On the Sybil attack detection in VANET

Gilles Guette and Bertrand Ducourthial

Laboratoire Heudiasyc, UMR CNRS 6599
Université de Technologie de Compiègne

IEEE MoVeNet 2007, Pisa

Outlines

Plan

Security in VANET

- Network of vehicles
  - mobiles communicating nodes
    with unstable topology
  - few access to an infrastructure C2C vs. C2I
    $\rightsquigarrow$ generally highly dynamic ad hoc networks
    VANET
  - identity preservation
- Inter-vehicles applications
- Need for security
- Solutions

Security in VANET

- Network of vehicles
- Inter-vehicles applications
  - infrastructure oriented with C2I
    e.g., gathering information related to traffic conditions
  - vehicle oriented
    e.g., obstacle detection, position on the road, distance to previous car
  - driver oriented
    e.g., best way to reach the station, weather forecast, gaz prices...
  - passengers oriented
    e.g., shared juxe box, touristic informations, games...
- Need for security
- Solutions

Security in VANET

- Network of vehicles
- Inter-vehicles applications
- Need for security
  - same as in ad hoc networks
    - passive listening
    - routing disturbance
  - specific to VANET
    depends on the applications
    - traffic jam illusion
    - creation of accidents
    - ...
  - easy : just send the right messages
- Solutions

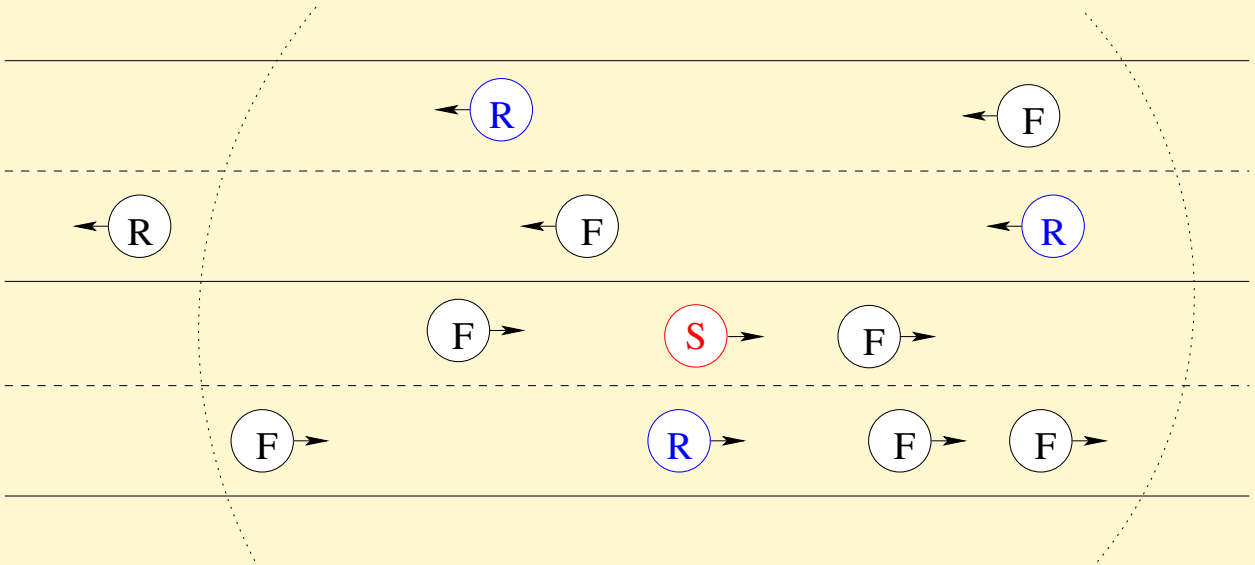
Security in VANET

- Network of vehicles
- Inter-vehicles applications
- Need for security
- Solutions
  - pessimistic security
    - PKI
    - not easy in VANET
      sparse connexion to the infrastructure, revocation scheme ?...
  - optimistic security
    - combining several sources of information
    - what in case of fake nodes creation ?

