Providing Location Security in Vehicular Adhoc Networks

Gongjun Yan

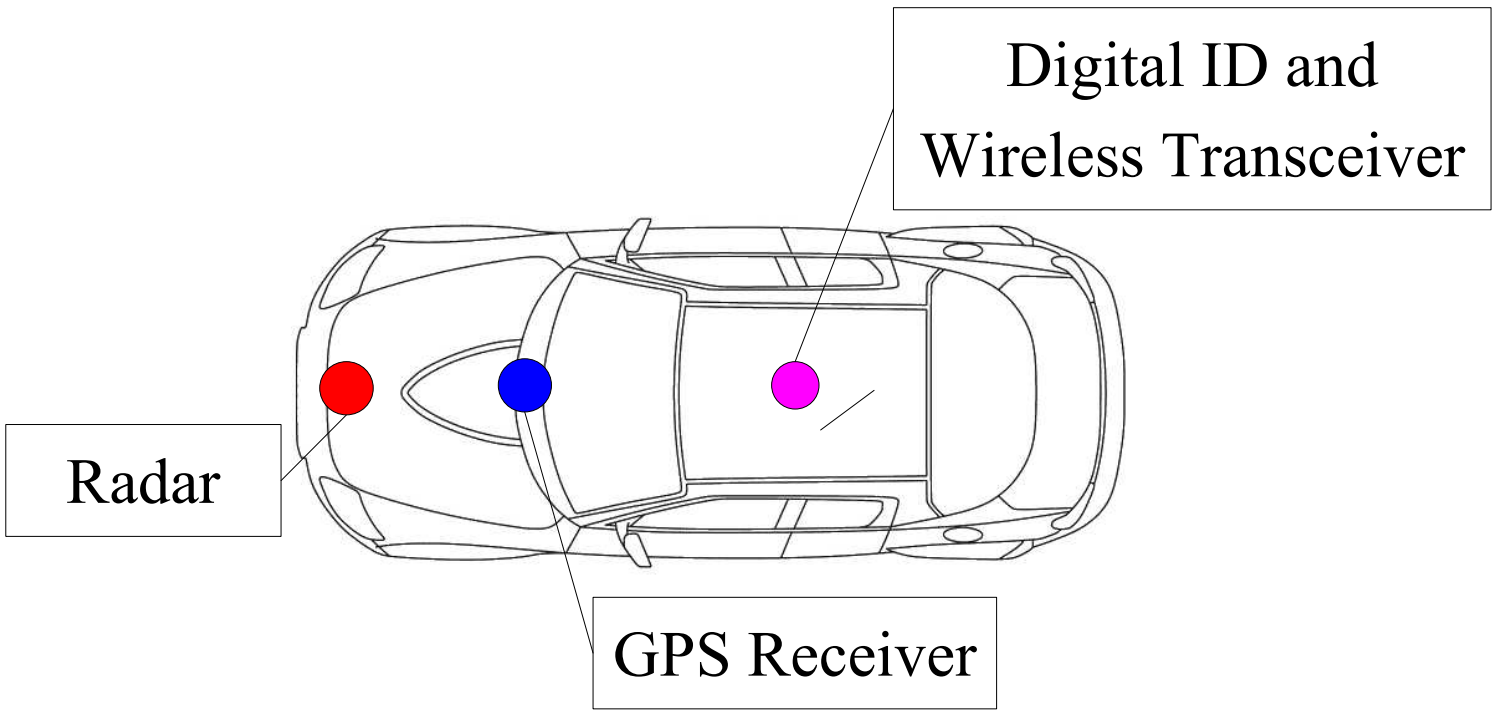
Co-advisors: Dr. Stephan Olariu
Dr. Michele C. Weigle

Computer Science Department
Old Dominion University,
Norfolk, VA 23529

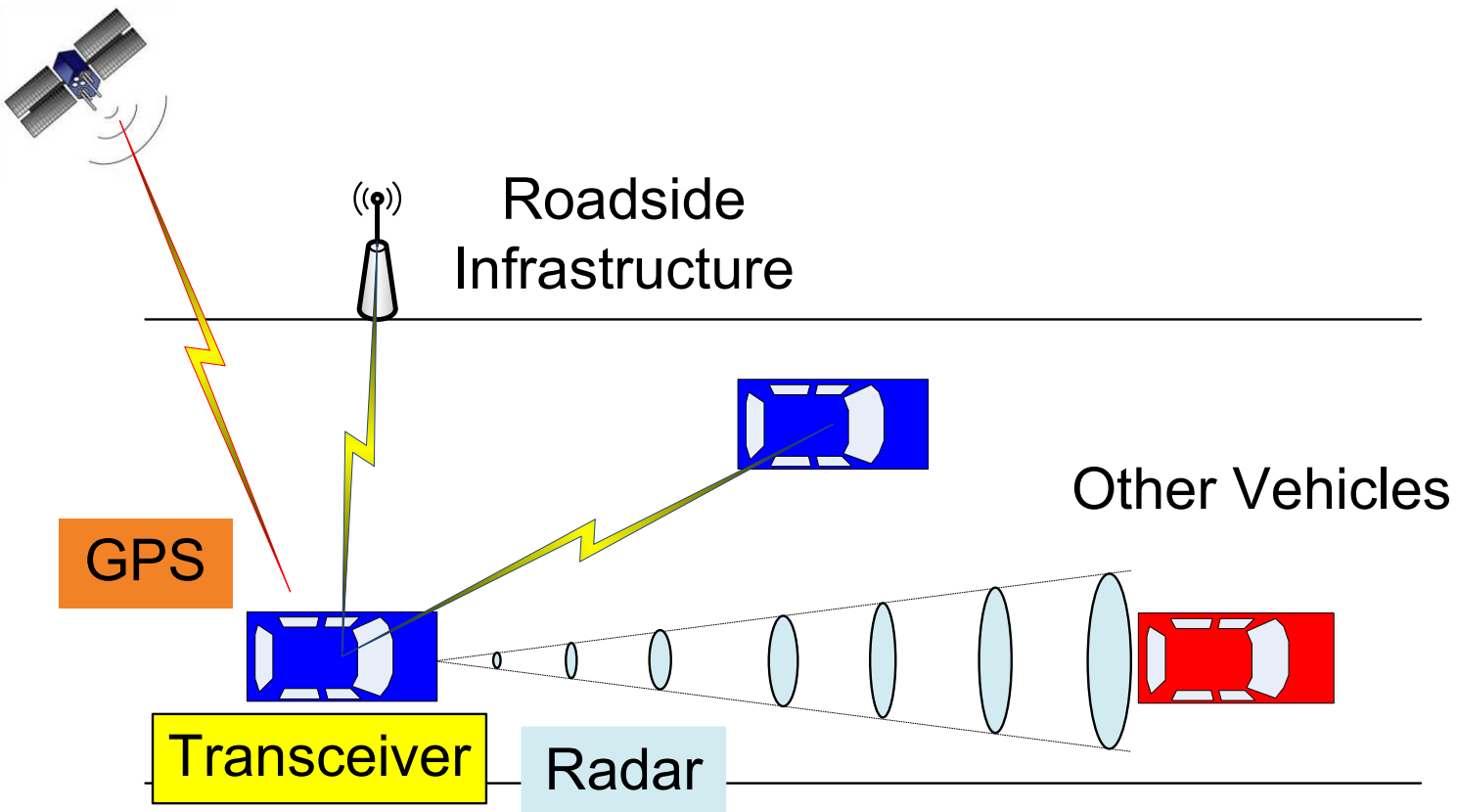
April 26, 2010

Table of Contents

Introduction: Modern Vehicles

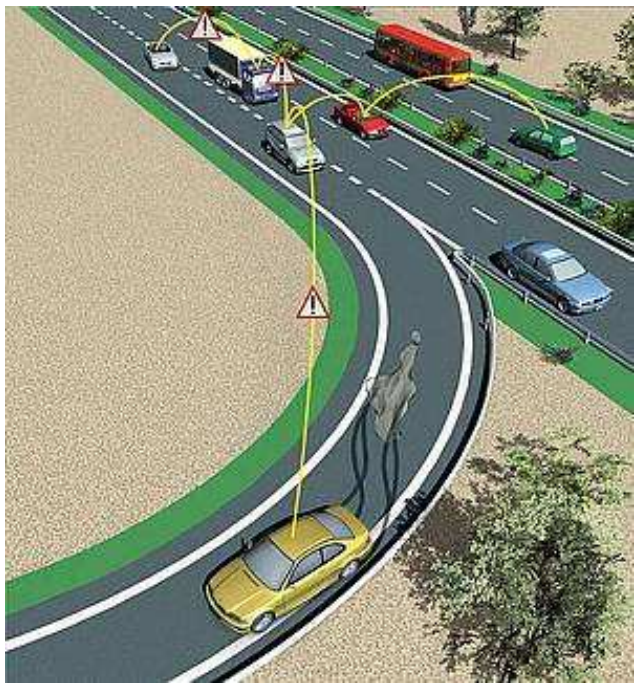


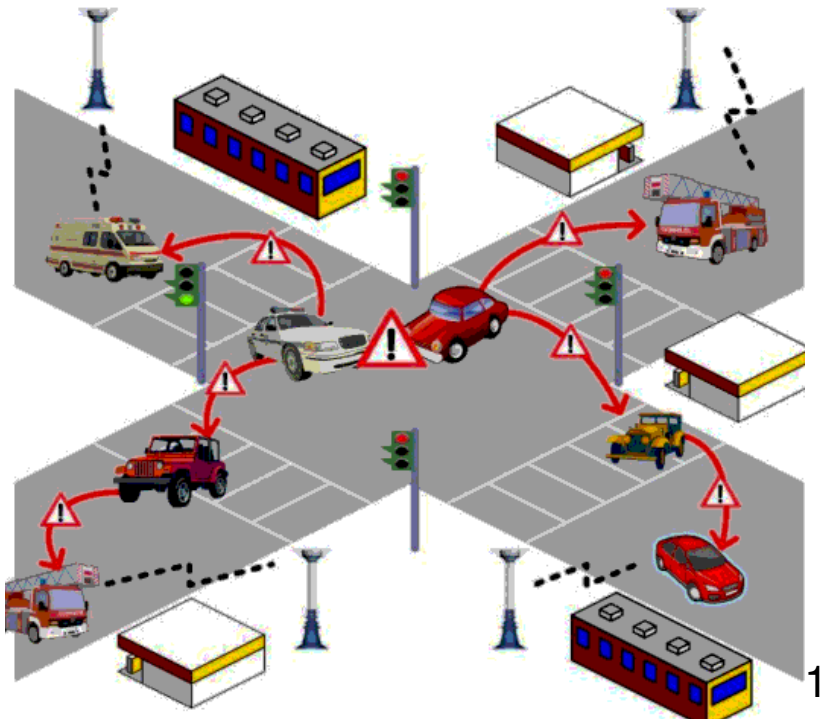
Introduction: Modern Vehicles



*V*ehicular *A*dhoc *Net*work (VANET)

- Create a *V*ehicular *A*dhoc *Net*work (VANET).
- Supported by gov, industry, and academic.

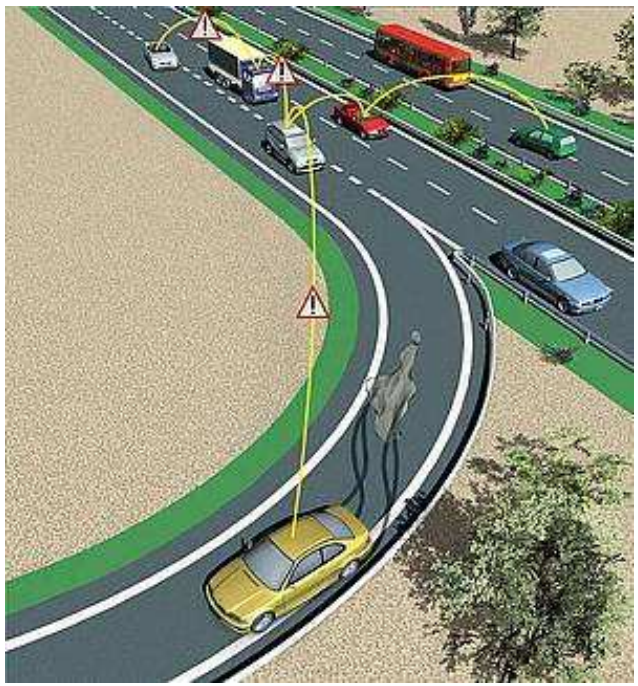


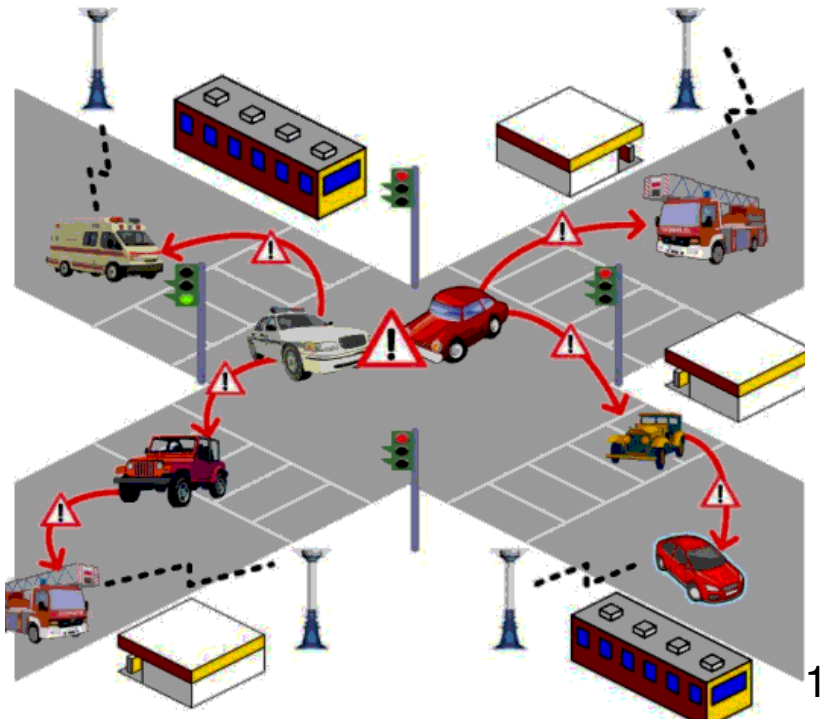


[1] http://www.comnets.rwth-aachen.de/

*V*ehicular *A*dhoc *Net*work (VANET)

- Create a *V*ehicular *A*dhoc *Net*work (VANET).
- Supported by gov, industry, and academic.





[1]

[1] http://www.comnets.rwth-aachen.de/

Vehicular Adhoc Network

- ***V**ehicular **A**dhoc **Net**work (VANET) applications:*
  - Safety:
    - Collision warning, road sign alarms, merge assistance
    - Left turn assistance, pedestrians crossing alert, etc.
  - Comfort (infotainment) to passengers:
    - Intelligent navigation
    - Multimedia, internet connectivity
    - Automatic payment of parking, toll collection, etc.

Vehicular Adhoc Network

- ***V***ehicular ***A***dhoc ***Net***work (VANET) applications:
  - Safety:
    - Collision warning, road sign alarms, merge assistance
    - Left turn assistance, pedestrians crossing alert, etc.
  - Comfort (infotainment) to passengers:
    - Intelligent navigation
    - Multimedia, internet connectivity
    - Automatic payment of parking, toll collection, etc.

Vehicular Adhoc Network

- ***V***ehicular ***A***dhoc ***Net***work (VANET) applications:
  - Safety:
    - Collision warning, road sign alarms, merge assistance
    - Left turn assistance, pedestrians crossing alert, etc.
  - Comfort (infotainment) to passengers:
    - Intelligent navigation
    - Multimedia, internet connectivity
    - Automatic payment of parking, toll collection, etc.

Vehicular Adhoc Network

- ***V***ehicular ***A***dhoc ***Net***work (VANET) applications:
  - Safety:
    - Collision warning, road sign alarms, merge assistance
    - Left turn assistance, pedestrians crossing alert, etc.
  - Comfort (infotainment) to passengers:
    - Intelligent navigation
    - Multimedia, internet connectivity
    - Automatic payment of parking, toll collection, etc.

Vehicular Adhoc Network

- ***V***ehicular ***A***dhoc ***Net***work (VANET) applications:
  - Safety:
    - Collision warning, road sign alarms, merge assistance
    - Left turn assistance, pedestrians crossing alert, etc.
  - Comfort (infotainment) to passengers:
    - Intelligent navigation
    - Multimedia, internet connectivity
    - Automatic payment of parking, toll collection, etc.

Vehicular Adhoc Network

- ***V***ehicular ***A***dhoc ***Net***work (VANET) applications:
  - Safety:
    - Collision warning, road sign alarms, merge assistance
    - Left turn assistance, pedestrians crossing alert, etc.
  - Comfort (infotainment) to passengers:
    - Intelligent navigation
    - Multimedia, internet connectivity
    - Automatic payment of parking, toll collection, etc.

