On the Sybil attack detection in VANET

Gilles Guette and Bertrand Ducourthial

Laboratoire Heudiasyc UMR CNRS 6599
Université de Technologie de Compiègne, France
Email: firstname.lastname@hds.utc.fr

***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. 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.**

I. Introduction

A. Security in VANET

The recent gain of interest for wireless communication in Vehicular Ad hoc Network (VANET) implies an always increasing number of applications in this kind of network. 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 applications such as emergency brake. Moreover, due to the limited communication range of a vehicle, the cooperation between nodes is essential. This necessity of cooperation shows the vulnerability of these networks and the need of fake nodes detection. The multiplication of fake nodes in a wireless network in order to launch different kind of attack is known as the Sybil attack [4]. We give a brief survey of related work about this attack and the possible defenses in the following.

B. Related Work

1) The Sybil attack: The Sybil attack was first described and formalized by Douceur in [4]. It consists in sending multiple messages from one node with multiple identities. Applications of the Sybil attack to Vehicular Ad-Hoc Networks have been discussed in [1], [10] and show the importance of Sybil nodes detection in VANET. One important result shown in [4] 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.

2) Resources testing: [4] and [8] 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 [4] uses computational puzzles [7] to test nodes computational resources. In [8], 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. Instead, they propose a radio resource testing.

3) Use of public key cryptography: In [11], the authors try to solve the security problem of the Sybil attack with public key cryptography. 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. They also propose a mechanism for key revocation. As each vehicle may be authenticated with its public key, 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.

4) Assuming a given propagation model: Some papers dealing with detection of Sybil attack in wireless networks assume a predefined propagation model [9], [13]. They use the received signal power to deduce some inconsistencies between the power of the signal and the claimed position. In [13], a node collects signal strength measurement from other nodes and estimates their new position according to a given propagation model. A node is considered suspect if its claimed position is too far from the evaluated one.

5) Secure positioning: Another possibility to defeat Sybil attack is to provide a secure positioning system and the reliability of the position claimed by vehicles. In [12], 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.

In [3], the authors present a novel approach called *verifiable multilateration*, using distance bounding protocol [2] and base stations to provide secure positioning. They also assume that all network nodes can establish pairwise secret keys.

6) Distinguishability: In [5], 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 notably rely on the fact that nodes are equipped with specific devices allowing to tie a message with a physical sources.

C. 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

1-4244-1455-5/07/$25.00

role of the assumptions on the success rate of Sybil attacks. In order to measure such a success, we 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 characterize 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. 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 II formally describes the problem addressed in this paper. Section III, IV and V are dedicated to specific cases, while Section VI presents the main results[1]. These results are analyzed in Section VII. Concluding remarks end the paper.

II. Problem statement

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

A. Notations

Let S and R be two mobile nodes such that S is the sender and R the receiver. 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 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 $4\pi \cdot \mathrm{d}^2(S,R)$ and 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 for $\mathrm{d}(S,R)$ sufficiently large, R will receive a power P_{rcv} equals to:

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

The previous formula assumes that there is no signal attenuation. Hence it gives the *maximal* received power. By denoting $G_{\mathsf{SR}} = G_{\mathrm{snd}} \times G_{\mathrm{rcv}} \times \lambda^2/(16\pi^2)$ the gain of the link from S to R, the maximal power $P_{\mathrm{rcv}}^{\max}(\mathrm{d}(S,R))$ at distance $\mathrm{d}(S,R)$ from the sender is:

$$P_{\mathrm{rcv}}^{\max}\left(\mathrm{d}(S,R)\right) = P_{\mathrm{snd}} \times G_{\mathsf{SR}} \times \frac{1}{\mathrm{d}^2(S,R)} \qquad (1)$$

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

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

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

[1]Due to lack of space, all the proofs may be found in [6]

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 $P_{\mathrm{rcv}}^{\min}$.

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

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:

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

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. The reason is, we use this disk as un upper bound. In reality the range of an antenna is entirely included in such a disk $\mathcal{C}_{\max}$.

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

$$P_{\mathrm{rcv}}^{\max} = P_{\mathrm{snd}} \times G_{\mathsf{SR}} \times \frac{1}{\mathrm{d}_{\min}^2} \qquad (5)$$

B. 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 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 [9], [13]. 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, the sender may use a non standard equipment. This implies that its transmission power could vary instead of being fixed:

$$P_{\mathrm{snd}}^{\mathrm{attack}} = \beta \times P_{\mathrm{snd}} \qquad \beta > 0 \qquad (6)$$

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, defining two half plan, allowing to detect whether the sender of a message is ahead or back of the car. 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 Euclidean plan into two half plans.

C. 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.

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 results obtained in this first phase (Sections III-V) 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 VI) are discussed in Section VII.

III. 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 III to V describe what can be deduced when the distance is the only factor of signal attenuation. This *far from reality* assumption allows to ease the presentation of our main contribution in section VI where this assumption is relaxed.