Plan

Sybil attack

- Creation of fake nodes [Douceur et al. 2002]
  - by sending messages with false GPS positions
  - in the transmission area



Hypotheses in the litterature

- Same material or same technical characteristics
  - true if the material comes from a single authority
  - allows to test the resources
    radio ↔ range, delai for several messages...
    [Newsome et al. 2004]
    CPU ↔ computational puzzles [Douceur et al. 2002]
- Public key infrastructure available
- Local checking
- Continuous propagation model
- Nodes cooperation
- Tests and validation scenarios

Hypotheses in the litterature

- Same material or same technical characteristics
- Public key infrastructure available
  - key $\leftrightarrow$ unique identifier
  - access to a reliable revocation system
  - several keys for privacy preservation
- Local checking
- Continuous propagation model
- Nodes cooperation
- Tests and validation scenarios

Hypotheses in the litterature

- Same material or same technical characteristics
- Public key infrastructure available
- **Local checking**

  there exists a physical mean to associate a sender to a real device (*e.g.*, camera) [Golle et al. 2004]
- Continuous propagation model
- Nodes cooperation
- Tests and validation scenarios

Hypotheses in the litterature

- Same material or same technical characteristics
- Public key infrastructure available
- Local checking
- Continuous propagation model

  this allows to compute the exact expected reception power depending on the given sender-receiver distance [Xiao et al. 2006]
- Nodes cooperation
- Tests and validation scenarios

Hypotheses in the litterature

- Same material or same technical characteristics
- Public key infrastructure available
- Local checking
- Continuous propagation model
- Nodes cooperation

  combining local informations [Golle et al. 2004]
- Tests and validation scenarios

Hypotheses in the litterature

- Same material or same technical characteristics
- Public key infrastructure available
- Local checking
- Continuous propagation model
- Nodes cooperation
- Tests and validation scenarios
  - few informations on the scenarios used
  - in a VANET, random positions are not realistic nor representative

Plan

Study
hypotheses vs. impact of Sybil attacks

- Aim
  - characterize the impact of a Sybil attack
    number of cheated vehicles
  - characterize the influence of the hypotheses on the impact
- Method
- Hypotheses

Study
hypotheses vs. impact of Sybil attacks

- Aim
- Method
  - computing the geographic area where the attack succeeds
  - depending on the kind of antenna and the tuning of the sending power P_{snd}
- Hypotheses

Study
hypotheses vs. impact of Sybil attacks

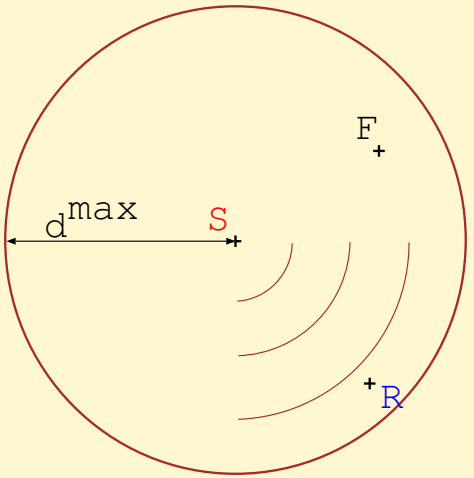
- Aim
- Method
- Hypotheses
  - GPS, coordinates announced in messages
  - measures of the received power
  - sender (attacker)
    - standard P_{snd} : propagation with attenuation
    - tuned P_{snd} : attenuation + tuning
  - receiver
    - omnidirectional antenna
    - bidirectional antenna : front/rear

Receiver \ Sender	standard P_{snd}	tuned P_{snd}
omnidirectional antenna		
bidirectional antenna		

How to detect a fake node

- At the reception, a node compares the measuring reception power and the computed reception power

  computed with coordinates announced in the messages
- Without attenuation nor tuning of P_{snd}
  - $P_{\text{rcv}}(S,R) = P_{\text{snd}} \times G_{\text{SR}} \times \frac{1}{\text{d}^2(S,R)}$
  - R detects that $F \neq S$ if $P_{\text{rcv}}(S,R) \neq P_{\text{rcv}}(F,R)$



