On the Sybil attack detection in VANET
(Extended Version)

Gilles guette and Bertrand Ducourthial

Laboratoire Heudiasyc UMR CNRS 6599
Université de Technologie de Compiègne
BP 20529, 60205 Compiègne, France
firstname.lastname@hds.utc.fr

August 8, 2007

Abstract

Since few years, Vehicular Ad hoc Networks deserve much attention. The development of wireless communication in VANET implies to take into account the need of security for these networks. IN VANET, many attacks rely on having the attacker generate multiple identities to simulate multiple nodes: this is called the Sybil attack. In this paper, we propose a precise quantification of the effects of various assumptions (type of antenna, transmission signal strength) on the effectiveness of a Sybil attack.

1 Introduction

1.1 Security in VANET

The recent gain of interest for wireless communication in Vehicular Ad hoc Network (VANET) implies an always increasing number of potential applications in this kind of network. These applications have different goals going from driving assistance (road traffic alert or emergency brake) to the comfort of passenger (distributed games). All these applications need to exchange data with other vehicles. The communication security problem must be taken into account due to the critical goal of safety related functions such as emergency brake. As data is broadcasted over a shared communication media, it is simple for a malicious vehicle to intercept, modify or inject data in VANET. Moreover, due to the limited communication range of a vehicle, the cooperation between nodes is essential. Exchanging data with other nodes allows to discover its neighborhood and to share information.

This necessity of cooperation shows the vulnerability of these networks if no security mechanism is available. How to trust data received from another node? Is this node even a physical entity? The multiplication of fake nodes in a wireless network in order to launch different kind of attack is known as the Sybil attack [Dou02]. We give a brief survey of related work about this attack and the possible defenses in the following.

1.2 Related Work

1.2.1 The Sybil attack

The Sybil attack was first described and formalized by Douceur in [Dou02]. It consists in sending multiple messages from one node (the attacker) with multiple identities. Hence, the attacker simulates several nodes in the network. Different types of attacks that can be launched with Sybil nodes in sensor networks are described in [NSSP04]. Applications of the Sybil attack to Vehicular Ad-Hoc Networks have been discussed in [BE04, RH07]. Goal of these attacks may be simply to give illusion of a traffic jam to force other vehicles to leave the road to the benefit of the attacker. Nevertheless, the attack may be more dangerous, trying to provoke collision in a vehicle platoon [BE04]. This shows the importance of Sybil nodes detection in VANET.

One important result shown in [Dou02] is that without a logically centralized authority, Sybil attacks are always possible (*i.e.* may remain undetected) except under extreme and unrealistic assumption of resource parity and coordination among entities. That is to say, entities have the same resources constraints, all identities are validated simultaneously by all entities. We explore in the following a classification of the different defenses proposed.

1.2.2 Resources testing

[Dou02] and [NSSP04] propose resources testing as a defense against Sybil attack. This resource testing is based on the assumption that each physical entity is limited in some resource. The method described in [Dou02] uses computational puzzles [Mer78] to test nodes computational resources. In [NSSP04], the authors show that this approach is not suitable to ad-hoc networks, and hence typically VANET, because the attacker can have more computational resources than an *honest* node. Moreover, they emphasize a problem of network congestion due to the multiple requests/replies for identities checking. Instead, they propose a radio resource testing. Nevertheless, in VANET the attacker can use multiple radio devices to defeat this detection method.

In [PSL06], the authors present two methods to detect Sybil attacks, Passive Ad hoc Sybil Identity Detection (PASID) and PASID with Group Detection (PASID-GD). The idea is to record the identities (namely MAC and IP address) of other nodes and to build a profile of nodes that transmit together. Computing an affinity function between each couple of nodes will then help to reveal Sybil attacker. The idea is that the attacker and the Sybil nodes will appear and disappear simultaneously, and this will be revealed by the affinity function.

1.2.3 Use of public key cryptography

In [RPH06], the authors try to solve the security problem of the Sybil attack with public key cryptography and authentication mechanism. The authors propose the use of a PKI for VANET (VPKI). They describe a complete solution to provide security of communications and they address the problem of key distribution and privacy. They also propose a mechanism for the most challenging problem: the key revocation. As each vehicle may be authenticated with public key cryptography, the Sybil attack is always detected. Nevertheless, deploying PKI for VANET is an heavy and difficult solution that must be tested to assess its possible use in a real world. In a VANET, access to network infrastructure is not guaranteed and cryptographic treatment may be too long to be usable (tests regarding the time required to sign typical VANET messages can be found in [RH05]).

1.2.4 Assuming a given propagation model

Some papers dealing with detection of Sybil attack in wireless networks assume a predefined propagation model [PdPFWL04, XYG06]. They use the received signal power to deduce some inconsistencies between the power of the signal and the claimed position. In [XYG06], when a node received a beacon message, it collects signal strength measurement from this node and estimates its new position according to a given propagation model. A node is considered suspect if its claimed position is too far from the evaluated one. Note that [PdPFWL04] made very strong assumptions about devices and environment. Moreover, as the detection systems use a given propagation model to estimate the next position of a node, a malicious node can use the same model to compute the transmission signal strength to use to fool the detection systems.

1.2.5 Secure positioning

Another possibility to defeat Sybil attack is to provide the security of the positioning system and the reliability of the position claimed by vehicles. In [SY05], the authors propose methods for determining a transmitting peer's node location using signal properties and trusted peers collaboration for identification and authentication purposes. The method uses characteristics such as signal strength and direction so it assumes directional antennas and node's cooperation.

In [CH05], the authors made a brief survey of positioning techniques and related papers and describe their vulnerabilities to distance enlargement or reduction for position spoofing. They also present a novel approach called *verifiable multilateration*, using distance bounding protocol [BC94] and base stations support. They also assume that all network nodes can establish pairwise secret keys.

1.2.6 Distinguishability

In [GGS04], the authors propose an approach to evaluate the validity of VANET data. Data are correlated and scored; data with the higher score will be accepted. The proposed model rely on four assumptions. The second assumption is called local distinguishability and rely on the fact that nodes are equipped with specific devices allowing to tie a message with a physical sources. This model uses also short lived public key pair generated by the node to extend the distinguishability allowing to authenticate messages coming from a node that keeps its public key during a given time.

1.3 Contributions

Previous work are based upon different assumptions, which are often not realistic in a VANET context. It is important to provide a theoretical insight of which assumptions reduce the potential for Sybil attacks.

In this paper, we investigate the role of the assumptions on the success rate of Sybil attacks. In order to measure such a success, we propose to evaluate the number of nodes that could be cheated. From the sender point of view, we evaluate the impact of transmission power tuning. From the receiver point of view, we charaterize the impact of bi-directional antenna over omni-directional antenna. To remain general, this study only relies on reception signal strength and direction; no propagation model is used to compute a precise location of a given node. Nevertheless, in our study we use a free space propagation model to compute an upper bound on the distance between the transmitter and the receiver. We also assume that even with multi path propagation effects the sending signal strength is always greater than the received signal strength.

