in this area.

In this thesis, it is furthermore assumed to exists a short range wireless communication technology. In particular, the IEEE has recently standardized a new amendment of the 802.11 family (the IEEE 802.11p)[4] which was designed to be used in the new ISM (industrial, scientific and medical) band that the European spectrum authority assigned for vehicular networks (around 5.9GHz). It covers PHY and MAC layer of the OSI model and uses seven different channel of 10MHz around the 5.9 GHz band. Six of them are service channel (used for data transmission) and the last is used for control purposes. This control channel is used in ad hoc mode and it is employed for the initial vehicle detection and for the establishment of communications. The WAVE (Wireless Access in Vehicular Environments) 1609 family of standard complements 802.11p defining additional aspects such as security mechanisms, multi channel operations or network services.

All the standardization working groups previously cited are developing a multi hop IP sublayer, either for safety or non safety purposes, extending the coverage using other vehicles as relays. This scenario offers many possible applications for this technology but, on the other hand, it poses the difficulty of deploying IPv6 in terms of routing, security, privacy and mobility.

IP address autoconfiguration in VANETs is still an open issue, especially because no suitable solution has been found for MANETs yet [5]. The most important problem will be pointed out after introducing the proposed solution by the car-to-car communication consortium for the VANET architecture, which will be the base for this thesis.

---

[1] `www.standards.its.dot.gov/fact_sheet.asp?f=80`

[2] `www.tc204wg16.de`

[3] `www.etsi.org`

[4] `www.ieee802.org/11/Reports/tgp_update.htm`

[5] AUTOCONF WG is still working on the standardization of a solution

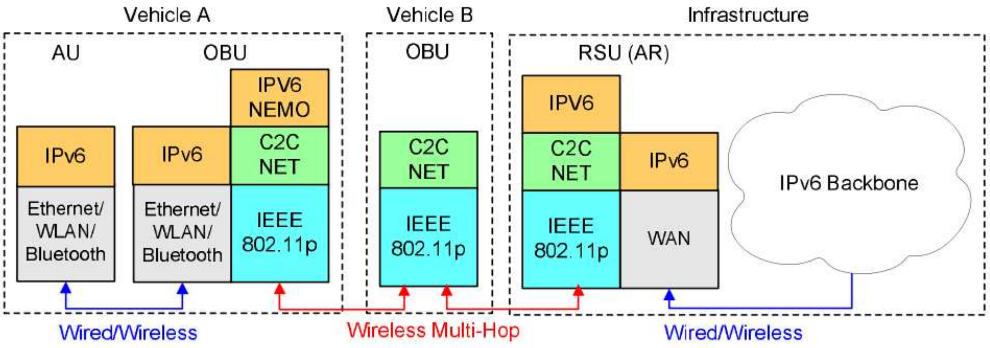

Figure 2.1: The car-to-car architecture

2.1 Car to Car system architecture

The C2C system architecture is composed by two main families of devices: OBUs and RSUs. Vehicles are equipped with an OBU (On Board Unit) that implements the C2C protocol stack. Different cars can communicate among each other and to fixed stations installed along the roads, called RSU (Road Side Unit). Usually these RSUs can be connected to an infrastructured core network and can act as IPv6 access routers (ARs) (or operating as a bridge attached to an AR).

Inside the vehicle it is also possible to deploy a mobile network, using one of the well know protocol for network mobility [3]. In this way, many devices inside the network can exploit the OBU connection to the VANET to get connectivity to the internet. These kinds of devices are called application units (AU). They can be user devices, as PDA or mobile phones, or applications under the control of the vehicle main computer.

The car-to-car network layer is a sub-IP layer that manages the multi hop connectivity inside the VANET and gives to the IP layer a transparent view of the wireless medium. It uses geographic routing concepts, exploiting the positioning devices that are present on the vehicles such as GPS.

Autoconfiguring IP addresses using the car-to-car architecture in VANETs needs to accomplish to different functionalities, in order to get a well coupled interconnection between them.

- Each vehicle has to configure a globally valid address. Every node needs to be connected and always reachable from any node in the VANET and in the Internet.
- This goal should be achieved reducing the required changes to existing standardized protocols, without affecting its normal operation (i.e., designed mechanism should be interoperable with existing ones), both for single hop and multi hop scenarios.
- The solution should minimize the number of control messages, in order to save bandwidth.

- The technique has to be functionally coupled with a network mobility protocol. In other words, it has to be suitable for movement detection.
- If several RSUs are reachable by a node, a gateway selection procedure needs to be activated.
- The mechanism must not rely on a single centralized entity on the network (i.e. a potential point of failure), but rather be completely distributed.
- The solution has to provide security, integrity and privacy. Vehicles movement should not be trackable from the network.

2.2 Related work

The most important issue in VANETs that makes standard IP autoconfiguration protocols unsuitable is the lack of a single multicast capable link for signalling. This problem is present also in MANETs due to the fact that there is not a clear notion of link. Because of their multi hop nature, defining a not ambiguous concept of nodes belonging to the same link it is not trivial. For the same reason, also duplicate address detection (DAD) schemes become more complicated than in wired networks. For solving this issue an IETF Working Group called AUTOCONF was created in 2005. But even before its creation a lot of proposals have been raised, especially for MANETs. Some of them make the assumption of not being connected to the Internet but, as one of our goals is to be fully compliant with standard Internet protocols, we are focusing only on protocols that assume to be connected to the Internet through one or more gateways.

Ruffino et. al. [8] propose a solution based on a slightly modification of OLSR, a routing protocol for ad-hoc networks. Each node needs to set up a temporary address (PADD) which is MANET scoped and exchanges OLSR messages using it. In this solution, gateways act as access routers, and spread their prefix (each gateway has a different IPv6 prefix) by means of a new OLSR message type called Prefix Advertisement (PA). When a node gets PA messages, it is able to build a set of valid IPv6 global addresses and finally chooses among them its Designated Secondary Address (DSADD). Every node broadcasts all its valid prefixes into OLSR messages, so the network will be spread with all the prefixes available from the gateways. This solution needs a specific routing protocol to be active in the network (OLSR) and each node has to create a MANET scoped address. Moreover the authors do not provide a duplicated address detection mechanism.