- More complex with attenuation or tuning

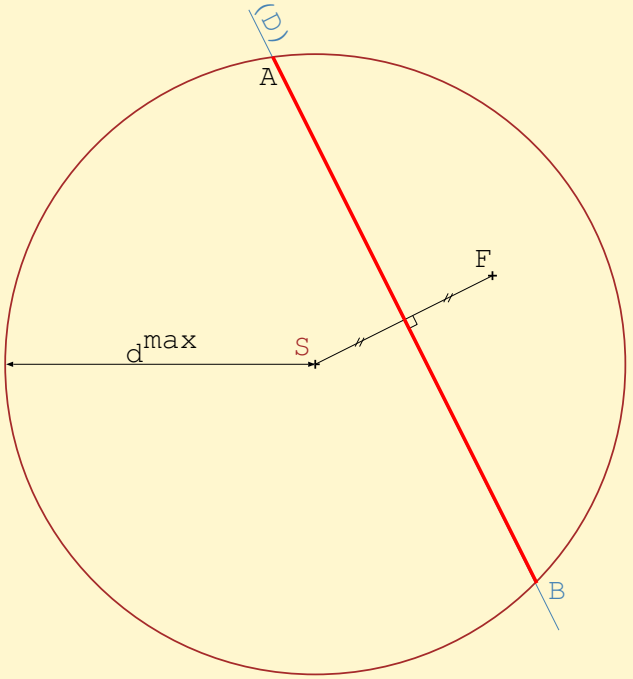
Plan

Results without attenuation

- No attenuation
  - $\rightsquigarrow$ exact position $\rightsquigarrow$ lines (instead of area)
  - gives the borders of further areas

Standard P_{snd} without attenuation and omni-directional antenna

$\rightsquigarrow$ cheated nodes are on line segment $[A, B]$

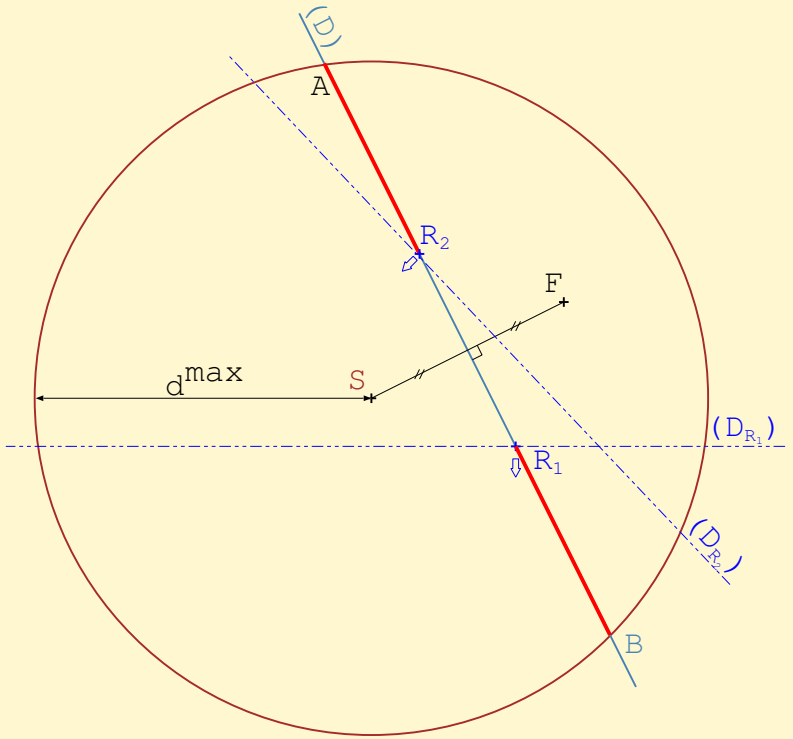


Results without attenuation

Standard P_{snd} without attenuation and bi-directional antenna and unknown directions

$\rightsquigarrow$ the attack can be detected from everywhere

depends on the direction of the receiver : R_1 is cheated, R_2 not.