Our main contribution is the quantification of the effects of various assumptions on the attacker and the antennas on the effectiveness of attack detection.

Section 2 formally describes the problem addressed in this paper as well as the different steps of the study. Section 3, 4 and 5 are dedicated to specific cases, while Section 6 presents the main results. These results are analysed in Section 7. Concluding remarks end the paper.

2 Problem statement

The problem we address in this paper is the evaluation of the severity of a Sybil attack regarding the effect of various assumptions such as the transmission power strength or the type of antenna used.

2.1 Notations

Let S and R be two mobile nodes such that S sends some messages received by R. We assume that the transmission of a single message is immediate. As detection of Sybil nodes is generally done at the reception of a message, we can consider the positions of S and R as fixed points of the space at the time of reception. We denote by $\mathrm{d}(S,R)$ the distance between S and R.

Let denote by P_{snd} the transmission power of the node S. With an isotropic antenna of gain G_{snd}, a power $P_{\mathrm{snd}} \times G_{\mathrm{snd}}$ is equally received on the surface of the sphere of radius $\mathrm{d}(S,R)$. Such a surface is equal to $4\pi \cdot \mathrm{d}^2(S,R)$. Hence, with a surface antenna A_{rcv} and for $\mathrm{d}(S,R)$ sufficiently large, the node R will receive a power P_{rcv} equals to:

$$P_{\mathrm{rcv}} = P_{\mathrm{snd}} \times G_{\mathrm{snd}} \times \frac{A_{\mathrm{rcv}}}{4\pi \times \mathrm{d}^2(S,R)}$$

The gain of an antenna of surface A_{rcv} is equal to $G_{\mathrm{rcv}} = 4\pi A_{\mathrm{rcv}}/\lambda^2$, where λ denotes the wavelength of the radiation. Hence, we have:

$$P_{\mathrm{rcv}} = P_{\mathrm{snd}} \times \frac{G_{\mathrm{snd}} \times G_{\mathrm{rcv}} \times \lambda^2}{16\pi^2 \times \mathrm{d}^2(S,R)}$$

The previous formula makes a link between the transmission power P_{snd}, some parameters relying on the protocol and the equipments, and the distance between the sender and the receiver. However, it assumes that there is no signal attenuation. Hence it gives the *maximal* received power. By denoting $G_{\mathrm{SR}} = G_{\mathrm{snd}} \times G_{\mathrm{rcv}} \times \lambda^2/(16\pi^2)$ the gain of the link from S to R, the maximal power $P^{\max}_{\mathrm{rcv}}(\mathrm{d}(S,R))$ at distance $\mathrm{d}(S,R)$ from the sender is:

$$P^{\max}_{\mathrm{rcv}}(\mathrm{d}(S,R)) = P_{\mathrm{snd}} \times G_{\mathrm{SR}} \times \frac{1}{\mathrm{d}^2(S,R)} \tag{1}$$

By taking into account signal attenuation, the power received by R is smaller than $P^{\max}_{\mathrm{rcv}}$:

$$P_{\mathrm{rcv}}(\mathrm{d}(S,R)) = \alpha \times P^{\max}_{\mathrm{rcv}}(\mathrm{d}(S,R)) \qquad 0 \le \alpha \le 1 \tag{2}$$

where α depends on several parameters (distance $\mathrm{d}(S,R)$, λ, atmospheric conditions...).

Moreover, a message is understood by the receiver if the ratio signal/noise is larger than a threshold. Equivalently, this means that the message sent by S is received by R if the received power is larger than a given power denoted by $P_{\text{rcv}}^{\min}$. We then have:

$$P_{\text{rcv}}^{\min} \leq P_{\text{rcv}}\left(\mathrm{d}(S,R)\right) \leq P_{\text{rcv}}^{\max}\left(\mathrm{d}(S,R)\right) \tag{3}$$

By Equation 1, the larger the distance $\mathrm{d}(S,R)$ is, the weaker the received power is. We define the maximal distance $\mathrm{d}_{\max}$ between a sender and a receiver by:

$$P_{\text{rcv}}(\mathrm{d}_{\max}) = P_{\text{rcv}}^{\min} \tag{4}$$

We note $\mathcal{C}_{\max}$ the disk centered on S with radius $\mathrm{d}_{\max}$ representing the range of S. Representing range of a transmitting node by a disk eases our study without loss of generality. It is mainly because we use this disk as un upper bound and because in reality the range of an antenna is entirely included in such disk $\mathcal{C}_{\max}$.

We denote by $\mathrm{d}_{\min}$ the minimal distance between the antenna of a sender and the antenna of a receiver. We can then define the maximal received power $P_{\text{rcv}}^{\max}$ as the power received by a receiver close to a sender:

$$P_{\text{rcv}}^{\max} = P_{\text{snd}} \times G_{\text{SR}} \times \frac{1}{\mathrm{d}_{\min}^2} \tag{5}$$

2.2 Sybil attacks and assumptions

We suppose that each vehicle is equipped with a standard embedded device, in such a way that antennas, gains and transmission powers are fixed and known. Moreover we assume that each car periodically diffuses some hello messages containing their GPS position.

To create a Sybil node F, a sender S could give some false GPS positions in its messages. However, thanks to the previous equations, a receiver R may detect a mismatch between the measured received power P_{rcv} and the GPS positions inside the message. Here, we do not use a given model to compute an estimation of the next position of a node as in [PdPFWL04, XYG06]. We just consider the free space propagation model as the best case for signal attenuation. This allows to verify if the claimed position contained in a message fall into a signal propagation case better than the best case. To complicate the Sybil node detection by the receivers, the sender may use a non standard equipment. This implies that its transmission power could vary instead of being fixed:

$$P_{\text{snd}}^{\text{attack}} = \beta \times P_{\text{snd}} \qquad \beta > 0 \tag{6}$$

Hence, two kind of attacks should be considered: (i) fake GPS position, and (ii) fake GPS position plus tuned transmission power.

From the receiver point of view, it is interesting to consider the impact of the embedded equipment. Such an equipment may be simple and cheap or more complex and more expensive. We will consider two kind of antenna: (i) an omni-directional antenna and (ii) a pair of bi-directional antenna. In the last case, each vehicle is equipped with a front antenna and a rear antenna, allowing to detect whether the sender of a message is ahead or back of the car. From a transmission point of view, the above equations remain similar, but the reception area is a half sphere instead of a complete one.

The different cases to be considered are summarized in the table of Figure 1.

	False GPS positions	
P_{snd} / Antenna	standard P_{snd}	tuned P_{snd}
omni-directional		
bi-directional		

Figure 1: Different cases considered.