Templin et. al.[5] propose a solution based on DHCPv6. Their idea is to set up a “virtual ethernet” adaptor placed on a “virtual link” that connects each node in the MANET. Using this virtual interface, nodes can configure globally valid addresses using the standard DHCPv6. The main advantage of this approach is that it reuses a well known and standardized protocol like DHCPv6, enables prefix delegation and ensures unique address assignment. On the other hand, it needs to store state into the nodes, it is not fully distributed and does not provide any mechanism for movement detection.

Vehicular Address Configuration (VAC) is the proposal [4] made by Fazio et. al. This solution was specifically tailored for vehicular environments, exploiting VANETs topology with an enhanced DHCP protocol. In this solution each node is supposed to be into the coverage range of a leader. Leaders are organized in a connected chain, in a hierarchical way. Only leaders communicate among each other keeping addressing information up to date. This limits the signalling also because each leader behave as a small DHCP server for non-leader nodes. The main drawback for this solution is the possible security problem, having all the critical tasks maintained by the leaders.

Chapter 3

GeoSAC

GeoSAC [2] (Geographic scoped stateless address configuration) is a proposal made by Baldessari et. al. in 2008. It consists in adapting the existing IPv6 SLAAC mechanism (Stateless address autoconfiguration), tailoring it for the vehicular network scenario.

In wired networks there is the concept of link and all the nodes belonging to a common Access Router can be easily identified and addressed. In VANETs, this concept is not clear, as nodes that maybe are not sharing the same layer 2 link, have to be in the same layer 3 link. This is because of the multi hop behavior of VANET. GeoSAC defines the concept of layer 3 link in a geographical way: all the nodes that are belonging to a well defined geographical area have to share the same layer 3 link and will receive the same copy of a multicast message. Every area has an access router that is in charge of it, by sending router advertisements. GeoSAC protocol was built upon the car-to-cat network stack. Using this stack, GeoSAC can exploit its subIP layer, which provides multi hop connectivity and emulate a link which the IP layer can use. Broadcast and multicast domains are managed by this sublayer and the layer 3 scope is actually managed by geographical filtering of messages. It would be also possible to define areas based on hop distance, but the extremely short life of the links discourage this kind of approach. In this way, any gateway (that acts also as Access router) which is connected to the network can multicast IPv6 router advertisements that reach all the nodes placed within a well defined area. In car-to-car architecture, RSUs will act as ARs. When a node receives an RA, it applies a geographic checking and processes the message (i.e. forwards it up on the stack to the IPv6 layer) only if the node is located inside the area leaded by the sender Access Router. This phase could be called geocast procedure. If all the nodes within an area have connectivity to the AR (that is, if there exists a multi hop path between every node and the AR) after a certain amount of time all the nodes of the area will have received a Router Advertisement.

From that moment nodes follow standard IPv6 SLAAC mechanism: they generate a valid global IPv6 address using the global prefix broadcast in the RA and their own MAC layer address. As it is supposed that each MAC address is different (and at least in different macro areas they do) from the others, and each Access Router broadcasts a different prefix, it is ensured the uniqueness of the address, and a DAD procedure is not needed anymore.

The benefit of GeoSAC can be furthermore maximized by choosing areas and prefixes according to geographic criteria. Using adjacent and not overlapping areas, the following advantages can be achieved.

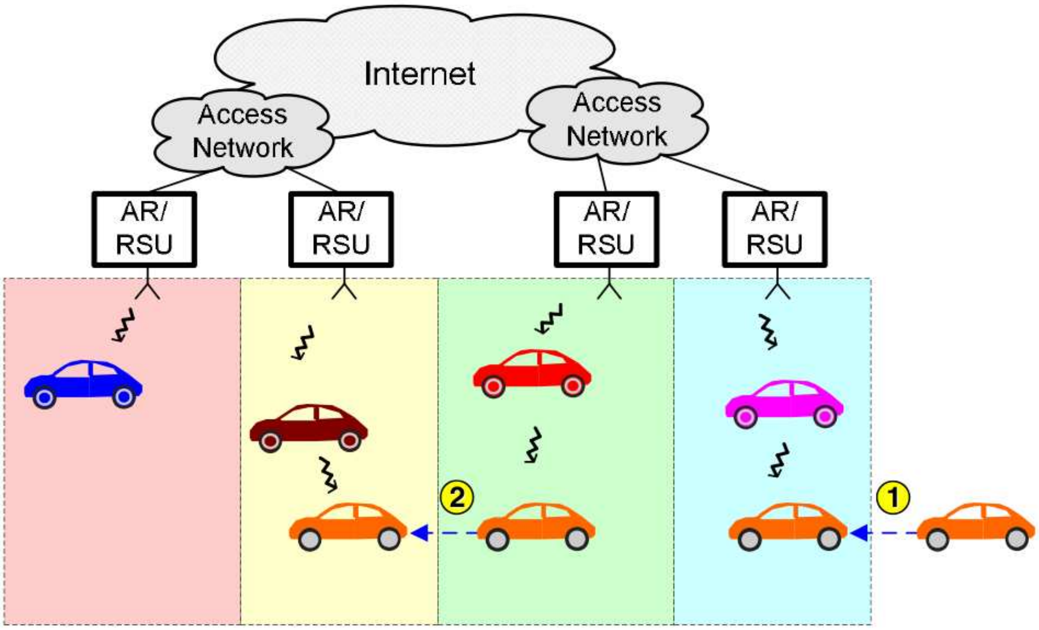

Figure 3.1: The GeoSac architecture

3.1 GeoSAC advantages

- The network infrastructure is in charge of the gateway selection, by assigning a different gateway for every area, and each gateway is unique because there is only one gateway per each area.