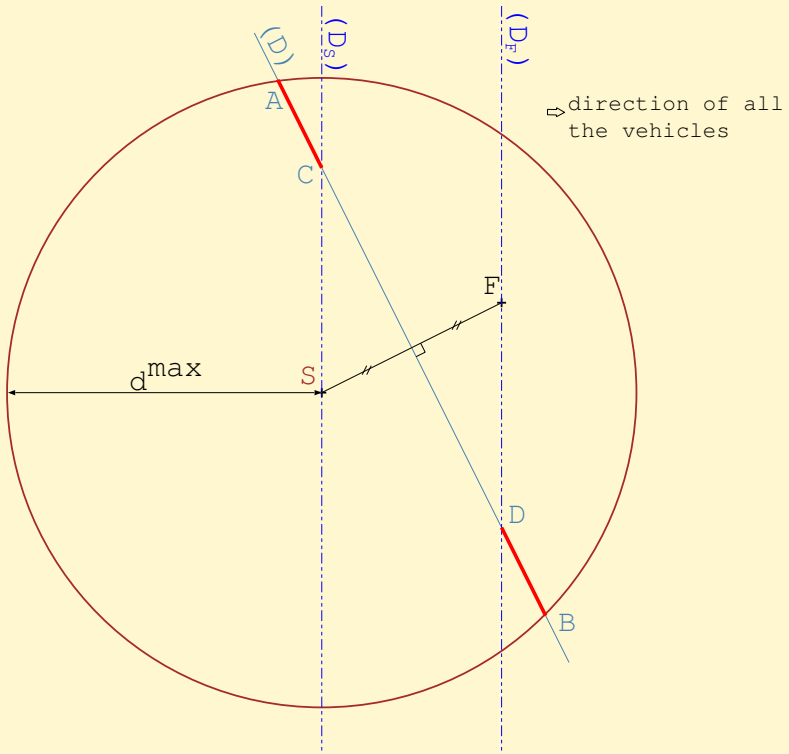


Results without attenuation

Standard P_{snd} without attenuation and bi-directional antenna and same directions

$\rightsquigarrow$ cheated nodes are on $[A, C]$ and $[D, B]$

R is cheated if it sees S and F in the same semi-plan.



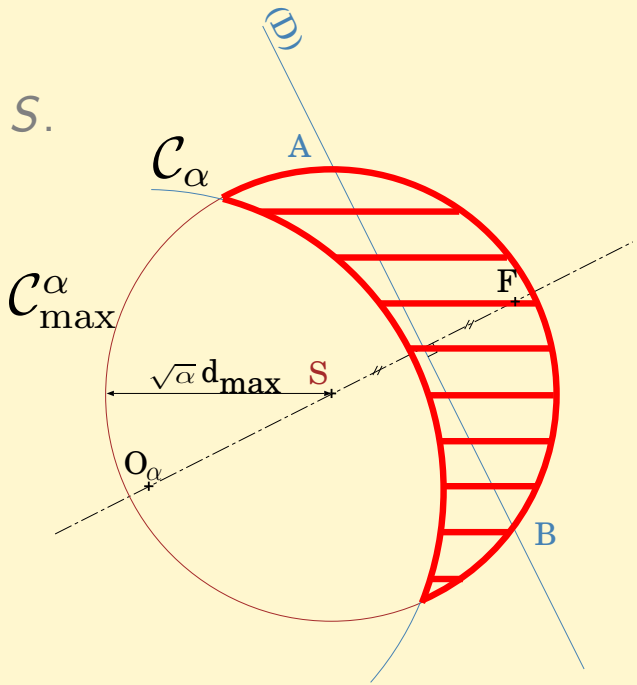
Results with attenuation

- With attenuation
  - real environment $\rightsquigarrow$ unknown attenuation
  - upper bound computed with the free space propagation model (factor α)

Standard P_{snd} with attenuation and omni-directional antenna

transmission range reduced ;

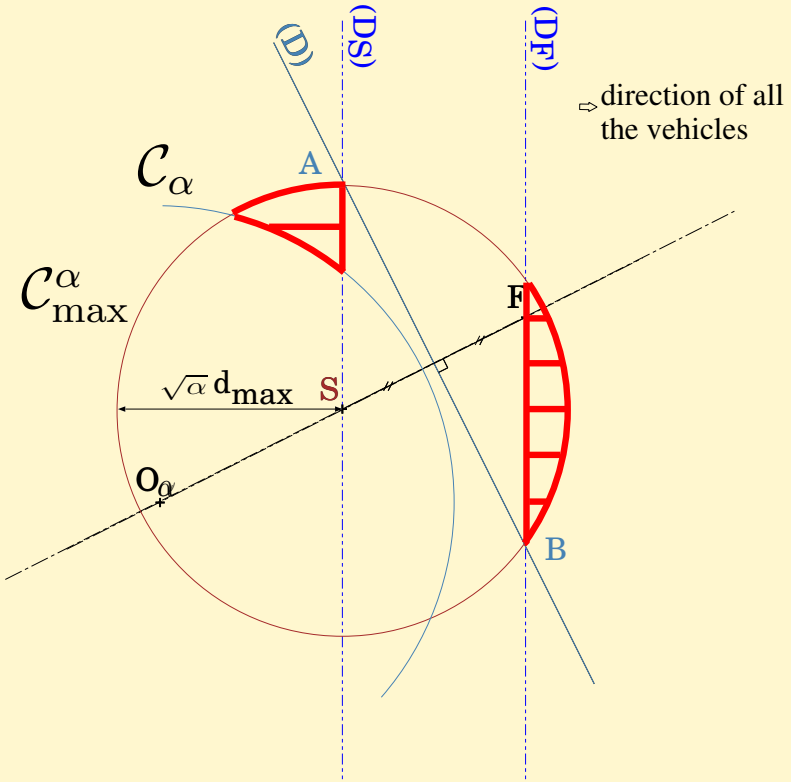
cheated nodes cannot be close to S.