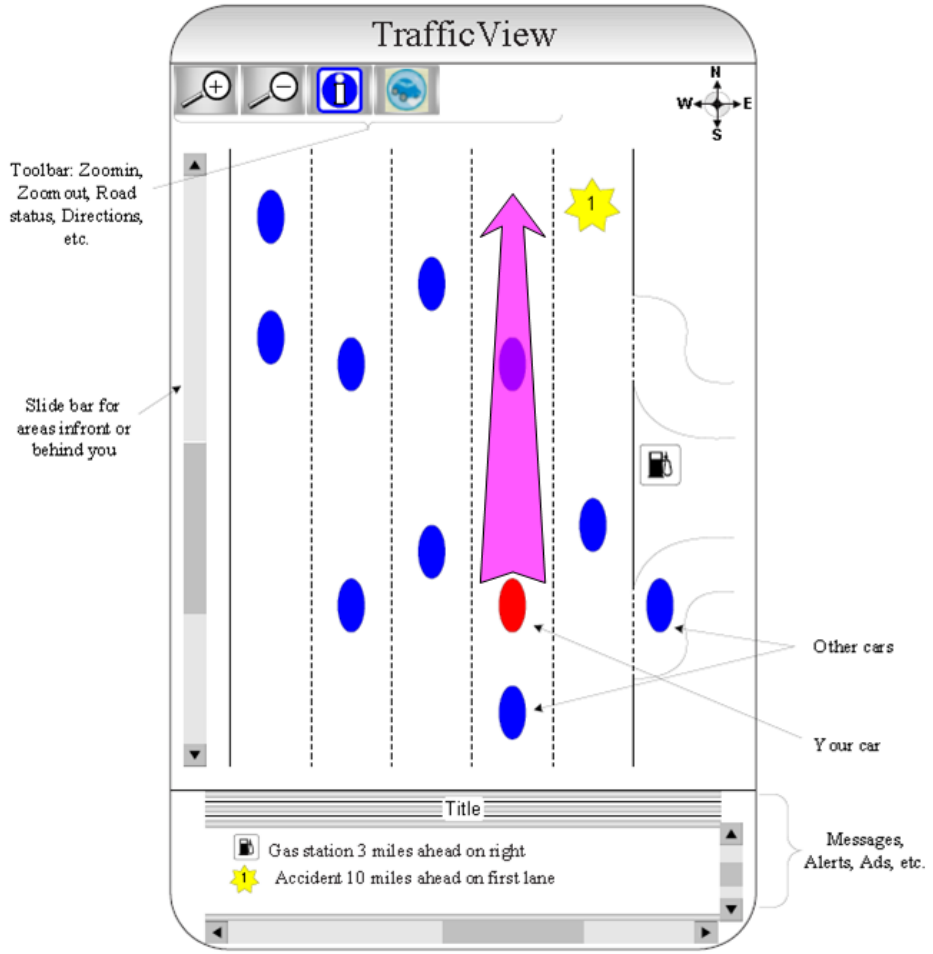
Vehicular Adhoc Network

- ***V***ehicular ***A***dhoc ***Net***work (VANET) applications:
  - Safety:
    - Collision warning, road sign alarms, merge assistance
    - Left turn assistance, pedestrians crossing alert, etc.
  - Comfort (infotainment) to passengers:
    - Intelligent navigation
    - Multimedia, internet connectivity
    - Automatic payment of parking, toll collection, etc.

Vehicular Adhoc Network

- ***V***ehicular ***A***dhoc ***Net***work (VANET) applications:
  - Safety:
    - Collision warning, road sign alarms, merge assistance
    - Left turn assistance, pedestrians crossing alert, etc.
  - Comfort (infotainment) to passengers:
    - Intelligent navigation
    - Multimedia, internet connectivity
    - Automatic payment of parking, toll collection, etc.

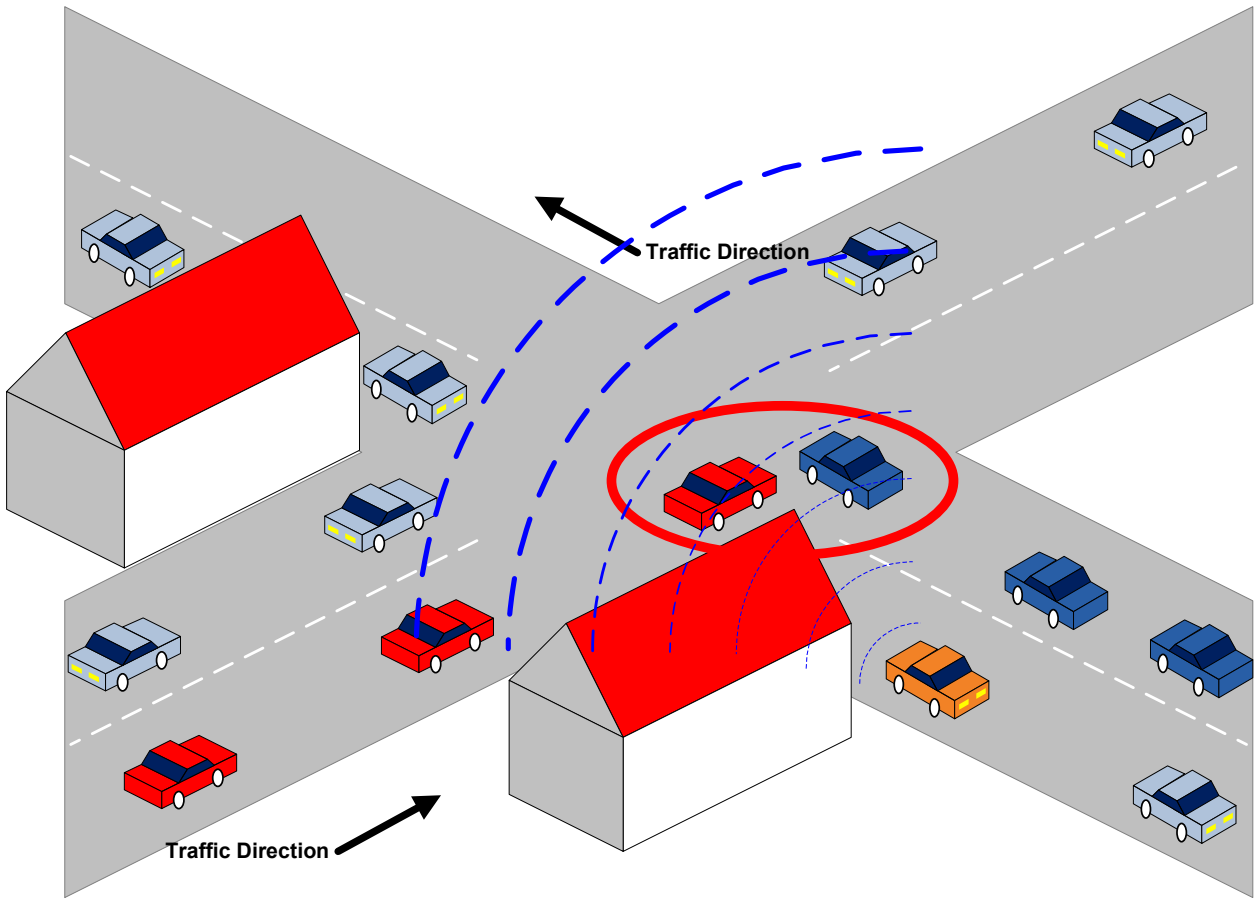
Applications: TrafficView



[Nadeem et al.(2004)]

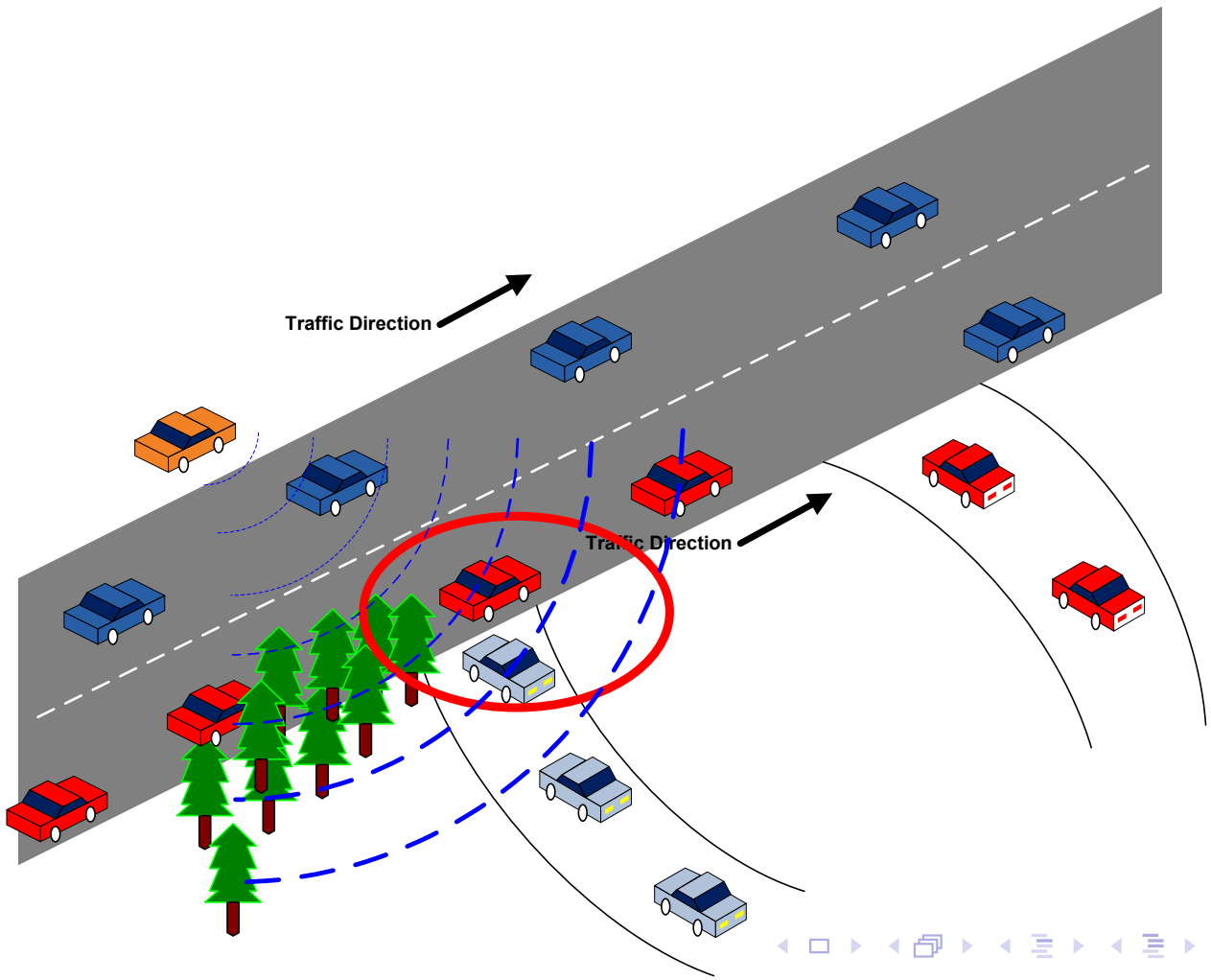
Location Attack: Intersection

The line of sight is blocked and you trust only the location over VANET. No traffic lights.



Location Attack: Highway

The line of sight is blocked and you trust only the location over VANET.



Research Question

- Most, if not all, applications rely on locations.
- Research question:
  How to improve location security?
- What do we protect?
  Right time, right ID, right location
- Synchronized time can be obtain from GPS
- What is ID?
  - A unique digital identity
  - Anonymous to drivers/passengers' identity
- What is location?
  - location $\equiv$ <latitude, longitude, altitude>
  - Obtained from: transceivers, radar, GPS

Research Question

- Most, if not all, applications rely on locations.
- Research question:

  How to improve location security?

- What do we protect?

  Right time, right ID, right location

- Synchronized time can be obtain from GPS
- What is ID?
  - A unique digital identity
  - Anonymous to drivers/passengers' identity
- What is location?
  - location ≡ <latitude, longitude, altitude>
  - Obtained from: transceivers, radar, GPS

Research Question

- Most, if not all, applications rely on locations.
- Research question:

  How to improve location security?
- What do we protect?

  Right time, right ID, right location
- Synchronized time can be obtain from GPS
- What is ID?
  - A unique digital identity
  - Anonymous to drivers/passengers' identity
- What is location?
  - location ≡ <latitude, longitude, altitude>
  - Obtained from: transceivers, radar, GPS

Research Question

- Most, if not all, applications rely on locations.
- Research question:

  How to improve location security?
- What do we protect?

  Right time, right ID, right location
- Synchronized time can be obtain from GPS
- What is ID?
  - A unique digital identity
  - Anonymous to drivers/passengers' identity
- What is location?
  - location ≡ <latitude, longitude, altitude>
  - Obtained from: transceivers, radar, GPS

Research Question

- Most, if not all, applications rely on locations.
- Research question:

  How to improve location security?
- What do we protect?

  Right time, right ID, right location
- Synchronized time can be obtain from GPS
- What is ID?
  - A unique digital identity
  - Anonymous to drivers/passengers' identity
- What is location?
  - location ≡ <latitude, longitude, altitude>
  - Obtained from: transceivers, radar, GPS

Research Question

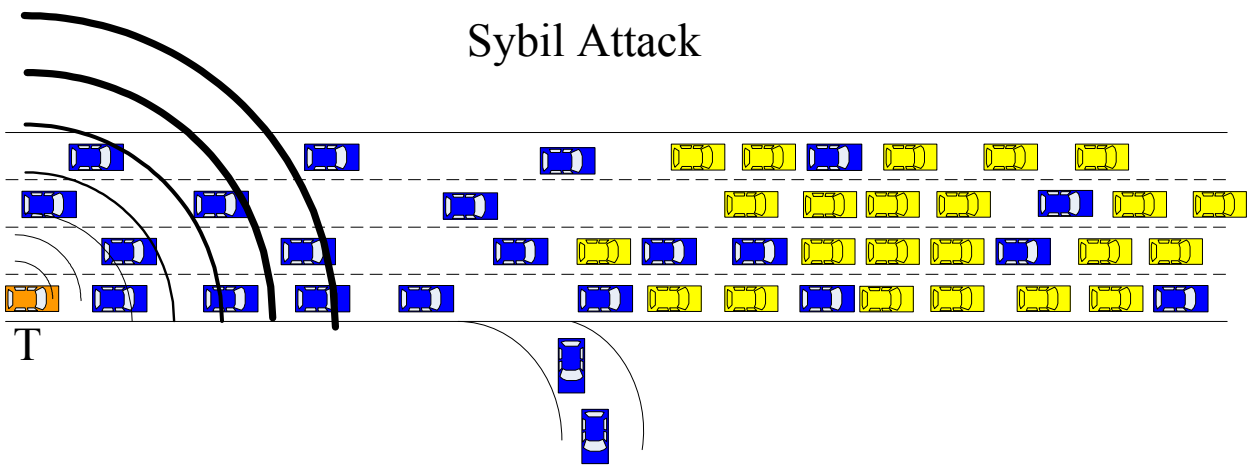
- Most, if not all, applications rely on locations.
- Research question:

  How to improve location security?
- What do we protect?