In the following, we note (D) the perpendicular bisector of segment $[S, F]$ and A and B the intersection points of (D) and $\mathcal{C}_{\max}$.

A. Omni-directional antenna

Proposition 1: With omni-directional antenna and standard transmission power, Sybil node attack of S cannot be detected by nodes on the line segment $[A, B]$ (Figure 1).

B. Bi-directional antenna

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

Proposition 2: 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, Figure 2).

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

Proposition 3: 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).

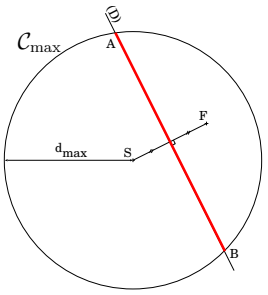

Fig. 1. Omni-directional antenna and standard transmission power. Cheated nodes are on line segment $[A, B]$.

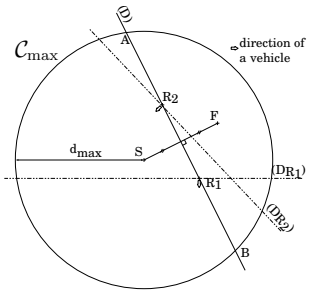

Fig. 2. Bi-directional antenna, standard transmission power and any direction for the vehicles. Cheated nodes R are on the line segment $[A, B]$ such that S and F are in the same half plan defined by (D_R). Here, R_1 is cheated while R_2 is not. Consequently, the Sybil attack can be detected from any place.

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 $[D, B]$ (Figure 3).

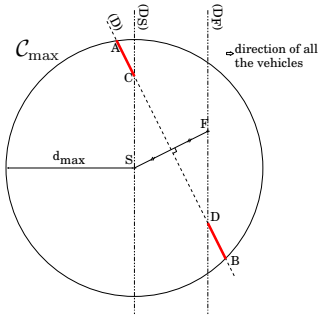

Fig. 3. Bi-directional antenna, standard transmission power and same direction for all the vehicles. The Sybil attack of S cannot be detected by vehicles on line segments $[A, C]$ and $[D, B]$.

IV. 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 $\beta \times P_{\text{snd}}$, $0 < \beta < 1$.

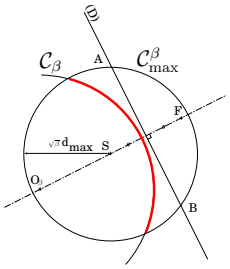

Fig. 4. Omni-directional antenna and tuned transmission power (drawing with $\beta = 1/2$). Cheated nodes are on the circle $\mathcal{C}_\beta$ and inside $\mathcal{C}^\beta_{\max}$.

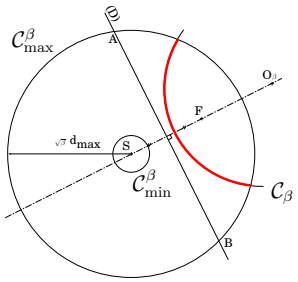

Fig. 5. Omni-directional antenna and non standard transmission power (drawing with $\beta = 2$). Cheated nodes are on the circle $\mathcal{C}_\beta$ and inside the disk $\mathcal{C}^\beta_{\max}$ and outside the disk $\mathcal{C}^\beta_{\min}$.

In the following, we denote O_β a point of the (S, F) line such that $\overline{SO_\beta} = \frac{\beta}{\beta-1} \times \overline{SF}$. And, $\mathcal{C}_\beta$ the circle of radius $\frac{\sqrt{\beta}}{|\beta-1|} \times \mathrm{d}(S, F)$ and centered on O_β.

A. Omni-directional antenna

Proposition 4: 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 $\mathcal{C}^\beta_{\max}$ of radius $\sqrt{\beta} \times \mathrm{d}_{\max}$ centered on S (Figure 4).

B. Bi-directional antenna

Proposition 5: With a bi-directional antenna, a tuned 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.
- the 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).

V. Case 3: no signal attenuation and high transmission power

A. Omni-directional antenna

Proposition 6: 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 $\mathcal{C}^\beta_{\min}$ (Figure 5).

B. Bi-directional antenna

Proposition 7: With a bi-directional antenna, a non standard transmission power $\beta \times P_{\mathrm{snd}}$ with $\beta > 1$ with $0 < \beta < 1$ 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) on the circle $\mathcal{C}_\beta$, (ii) inside the disk $\mathcal{C}^\beta_{\max}$, (iii) not between the axis line (D_F) and (D_S) and (iv) outside the disk $\mathcal{C}^\beta_{\min}$.

VI. General case: propagation with signal attenuation

In this section, we consider a real propagation environment by considering a signal attenuation (factor α, see Section II). 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. 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 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.

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

A. 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 IV). The following result is then deduced from Proposition 4 (Figure 6).

Proposition 8: 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 $\mathcal{C}^\alpha_{\max}$.