2.3 Method

Due to the combination of the above sender and receiver hypotheses, not all the Sybil attacks are of the same importance. In order to compare them, we need a metric. We propose to measure the impact of a Sybil attack by the number of receiver nodes that could be cheated.

We assume that all the mobile nodes (cars) are on the same two-dimensional Euclidean space, approximating the earth's surface. To compute the number of cheated cars, we can equivalently compute the area of the Euclidean plan where the Sybil attack cannot be detected.

In order to complete the table of Figure 1, we will proceed in two phases. In the first one, we consider the ideal propagation case with no attenuation. We study the influence of the tuning of the signal power. With ideal propagation, there is an exact relation between the distance and the received power (Equation 1). The geometric positions of the potentially cheated nodes are then determined by some equations on the distance (leading to border area instead of area). The results obtained in this first phase (Sections 3-5) are used in the second one.

In a second phase, we consider the propagation with attenuation. In this case, the geometric positions of the cheated nodes are determined by some inequalities on the distance, leading to non-empty area. The bounds of such areas are given by the first case. The results shown in this second phase (Section 6) are discussed in Section 7.

For all the four cases of the table in Figure 1, we consider a node S that tries to create a Sybil node F by modifying the GPS positions in its hello messages, and a receiver R which could be cheated by the message of S, depending on its position in the Euclidean two dimensional space.

When considering the bi-directional antenna case, we assume that each vehicle is equipped with a front and a rear antenna, defining two half plans. For a given vehicle V, we denote by (D_V) and we call it *axis line of* V the line perpendicular to the direction of the vehicle that divides the euclidian plan into two half plans.

3 Case 1: no attenuation and standard transmission power

In this section, we consider a standard transmission power P_{snd} in an ideal environment with no atmospheric attenuation. We consider both omni-directional and bi-directional antenna. Results in sections 3 to 5 describe what can be deduced when the distance is the only factor of signal attenuation. This *far from reality* assumption allows to use the free space propagation model to compute distance between nodes. This eases the presentation of our main contribution in section 6 where this assumption is relaxed. In our main contribution, we do not assume any propagation model that compute distances between nodes.

3.1 Omni-directional antenna

Proposition 1 *Let (D) be the perpendicular bissector of segment $[S, F]$. Let A and B be the intersection points of (D) and $\mathcal{C}_{\max}$ (Figure 2).*

With omni-directional antenna and standard transmission power, Sybil node attack of S cannot be detected by nodes on the line segment $[A, B]$.

Proof 1 *Obviously, since R receives the message of S and P_{snd} is standard, we have $\mathrm{d}(S, R) \leq \mathrm{d}_{\max}$.*

When receiving the message of S, the node R will measure the received power, and deduce the distance $\mathrm{d}(S, R)$ from the sender. Moreover, the node R will compute the distance $\mathrm{d}(F, R)$ from the position included in the message. The Sybil node is not detected if $\mathrm{d}(S, R) = \mathrm{d}(F, R)$, meaning that R is on the perpendicular bissector of $[S, F]$.

Hence if $R \in [A, B]$, R cannot detect the Sybil node.

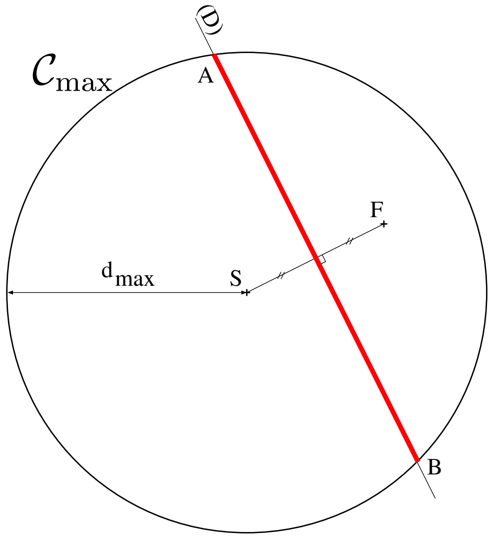

Figure 2: Omni-directional antenna and standard transmission power. Cheated nodes are on line segment $[A, B]$.

3.2 Bi-directional antenna

When considering the bi-directional antenna, the direction of the vehicles should be taken into account.

Proposition 2 *Let (D) be the perpendicular bissector of $[S, F]$. Let A and B be the intersection points of (D) and $\mathcal{C}_{\max}$ (Figure 3).*

With bi-directional antenna, standard transmission power and any direction for the vehicles, the Sybil attack of S can be detected from any place (depending on the direction of the receiver car).

Proof 2 *From Proposition 1, the cheated nodes can only be on line segment $[A, B]$. But the bi-directional antenna adds a new condition: both S and F must be in the same half plan of the cheated node. Since any vehicle direction is admitted, it is always possible to orient a vehicle R in such a way that S and F are not in the same half plan defined by the axis line (D_R) of the vehicle (Figure 3).*

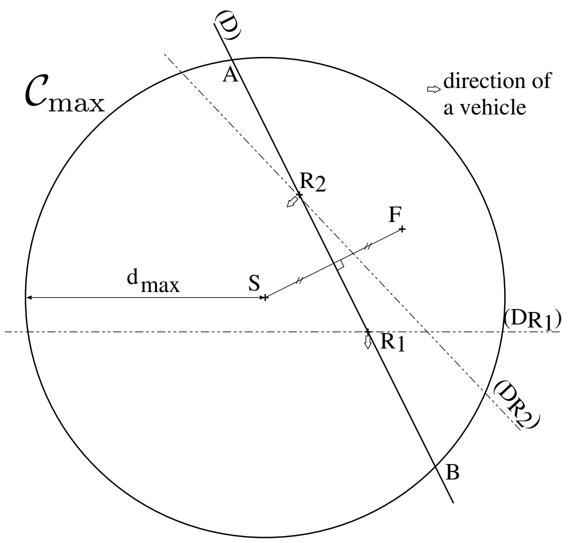

Figure 3: Bi-directional antenna, standard transmission power and any direction for the vehicles. Cheated nodes R are on the line segment $[A, B]$ such that S and F are in the same half plan defined by the bi-directional antenna axis (D_R). Here, R_1 is cheated while R_2 is not. Consequently, the Sybil attack of S can be detected from any place.

A particular case appears when all the vehicles have the same direction (same road for instance).

Proposition 3 *Let (D) be the perpendicular bissector of $[S, F]$. Let A and B be the intersection points of (D) and $\mathcal{C}_{\max}$ (Figure 4).*

Let (D_S) and (D_F) be the axis line of S and F respectively. Let C be the intersection of (D) and (D_S). Let D be the intersection of (D) and (D_F).

With bi-directional antenna, standard transmission power and same direction for all the vehicles, the Sybil attack of S cannot be detected from the nodes R on the line segments $[A, C]$ and $[D, B]$.