  Right time, right ID, right location
- Synchronized time can be obtain from GPS
- What is ID?
  - A unique digital identity
  - Anonymous to drivers/passengers' identity
- What is location?
  - location $\equiv$ <latitude, longitude, altitude>
  - Obtained from: transceivers, radar, GPS

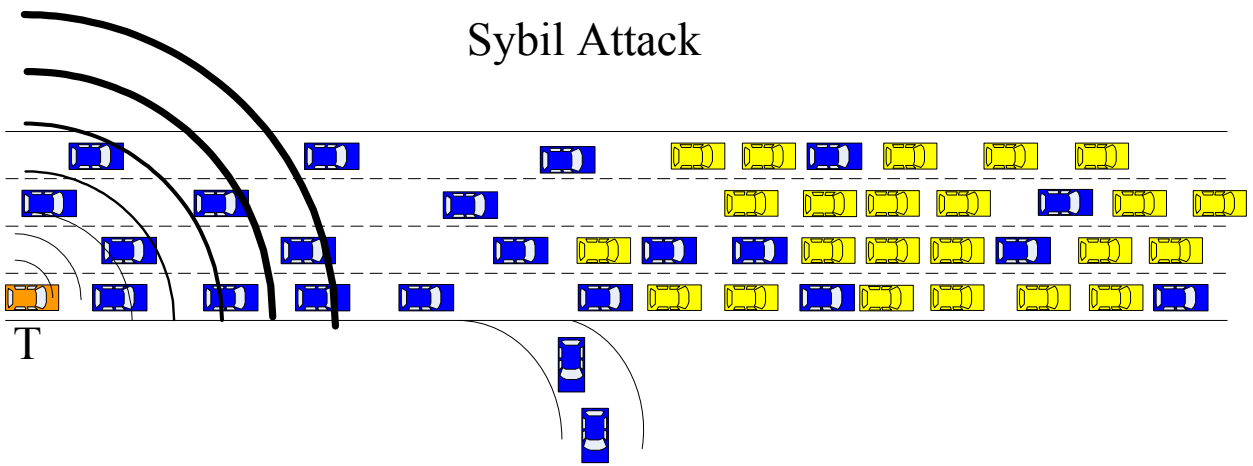
Location Security

- Assume: <time, ID, Location> can be attacked.
- What is threat model?
  - Dropping ⇒ Availability
  - Eavesdropping ⇒ Confidentiality
  - Modifying ⇒ Integrity + Confidentiality
  - Replaying ⇒ Integrity
  - Sybil Attack ⇒ Integrity



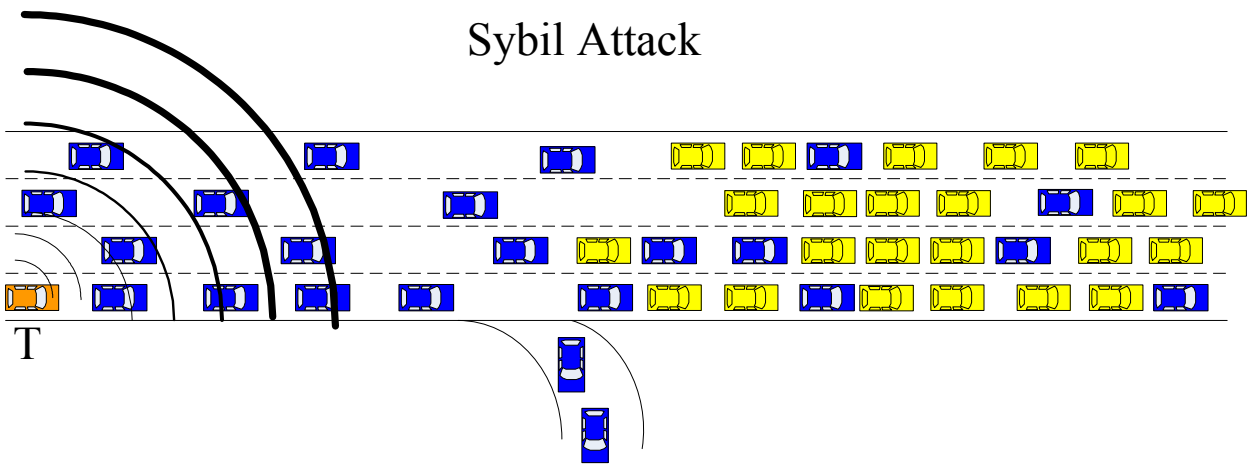
Location Security

- Assume: <time, ID, Location> can be attacked.
- What is threat model?
  - Dropping $\Rightarrow$ Availability
  - Eavesdropping $\Rightarrow$ Confidentiality
  - Modifying $\Rightarrow$ Integrity + Confidentiality
  - Replaying $\Rightarrow$ Integrity
  - Sybil Attack $\Rightarrow$ Integrity



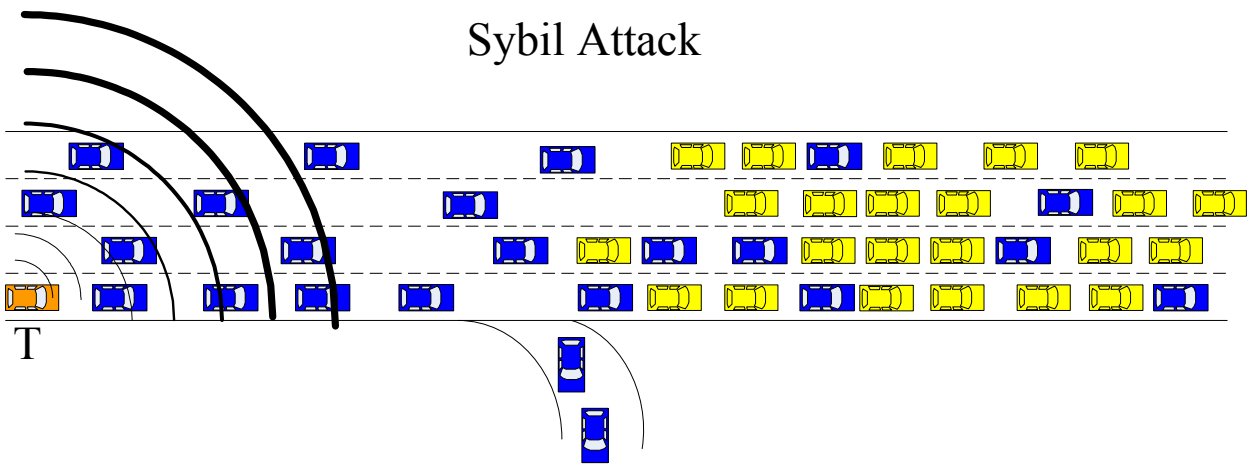
Location Security

- Assume: <time, ID, Location> can be attacked.
- What is threat model?
  - Dropping ⇒ Availability
  - Eavesdropping ⇒ Confidentiality
  - Modifying ⇒ Integrity + Confidentiality
  - Replaying ⇒ Integrity
  - Sybil Attack ⇒ Integrity



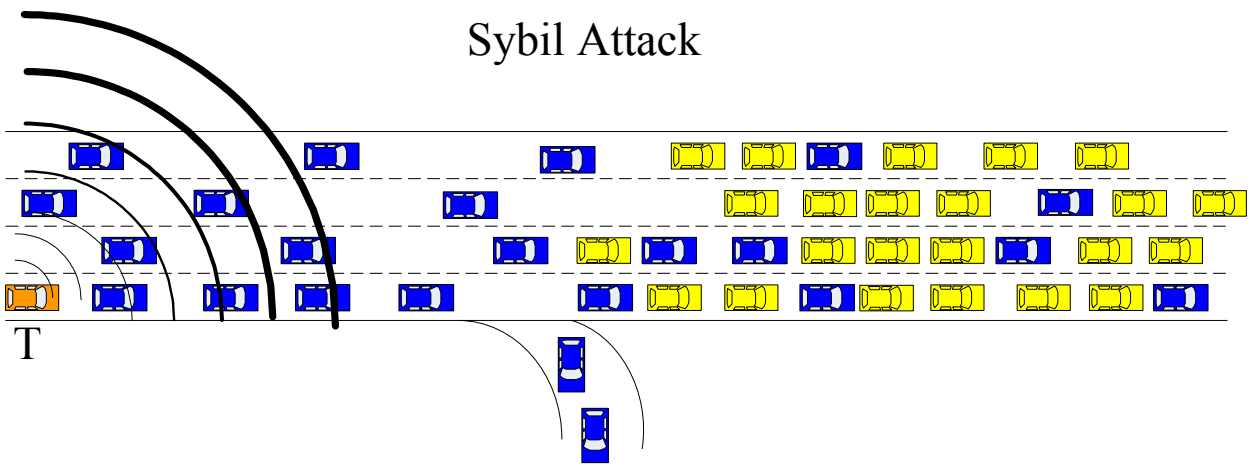
Location Security

- Assume: <time, ID, Location> can be attacked.
- What is threat model?
  - Dropping $\Rightarrow$ Availability
  - Eavesdropping $\Rightarrow$ Confidentiality
  - Modifying $\Rightarrow$ Integrity + Confidentiality
  - Replaying $\Rightarrow$ Integrity
  - Sybil Attack $\Rightarrow$ Integrity



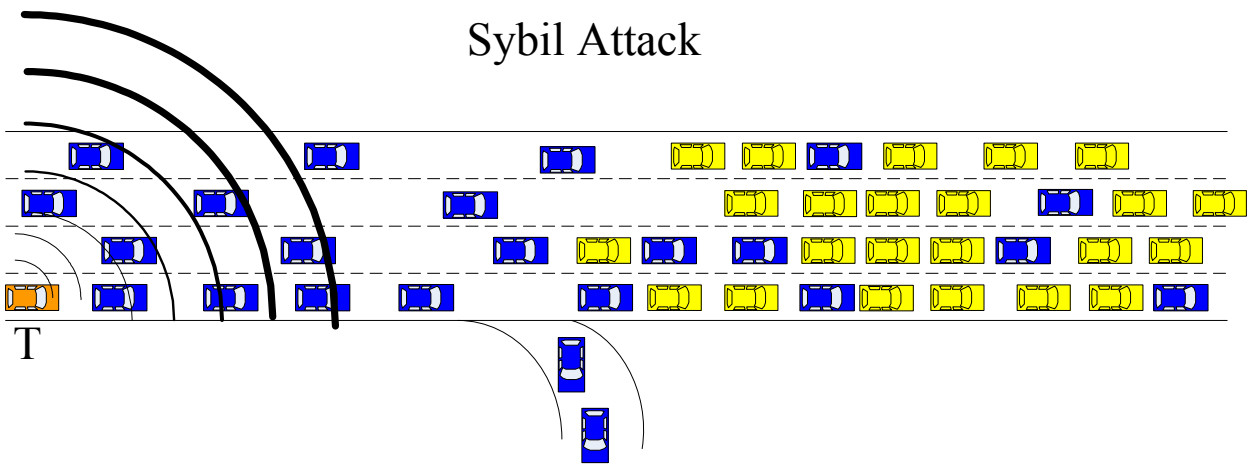
Location Security

- Assume: <time, ID, Location> can be attacked.
- What is threat model?
  - Dropping $\Rightarrow$ Availability
  - Eavesdropping $\Rightarrow$ Confidentiality
  - Modifying $\Rightarrow$ Integrity + Confidentiality
  - Replaying $\Rightarrow$ Integrity
  - Sybil Attack $\Rightarrow$ Integrity



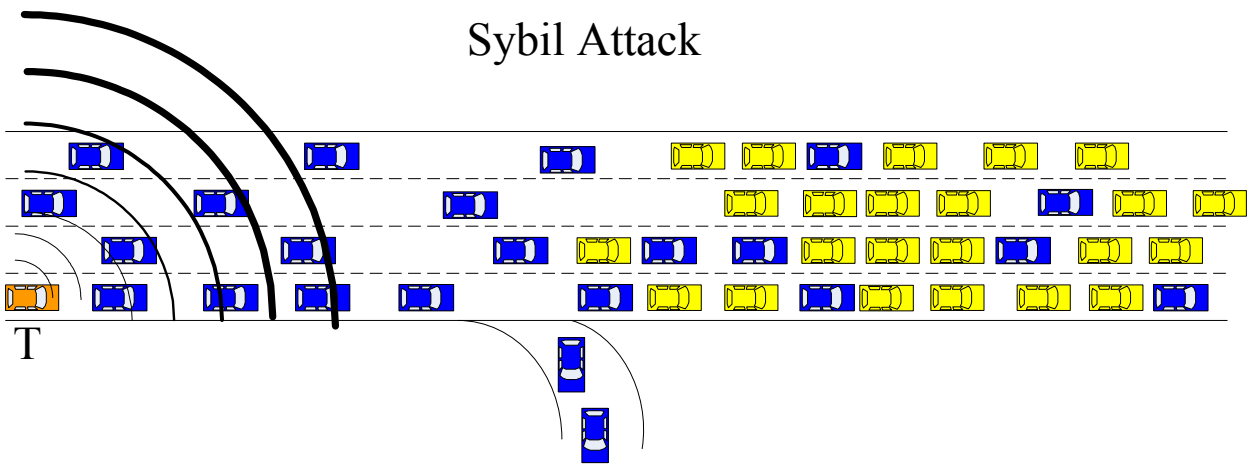
Location Security

- Assume: <time, ID, Location> can be attacked.
- What is threat model?
  - Dropping $\Rightarrow$ Availability
  - Eavesdropping $\Rightarrow$ Confidentiality
  - Modifying $\Rightarrow$ Integrity + Confidentiality
  - Replaying $\Rightarrow$ Integrity
  - Sybil Attack $\Rightarrow$ Integrity

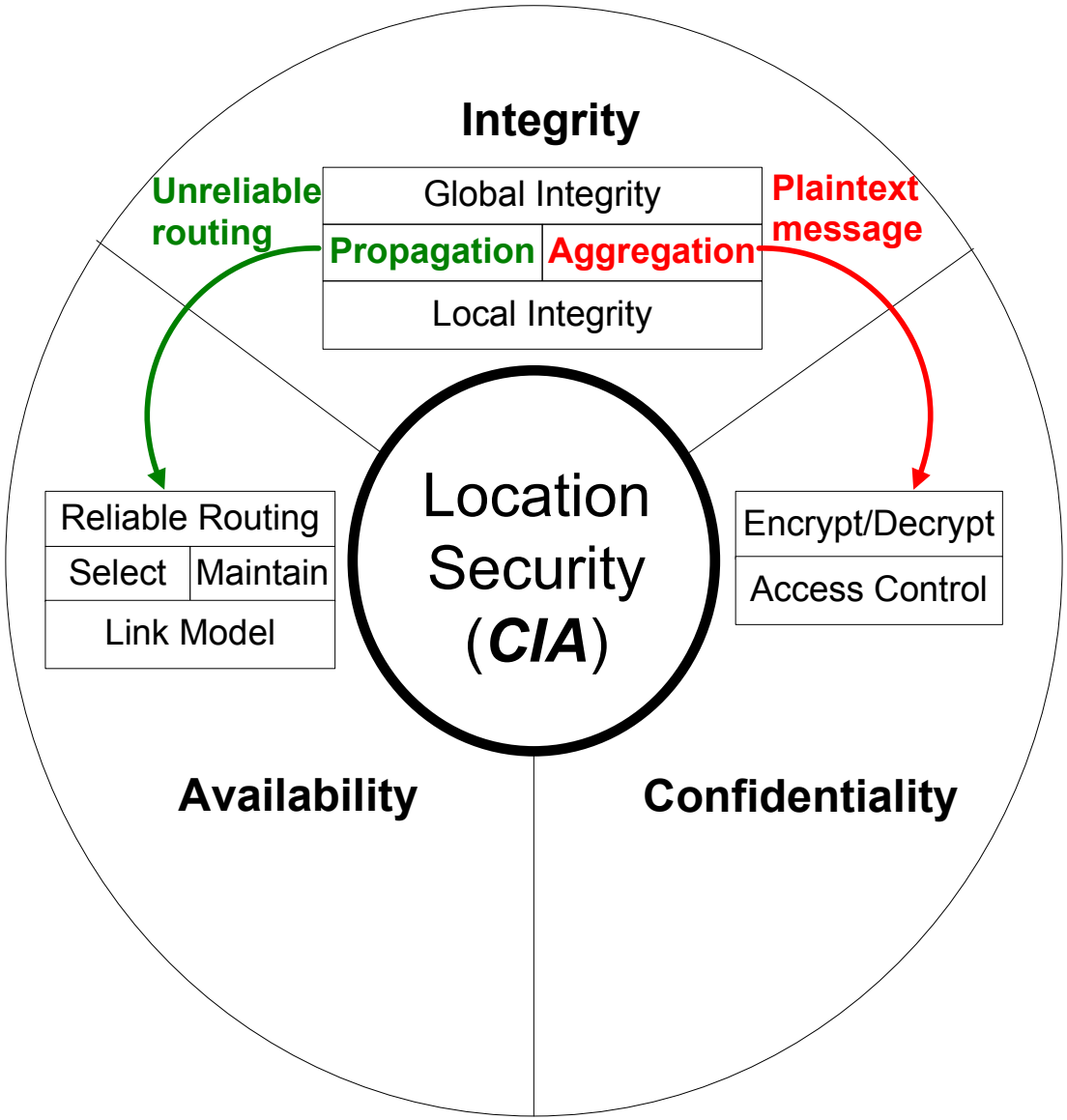


Location Security

- Assume: <time, ID, Location> can be attacked.
- What is threat model?
  - Dropping $\Rightarrow$ Availability
  - Eavesdropping $\Rightarrow$ Confidentiality
  - Modifying $\Rightarrow$ Integrity + Confidentiality
  - Replaying $\Rightarrow$ Integrity
  - Sybil Attack $\Rightarrow$ Integrity



Our Solution: Ensure *C*onfidentiality, *I*ntegrity, *A*vailability (*CIA*)



Related Work

Location integrity:

- **Digital signatures** [Armknecht et al.(2007), Choi et al.(2006)], etc.
- Resource:
  - **Radio signal** [Suen & Yasinsac(2005), Xiao et al.(2006)], etc.
  - **Computational resources** [Douceur(2002)], etc.
  - **Identification** [Piro et al.(2006)], etc.

Location confidentiality:

- **PKI** [Choi et al.(2006), Hubaux et al.(2004), Raya et al.(2006)], etc.
- **Location-based encryption** [Denning & MacDoran(1996)], etc.

Related Work

Location integrity:

- **Digital signatures** [Armknecht et al.(2007), Choi et al.(2006)], etc.
- Resource:
  - **Radio signal** [Suen & Yasinsac(2005), Xiao et al.(2006)], etc.
  - **Computational resources** [Douceur(2002)], etc.
  - **Identification** [Piro et al.(2006)], etc.

Location confidentiality:

- **PKI** [Choi et al.(2006), Hubaux et al.(2004), Raya et al.(2006)], etc.
- **Location-based encryption** [Denning & MacDoran(1996)], etc.

