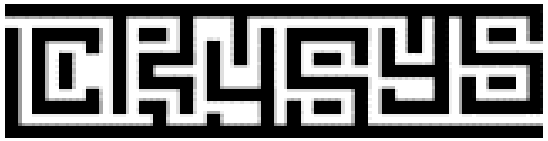


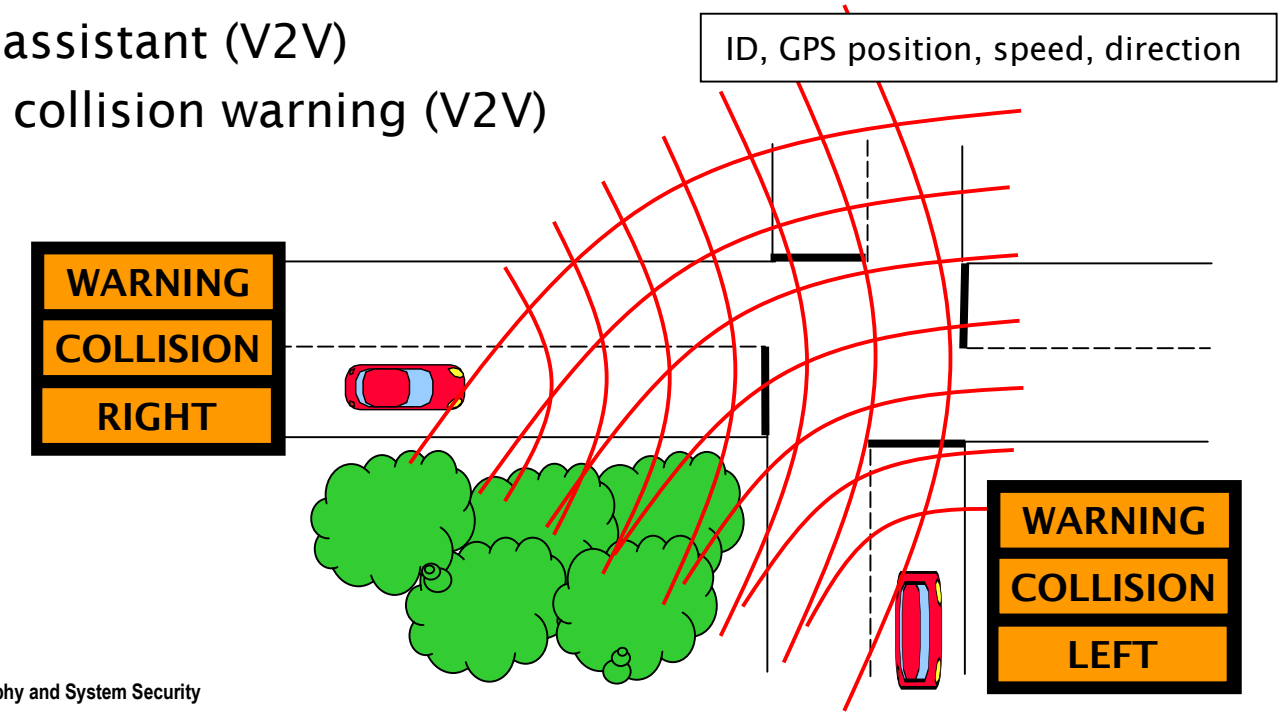
On the effectiveness of changing pseudonyms to provide location privacy in VANETS

Levente Buttyan
Laboratory of Cryptography and System Security (CrySyS)
Budapest University of Technology and Economics

this is joint work with ***Tamas Holczer*** *and* ***Istvan Vajda***

Vehicular communications

- the promise of vehicular communications is to make road traffic safer and more efficient
- a number potentially useful vehicle safety applications has been proposed, such as
  - curve speed warning (I2V)
  - road condition warning (I2V)
  - lane merge assistant (V2V)
  - cooperative collision warning (V2V)
  - …



The location privacy problem and a solution

- vehicles continuously broadcast *heart beat* messages, containing their ID, position, speed, etc.
- tracking the physical location of vehicles is easy just by eavesdropping on the wireless channel
- one possible solution is to change the vehicle identifier, or in other words, to use *pseudonyms*