Proof 3 *From Proposition 2, the cheated nodes R are those on line segment $[A, B]$ such that both S and F are in the same half plan defined by (D_R). This means that either both S and F are in front of R of back of R. Since all the vehicles have the same direction, this means that either R is back to S or in front of F regarding the common direction. This gives the result (Figure 4).*

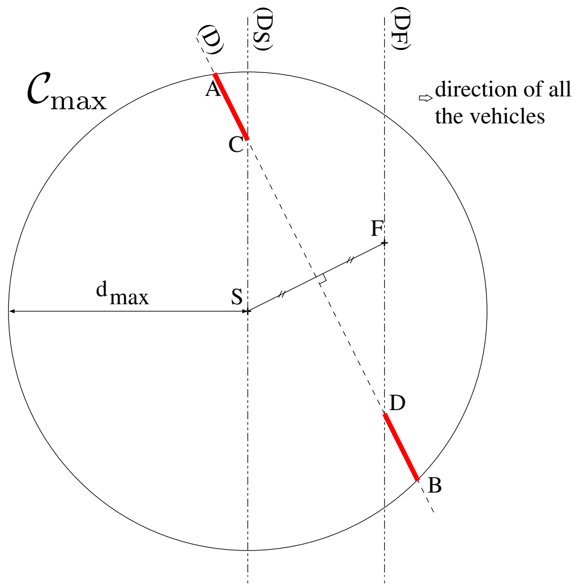

Figure 4: Bi-directional antenna, standard transmission power and same direction for all the vehicles. The Sybil attack of S cannot be detected by vehicles on line segments $[A, C]$ and $[D, B]$.

4 Case 2: no signal attenuation and low transmission power

In this section, we suppose that the sender node S can tune its transmission power. Instead of transmitting its messages with the standard transmission power P_{snd}, S diffuses its messages with the transmission power $\beta \times P_{\text{snd}}$, $0 < \beta < 1$.

4.1 Omni-directional antenna

We begin by a technical lemma.

Lemma 1 *Let S, F and O be three points on a line satisfying $\overline{SO} = \frac{\beta}{\beta-1} \times \overline{SF}$ (with $0 < \beta$ and $\beta \neq 1$). The set of points R satisfying $\sqrt{\beta} \times \mathrm{d}(F, R) = \mathrm{d}(S, R)$ is the circle $\mathcal{C}_\beta$ of radius $\frac{\sqrt{\beta}}{|\beta-1|} \times \mathrm{d}(S, F)$ and centered on O.*

Proof 4 *Let $(S, \frac{\overrightarrow{SF}}{\|SF\|}, \overrightarrow{j}\,)$ be an orthonormal frame. The coordinates of the O point in this frame are $(\frac{\beta}{\beta-1}, 0)$ and the equation of $\mathcal{C}_\beta$ is:*

$$(x - \frac{\beta}{\beta - 1})^2 + y^2 = \frac{\beta}{(\beta - 1)^2}$$

We have:

$$\begin{array}{ll} & \beta \times \mathrm{d}^2(F,R) = \mathrm{d}^2(S,R) \\ \Leftrightarrow & \beta \times (1-x)^2 + \beta \times y^2 = x^2 + y^2 \\ \Leftrightarrow & (\beta - 1)(x^2+y^2) - 2 \times \beta \times x = -\beta \\ \Leftrightarrow & x^2 - \frac{2\times\beta}{\beta-1} \times x + y^2 = \frac{-\beta}{\beta-1} \\ \Leftrightarrow & (x - \frac{\beta}{\beta-1})^2 + y^2 = \frac{\beta}{(\beta-1)^2} \end{array}$$

Hence, all the points R satisfying $\sqrt{\beta} \times \mathrm{d}(F,R) = \mathrm{d}(S,R)$ are on the circle $\mathcal{C}_\beta$.

We can now establish the following result for omni-directional antenna.

Proposition 4 *Let O_β be a point of the (S,F) line such that $\overline{SO_\beta} = \frac{\beta}{\beta-1} \times \overline{SF}$. Let $\mathcal{C}_\beta$ be the circle of radius $\frac{\sqrt{\beta}}{|\beta-1|} \times \mathrm{d}(S,F)$ and centered on O_β (Figure 5).*

With an omni-directional antenna and a non standard transmission power $\beta \times P_{\mathrm{snd}}$ with $0 < \beta < 1$, the Sybil attack of S cannot be detected from the nodes R on the circle $\mathcal{C}_\beta$ and inside the disk $\mathcal{C}^\beta_{\mathrm{max}}$ of radius $\sqrt{\beta} \times \mathrm{d}_{\mathrm{max}}$ centered on S.

Proof 5 *The receiver R does not know that the sender S tunes its sending power. Hence, when S sends a message with the transmission power P^β_{snd}, R will measure a power P^β_{rcv} and compute an erroneous distance $\mathrm{d}_\beta(S,R)$ from S to R using the standard transmission power (see Equation 1):*

$$\mathrm{d}_\beta(S,R) = \sqrt{\frac{P_{\mathrm{snd}}}{P^\beta_{\mathrm{rcv}}} \times G_{SR}}$$

By Equation 1, $P^\beta_{\mathrm{rcv}} = \beta \times P_{\mathrm{rcv}}$ and we have

$$\mathrm{d}_\beta(S,R) = \sqrt{\frac{P_{\mathrm{snd}}}{\beta \times P_{\mathrm{rcv}}} \times G_{SR}} = \frac{1}{\sqrt{\beta}} \times \mathrm{d}(S,R)$$

In the message from the node S, the node R will read the position of the Sybil node F and will compute the distance $\mathrm{d}(F,R)$. To be cheated by the Sybil attack, the receiver node R must satisfy $\mathrm{d}_\beta(S,R) = \mathrm{d}(R,F)$, that is $\mathrm{d}(S,R) = \sqrt{\beta} \times \mathrm{d}(F,R)$. By Lemma 1, the cheated nodes are then on the circle $\mathcal{C}_\beta$.

Moreover, R cannot receive a message if it is outside the sender's range equal to $\sqrt{\beta} \times \mathrm{d}_{\mathrm{max}}$. Hence, the cheated receiver nodes are those (i) on the circle $\mathcal{C}_\beta$ and (ii) inside the disk $\mathcal{C}^\beta_{\mathrm{max}}$.

4.2 Bi-directional antenna

Proposition 5 *Let O_β be a point of the (S,F) line such that $\overline{SO_\beta} = \frac{\beta}{\beta-1} \times \overline{SF}$.*

With a bi-directional antenna, a non standard transmission power $\beta \times P_{\mathrm{snd}}$ with $0 < \beta < 1$ and any direction for the vehicles, the Sybil attack of S can be detected from any place.