- It is achieved a network partitioning that supports movement detection. This is very useful for IPv6 mobility protocol and it could be furthermore exploited by using a location service. Another interesting property is that a vehicle moving through the areas will never be in grey areas, where it needs to choose among different prefixes or gateways.

- This VANET partitioning also enables a matching between geographical areas and IPv6 prefixes. This is effective when a location based application is deployed and can be used coupled with some already proposed scheme for geographic IPv6 prefix format, or extended DNS. Especially this second one can be useful in some applications. For example, imagine that you want to send a message warning for some accident to all the vehicles from the kilometre 2 to the kilometre 10 of a given road. This can be easily achieved by resolving this geographical location in a set of prefixes, and then broadcasting the information into the selected areas.

3.2 GeoSAC functionalities

Besides these advantages, GeoSAC also accomplishes with the functionality explained in chapter 2.

- GeoSAC configures a valid global IPv6 address in each node if the RA is broadcast within the area. This solution allows the standard SLAAC mechanism to be used in VANETs, using multi hop links instead of multicast capable links assumed in the standard version.
- This solution has a low complexity. Each node only needs to geographically filter a message and then process it in the normal way.
- Using a geocast solution, RAs are spread inside the area and these are the only messages sent during the configuration phase.
- GeoSAC supports mobility protocols by providing a movement detection mechanism.
- As said, this solution provides unique gateway selection.
- None of the nodes in the network plays a particular role in the configuration process. In this way, the process is fully distributed.
- This solution does not compromise integrity, privacy and security and can be coupled with some IP sublayer security techniques that are out of the scope of this thesis.

Based on the above considerations, we can say that GeoSAC fulfills all the functionality needed for an address autoconfiguration protocol in VANETs and that is the reason why we have chosen this solution as the one we analytical model and improve (through caching) in this work.

Chapter 4

GeoSAC performance analysis

In this chapter we will present an analysis of the performances of GeoSAC, particularly in terms of IP address configuration time. It is straightforward that the shorter are configuration times, the better will be the user experience, reducing the black period when a vehicle leaves an area to enter the next one. In order to build our analytical model, we used some variables that represent the behavior of GeoSAC.

- T_{RA}: the time between two consecutive router advertisements sent by an RSU. It follows a random variable uniformally distributed between a minimum R_m and a maximum time R_M [7].
- T_{relay}: the time taken by the packet to reach the vehicle that needs to be configured. It depends on the distance between the RSU and the vehicles. We can safely say that this time is negligible compared to T_{RA} and approximate its value as zero.
- T_{conf}: the time elapsed since a vehicle has entered a new geographical area until it can start to use its new autoconfigured IPv6 address.

4.1 With perfect multi hop connectivity

The first step we made to model GeoSAC is to consider a less complicated scenario, avoiding the problem of packet loss given by an hop failure due to lack of relay. We called this situation perfect multi hop connectivity (*pmhc*), where the nodes density is such that a vehicle always has a perfect multi hop connectivity to the RSU. Under the *pmhc* assumption the mean address configuration time $\bar{T}_{conf}^{pmhc}$ only depends on the RA sending frequency, as the presence of a connected chain of relays it is always assumed.

$$\bar{T}_{conf}^{pmhc} = \bar{T}_{RA}^{unsol} + \bar{T}_{relay} = \frac{R_M^2 + R_M R_m + R_m^2}{3(R_M + R_m)} + \bar{T}_{relay}. \tag{4.1}$$

The value of $\bar{T}_{RA}^{unsol}$ represents the time between a vehicle enters a new geographical area and the RSU of the new area sends an unsolicited RA message [6]. However the *pmhc* assumption does not hold in all cases, indeed it does not in more realistic scenarios, so we propose a more accurate evaluation of $\bar{T}_{conf}$.

4.2 Without perfect multi hop connectivity

The following variables are used:

- D_{RSU}: the distance between two consecutive RSUs, hence area boundaries are $\frac{D_{RSU}}{2}$ meters far from each RSU.
- β: represents the vehicular density.
- v: vehicles speed. We consider the speed of all the vehicles fixed and constant. This reduces the complexity of the model, but we argue that it does not affect the validity of the conclusion of our analysis.
- R: the wireless communication range.

We model the distance between two consecutive vehicles D as exponentially distributed, with mean parameter β and its probability density function (PDF) is given by:

$$f_D(d) = \beta e^{-\beta d}, d \geq 0. \tag{4.2}$$

In order to have a connected chain from the RSU to the final destination, the relay chain traversed by the RA needs to be composed only by vehicles that are placed at most R meters far from the other. So, we model the intervehicle distance with a truncated exponential function [1]:

$$f_{te}(d) = \begin{cases} \dfrac{\beta e^{(-\beta d)}}{(1-e^{-\beta R})} & 0 < d < R, \\ 0, & \text{otherwise}. \end{cases} \tag{4.3}$$