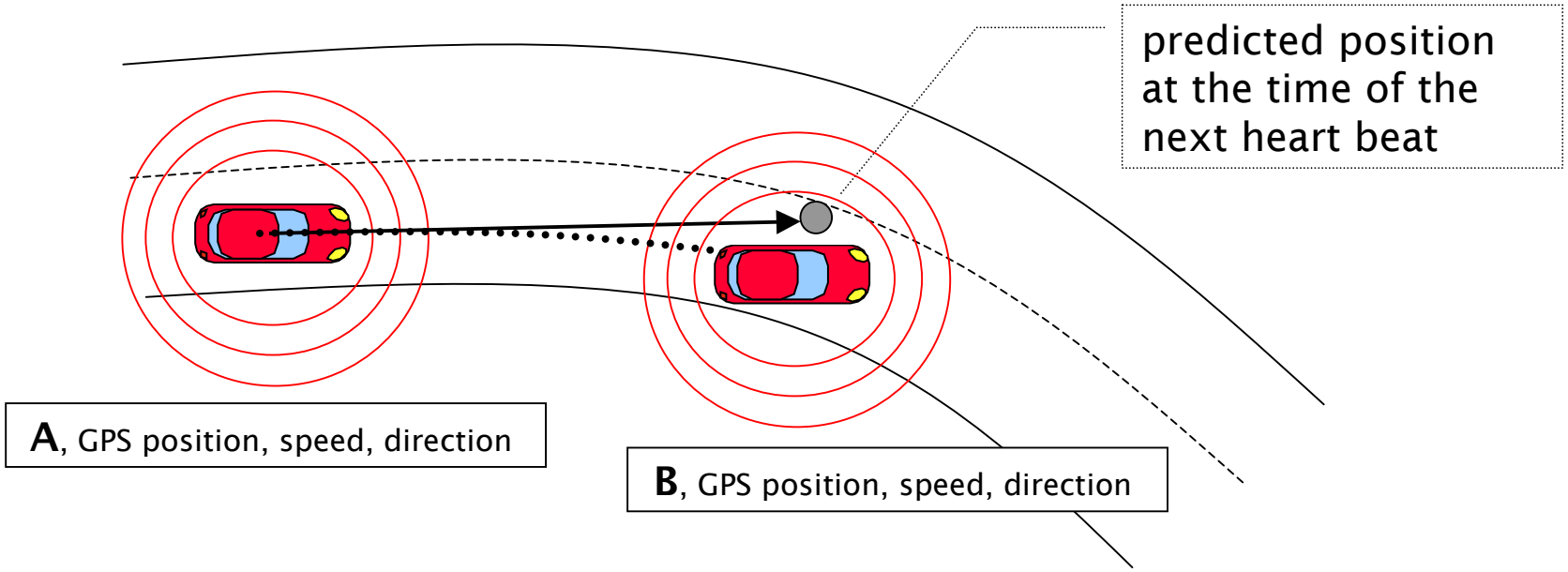
Our contributions

- we propose a framework to study the effectiveness of the pseudonym changing mechanism
  - we define a model based on the concept of the *mix zone*
  - we determine the best tracking strategy of adversary
  - we introduce a metric to quantify the level of privacy achieved

- we perform extensive simulations
  - we use a complex road map
  - traffic is generated with realistic parameters
  - we vary the strength of the adversary (number of monitoring spots)