Proof 6 *From Proposition 4, the cheated nodes are on the circle $\mathcal{C}_\beta$ and inside the disk $\mathcal{C}^\beta_{\mathrm{max}}$.*

Moreover, S and F must be in the same half plan defined by the axis line (D_R) of the node. Since any vehicle's direction is admitted, it is always possible to orient a vehicle in such a way that S and F are not in the same half plan defined by the axis line (D_R) of the vehicle.

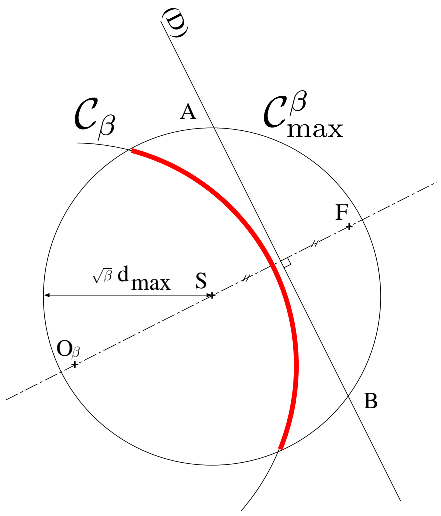

Figure 5: Omni-directional antenna and non standard transmission power (drawing with $\beta = 1/2$). Cheated nodes are on the circle $\mathcal{C}_\beta$ and inside $\mathcal{C}^\beta_{\max}$.

Proposition 6 *Let O_β be a point of the (S, F) line such that $\overline{SO_\beta} = \frac{\beta}{\beta-1} \times \overline{SF}$. Let $\mathcal{C}_\beta$ be the circle of radius $\frac{\sqrt{\beta}}{|\beta-1|} \times \mathrm{d}(S, F)$ and centered on O_β. Let (D_S) and (D_F) be the axis line of S and F respectively.*

With bi-directional antenna, non standard transmission power $\beta \times P_{\mathrm{snd}}$ with $0 < \beta < 1$ and same direction for all the vehicles, the Sybil attack of S cannot be detected from the nodes R (i) on the circle $\mathcal{C}_\beta$, (ii) inside the disk $\mathcal{C}^\beta_{\max}$ of radius $\sqrt{\beta} \times \mathrm{d}_{\max}$ centered on S, and (iii) not between the axis line (D_F) and (D_S) (Figure 6).

Proof 7 *From Proposition 4, the cheated nodes are on the circle $\mathcal{C}_\beta$ and inside the disk $\mathcal{C}^\beta_{\max}$ such that both S and F are in the same half plan defined by (D_R). This means that either both S and F are in front of R of back of R. Since all the vehicles have the same direction, this means that either R is back to S or in front of F regarding the common direction.*

5 Case 3: no signal attenuation and high transmission power

5.1 Omni-directional antenna

Lemma 2 *Let S be the sender of a message such as its transmission power is equal to $\beta \times P_{\mathrm{snd}}$, $\beta > 1$. The received signal power of this message is larger than $P^{\max}_{\mathrm{rcv}}$ if and only if the receiver is inside the disk $\mathcal{C}^\beta_{\min}$ of radius $\sqrt{\beta} \times \mathrm{d}_{\min}$ and centered on S.*

Proof 8 *Let S be a sender and R be a receiver such that the transmission power of S is $\beta \times P_{\mathrm{snd}}$,*

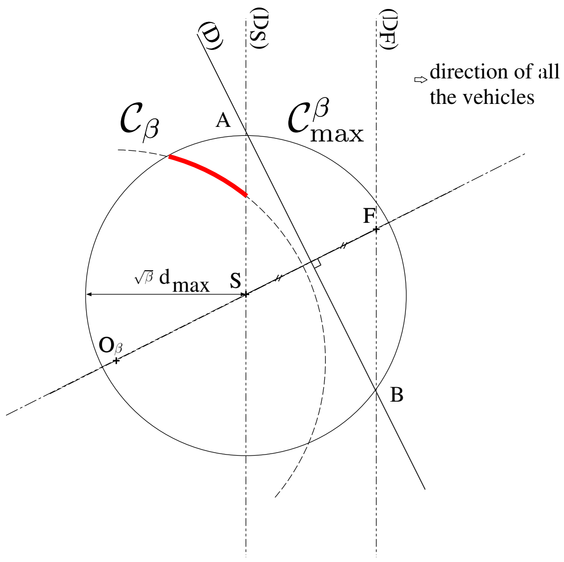

Figure 6: Bi-directional antenna, non standard sending (drawing with $\beta = 1/2$) power and same direction for all the vehicles. The Sybil attack of S cannot be detected from the nodes R on the circle $\mathcal{C}_\beta$ and inside the disk $\mathcal{C}^\beta_{\max}$ but not between the axis line (D_F) and (D_S)

($\beta > 1$) and the received power of the node R is P^β_{rcv}. Then, we have:

$$\begin{array}{lcl} P^\beta_{\mathrm{rcv}} & \leq & P^{\max}_{\mathrm{rcv}} \\ \beta \times P_{\mathrm{snd}} \times G_{SR} \times \frac{1}{\mathrm{d}^2(S,R)} & \leq & \frac{P_{\mathrm{snd}} \times G_{SR}}{\mathrm{d}^2_{\min}} \\ \sqrt{\beta} \times \mathrm{d}_{\min} & \leq & \mathrm{d}(S,R) \end{array}$$

Hence, if the transmission power of S is equal to $\beta \times P_{\mathrm{snd}}$, $\beta > 1$, every node R inside the circle $\mathcal{C}^\beta_{\min}$ received a signal power greater than $P^{\max}_{\mathrm{rcv}}$.

We can now establish the following result for omni-directional antenna.

Proposition 7 *Let O_β be a point of the (S, F) line such that $\overline{SO_\beta} = \frac{\beta}{\beta-1} \times \overline{SF}$. Let $\mathcal{C}_\beta$ be the circle of radius $\frac{\sqrt{\beta}}{|\beta-1|} \times \mathrm{d}(S, F)$ and centered on O_β (Figure 7).*

With an omni-directional antenna and a non standard transmission power $\beta \times P_{\mathrm{snd}}$ with $\beta > 1$, the Sybil attack of S cannot be detected from the nodes R (i) on the circle $\mathcal{C}_\beta$, (ii) inside the disk $\mathcal{C}^\beta_{\max}$ and (iii) outside the disk $\mathcal{C}^\beta_{\min}$.

Proof 9 *For conditions (i) and (ii), see Proposition 4. Condition (iii) is given by Lemma 2.*

5.2 Bi-directional antenna

The proof of the following proposition is similar to the one of Proposition 5.