The PDF of the distance between two successive vehicles is represented in 4.3, but in order to build a connected chain between a vehicle and the RSU of a certain area, at least *n* relays need to be present, where $n = \frac{\text{distance}}{R}$. To take into account this, we model the chain as a sum of truncated exponential. The length of a multi-hop chain made by *n+1* vehicles (Y) can be represented as the sum of *n* truncated exponential functions. With the method of characteristic function we obtain [1]:

$$\begin{aligned} g_Y(y;n) = \frac{(\beta b)^n}{(n-1)!} e^{-\beta y} \sum_{k=0}^{k_0} (-1)^k \binom{n}{k} (y-kR)^{n-1}; \\ k_0 R < y < (k_0+1)R. \end{aligned} \tag{4.4}$$

where $k_0 = 0, 1, \ldots, n-1$ and $b = (1-e^{-\beta R})$. Now let $a = (k_0' + c)R$, where $k_0' \in \mathbb{N}$ and $0 \leq c < 1$. The cumulative distribution function (CDF) of Y evaluated at *a* is $G_Y(a;n) = \int_0^a g_Y(y;n)dy$:

$$G_Y(a;n) = \frac{1}{(1-e^{-\beta R})^{-n}} \sum_{k=0}^{k_0} (-1)^k \binom{n}{k} e^{-\beta k R} Q[2(k_0' - k + c)R\beta, 2n]. \tag{4.5}$$

where $Q[u,v] = P(\chi^2(u) < w)$ and $\chi^2(w)$ is a chi-square distribution with w degrees of freedom. The probability of having a connected chain composed by *i* hops is given by the probability of having *i* vehicles placed at most *R* meters far from the successive and the (*i+1*)th that is not (a Geometric distribution):

$$P(i \text{ hops}) = (1 - e^{-\beta R})^i e^{-\beta R}. \tag{4.6}$$

Using the total probability theorem, we can find the PDF of the length (L) of a connected multi hop chain of vehicles.

$$f_L(l) = \sum_{i=0}^{\infty} P(i \text{ hops}) g_Y(l;i) = \sum_{i=0}^{\infty} (1 - e^{-\beta R})^i e^{-\beta R} g_Y(l;i). \tag{4.7}$$

And by integration, its CDF:

$$f_L(l) = P(L < l) = \int_0^l f_L(u)du = \sum_{i=0}^{\infty} (1 - e^{-\beta R})^i e^{-\beta R} G_Y(l;i). \tag{4.8}$$

4.3 Configuration time

Now we can calculate the analytical configuration time for a vehicle that enters a new area. We proceed as follows: a vehicle has *m* configuration opportunity once it has crossed area boundaries. Attempts are paced by the frequency of RA and their success or failure depends on the actual presence of a connected chain. The PDF of the time ($\bar{T}_{RA}^{unsol}$) of the first attempt is given by [6]:

$$f_{T_{RA}^{unsol}} = \begin{cases} \dfrac{2}{R_M + R_m} & t < R_m, \\ \dfrac{2(R_M - t)}{R_M^2 - R_m^2} & R_m < t < R_M, \\ 0 & \text{otherwise}. \end{cases} \tag{4.9}$$

If the first attempt succeeds it means that a connected chain from the vehicle to the RSU exists. If not, it means that the connected chain does not exists and it needs a second trial, that will happen in a time uniformally distributed between R_m and R_M. This goes until the vehicle gets configured or enters the RSU wireless coverage area, where it has no need of a connected chain of relays and can be configured directly. Here we make a further assumption: we consider the vehicular density to be not so high (there is always connectivity between the vehicle and the RSU), nor so low that the probability of having a connected chain is negligible. Under this assumption we can say that after $\bar{T}_{RA}^{unsol}$ seconds a vehicle enters a new area, the RSU sends a new RA. If the vehicle does not receive the message, it will try with the subsequent RA, that will be sent after $\bar{T}_{RA}$ seconds, where $\bar{T}_{RA}$ is the average time between two consecutive RAs sent by an RSU:

$$\bar{T}_{RA} = Rm + \frac{R_M - R_m}{2}. \tag{4.10}$$

Using the equations above, we calculate $\bar{T}_{conf}$ by taking into account all the possible *m* attempts of configuration, weighted by their probability.

$$\bar{T}_{conf} = \bar{T}_{RA}^{unsol}(1 - F_L(Da)) + \sum_{i=1}^{m} i\bar{T}_{RA}(F_L(Da - (i-1)\bar{T}_{RA}v) - F_C(F_a - i\bar{T}_{RA}v)). \tag{4.11}$$

where $m = \lceil \frac{T_a}{T_{RA}} \rceil$, $T_a = \frac{D_{RSU}/2 - R}{v} - \bar{T}_{RA}^{unsol}$ and $D_a = vT_a$. In (4.11) we can note that each new configuration attempt is needed only if there was not connectivity from the vehicle to the RSU during the previous one. This probability is obtained by using the CDF of L. This concludes the analysis of T_{conf}.

Chapter 5

Enabling caching to improve GeoSAC performance

In chapter 4 we have seen that the performance of GeoSAC depends on the frequency of RAs and on the presence of a connected chain of relays between the RSU and the vehicle. We cannot control the presence of such a chain, so in order to increase the performance, the only adjustable parameter is the RA frequency. Increasing the frequency has a cost, in terms of signalling overhead over the air, and this cannot be ignored because multicasting a RA within an area means flooding it several times at C2C NET layer. This motivates the need of an optimization of the original GeoSAC mechanism that improves performance without adding any overhead cost. In GeoSAC, the vehicular network is logically partitioned into several non overlapping areas. This is achieved by geographically filtering RAs according to vehicles position. However, although areas are separated logically, they are not separated physically. A vehicle that is placed inside the wireless radio range of others in a neighboring area also receives the message they send. Hence, the performance of GeoSAC can be improved by caching RAs coming from neighboring areas. The vehicles store the last RA, and they reuse it when crossing the area border, without waiting for the reception of the next RA. With this mechanism we introduce an improvement without adding any overhead in terms of signalling. We provide an analytical model of our improved mechanism. First, we calculate $P_{caching}$, that is the probability of getting a valid RA from an adjacent area, before entering it.