Related Work

Location integrity:

- **Digital signatures** [Armknecht et al.(2007), Choi et al.(2006)], etc.
- Resource:
  - **Radio signal** [Suen & Yasinsac(2005), Xiao et al.(2006)], etc.
  - **Computational resources** [Douceur(2002)], etc.
  - **Identification** [Piro et al.(2006)], etc.

Location confidentiality:

- **PKI** [Choi et al.(2006), Hubaux et al.(2004), Raya et al.(2006)], etc.
- **Location-based encryption** [Denning & MacDoran(1996)], etc.

Related Work

Location integrity:

- **Digital signatures** [Armknecht et al.(2007), Choi et al.(2006)], etc.
- Resource:
  - **Radio signal** [Suen & Yasinsac(2005), Xiao et al.(2006)], etc.
  - **Computational resources** [Douceur(2002)], etc.
  - **Identification** [Piro et al.(2006)], etc.

Location confidentiality:

- **PKI** [Choi et al.(2006), Hubaux et al.(2004), Raya et al.(2006)], etc.
- **Location-based encryption** [Denning & MacDoran(1996)], etc.

Contributions

The main contribution of this dissertation is:

To enhance location security in VANETs

Specifically,

1. *Enabling location integrity*
2. *Ensuring location confidentiality*
3. *Including integrity and availability in location security*
4. *Enabling location availability*
5. *Reducing control overhead*
6. *Reducing response time*
7. *New Geoencryption can operate with only one PKI peer*
8. *New Geolock can compute key dynamically*
9. *New Geolock can tolerate larger location errors*

Location Integrity: Overview

- The main task:

  Validate the tuple <time, ID, location>

- Three sub-solutions:
  1. Active integrity: strong assumption (radar, GPS, transceiver)
  2. Passive integrity: weaker assumption (GPS, transceiver)
  3. General integrity: real world environment

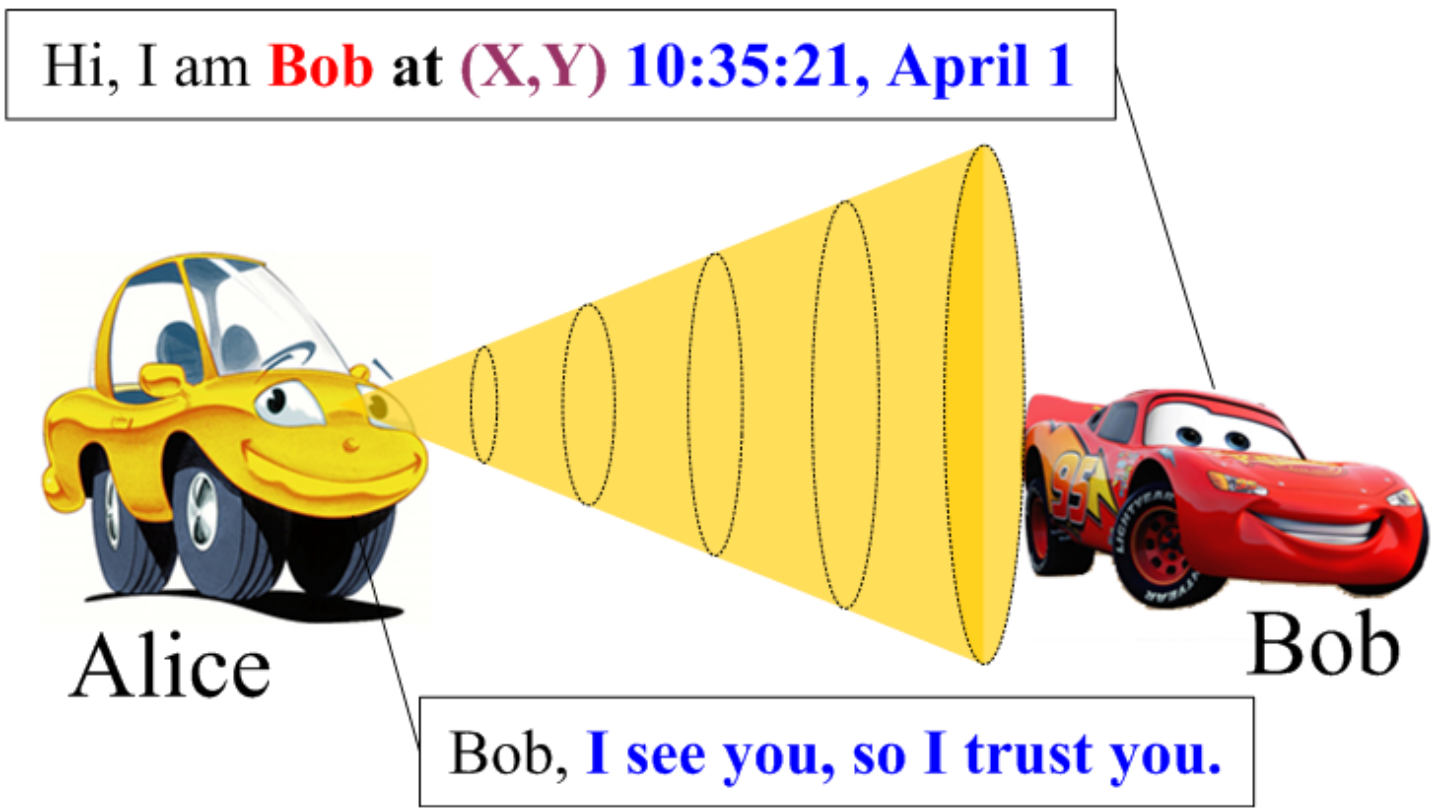
Location Integrity: Overview

- The main task:

  Validate the tuple <time, ID, location>

- Three sub-solutions:
  1. Active integrity: strong assumption (radar, GPS, transceiver)
  2. Passive integrity: weaker assumption (GPS, transceiver)
  3. General integrity: real world environment

Active Integrity: "Seeing is believing"



GPS Location

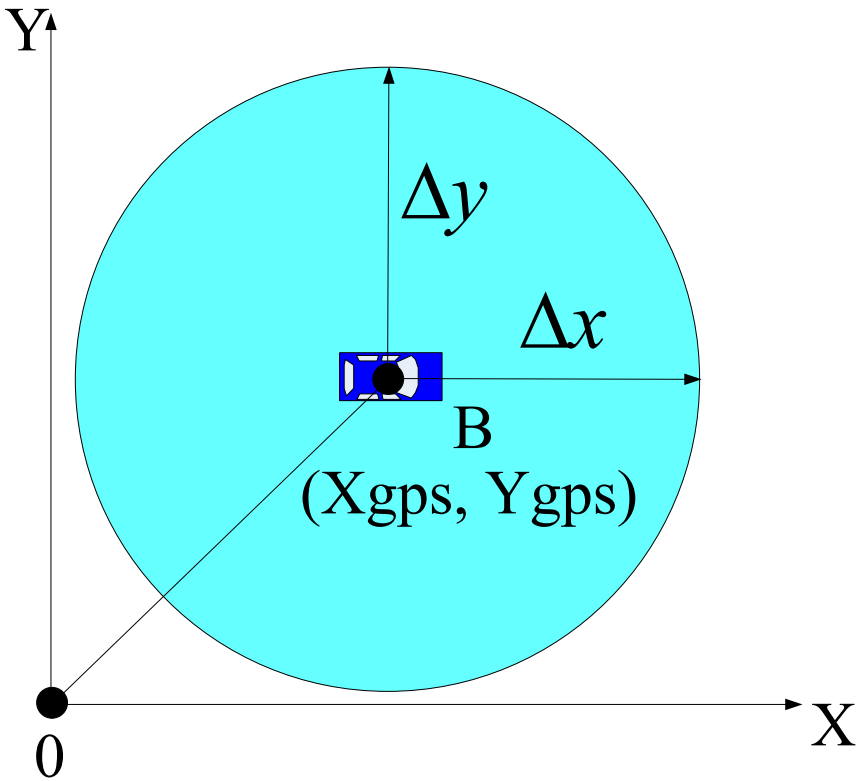
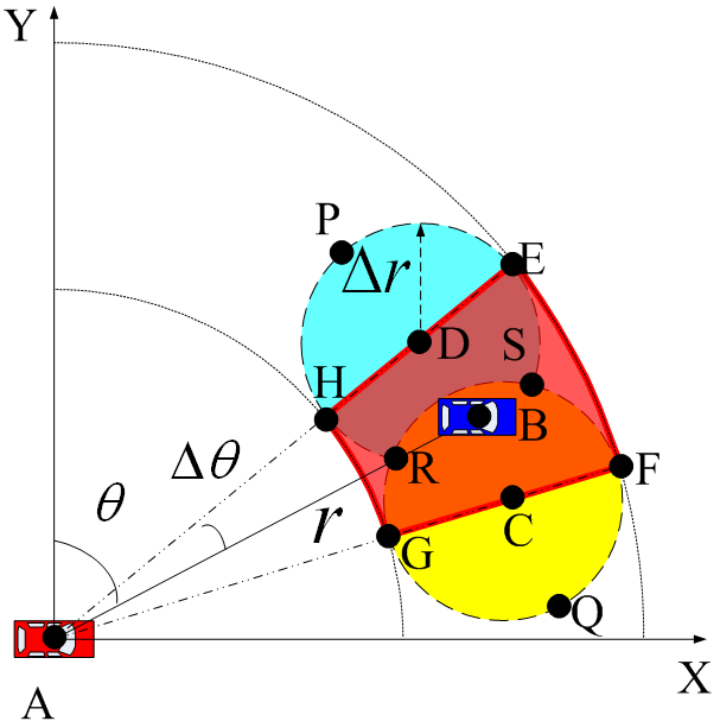


Figure: *GPS location.* (x_{gps}, y_{gps}) *is a measurement value of the GPS coordinates.*

For GPS: let measurement error $\Delta\alpha = \Delta x = \Delta y$, write

$$(x - x_{gps})^2 + (y - y_{gps})^2 \leq (\Delta\alpha)^2 \quad (1)$$

Radar Detection



- For Radar detection:

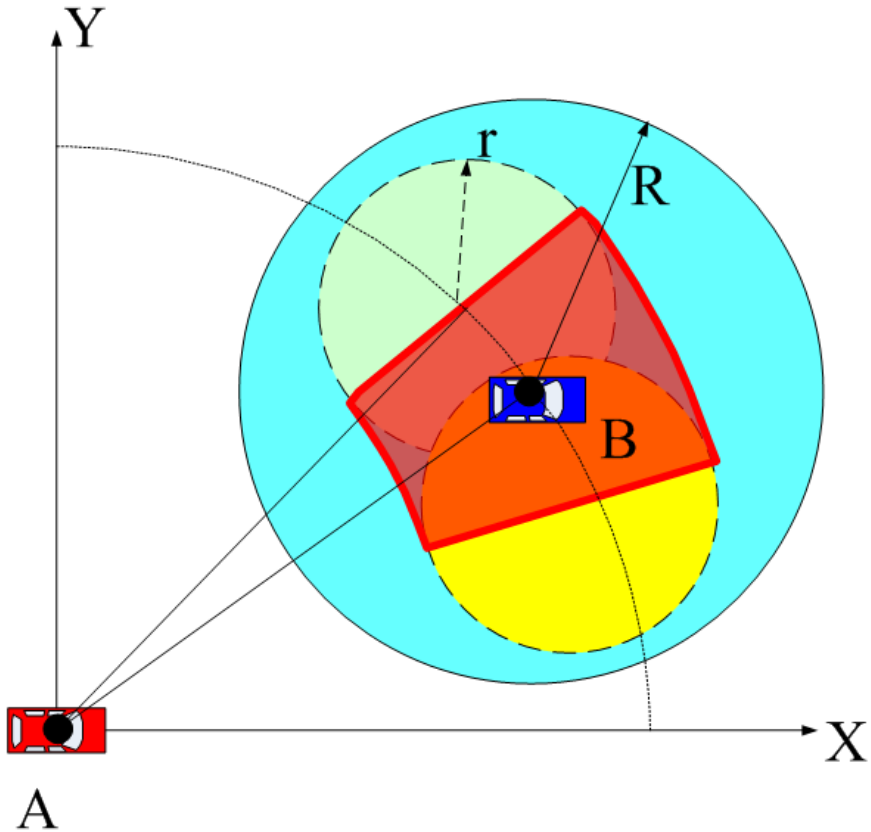
$$(x-\gamma\times\cos(\theta-\Delta\theta))_2^2+(y-\gamma\times\sin(\theta-\Delta\theta))_2^2\leq(\Delta\gamma)^2 \quad (2)$$
$$(x-\gamma\times\cos(\theta+\Delta\theta))^2+(y-\gamma\times\sin(\theta+\Delta\theta))^2\leq(\Delta\gamma)^2 \quad (3)$$

  θ: the detected angle; γ: the detected radius.

- For the region *FCGHDE*:

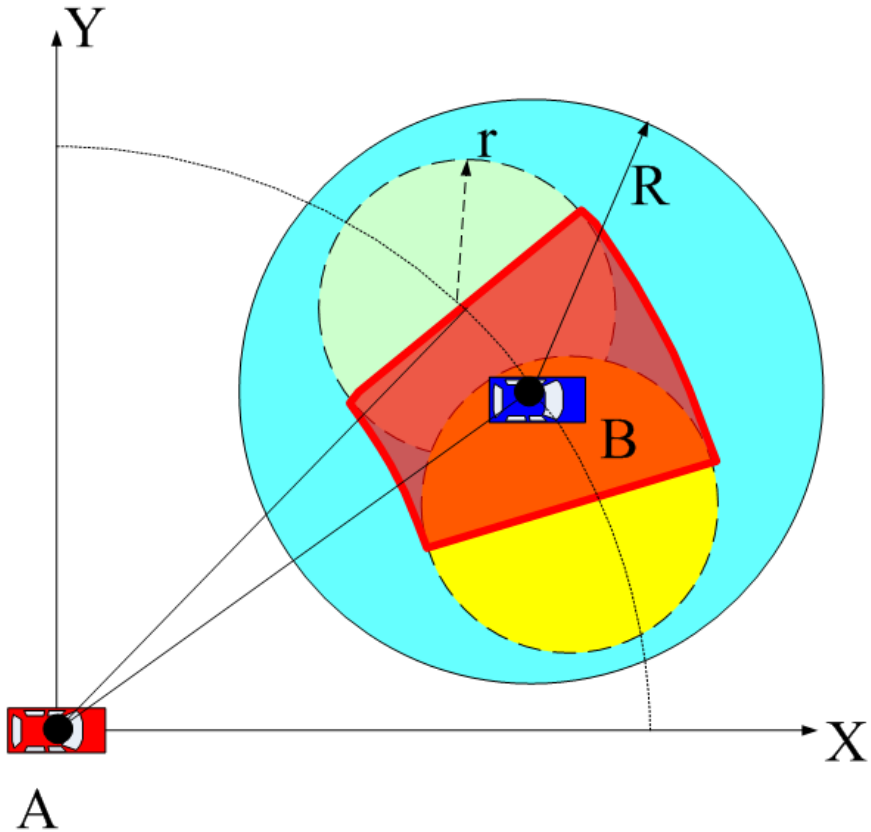
$$\begin{cases} \gamma-\Delta\gamma\leq\sqrt{x^2+y^2}\leq\gamma+\Delta\gamma \\ \theta-\Delta\theta\leq\arctan\frac{x}{y}\leq\theta+\Delta\theta \end{cases} \quad (4)$$

Validating GPS Location



- Validating GPS location means resolutions of: ***(1)*** $\cap$ { ***(2)*** $\cup$ ***(3)*** $\cup$ ***(4)*** }
- The accuracy of this solution is 99.1%.