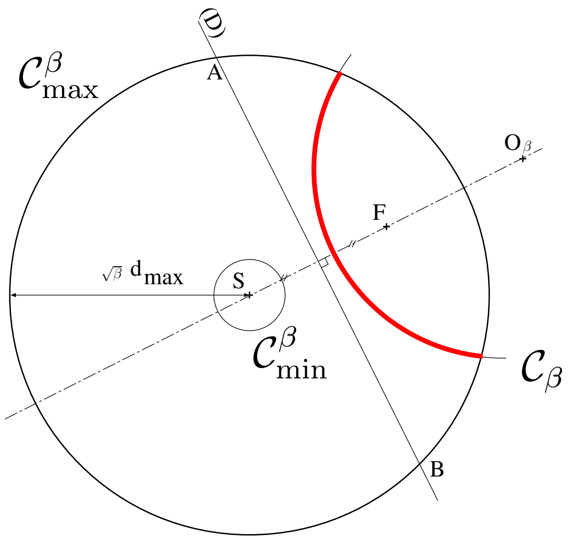

Figure 7: Omni-directional antenna and non standard transmission power (drawing with $\beta = 2$). Cheated nodes are on the circle $\mathcal{C}_\beta$ and inside the disk $\mathcal{C}_{\max}^{\beta}$ and outside the disk $\mathcal{C}_{\min}^{\beta}$.

Proposition 8 *Let O_β be a point of the (S, F) line such that $\overline{SO_\beta} = \frac{\beta}{\beta-1} \times \overline{SF}$.*

With a bi-directional antenna, a non standard transmission power $\beta \times P_{\text{snd}}$ with $\beta > 1$ and any direction for the vehicles, the Sybil attack of S can be detected from any place.

Proposition 9 *Let O_β be a point of the (S, F) line such that $\overline{SO_\beta} = \frac{\beta}{\beta-1} \times \overline{SF}$. Let $\mathcal{C}_\beta$ be the circle of radius $\frac{\sqrt{\beta}}{|\beta-1|} \times \mathrm{d}(S, F)$ and centered on O_β. Let (D_S) and (D_F) be the axis line of S and F respectively.*

With bi-directional antenna, non standard transmission power $\beta \times P_{\text{snd}}$ with $0 < \beta < 1$ and same direction for all the vehicles, the Sybil attack of S cannot be detected from the nodes R (i) on the circle $\mathcal{C}_\beta$, (ii) inside the disk $\mathcal{C}_{\max}^{\beta}$, (iii) not between the axis line (D_F) and (D_S) and (iv) outside the disk $\mathcal{C}_{\min}^{\beta}$.

Proof 10 *For conditions (i), (ii) and (iii), see Proposition 7. Condition (iv) is given by Lemma 2.*

6 General case: propagation with signal attenuation

In this section, we consider a real propagation environment by considering a signal attenuation (factor α, see Section 2). Such an attenuation depends on different parameters, including the distance from the sender to the receiver. As we cannot know the exact value of this attenuation for each received message, we cannot deduce the exact distance between nodes as in previous sections. Nevertheless, we can use the free space propagation model to compute an upper bound on the distance. We can deduce the maximal distance from the sender, corresponding to an attenuation factor α of 1. If the position announced by a node results into a distance larger than the estimated

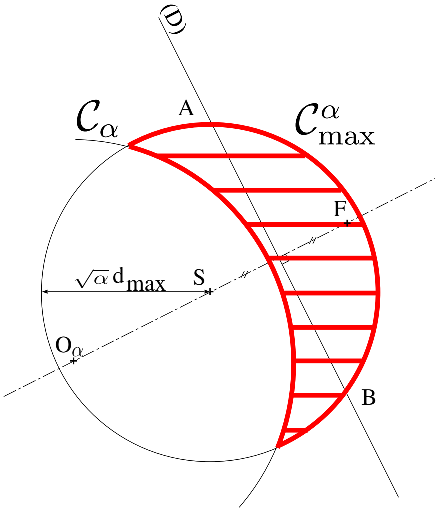

Figure 8: Omni-directional antenna and standard transmission power with attenuation (drawing with $\alpha = 1/2$). Cheated nodes are outside the circle $\mathcal{C}_\alpha$ and inside the disk $\mathcal{C}^\alpha_{\max}$.

upper bound, the node is a Sybil node. Otherwise, nothing can be deduced. Hence, we will no more obtain parts of lines or circles but surfaces. We examine the four cases described in the table of the Figure 1. This is the main contribution of this paper.

6.1 Omni-directional antenna and standard transmission power

When the sender S sends a message, a receiver R measures a received power that results both of the attenuation and of the tuning. When there is no tuning, the attenuation factor α plays the same role as the tuning factor β when it is smaller than 1 (Section 4).

The following result is then deduced from Proposition 4 (Figure 8).

Proposition 10 *Let O_α be a point of the (S, F) line such that $\overline{SO_\alpha} = \frac{\alpha}{\alpha-1} \times \overline{SF}$. Let $\mathcal{C}_\alpha$ be the circle of radius $\frac{\sqrt{\alpha}}{|\alpha-1|} \times \mathrm{d}(S, F)$ and centered on O_α.*

With an omni-directional antenna, a standard transmission power P_{snd} and a signal attenuation $\alpha < 1$, the Sybil attack of S cannot be detected from the nodes R (i) outside the circle $\mathcal{C}_\alpha$ and (ii) inside the disk $\mathcal{C}^\alpha_{\max}$.

6.2 Bi-directional antenna and standard transmission power

Similarly, from Propositions 5 and 6, we deduce the following result.

Proposition 11 *Let O_α be a point of the (S, F) line such that $\overline{SO_\alpha} = \frac{\alpha}{\alpha-1} \times \overline{SF}$. Let $\mathcal{C}_\alpha$ be the circle of radius $\frac{\sqrt{\alpha}}{|\alpha-1|} \times \mathrm{d}(S, F)$ and centered on O_α.*

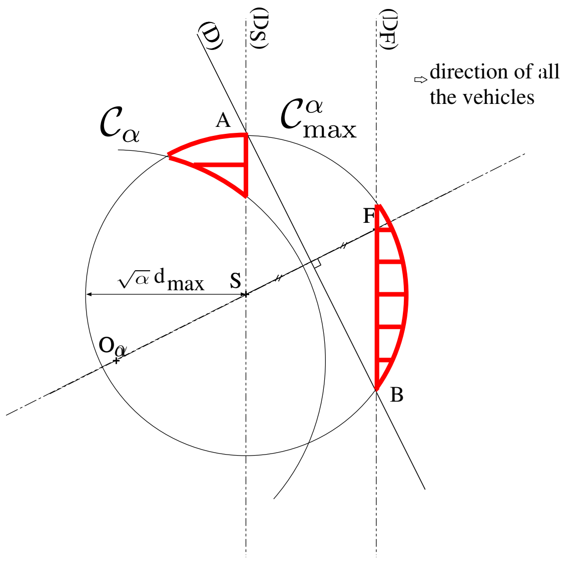

Figure 9: Bi-directional antenna and standard transmission power with attenuation (drawing with $\alpha = 1/2$). Cheated nodes are outside the circle $\mathcal{C}_\alpha$ and inside the disk $\mathcal{C}^\alpha_{\text{max}}$ but not between the axis lines (D_F) and (D_S).