5.1 Analytical model

Let a vehicle be inside the wireless range coverage (*R*) from an area border and T_{nRA}^{recv} the time required to receive a RA sent by an RSU from the adjacent area. With the *pmhc* assumption valid between the RSU and the vehicle, this time can be written as:

$$T_{nRA}^{recv} = T_{fwd} + T_{RA}^{unsol}. \tag{5.1}$$

where T_{fwd} is the time elapsed until a *forwarder* vehicle within the communication range of the vehicle about to cross the area is available in the adjacent area. As the intervehicle distance is modeled by (4.2), the distance between the vehicle that is about to enter and the *forwarder* follows that distribution. Since T_{fwd} and T_{RA}^{unsol} are independent variables, the PDF of T_{nRA}^{recv} is given by:

$$f_{T_{nRA}^{recv}}(t) = (f_{T_{fwd}} * f_{T_{RA}^{unsol}})(t) =$$

$$= \begin{cases} \frac{2(1-\beta v e^{-\beta v t})}{R_m+R_M} & 0 \leq t \leq R_m, \\ \frac{2(\beta v R_M-\beta v t+1-e^{-\beta v(t-R_m)}-\beta v(R_M-R_m)e^{-\beta v t})}{\beta v(R_M^2-R_m^2)} & R_m < t \leq R_M, \\ \frac{2e^{-\beta v(t-R_m)}-e^{\beta v R_m}-\beta v(R_M-R_m)}{\beta v(R_M^2-R_m^2)} & t > R_M. \end{cases} \tag{5.2}$$

Since a RA is considered cached if it has been received before the vehicle have crossed the border and it takes ${}^{R}/_{v}$ seconds for the vehicle to reach the border, the probability $P_{caching}^{pmhc}$ of caching under the *pmhc* assumption is:

$$P_{caching}^{pmhc} = \int_0^{R/v} f_{T_{nRA}^{recv}}(t)dt. \tag{5.3}$$

If the *pmhc* assumption is not ensured, there is the need to take into account the probability of having a multi hop chain between the *forwarder* and the RSU. We show a pessimistic approximation of that value:

$$P_{caching} = P_{caching}^{pmhc}\left[1 - F_L\left(\frac{D_{RSU}}{2} - R\right)\right]. \tag{5.4}$$

We explain why (5.4) is a pessimistic approximation in chapter 6.

Chapter 6

Model validation and results

We validate our the proposed models by means of simulation. We develope an ad hoc simulator, that simulates a stretch of road D_{RSU} meters long, where vehicles travel at v m/s and the distance between them follows (4.2). The area border is placed half the way (see figure 6.1).

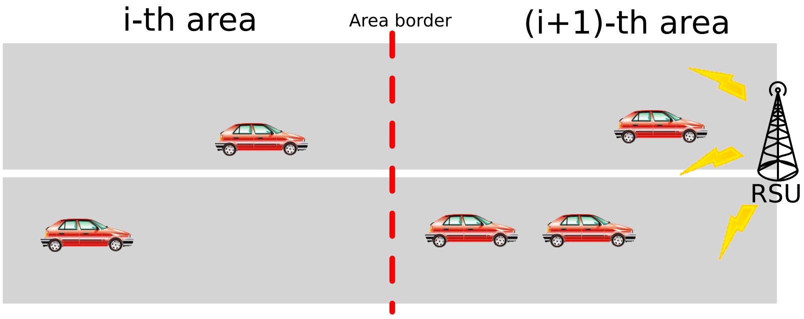

Figure 6.1: The simulator scheme

We ran simulations changing four different parameters: vehicular speed (v), vehicular density (β), time between RA (T_{RA}) and forwarding time (the average time that relays wait before forwarding a packet) (T_{forw}). Many possible values of (T_{forw}) were considered, but finally we decided to exclude this parameter from the set. In our model, RAs are considered to be forwarded as soon as possible, giving to the geocast phase a bursty behavior. Using higher values of (T_{forw}) would have introduced a discrepancy between the model and the simulation.

Parameter	Values
v	5, 50 ,80 ,120 Km/h
β	10, 20, 40, 50 vehicles/Km
T_{RA}	1, 4, 10, 20, 30 s
D_{RSU}	300, 500, 1000, 1500, 2000 m
R	150, 300 m

Table 6.1: The set of parameters used in the simulation runs

Finally, we used values of (T_{forw}) comparable to a normal delay between hops in a 802.11 wireless network (i.e. vehicles do not wait any additional time and forward any received RA immediately). Other parameters that we considered are the distance between two adjacent RSU (D_{RSU}) and the wireless coverage range of vehicles (R). The set of the values given to the parameters is shown in table (6.1) Values of R_m and R_M are calculated as 75% and 125% of the value of T_{RA}. Not all the possibles combinations of values are valid, because they can create situations that are not feasible in real environments, like very high speed combined with high density. So we focused our attention on possibles scenarios.