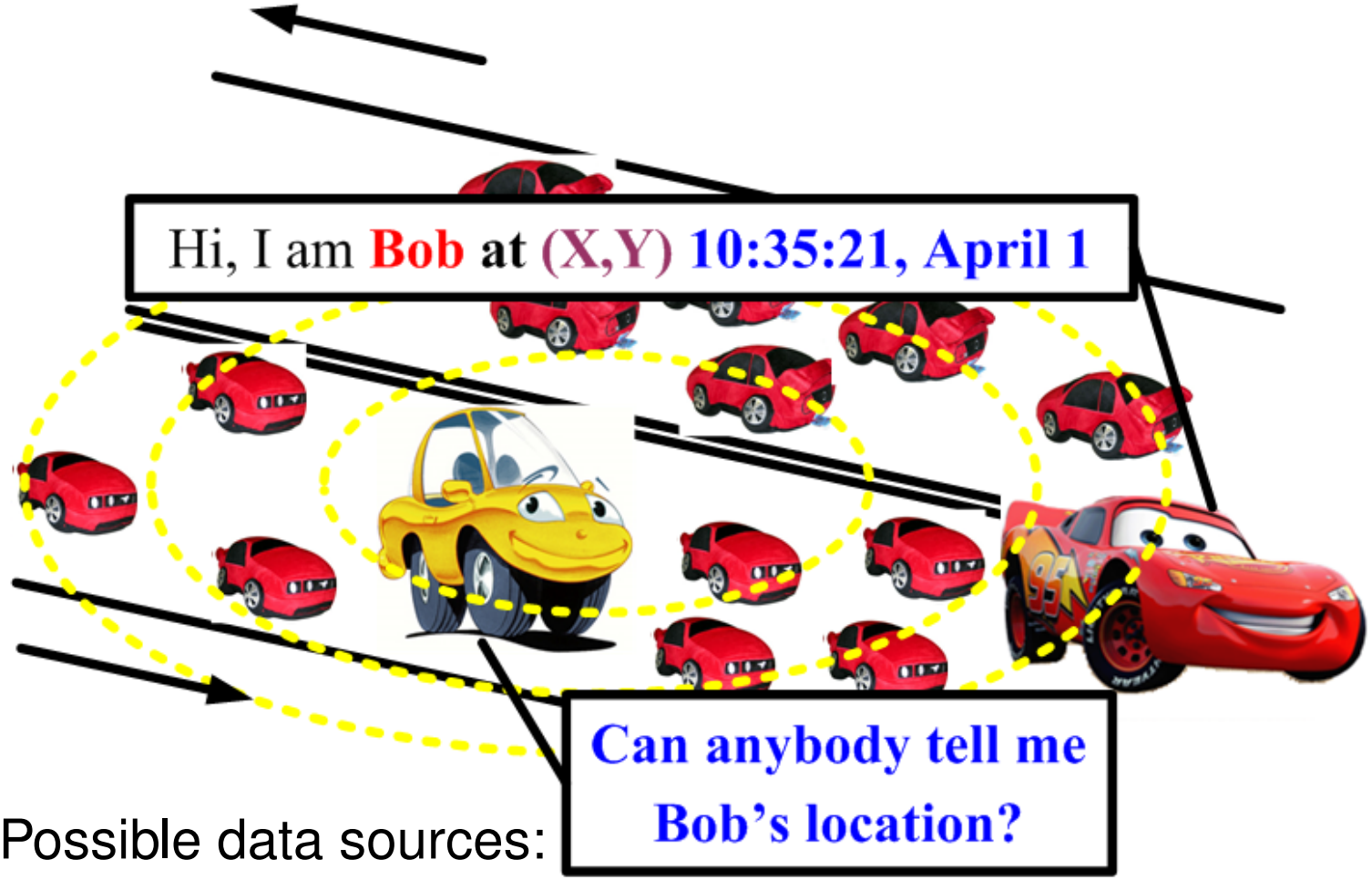
Validating GPS Location



- Validating GPS location means resolutions of: ***(1)*** $\cap$ { ***(2)*** $\cup$ ***(3)*** $\cup$ ***(4)*** }
- The accuracy of this solution is 99.1%.

Passive Integrity:

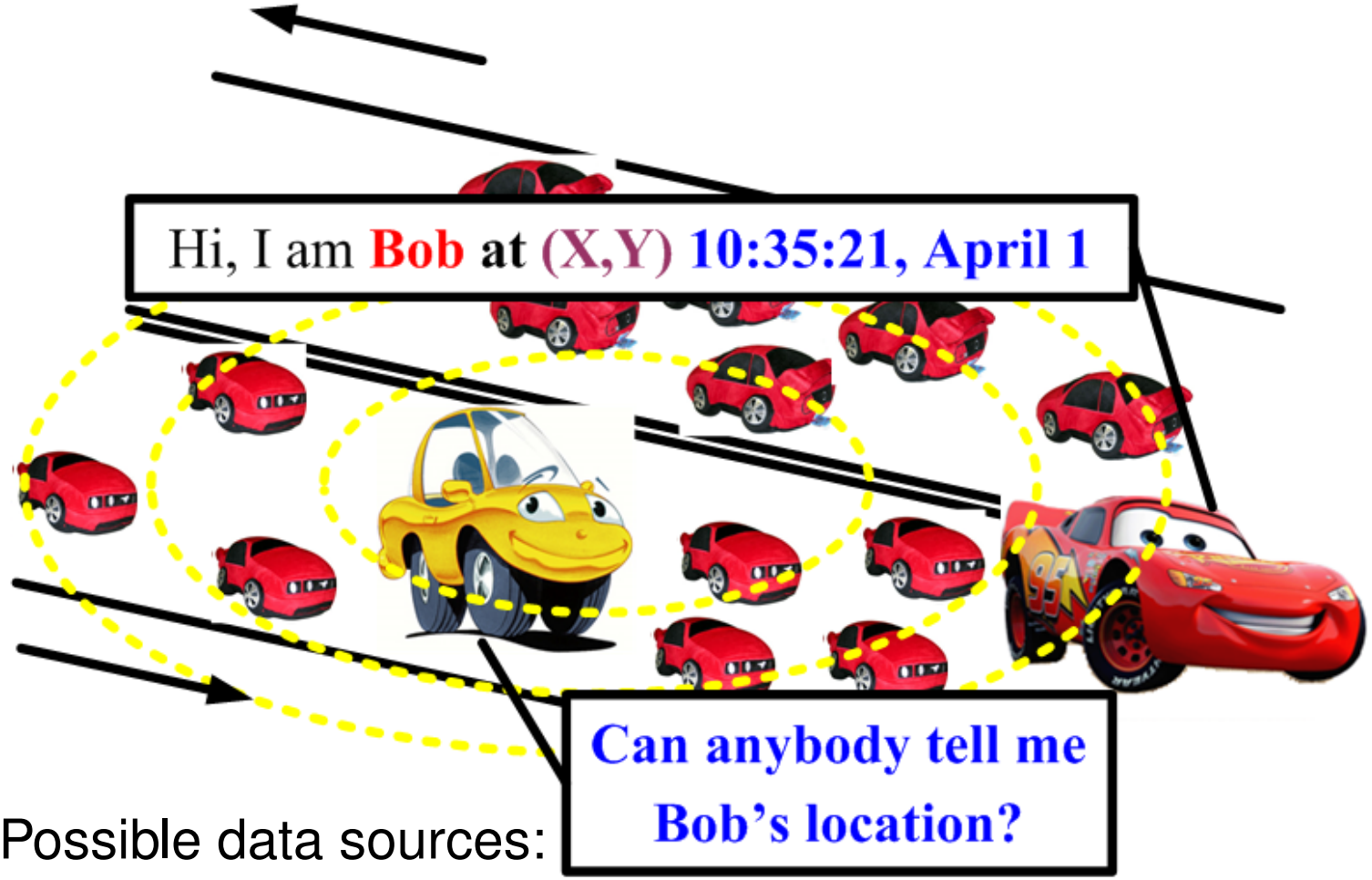
Statistically remove and refine



Possible data sources:

- Neighbors: All vehicles in the transmission range
- On-coming vehicles: All neighbors in opposite direction

Passive Integrity:
Statistically remove and refine



Possible data sources:

- Neighbors: All vehicles in the transmission range
- On-coming vehicles: All neighbors in opposite direction

Passive Integrity: Data Input

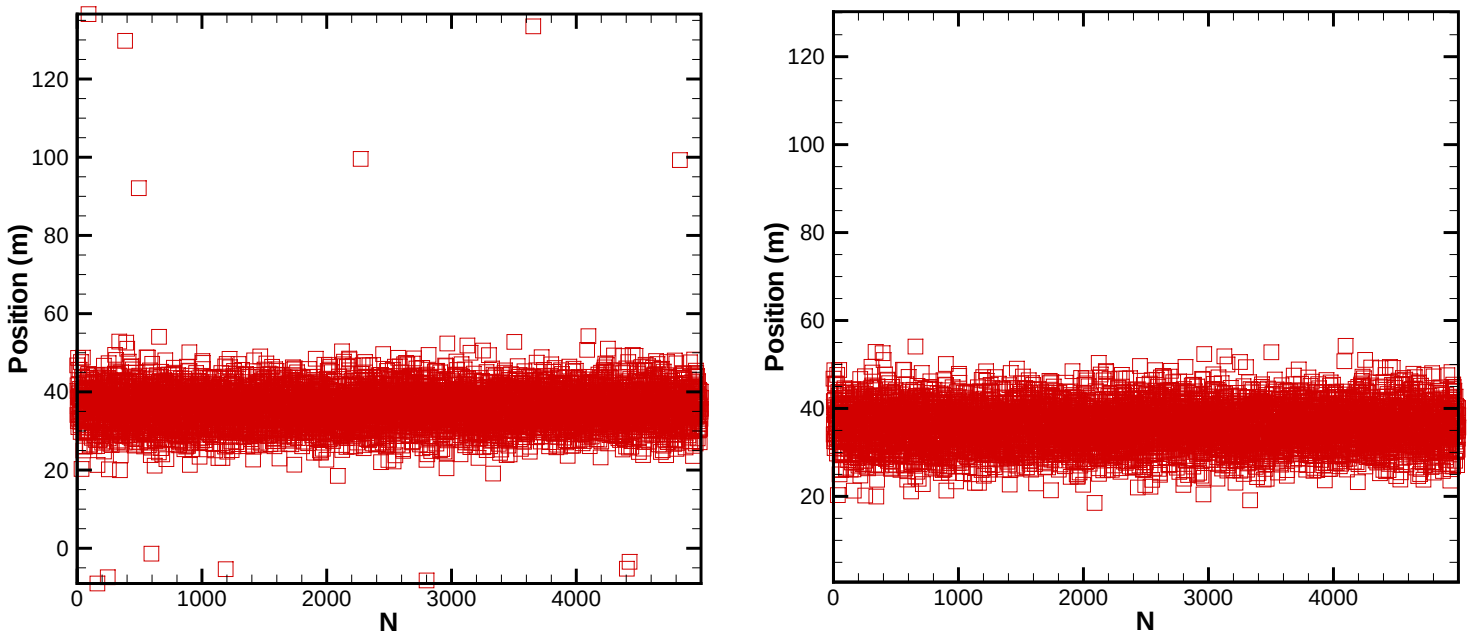


Figure: Bob's location collected by Alice (raw vs. filtered)

M-Distance

- Mahalanobis distance (M-Distance) introduced by P. C. Mahalanobis [Mahalanobis(1936)]
- Vectors $\vec{x}$ and $\vec{y}$ with the covariance matrix V, M-Distance:

$$d(\vec{x},\vec{y}) = \sqrt{(\vec{x}-\vec{y})^T V^{-1} (\vec{x}-\vec{y})}.$$

- Let $\overline{x}$: the sample mean vector;
  V: the sample covariance matrix,

$$V = \frac{1}{n-1}\sum_{i=1}^{n}(x_i-\overline{x})(x_i-\overline{x})^T. \quad (5)$$

M-Distance

- Mahalanobis distance (M-Distance) introduced by P. C. Mahalanobis [Mahalanobis(1936)]
- Vectors $\vec{x}$ and $\vec{y}$ with the covariance matrix V, M-Distance:

$$d(\vec{x},\vec{y}) = \sqrt{(\vec{x}-\vec{y})^T V^{-1}(\vec{x}-\vec{y})}.$$

- Let $\overline{x}$: the sample mean vector;
  V: the sample covariance matrix,

$$V = \frac{1}{n-1}\sum_{i=1}^{n}(x_i-\overline{x})(x_i-\overline{x})^T. \quad (5)$$

M-Distance

- Mahalanobis distance (M-Distance) introduced by P. C. Mahalanobis [Mahalanobis(1936)]
- Vectors $\vec{x}$ and $\vec{y}$ with the covariance matrix V, M-Distance:

$$d(\vec{x},\vec{y}) = \sqrt{(\vec{x}-\vec{y})^T V^{-1}(\vec{x}-\vec{y})}.$$

- Let $\overline{x}$: the sample mean vector;
  V: the sample covariance matrix,

$$V = \frac{1}{n-1}\sum_{i=1}^{n}(x_i-\overline{x})(x_i-\overline{x})^T. \quad (5)$$

Intuitive Explanation

An intuitive explanation: the distance of a test point from the center of mass divided by the width of the ellipse/ellipsoid

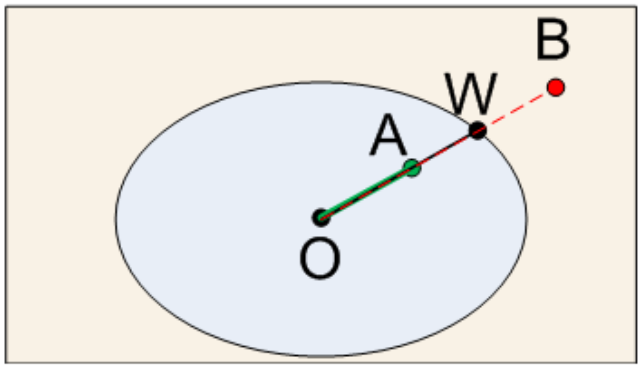


Figure: Two-dimensional space.

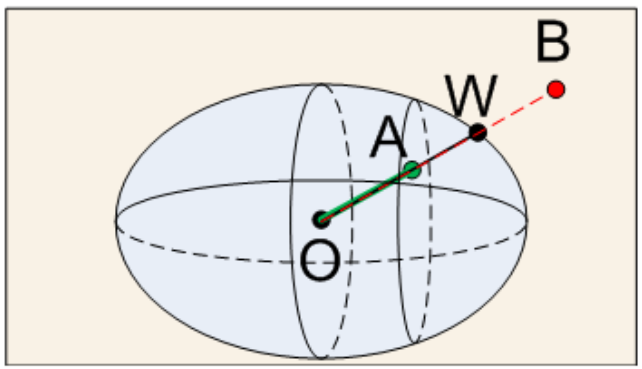


Figure: Three-dimensional space.

Passive Integrity

- Outliers can change the value of mean and covariance.
- We replace the mean $\overline{x}$ by the median x^* and obtain the robust covariance S.

$$S = \frac{\sum_{i=1}^{n} K(\|x_i - x^*\|)(x_i - x^*)(x_i - x^*)^T}{\sum_{i=1}^{n} K(\|x_i - x^*\|)}, \quad (6)$$

where $\|X\| = XV^{-1}X^T$, $K(u) = \exp(-hu)$,

- By [Caussinus & Ruiz(1990)], $h = 0.1$,

Passive Integrity

- Outliers can change the value of mean and covariance.
- We replace the mean $\overline{x}$ by the median x^* and obtain the robust covariance S.

$$S = \frac{\sum_{i=1}^{n} K(\|x_i - x^*\|)(x_i - x^*)(x_i - x^*)^T}{\sum_{i=1}^{n} K(\|x_i - x^*\|)}, \quad (6)$$

where $\|X\| = XV^{-1}X^T$, $K(u) = \exp(-hu)$,

- By [Caussinus & Ruiz(1990)], $h = 0.1$,

Passive Integrity

- Outliers can change the value of mean and covariance.
- We replace the mean $\overline{x}$ by the median x^* and obtain the robust covariance S.

$$S = \frac{\sum_{i=1}^{n} K(\|x_i - x^*\|)(x_i - x^*)(x_i - x^*)^T}{\sum_{i=1}^{n} K(\|x_i - x^*\|)}, \quad (6)$$

where $\|X\| = XV^{-1}X^T$, $K(u) = \exp(-hu)$,

- By [Caussinus & Ruiz(1990)], $h = 0.1$,

Passive Integrity

- The new M-distance D_i^r:

$$D_i^r = \sqrt{\{(x_i - x^*)S^{-1}(x_i - x^*)^T\}} \quad (7)$$

- Exclude the deviation caused by the outliers
- For multivariate normally distributed data, the values of D_i^r are approximately chi-square distributed (χ_2^2) [Filzmoser(2004)]
- The observations can be abandoned by using the chi-squared distribution (e.g., the 97.5% quantile).
- The sample mean:

$$\overline{x}^* = \frac{\sum_{k=1}^{N} x_k^*}{N} \quad (8)$$

- The accuracy of this solution is 96.2%.

Passive Integrity

- The new M-distance D_i^r:

$$D_i^r = \sqrt{\{(x_i - x^*)S^{-1}(x_i - x^*)^T\}} \quad (7)$$

- Exclude the deviation caused by the outliers
- For multivariate normally distributed data, the values of D_i^r are approximately chi-square distributed (χ_2^2) [Filzmoser(2004)]
- The observations can be abandoned by using the chi-squared distribution (e.g., the 97.5% quantile).
- The sample mean:

$$\overline{x}^* = \frac{\sum_{k=1}^{N} x_k^*}{N} \quad (8)$$

- The accuracy of this solution is 96.2%.

Passive Integrity

- The new M-distance D_i^r:

$$D_i^r = \sqrt{\{(x_i - x^*)S^{-1}(x_i - x^*)^T\}} \quad (7)$$

- Exclude the deviation caused by the outliers
- For multivariate normally distributed data, the values of D_i^r are approximately chi-square distributed (χ_2^2) [Filzmoser(2004)]
- The observations can be abandoned by using the chi-squared distribution (e.g., the 97.5% quantile).
- The sample mean:

$$\overline{x}^* = \frac{\sum_{k=1}^{N} x_k^*}{N} \quad (8)$$

- The accuracy of this solution is 96.2%.