Results with attenuation

Standard P_{snd} with attenuation and bi-directional antenna and same directions

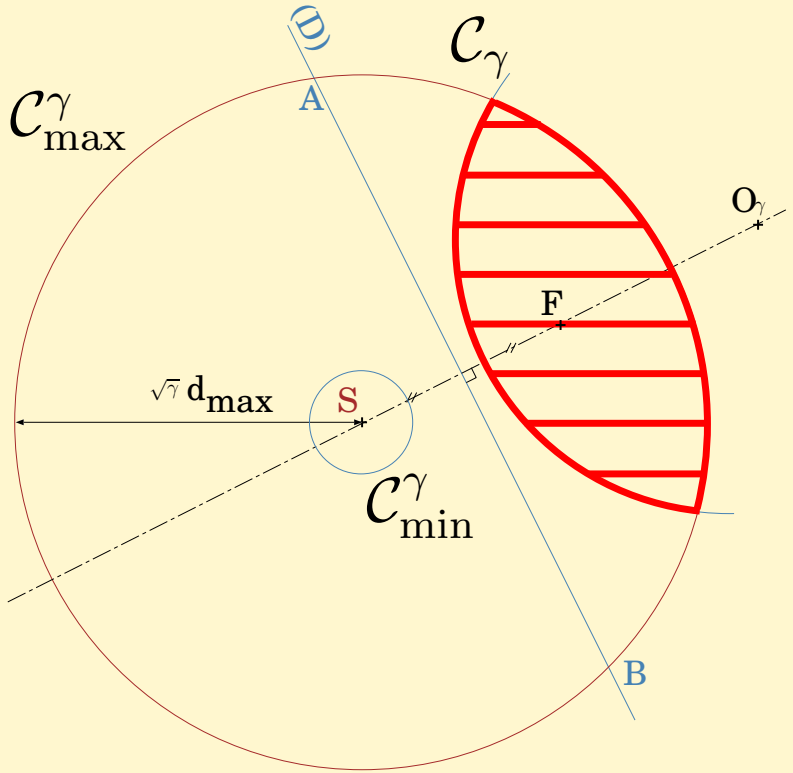
R is cheated if it sees S and F in the same semi-plan.



Results with attenuation + tuning

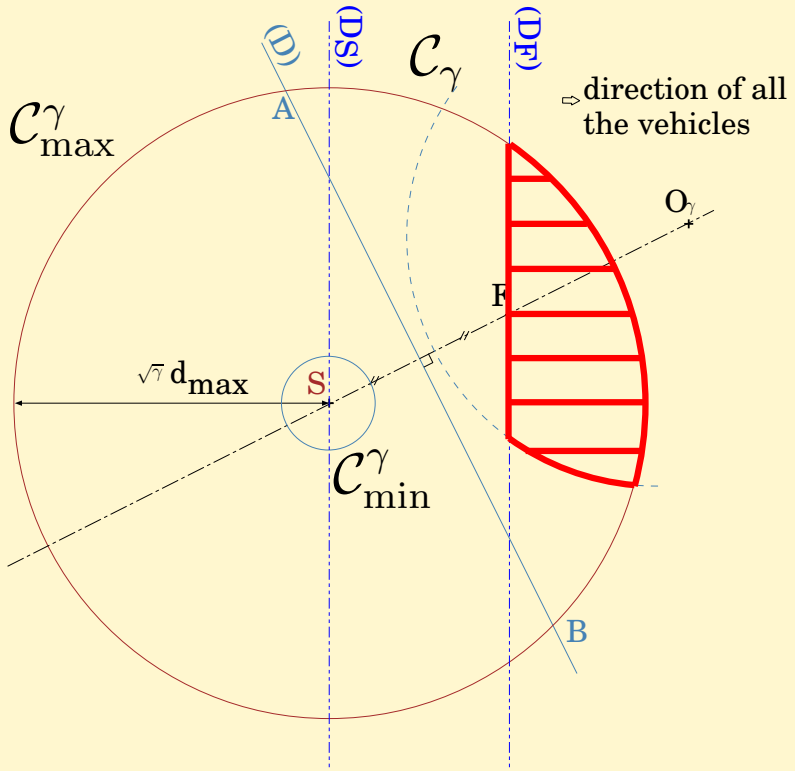
- With attenuation + tuning of the sending power
  - increasing factor β for the sending power
  - $\gamma = \alpha \times \beta$ α : attenuation factor