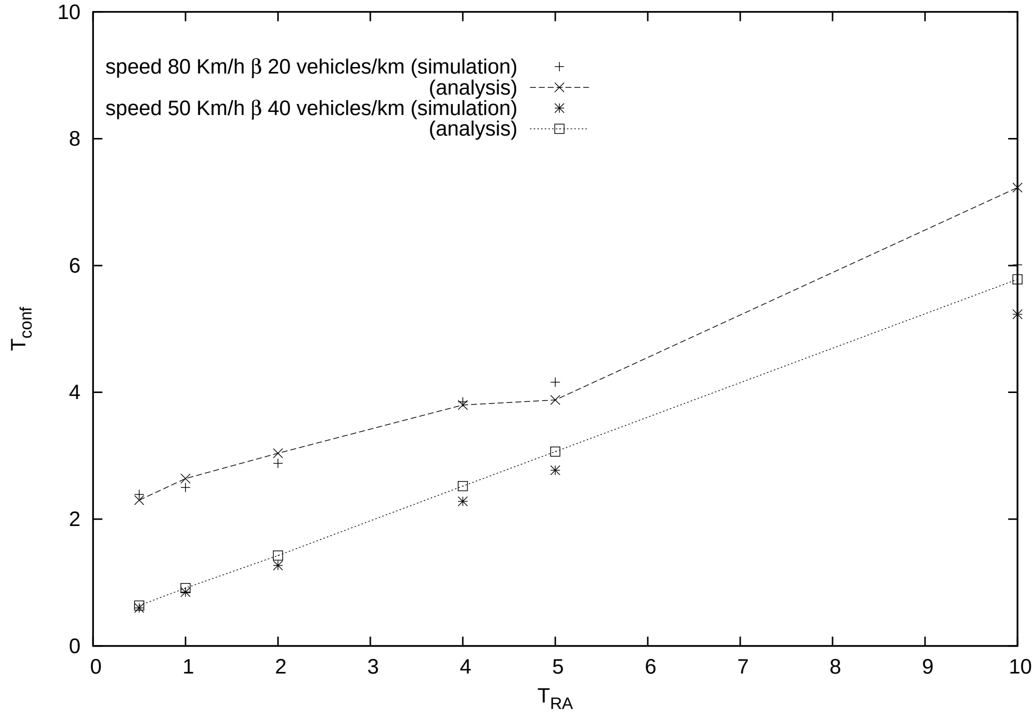

Figure 6.2: T_{conf}, D_{RSU} =1000m R=150m

In figure (6.2) it is shown the configuration time of vehicles with different values of T_{RA}, using the standard version of GeoSAC. We can see that our model matches pretty accurately, floating around the values obtained by simulation. With lower values of T_{RA}, analytical results fit more tightly the curve coming from the simulation, because as configuration opportunities are paced by RA frequency, lower frequencies make our model less accurate.

In figure (6.3) it is plotted the caching probability ($P_{caching}$) of an RA against different values of T_{RA}. We can see that our analysis is always pessimistic. This is because in (5.4) we force the chain length to be at least $\frac{D_{RSU}}{2} - R$, that is the maximum possible value. Moreover, we consider just a single opportunity of receiving an RA from the subsequent area, while there might be more than one before crossing the area border.

Also figure (6.4) shows that our analysis applies to other scenarios as well. With a shorter distance between RSUs the probability of having a connected chain of vehicles arises, so the

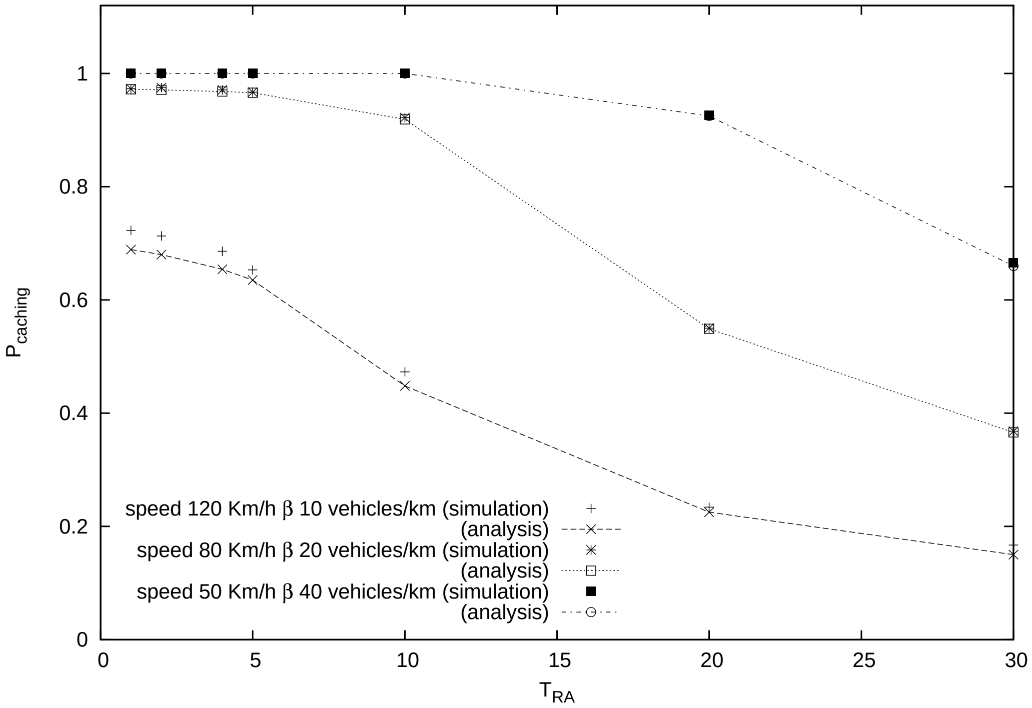

Figure 6.3: Probability of caching of a RA, D_{RSU} =1500m R=300m

total caching probability. We can see this effect comparing the scenario with v = 120 Km/h where the probability in case of D_{RSU} equal to 1000m is higher than the same with D_{RSU} equal to 2000m.

Figure (6.5) only shows two of three possible scenarios, because in one of the considered ones (the one where v = 120 km/h) the probability of having a connected chain of vehicles is too low, and in this case our analysis is not accurate. This is due to the very low density chosen for this case. The remaining two still corroborate our analysis, emphasizing its pessimistic trend.

6.1 Performance evaluation

By running simulations we also prove the effectiveness of our caching technique. The simulation scenario is the same used for validating our analytical model, but in this case we compare our improvement with the standard GeoSAC technique.