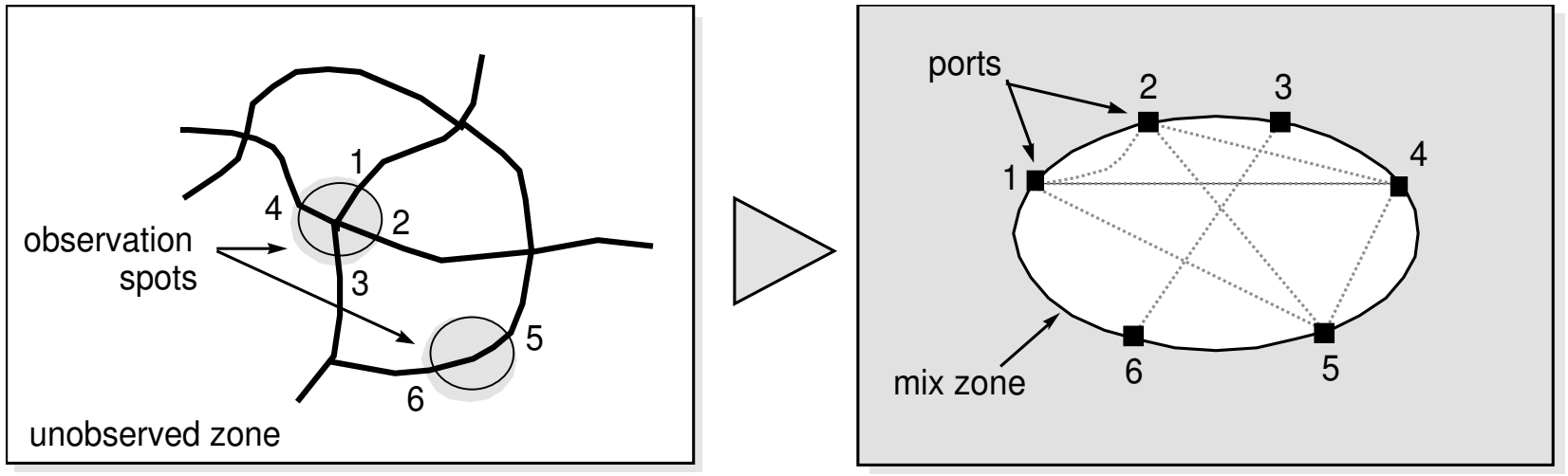
Adversary model

- changing pseudonyms is ineffective against a global eavesdropper



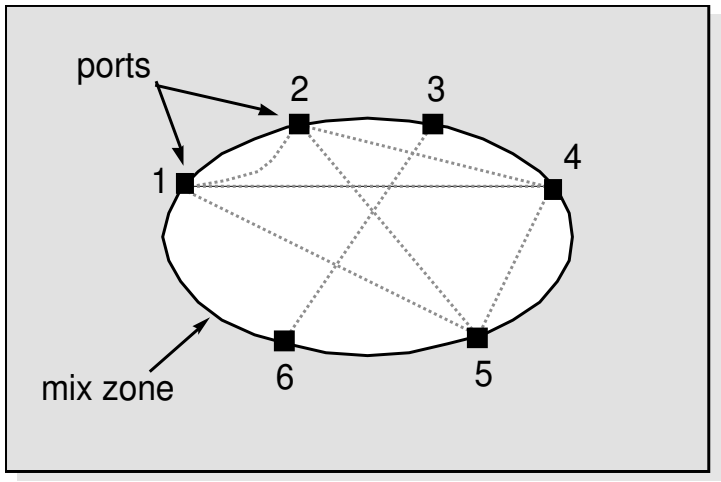
- hence, the adversary is assumed to be able to monitor the communications only at a limited number of places and in a limited range

The mix zone concept



- the unobserved zone functions as a *mix zone* where the vehicles change pseudonym and mix with each other
- note that the vehicles do not know where the mix zone is (this depends on where the adversary installs observation spots)
- we assume that the vehicles change pseudonyms frequently so that each vehicle changes pseudonym while in the mix zone

Model of the mix zone



- we assume that the adversary knows
  - q_{ij} - the conditional probability of exiting the mix zone at port j given that the entry port was port i (for all i, j)
  - $f_{ij}(t)$ – the (discrete) probability distribution of the delay when traversing the mix zone between ports i and j

Tracking strategy of the adversary

- the adversary observes entering and exiting events, and wants to relate them to each other

- more specifically, the adversary
  - picks a vehicle v in the observed zone
  - tracks v until it enters the mix zone at port s
  - then, observes the exiting events until time T (where the probability that v leaves the mix zone until T is close to one)
  - for each exiting vehicle at port j and time t, computes $p_{jt} = q_{sj} f_{sj}(t)$
  - the adversary decides to the exiting vehicle v' for which p_{jt} is maximal
  - the adversary is successful if v' = v

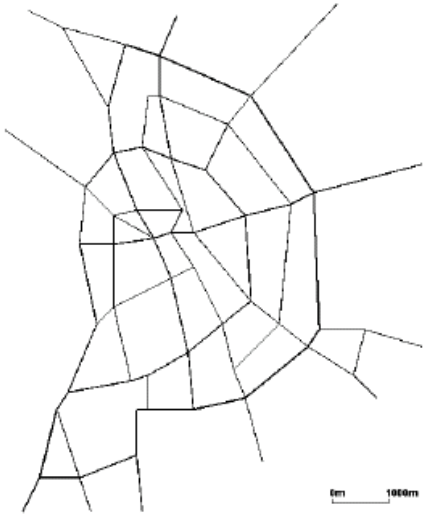
- this algorithm realizes a Bayesian decision
  - it minimizes the error probability of the decision
  - in this sense, it is optimal

Privacy metric

- the level of privacy achieved is characterized by the success probability of the adversary
  - if success probability is high, then level of privacy is low
- how to determine it?
- we used simulations to determine its empirical value in realistic scenarios