B. Bi-directional antenna and standard transmission power

Proposition 9: 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

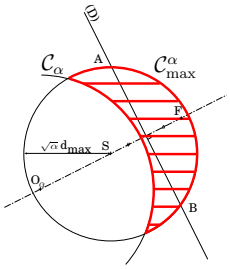

Fig. 6. Omni-directional antenna and standard transmission power with attenuation (drawing with $\alpha = 1/2$). Cheated nodes are outside the circle $\mathcal{C}_\alpha$ and inside the disk $\mathcal{C}^\alpha_{\max}$.

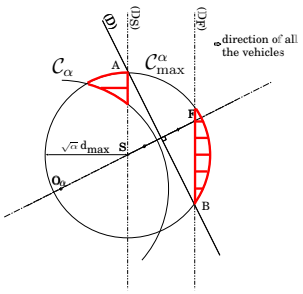

Fig. 7. Bi-directional antenna and standard transmission power with attenuation (drawing with $\alpha = 1/2$). Cheated nodes are outside the circle $\mathcal{C}_\alpha$ and inside the disk $\mathcal{C}^\alpha_{\max}$ but not between the axis lines (D_F) and (D_S).

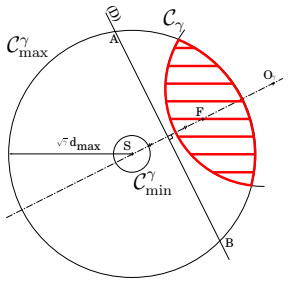

Fig. 8. Omni-directional antenna and non standard transmission power with attenuation (drawing with $\gamma = 2$). Cheated nodes are inside the circle $\mathcal{C}_\gamma$, outside the circle $\mathcal{C}^\gamma_{\min}$ and inside the disk $\mathcal{C}^\gamma_{\max}$.

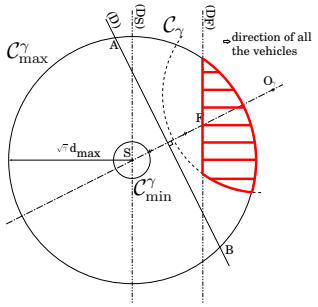

Fig. 9. Bi-directional antenna and non standard transmission power with attenuation (drawing with $\gamma = 2$). Cheated nodes are inside the circle $\mathcal{C}_\gamma$, inside the disk $\mathcal{C}^\gamma_{\max}$, outside the disk $\mathcal{C}^\gamma_{\min}$ but not between (D_F) and (D_S).

circle $\mathcal{C}_\alpha$, (ii) inside the disk $\mathcal{C}^\alpha_{\max}$ and (iii) not between the axis line (D_F) and (D_S) (Figure 7).

C. 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 $\alpha \times \beta$.

Proposition 10: 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 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 $\mathcal{C}^\gamma_{\max}$ and (iii) outside the disk $\mathcal{C}^\gamma_{\min}$ if $\gamma = \alpha \times \beta > 1$ (Figure 8).
- (i) outside the circle $\mathcal{C}_\gamma$ and (ii) inside the disk $\mathcal{C}^\gamma_{\max}$ if $\gamma < 1$ (Figure 6).
- (i) belonging to the half plan defined by the intersection of the perpendicular bisector (D) and the disk $\mathcal{C}_{\max}$ and that does not contain S if $\gamma = 1$.

D. Bi-directional antenna and tuned transmission power

Proposition 11: 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 $\beta \times P_{\text{snd}}$, 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 (D_F) and (D_S) if $\gamma = \alpha \times \beta > 1$ (Figure 9).
  - (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 6).
  - (i) belonging to the half plan defined by the intersection of the perpendicular bisector (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 $\gamma = 1$.

VII. Discussions

We examined four cases of Sybil attacks: with or without tuning transmission power, and with omni- or bi-directional antennas. 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.

A. 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 10 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 $\mathrm{d}(S, F)$.

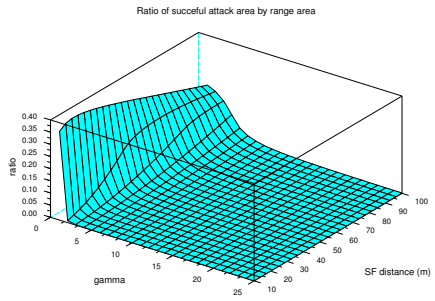

Fig. 10. Ratio of the successful attack area by the attacker's signal range area.

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.

B. 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 8 versus Figure 9). 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.

VIII. 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

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

[2] 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.

[3] 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.

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

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

[6] Gilles Guette and Bertrand Ducourthial. On the Sybil attack detection in VANET (extended version). Technical report, Heudiasyc Laboratory, University of Compigne, 2007.

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

[8] J. Newsome, E. Shi, D. Song, and A. Perrig. The Sybil Attack in Sensor Networks: Analysis & Defenses. In *International symposium on information processing in sensor networks*, pages 259–268, 2004.

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

[10] 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.

[11] 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.

[12] 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, 2005.

[13] 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.