In table 6.1 we can see that the improvement achieved by enabling caching of RAs is effective. Looking into the “saving” column, we can see that we always get shorter configuration times. This value becomes bigger (even 100%, i.e. all the vehicles can configure their IP address just after entering the new area) if vehicles travel slowly in a high density scenario (e.g. urban traffic jam). Moreover, these shorter configuration times are reached without increasing signalling overhead.
The use of our proposed caching technique may not only be exploited in order to get shorter

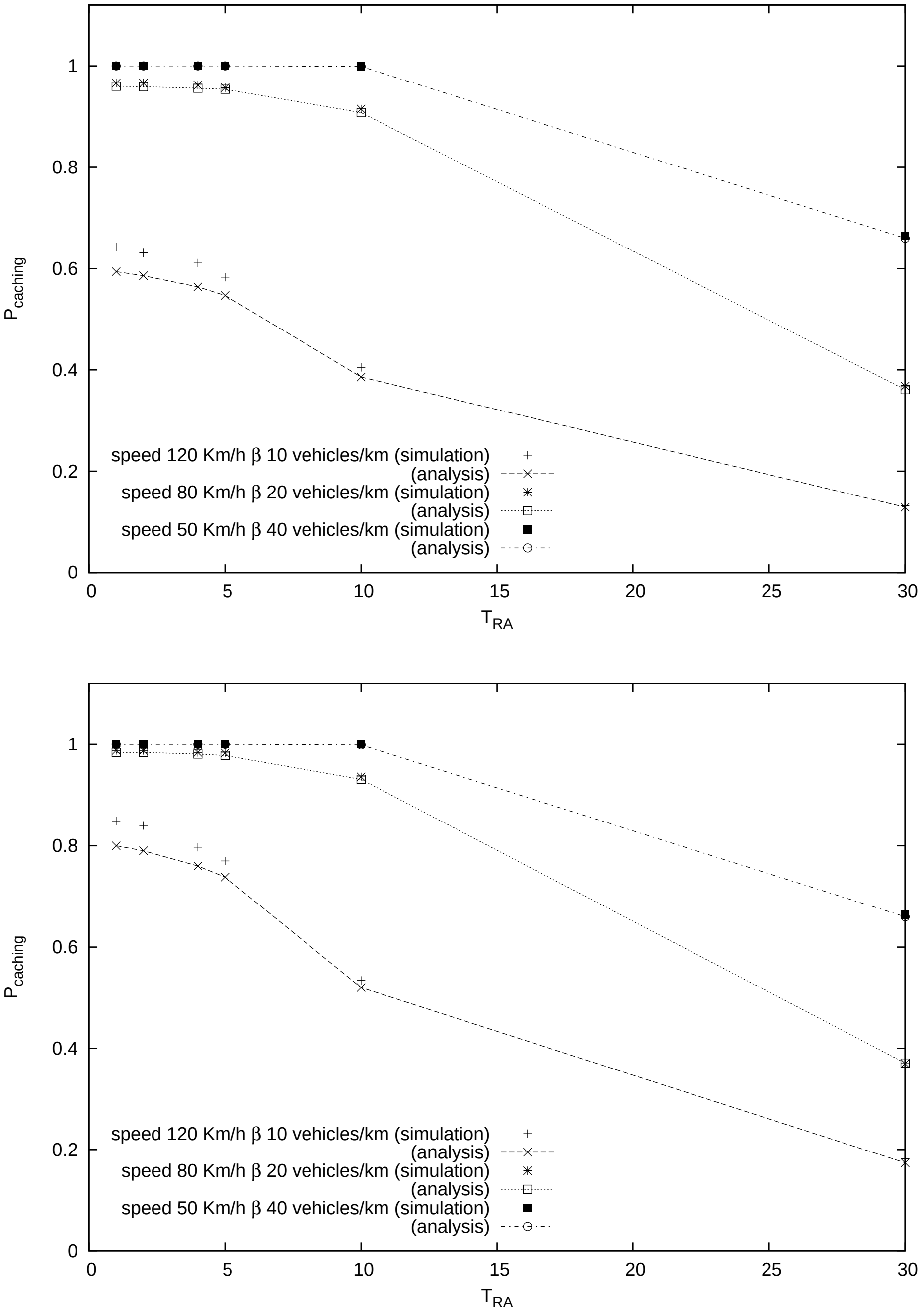

Figure 6.4: Probability of caching of an RA, D_{RSU} =2000m (top) D_{RSU} =1000m (bottom) with R=300m