Passive Integrity

- The new M-distance D_i^r:

$$D_i^r = \sqrt{\{(x_i - x^*)S^{-1}(x_i - x^*)^T\}} \quad (7)$$

- Exclude the deviation caused by the outliers
- For multivariate normally distributed data, the values of D_i^r are approximately chi-square distributed (χ_2^2) [Filzmoser(2004)]
- The observations can be abandoned by using the chi-squared distribution (e.g., the 97.5% quantile).
- The sample mean:

$$\overline{x}^* = \frac{\sum_{k=1}^{N} x_k^*}{N} \quad (8)$$

- The accuracy of this solution is 96.2%.

Passive Integrity

- The new M-distance D_i^r:

$$D_i^r = \sqrt{\{(x_i - x^*)S^{-1}(x_i - x^*)^T\}} \quad (7)$$

- Exclude the deviation caused by the outliers
- For multivariate normally distributed data, the values of D_i^r are approximately chi-square distributed (χ_2^2) [Filzmoser(2004)]
- The observations can be abandoned by using the chi-squared distribution (e.g., the 97.5% quantile).
- The sample mean:

$$\overline{x}^* = \frac{\sum_{k=1}^{N} x_k^*}{N} \quad (8)$$

- The accuracy of this solution is 96.2%.

Passive Integrity

- The new M-distance D_i^r:

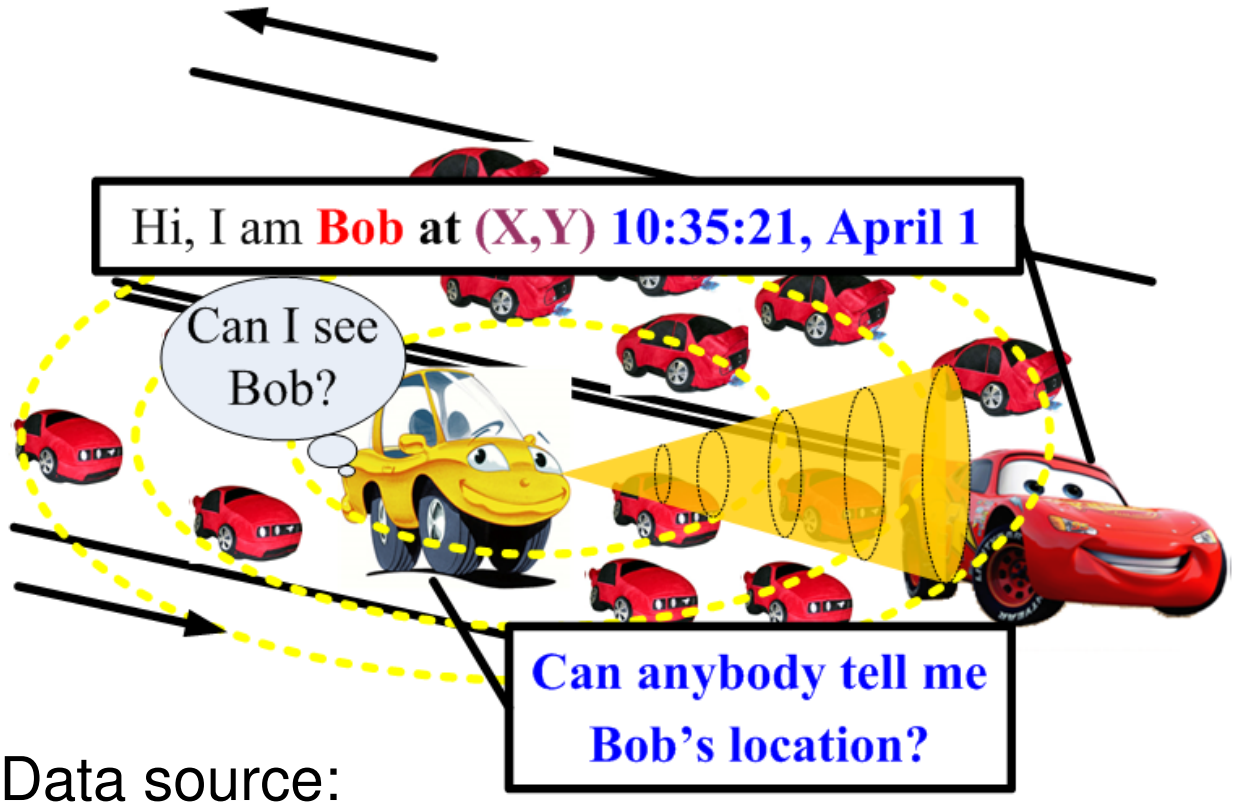
$$D_i^r = \sqrt{\{(x_i - x^*)S^{-1}(x_i - x^*)^T\}} \quad (7)$$

- Exclude the deviation caused by the outliers
- For multivariate normally distributed data, the values of D_i^r are approximately chi-square distributed (χ_2^2) [Filzmoser(2004)]
- The observations can be abandoned by using the chi-squared distribution (e.g., the 97.5% quantile).
- The sample mean:

$$\overline{x}^* = \frac{\sum_{k=1}^{N} x_k^*}{N} \quad (8)$$

- The accuracy of this solution is 96.2%.

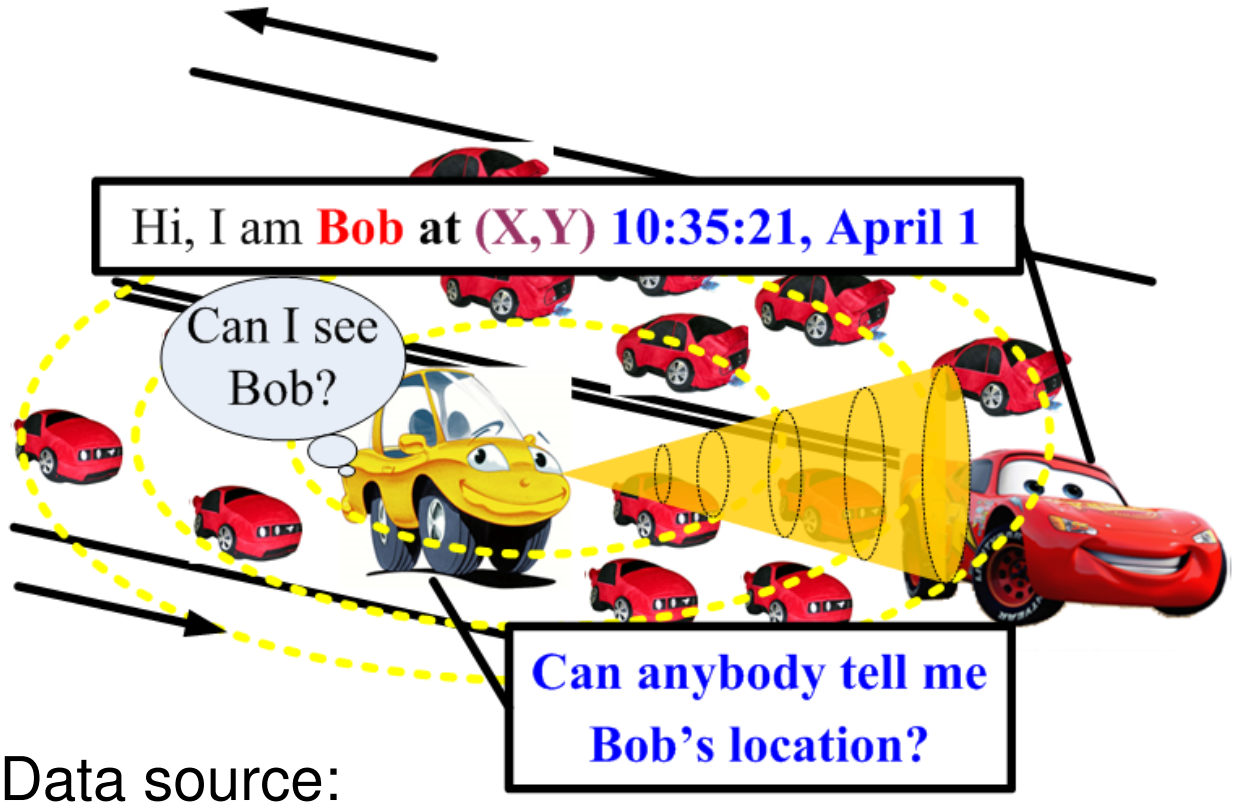
General Integrity: Real World Solution



Data source:

- Radar: Radar of observer
- Neighbors: All vehicles in the transmission range
- On-coming vehicles: All neighbors in on-coming direction

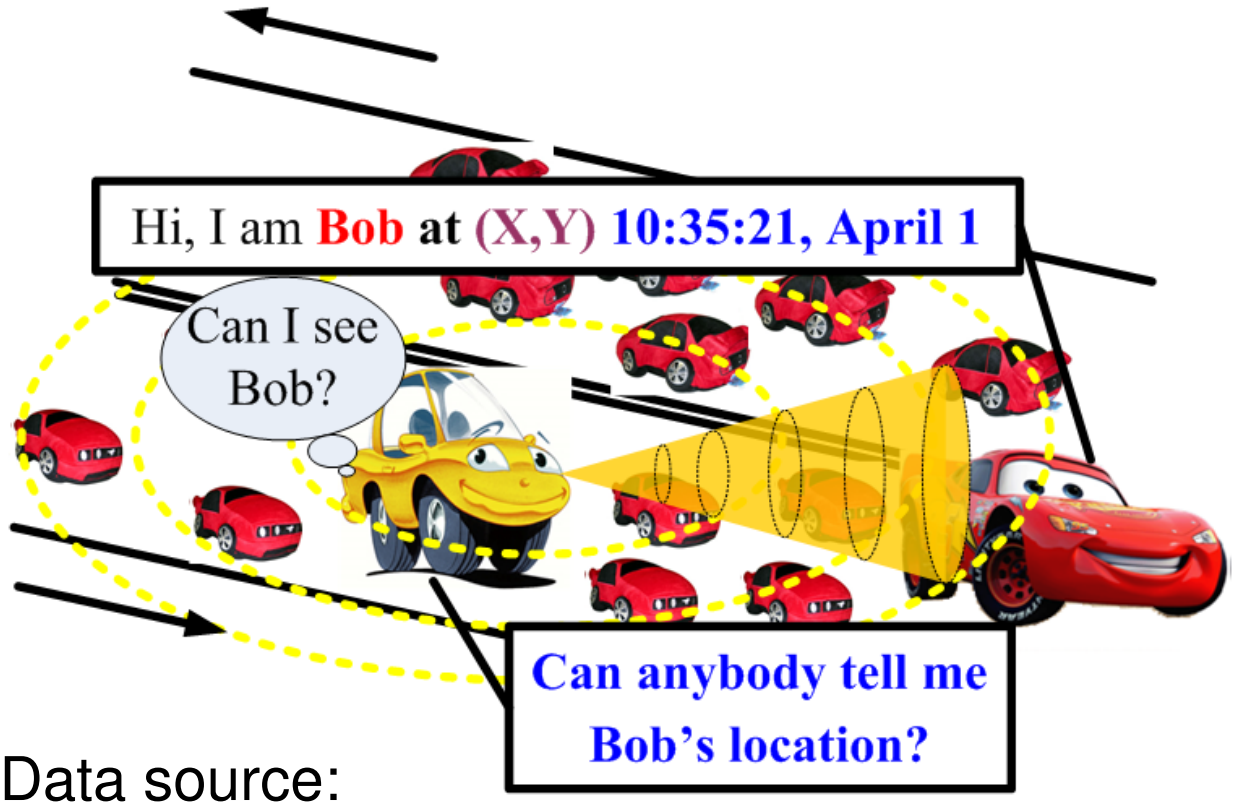
General Integrity: Real World Solution



Data source:

- Radar: Radar of observer
- Neighbors: All vehicles in the transmission range
- On-coming vehicles: All neighbors in on-coming direction

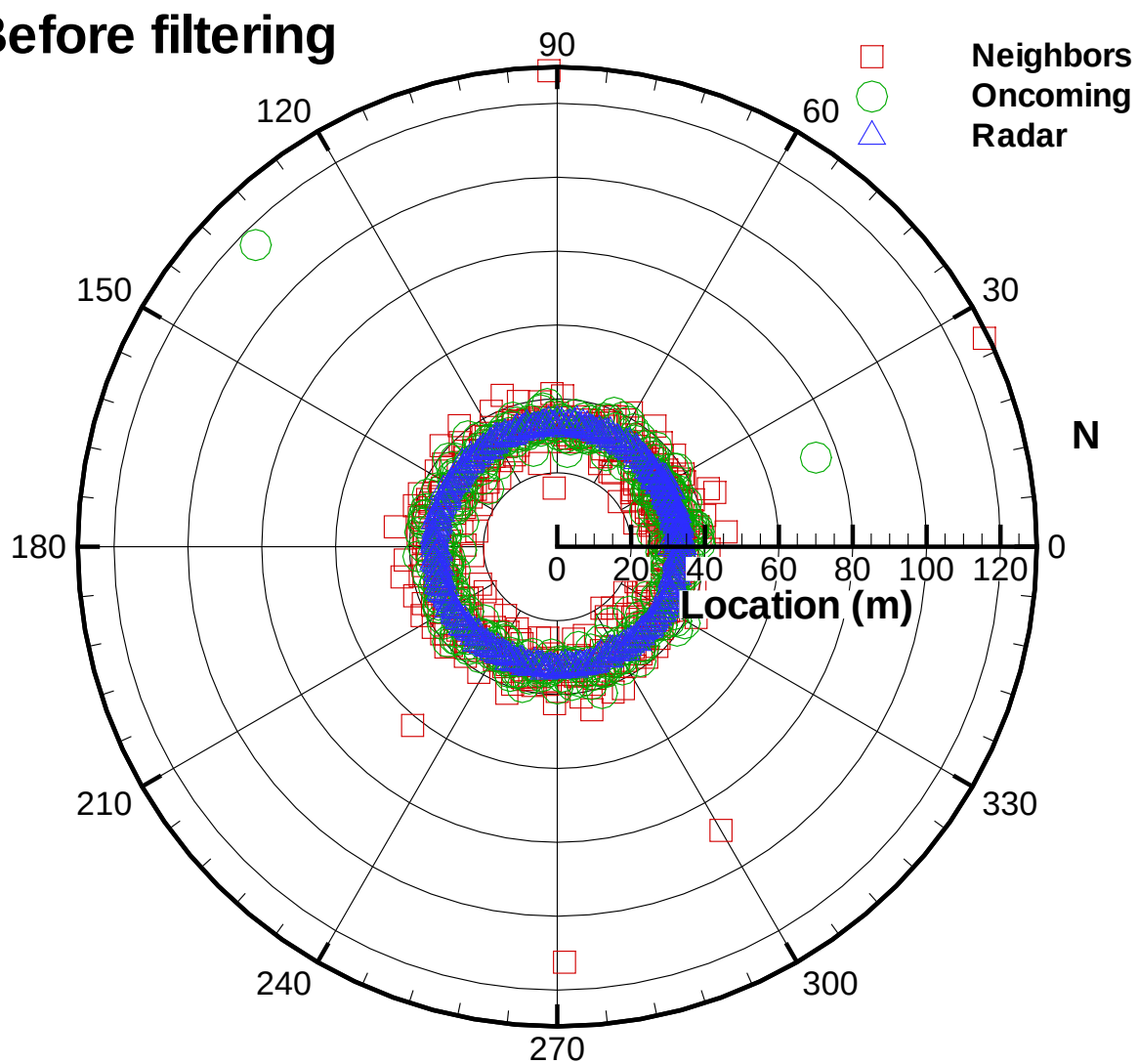
General Integrity: Real World Solution



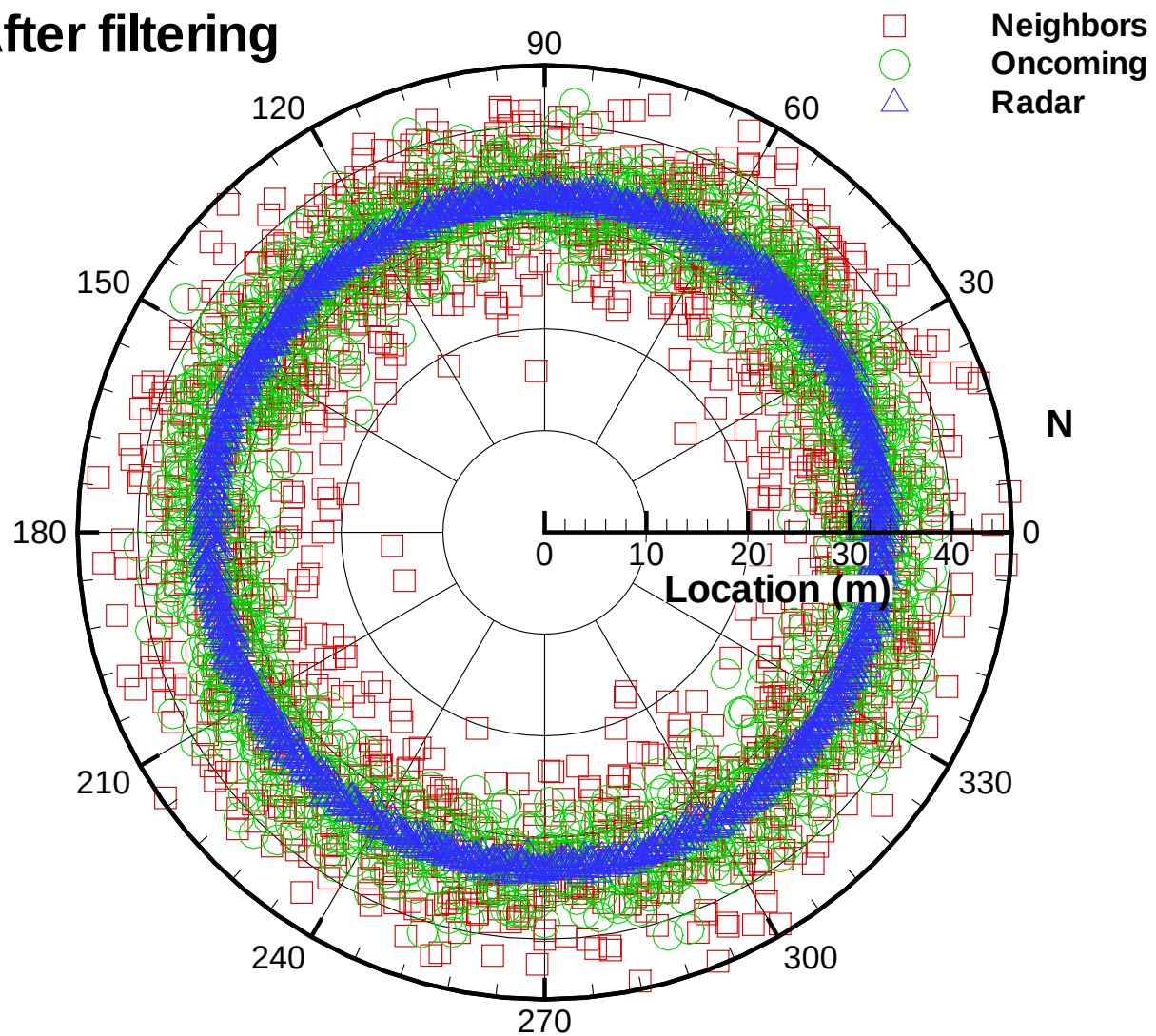
Data source:

- Radar: Radar of observer
- Neighbors: All vehicles in the transmission range
- On-coming vehicles: All neighbors in on-coming direction

General Integrity: Data Input



General Integrity: Location Measurement



General Integrity

- Let:
  - **X**: radar detection
  - **Y**: on-coming vehicle detection
  - **Z**: neighbor detection
- The final estimation of location:

$$P = w_1 * \overline{X}^* + w_2 * \overline{Y}^* + w_3 * \overline{Z}^*$$

where the weights of
  - w_1: radar detection
  - w_2: on-coming vehicle detection
  - w_3: neighbor detection
  - $w_1 \geq w_2 \geq w_3$
- The accuracy of this solution is 94.7% ($w_1 = 0.4, w_2 = 0.4, w_3 = 0.2$).

General Integrity

- Let:
  - **X**: radar detection
  - **Y**: on-coming vehicle detection
  - **Z**: neighbor detection
- The final estimation of location:

$$P = w_1 * \overline{X}^* + w_2 * \overline{Y}^* + w_3 * \overline{Z}^*$$

where the weights of
  - w_1: radar detection
  - w_2: on-coming vehicle detection
  - w_3: neighbor detection
  - $w_1 \geq w_2 \geq w_3$
- The accuracy of this solution is 94.7% ($w_1 = 0.4, w_2 = 0.4, w_3 = 0.2$).

General Integrity

- Let:
  - **X**: radar detection
  - **Y**: on-coming vehicle detection
  - **Z**: neighbor detection
- The final estimation of location:

$$P = w_1 * \overline{X}^* + w_2 * \overline{Y}^* + w_3 * \overline{Z}^*$$

where the weights of
  - w_1: radar detection
  - w_2: on-coming vehicle detection
  - w_3: neighbor detection
  - $w_1 \geq w_2 \geq w_3$
- The accuracy of this solution is 94.7% ($w_1 = 0.4, w_2 = 0.4, w_3 = 0.2$).

General Integrity

- Let:
  - **X**: radar detection
  - **Y**: on-coming vehicle detection
  - **Z**: neighbor detection
- The final estimation of location:

$$P = w_1 * \overline{X}^* + w_2 * \overline{Y}^* + w_3 * \overline{Z}^*$$

where the weights of
  - w_1: radar detection
  - w_2: on-coming vehicle detection
  - w_3: neighbor detection
  - $w_1 \geq w_2 \geq w_3$
- The accuracy of this solution is 94.7% ($w_1 = 0.4, w_2 = 0.4, w_3 = 0.2$).

General Integrity

- Let:
  - **X**: radar detection
  - **Y**: on-coming vehicle detection
  - **Z**: neighbor detection
- The final estimation of location:

$$P = w_1 * \overline{X}^* + w_2 * \overline{Y}^* + w_3 * \overline{Z}^*$$

where the weights of

  - w_1: radar detection
  - w_2: on-coming vehicle detection
  - w_3: neighbor detection
  - $w_1 \geq w_2 \geq w_3$

- The accuracy of this solution is 94.7% ($w_1 = 0.4, w_2 = 0.4, w_3 = 0.2$).

General Integrity

- Let:
  - **X**: radar detection
  - **Y**: on-coming vehicle detection
  - **Z**: neighbor detection
- The final estimation of location:

$$P = w_1 * \overline{X}^* + w_2 * \overline{Y}^* + w_3 * \overline{Z}^*$$

  where the weights of
  - w_1: radar detection
  - w_2: on-coming vehicle detection
  - w_3: neighbor detection
  - $w_1 \geq w_2 \geq w_3$
- The accuracy of this solution is 94.7% ($w_1 = 0.4, w_2 = 0.4, w_3 = 0.2$).

Simulation Methods

- For simulation, we find the location attackers out of all vehicles.
- Q-Q plot (Quantile-Quantile Plots) [Thode(2002)]
  - A commonly used tool in statistics to show the outliers.
  - Is a kind of graphical method for comparing two probability distributions
  - Plots the two distributions' quantiles against each other.
- A Q-Q plot is applied to show the Mahalanobis distance vs. normal quantile.

Simulation Methods

- For simulation, we find the location attackers out of all vehicles.
- Q-Q plot (Quantile-Quantile Plots) [Thode(2002)]
  - A commonly used tool in statistics to show the outliers.
  - Is a kind of graphical method for comparing two probability distributions
  - Plots the two distributions' quantiles against each other.
- A Q-Q plot is applied to show the Mahalanobis distance vs. normal quantile.

Simulation Methods

- For simulation, we find the location attackers out of all vehicles.
- Q-Q plot (Quantile-Quantile Plots) [Thode(2002)]
  - A commonly used tool in statistics to show the outliers.
  - Is a kind of graphical method for comparing two probability distributions
  - Plots the two distributions' quantiles against each other.
- A Q-Q plot is applied to show the Mahalanobis distance vs. normal quantile.

Simulation Settings

Table: Parameters and Values

Parameters	Values
Initial traffic density	30 vehicles/Km/lane
The length of the road L	3 Km
Average speed	60 km/h
The number of lanes	4/direction
The mean error μ	1 m
The deviation of error σ	1 m
Error ε	3 m
The sample size n	1000
# of neighbor outliers m_n	8
# of opposite outliers m_o	2
The weight for radar w_1	0.5
The weight for opposite w_2	0.3
The weight for neighbors w_3	0.2

Neighboring Report Filtering

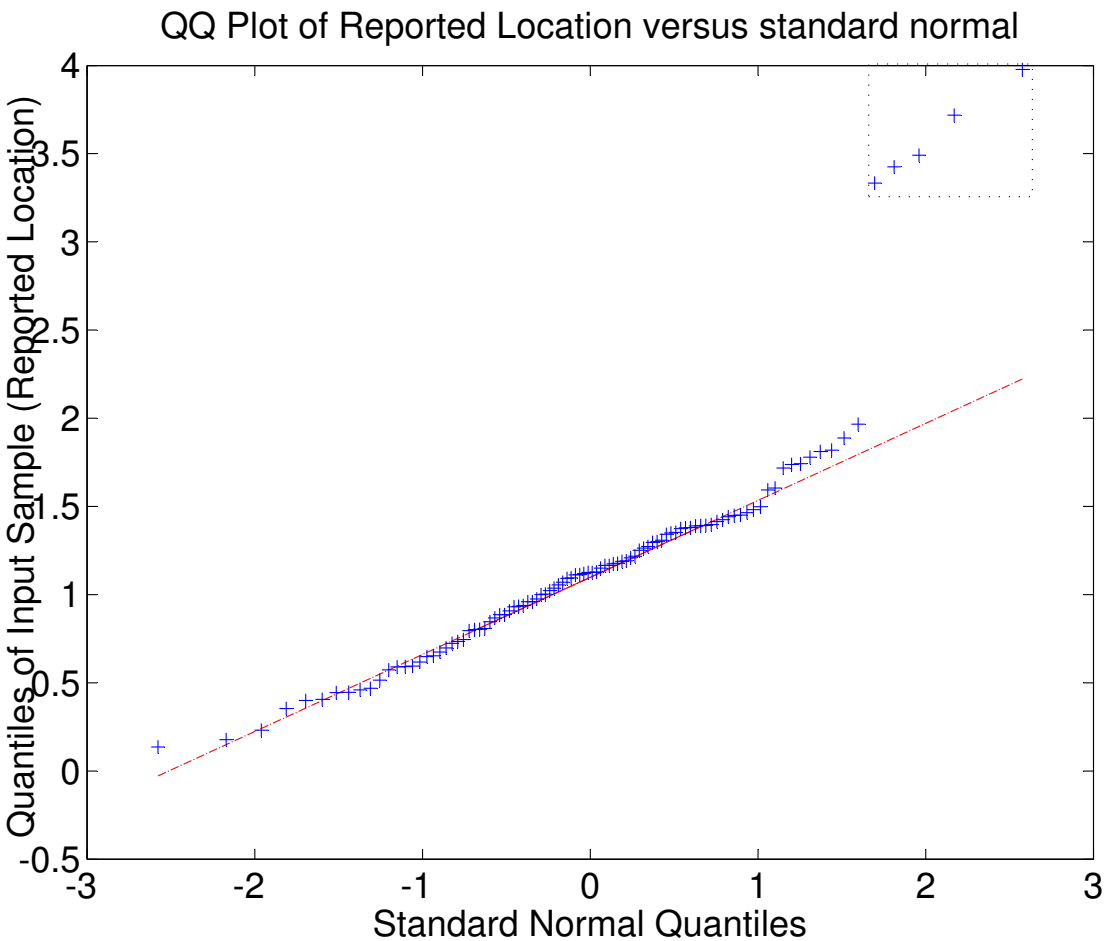


Figure: Q-Q plot of the Mahalanobis distance for neighboring samples.

All Measurements Estimation

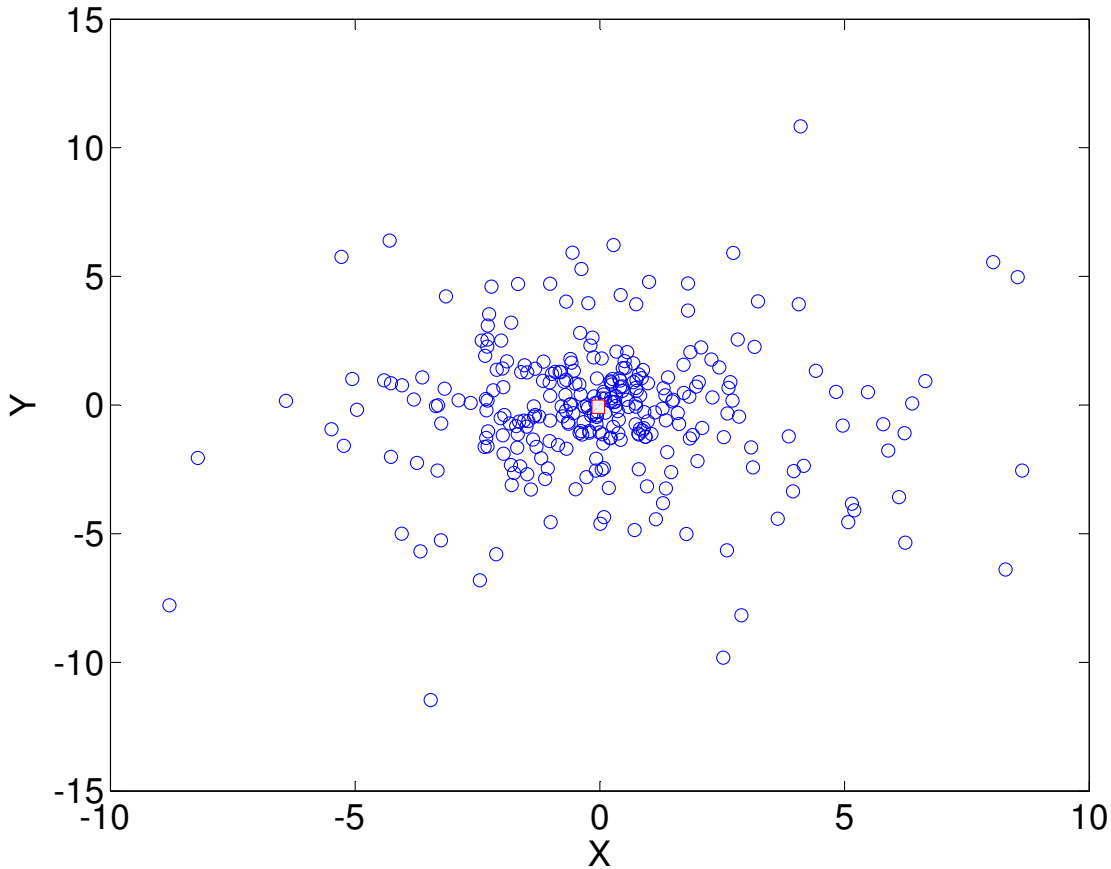


Figure: The x-y coordinates of location observation and the location estimation.

Location Integrity: Summary

- Main points:
  - Validate the tuple <time, ID, location>
  - Start with a homogenous model and strong assumptions
  - Improve to a real world solution
- Contributions:
  - Novel idea: active location security
  - Real world solution

Location Integrity: Summary

- Main points:
  - Validate the tuple <time, ID, location>
  - Start with a homogenous model and strong assumptions
  - Improve to a real world solution
- Contributions:
  - Novel idea: active location security
  - Real world solution

Location Integrity: Summary

- Main points:
  - Validate the tuple <time, ID, location>
  - Start with a homogenous model and strong assumptions
  - Improve to a real world solution
- Contributions:
  - Novel idea: active location security
  - Real world solution

Location Integrity: Summary

- Main points:
  - Validate the tuple <time, ID, location>
  - Start with a homogenous model and strong assumptions
  - Improve to a real world solution
- Contributions:
  - Novel idea: active location security
  - Real world solution

Location Integrity: Summary

- Main points:
  - Validate the tuple <time, ID, location>
  - Start with a homogenous model and strong assumptions
  - Improve to a real world solution
- Contributions:
  - Novel idea: active location security
  - Real world solution

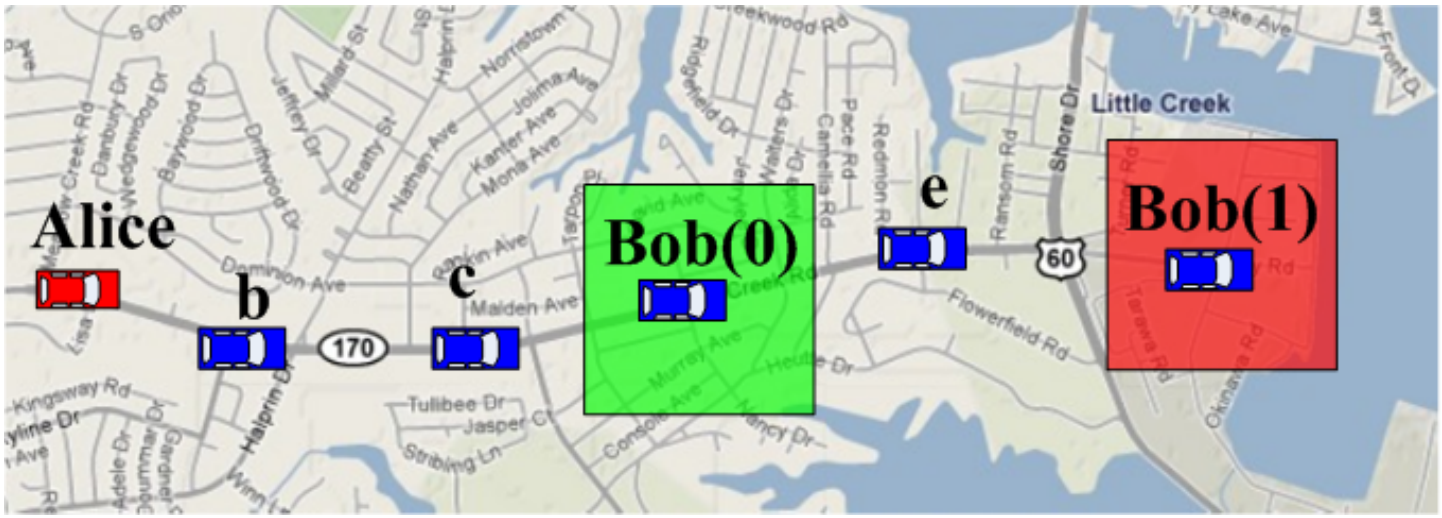
Location Integrity: Summary

- Main points:
  - Validate the tuple <time, ID, location>
  - Start with a homogenous model and strong assumptions
  - Improve to a real world solution
- Contributions:
  - Novel idea: active location security
  - Real world solution