Simulation settings

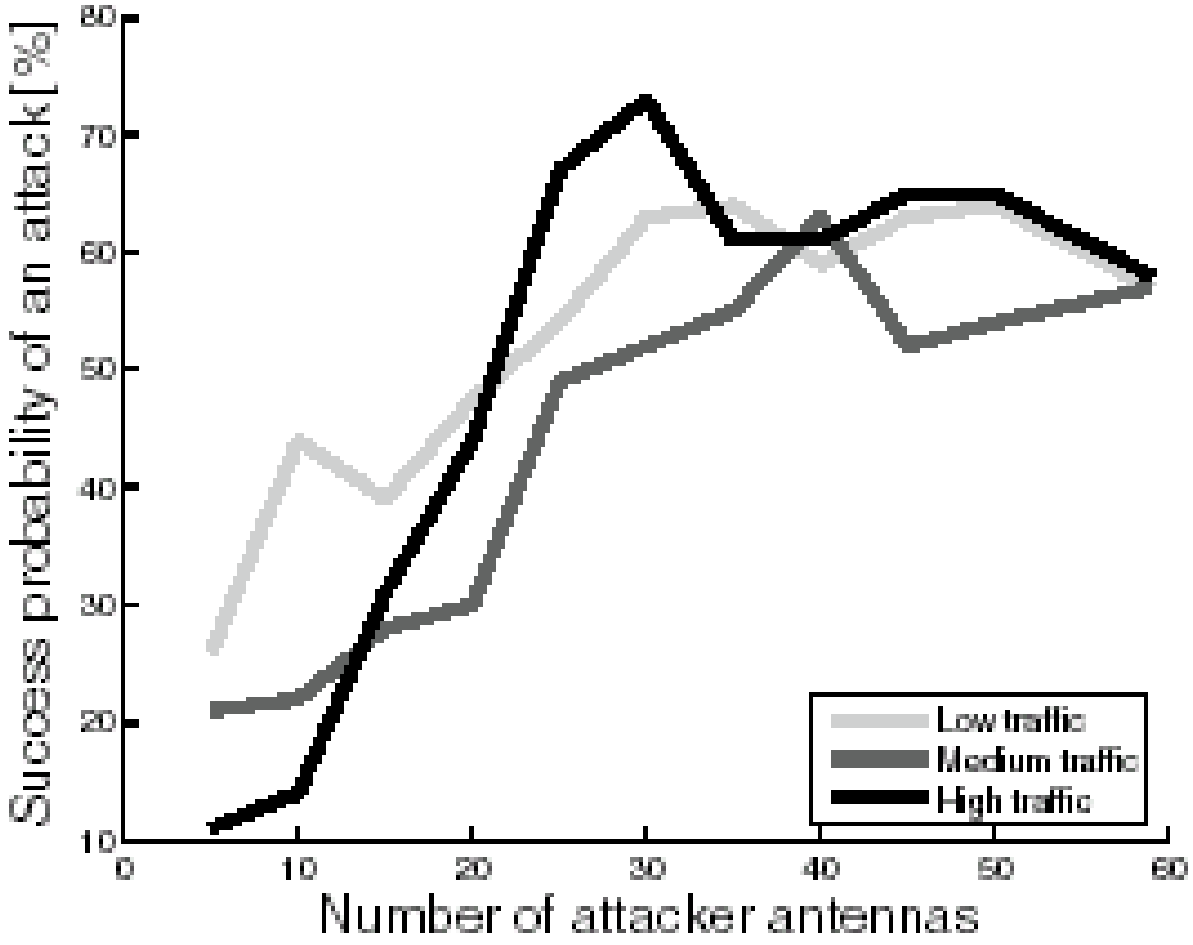
- we generated a simplified map of Budapest with MOVE
- we generated movement of the vehicles on the map with SUMO
  - low traffic: 250 new vehicles / time step
  - medium traffic: 500 new vehicles / time step
  - high traffic: 750 new vehicles / time step
- we selected the adversary's observation spots in intersections of roads
  - number of observation spots were varied from 5 to 59 with a step size of 5



Simulation settings

- we let the adversary build her model of the mix zone by letting her fully tracking vehicles for some time
- after that, we let the adversary pick a vehicle, track it until it enters the mix zone, observe exiting vehicles, and make a decision
- we run 100 simulations for each simulation setting
- we look at the percentage of the simulation runs where the adversary is successful

Simulation results



Conclusion and future work

- changing pseudonyms has been proposed as a mechanism to provide location privacy in vehicular networks
- we studied the effectiveness of this approach
- main contributions
  - a model based on the concept of the mix zone
  - characterization of the adversary's tracking strategy
  - privacy metric
  - simulation results using realistic settings
- in our future work, we intend to study how the frequency of the pseudonym change influences the level of privacy achieved

- this work has been carried out in the context of the SeVeCom Project (www.sevecom.org)