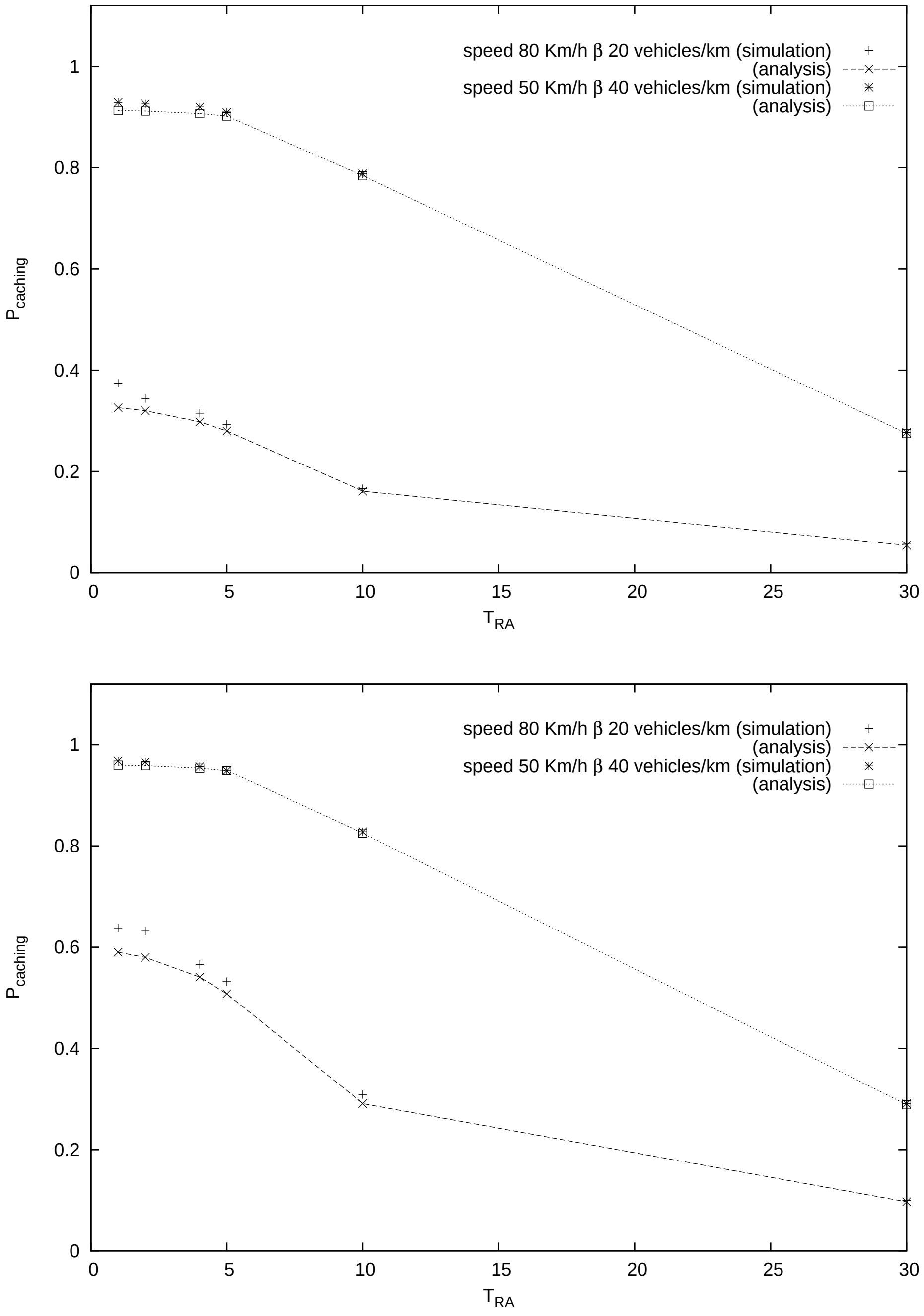

Figure 6.5: Probability of caching of a RA, D_{RSU} =2000m (top) D_{RSU} =1000m (bottom) with R=150m

Table 6.2: Comparison between average T_{conf} with and without caching improvement (R = 300m)

D_{RSU} (m)	v (km/h)	β (vehicles/km)	$\bar{T}_{RA}$	$\bar{T}_{conf}$	$\bar{T}_{conf}^{cache}$	saving
1500	120	10	1 s	2.67 s	2.30 s	13.0 %
			4 s	4.21 s	2.77 s	34.2 %
			10 s	7.02 s	4.01 s	42.9 %
			30 s	12.05 s	9.15 s	24.1 %
1500	80	20	1 s	0.79 s	0.30 s	62.0 %
			4 s	2.87 s	0.37 s	34.2 %
			10 s	5.36 s	0.48 s	42.9 %
			20 s	10.48 s	2.72 s	74.0 %
			30 s	15.13 s	6.45 s	57.4 %
1500	50	40	1 s	0.50 s	0.0 s	100 %
			4 s	2.04 s	0.0 s	100 %
			10 s	5.13 s	0.0 s	100 %
			30 s	15.29 s	2.03 s	86.7 %

IP address configuration times, but also to reduce signalling overhead. As shown in table 6.1, comparable configuration times can be achieved with less intensive RA frequency. For example, we can see that with v = 120 km/h we get an average T_{conf} of 2.67 s sending an RA every second, but we can get an almost identical result by enabling caching an sending RA every 4 s. This is a big saving in terms of bandwidth and reduces the possibility of collision with data traffic present in the network. Comparable situations are T_{RA} equal to 4s and 20s in case of v = 80 km/h and T_{RA} equal to 4s and 30s in case of v = 50 km/h.

Chapter 7

Conclusions and future work

In this thesis we have developed an analytical model for GeoSAC [2], that provides an expression of the IP address configuration time. Using our model, GeoSAC parameters can be tuned to fit network requirements in terms of delay or distance between RSUs. We also proposed an improvement for GeoSAC based on RA caching. We conclude from results that:

- our caching mechanism is very effective reducing configuration times, as shown in table 6.1.
- this improvement can be used to achieve certain configuration time sending less control messages, hence introducing less signalling overhead on the air, by sending unsolicited RAs less frequently.

In our experiments we always considered inter-vehicular distance following an exponential distribution, but in real life environments this may not be always true. Current ongoing work include the analysis of different vehicle distribution, as well as to deploy a testbed and conducting real experiment to validate our analysis.

References

[1] Lee J. Bain and David L. Weeks. A Note on the Truncated Exponential Distribution. *The Annals of Mathematical Statistics*, 35(3):1366–1367, September 1964.

[2] R. Baldessari, C.J. Bernardos, and M. Calderon. GeoSAC - Scalable address autoconfiguration for VANET using geographic networking concepts. In *Proc. IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications PIMRC 2008*, pages 1–7, 2008.

[3] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert. Network Mobility (NEMO) Basic Support Protocol. RFC 3963 (Draft Standard), January 2005.

[4] Maria Fazio, Claudio E. Palazzi, Shirshanka Das, and Mario Gerla. Automatic IP address configuration in VANETs. In *VANET '06: Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, pages 100–101, New York, NY, USA, 2006. ACM.

[5] F.Templin and S. Russert. MANET Autoconfiguration. Draft Informational, April 2009.

[6] Youn-Hee Han, J. Choi, and Seung-Hee Hwang. Reactive Handover Optimization in IPv6-Based Mobile Networks. *Selected Areas in Communications, IEEE Journal on*, 24(9):1758–1772, Sept. 2006.

[7] T. Narten, E. Nordmark, W. Simpson, and H. Soliman. Neighbor Discovery for IP version 6 (IPv6). RFC 4861 (Draft Standard), September 2007.

[8] S. Ruffino and P. Stupar. Automatic configuration of IPv6 addresses for MANET with multiple gateways (AMG). Internet Draft, 2006.