With a bi-directional antenna, a standard transmission power P_{snd}, a signal attenuation factor α, and

- *any direction for the vehicles, the Sybil attack of S can be detected from any place.*
- *the same directions for all the vehicles, the Sybil attack of S cannot be detected from the nodes R (i) outside the circle $\mathcal{C}_\alpha$, (ii) inside the disk $\mathcal{C}^\alpha_{\text{max}}$ and (iii) not between the axis line (D_F) and (D_S) (Figure 9).*

6.3 Omni-directional antenna and tuned transmission power

In this section, we consider the combined action of the attenuation factor α and the tuning factor β. We denote by γ the product $\alpha \times \beta$.

The following result is given by Propositions 4 and 7.

Proposition 12 *Let O_γ be a point of the (S, F) line such that $\overline{SO_\gamma} = \frac{\gamma}{\gamma-1} \times \overline{SF}$. Let $\mathcal{C}_\gamma$ be the circle of radius $\frac{\sqrt{\gamma}}{|\gamma-1|} \times \text{d}(S, F)$ and centered on O_γ.*

With an omni-directional antenna, an attenuation factor α and a tuned transmission power $\beta \times P_{\text{snd}}$, the Sybil attack of S cannot be detected from the nodes R

- *(i) inside the circle $\mathcal{C}_\gamma$ and (ii) inside the disk $\mathcal{C}^\gamma_{\text{max}}$ and (iii) outside the disk $\mathcal{C}^\gamma_{\text{min}}$ if $\gamma = \alpha \times \beta > 1$ (Figure 10).*
- *(i) outside the circle $\mathcal{C}_\gamma$ and (ii) inside the disk $\mathcal{C}^\gamma_{\text{max}}$ if $\gamma < 1$ (Figure 8).*

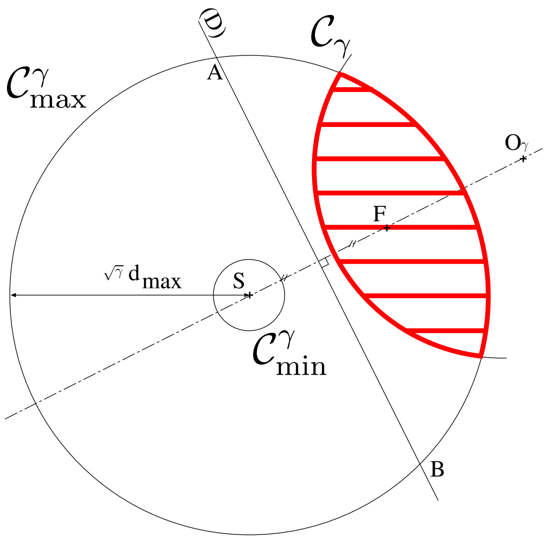

Figure 10: Omni-directional antenna and non standard transmission power with attenuation (drawing with $\gamma = 2$). Cheated nodes are inside the circle $\mathcal{C}_\gamma$, outside the circle $\mathcal{C}^\gamma_{\min}$ and inside the disk $\mathcal{C}^\gamma_{\max}$.

- *(i) belonging to the half plan defined by the intersection of the perpendicular bissector* (D) *and the disk* $\mathcal{C}_{\max}$ *and that does not contain* S *if* $\gamma = 1$.

6.4 Bi-directional antenna and tuned transmission power

Similarly, the following result is deduced from Propositions 5, 6, 8 and 9:

Proposition 13 *Let* O_γ *be a point of the* (S, F) *line such that* $\overline{SO_\gamma} = \frac{\gamma}{\gamma-1} \times \overline{SF}$. *Let* $\mathcal{C}_\gamma$ *be the circle of radius* $\frac{\sqrt{\gamma}}{|\gamma-1|} \times \mathrm{d}(S, F)$ *and centered on* O_γ.

With a bi-directional antenna, a signal attenuation factor α, *a non standard transmission power* $\beta \times P_{\mathrm{snd}}$, *and*

- *any direction for the vehicles, the Sybil attack of* S *can be detected from any place.*
- *the same direction for all the vehicles, the Sybil attack of* S *cannot be detected from the nodes* R
  - *(i) inside the circle* $\mathcal{C}_\gamma$ *and (ii) inside the disk* $\mathcal{C}^\gamma_{\max}$, *(iii) outside the disk* $\mathcal{C}^\gamma_{\min}$ *and (iv) not between the axis line* (D_F) *and* (D_S) *if* $\gamma = \alpha \times \beta > 1$ *(Figure 11).*
  - *(i) outside the circle* $\mathcal{C}_\gamma$, *(ii) inside the disk* $\mathcal{C}^\gamma_{\max}$ *and (iii) not between the axis line* (D_F) *and* (D_S) *if* $\gamma < 1$ *(Figure 8).*
  - *(i) belonging to the half plan defined by the intersection of the perpendicular bissector* (D) *and the disk* $\mathcal{C}_{\max}$ *and that does not contain* S, *and (ii) not between the axis line* (D_F) *and* (D_S) *if* $\gamma = 1$.

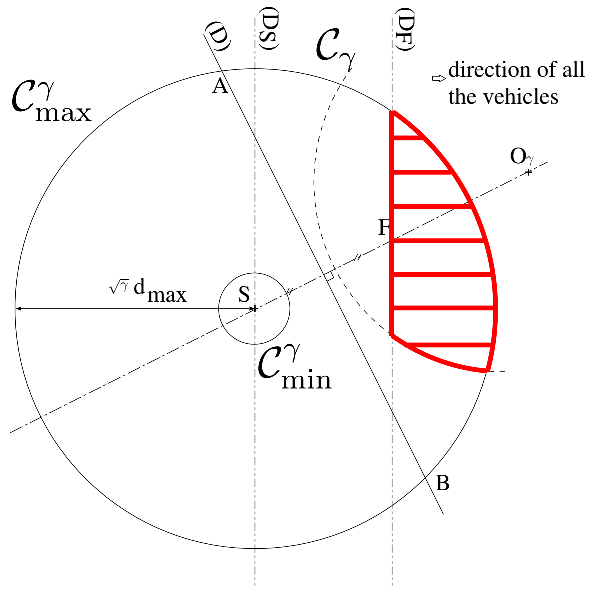

Figure 11: Bi-directional antenna and non standard transmission power with attenuation (drawing with $\gamma = 2$). Cheated nodes are inside the circle $\mathcal{C}_\gamma$, inside the disk $\mathcal{C}^\gamma_{\max}$, outside the disk $\mathcal{C}^\gamma_{\min}$ but not between the axis lines (D_F) and (D_S).