Standard P_{snd} with attenuation + tuning and omni-directional antenna



Results with attenuation + tuning

Standard P_{snd} with attenuation + tuning and bi-directional antenna and same directions



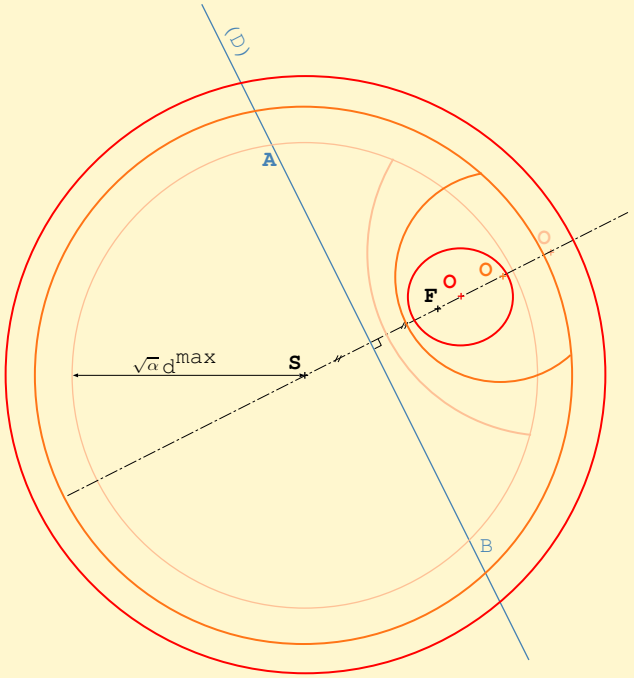
Plan

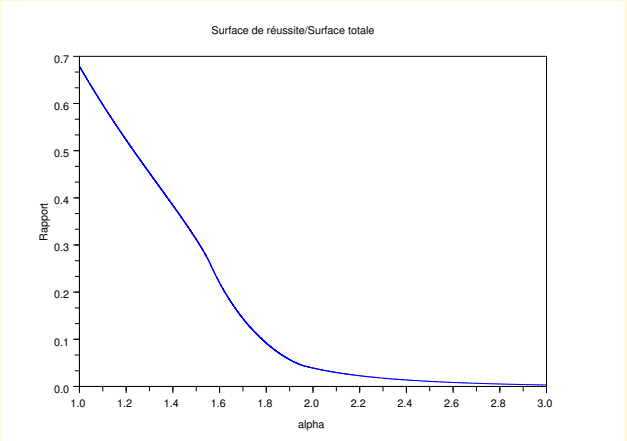
Discussion

Sender : impact of the tuning factor

- When P_{snd} increases
  - the transmission range increases
  - the area of success decreases

$\rightsquigarrow$ the attacker will be detected more easily while his attack will cheat less vehicles.





Discussion

Receiver : impact of the bidirectionnal antenna

- When bidirectional antenna are used
  - when the attacker does not know the directions of the victims, it will be discover

  $\rightsquigarrow$ bidirectional antenna very useful in urban environments

  many vehicles with different directions

  - on roads, the Sybil nodes should be placed near the attacker

  $\rightsquigarrow$ less impact of the Sybil node creation

  when using combination of the information in neighborhood

Conclusion

- Summary
  - Realistic hypotheses
    GPS, measure of the received power
  - Geometric characterization of the Sybil attack success, metric for comparison (area)
  - Attacker : tuning or not
  - Sender : omni- or bidirectional antenna

- Results
  - guide for further tests and scenarii design
    for Sybil attack studies
  - tuning sending power : limited interest
  - bidirectional antenna : urban environment

- Future work
  - Cooperation in neighborhood