7 Discussions

We examined four cases of Sybil attacks: with or without tuning transmission power, and with omni- or bi-directional antennas (Figure 1). The geometrical analysis is a way to determine the area of nodes that could be cheated, and then to evaluate the severity of the attack. We now discuss on the interest of tuning the transmission power and using a bi-directional antenna instead of an omni-directional one.

7.1 Tuning transmission power

We can reasonably assume that a standard for vehicular communication would fix the transmission power of each vehicles. Such a standard transmission power would then be used by all honest transmitting nodes. As a Sybil node is not transmitting anything, it will also be considered as an honest node (from this point of view). The only vehicles that may voluntarily bypass this rule are then the attacking nodes.

Increasing the transmission power allows to increase the area of successful attacks. However it also increase the area of reception. Fortunately, the receiving nodes that are not cheated can detect the Sybil attack. Then, by vehicle cooperation, the attack has a high probability to fail. Hence, increasing the transmission power could decrease the severity of the attack and could also be dangerous for the attacker (indeed, one may imagine police vehicles that measure excessive sending power). Therefore, there is a tradeoff between the area of successful attack, and the area of detection.

To evaluate this tradeoff, we study the ratio *area of successful attack over area of reception.*

Figure 12 shows the ratio depending on the factor γ (product of attenuation α and tuning factor β) and on the distance between the attacker node S and the Sybil node F. We can see that the ratio is maximal for values of γ near to 1 and for short distances $\mathrm{d}(S, F)$.

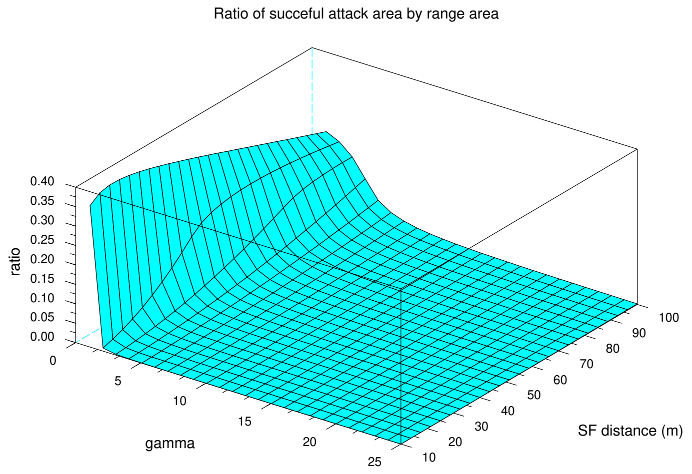

Figure 12: Ratio of the successful attack area by the attacker's signal range area.

This means that increasing the transmission power is of limited interest for an attacker. The attacker should just tune its transmission power in the aim of compensating the signal attenuation (to obtain $\gamma = 1$). But this is not easily determined.

Note also that if the Sybil nodes should be near the attacker, it will be less easy to simulate a traffic jam by means of many Sybil nodes.

7.2 Antenna

The results presented in the previous section shows the great benefits of bi-directional antennas over omni-directional antennas. Such antennas are particularly efficient in urban environment where vehicles often change their direction. In such an environment, the attack could always be detected by a vehicle, which could then warn its neighbors.

Bi-directional antenna are less interesting in country roads or high-way where all the vehicles have the same direction. However they allow to significantly reduce the area of successful attacks (Figure 10 versus Figure 11). To reduce the area of detection (between (D_S) and (D_F)), the attacker should place the Sybil node close to it. As already said, this may limit the interest of the attack.

8 Conclusion and Future Work

In this paper, the influence of different assumptions on the success of Sybil attacks has been studied. The transmission signal tuning and the kind of reception antenna (either omni- or bi-directional) have been taken into account. We have characterized the success area of a Sybil attack and shown that with the basic assumptions, a Sybil attack is detected by at least half of the receivers. The number of detectors is largely increased with the use of bi-directional antenna; this result argues in favor of the use of such antenna in VANET.

We showed that only certain areas may contain cheated nodes. As we have characterized such areas, we think that the results given in this paper provide a good framework to elaborate realistic test suites for Sybil attack detection methods and to evaluate them from an objective point of view.

The results presented in this paper consider only the signal strength and direction analysis. As future work, we plan to study how node collaboration can reduce the success area of Sybil attacks. This model is based on trust relations establishment between nodes and may not require cryptography.

References

[BC94] S. Brands and D. Chaum. Distance-bounding protocols. In *Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, pages 344–359, 1994.

[BE04] J. Blum and A. Eskandarian. The Threat of Intelligent Collisions. *IT Professional*, 6(1):24–29, January-February 2004.

[CH05] S. Capkun and JP. Hubaux. Secure positioning of wireless devices with application to sensor networks. In *IEEE INFOCOM 2005*, volume 3, pages 1917–1928, 2005.

[Dou02] J. Douceur. The Sybil Attack. In *First International Workshop on Peer-to-Peer Systems*, pages 251–260, March 2002.

[GGS04] P. Golle, D. Greene, and J. Staddon. Detecting and Correcting Malicious Data in VANETS. In *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pages 29–37, October 2004.

[Mer78] R. C. Merkle. Secure Communications over Insecure Channels. *Communications of the ACM*, 21(4):294–299, April 1978.

[NSSP04] J. Newsome, E. Shi, D. Song, and A. Perrig. The Sybil Attack in Sensor Networks: Analysis & Defenses. In *Proceedings of the third international symposium on Information processing in sensor networks*, pages 259–268, 2004.

[PdPFWL04] W. Pires, T. de Paula Figueiredo, HC. Wong, and A. Loureiro. Malicious Node Detection in Wireless Sensor Networks. In *Proceedings of the 8th IEEE International Parallel & Distributed Processing Symposium*, 2004.

[PSL06] C. Piro, C. Shields, and B. N. Levine. Detecting the Sybil Attack in Mobile Ad hoc Networks. In *Second International Conference on Security and Privacy in Communication Networks*, 2006.

[RH05] M. Raya and JP. Hubaux. The Security of Vehicular Ad Hoc Networks. In *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, pages 11–21, 2005.

[RH07] M. Raya and JP. Hubaux. Securing Vehicular Ad Hoc Networks. *Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks*, 15(1):39–68, 2007.

[RPH06] M. Raya, P. Papadimitratos, and JP. Hubaux. Securing Vehicular Communications. *IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications*, 13(5):8–15, 2006.

[SY05] T. Suen and A. Yasinsac. Ad Hoc Network Security: Peer Identification and Authentication Using Signal Properties. In *Systems, Man and Cybernetics (SMC) Information Assurance Workshop*, pages 432–433, June 2005.

[XYG06] Bin Xiao, Bo Yu, and Chuanshan Gao. Detection and Localization of Sybil Nodes in VANETs. In *ACM/SIGMOBILE Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks*, pages 1–8, 2006.