Location Integrity: Summary

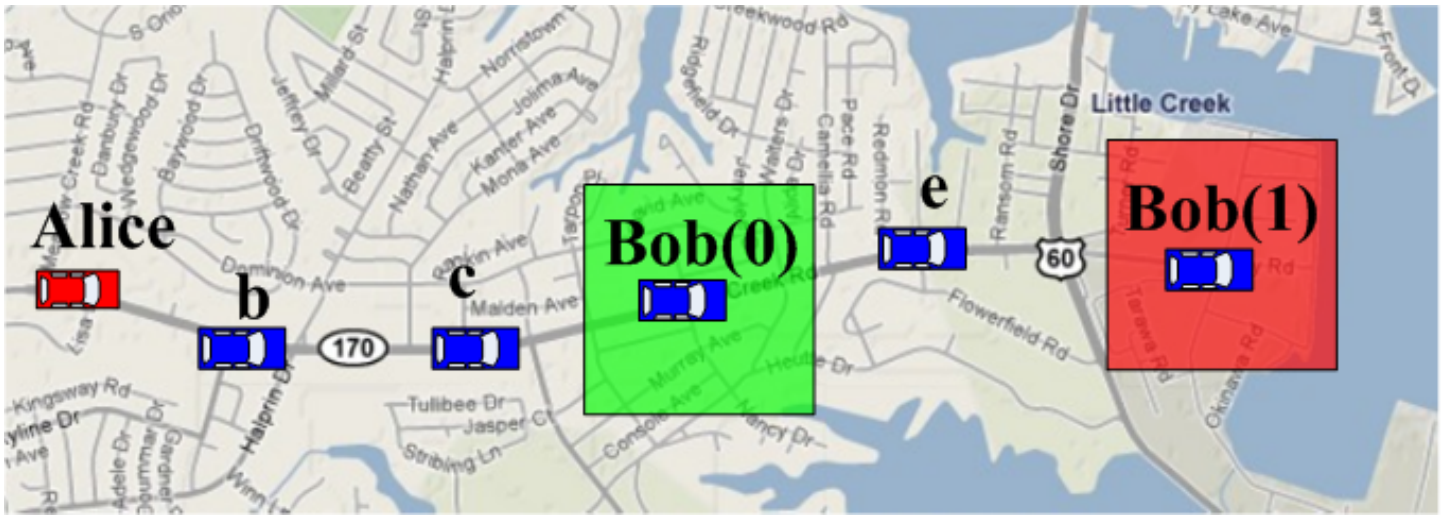
- Main points:
  - Validate the tuple <time, ID, location>
  - Start with a homogenous model and strong assumptions
  - Improve to a real world solution
- Contributions:
  - Novel idea: active location security
  - Real world solution

Location Confidentiality: Overview



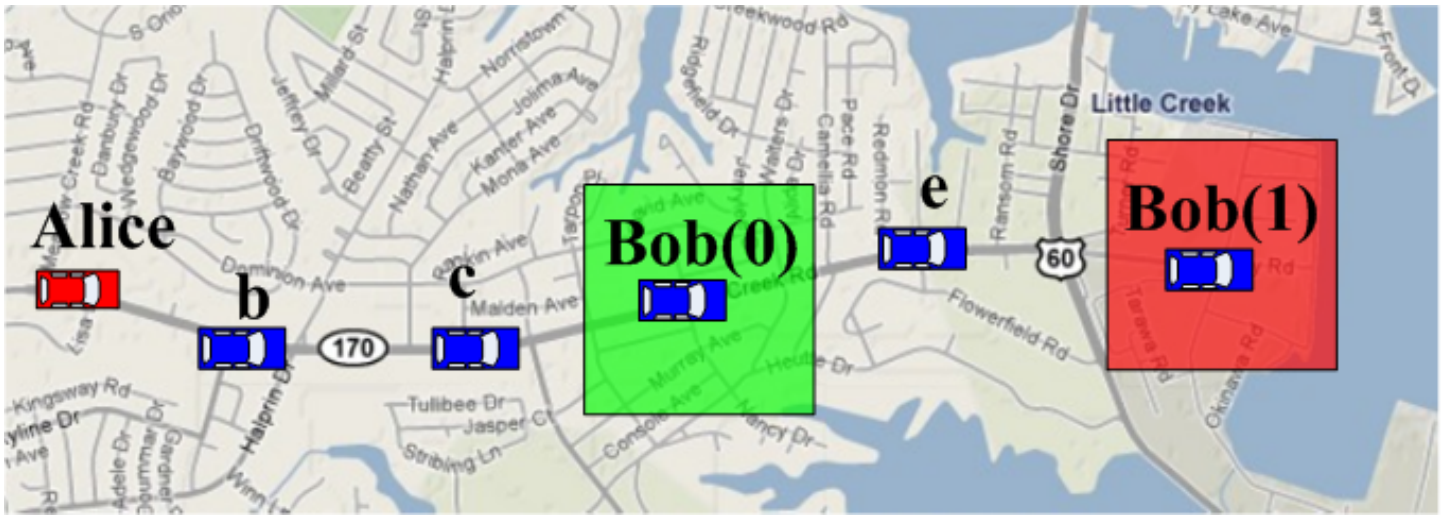
- Denning's GeoEncryption:
- Public Key Infrastructure (PKI): public key & private key
- Geolock table

Location Confidentiality: Overview



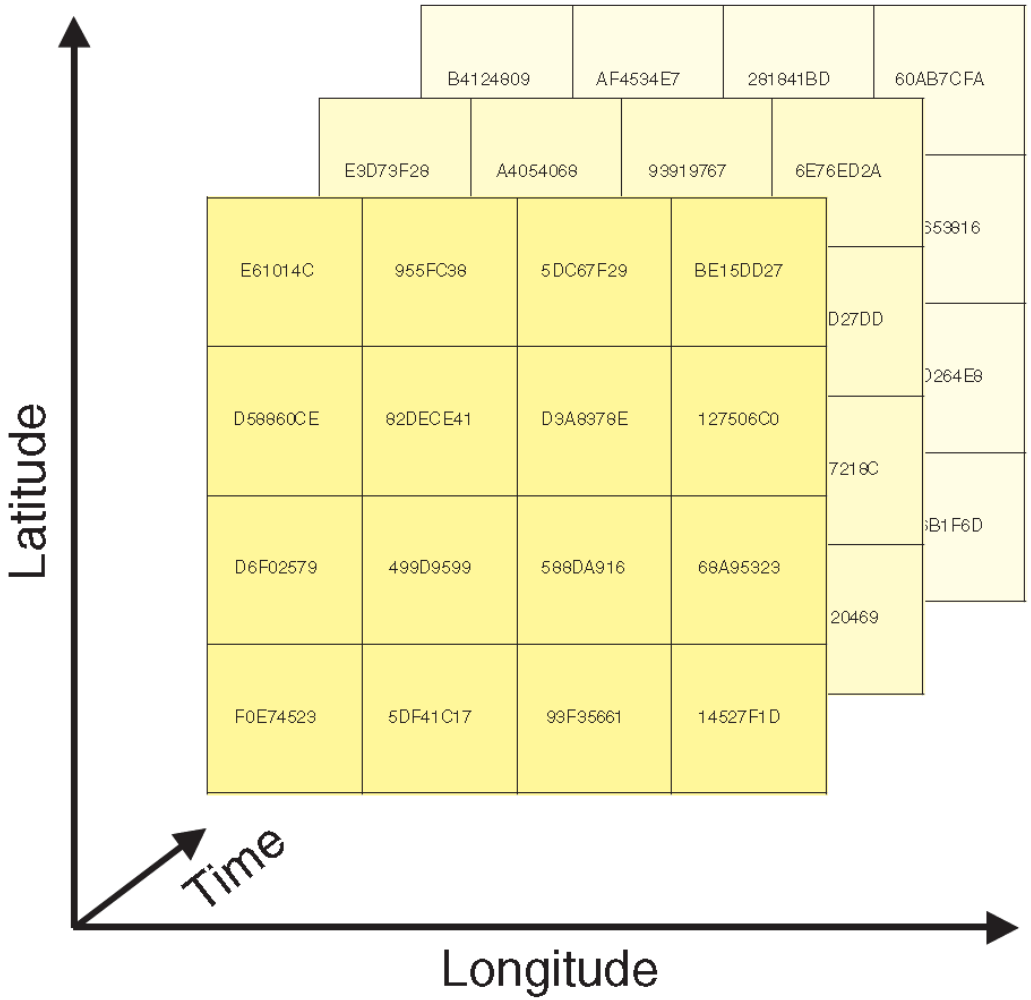
- Denning's GeoEncryption:
- Public Key Infrastructure (PKI): public key & private key
- Geolock table

Location Confidentiality: Overview



- Denning's GeoEncryption:
- Public Key Infrastructure (PKI): public key & private key
- Geolock table

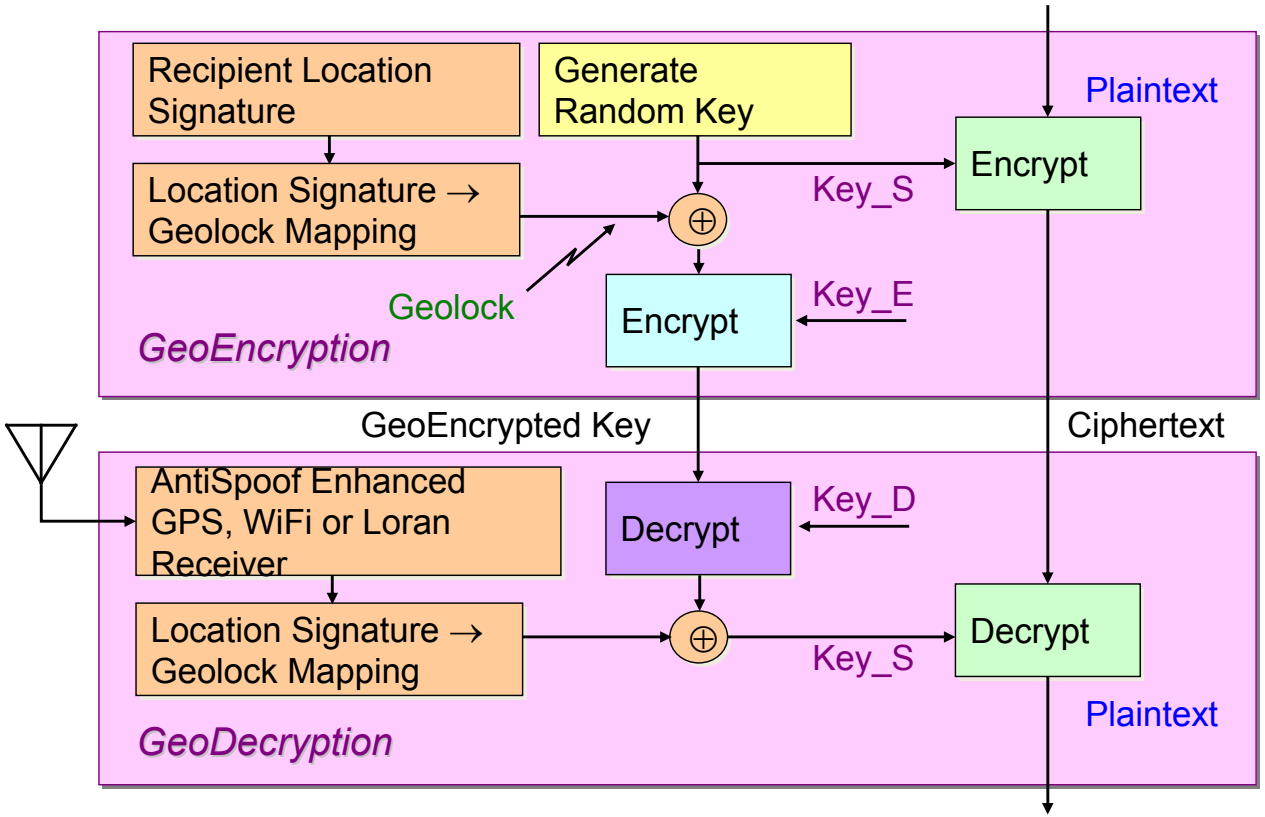
Denning's GeoLock Table [2]



Geolock table is preinstalled on all the nodes.

[2][Denning & MacDoran(1996)]

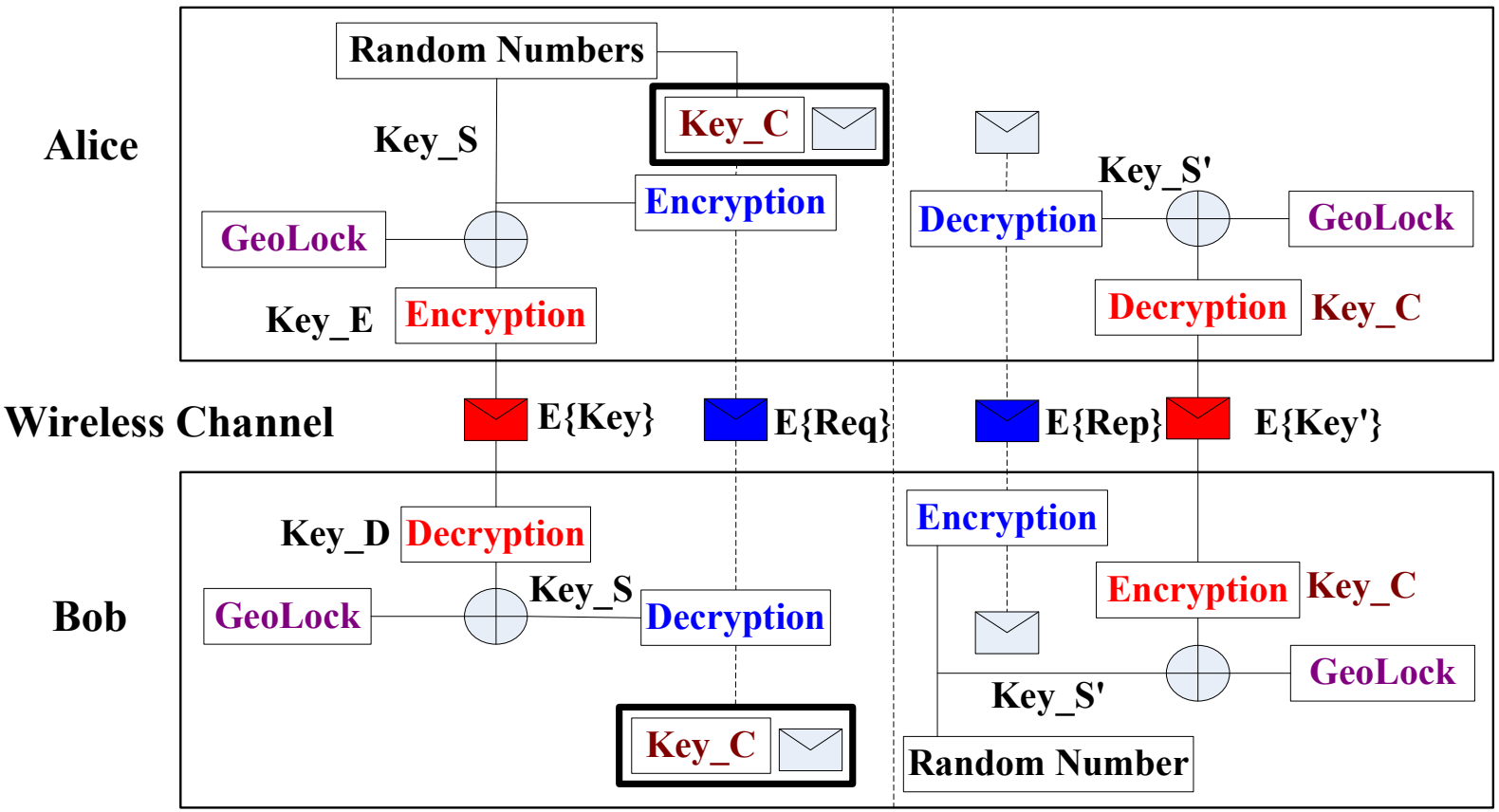
Denning's GeoEncryption [3]



- Drawbacks?
  - Both sender and receiver have PKI
  - Pre-deployed mapping tables

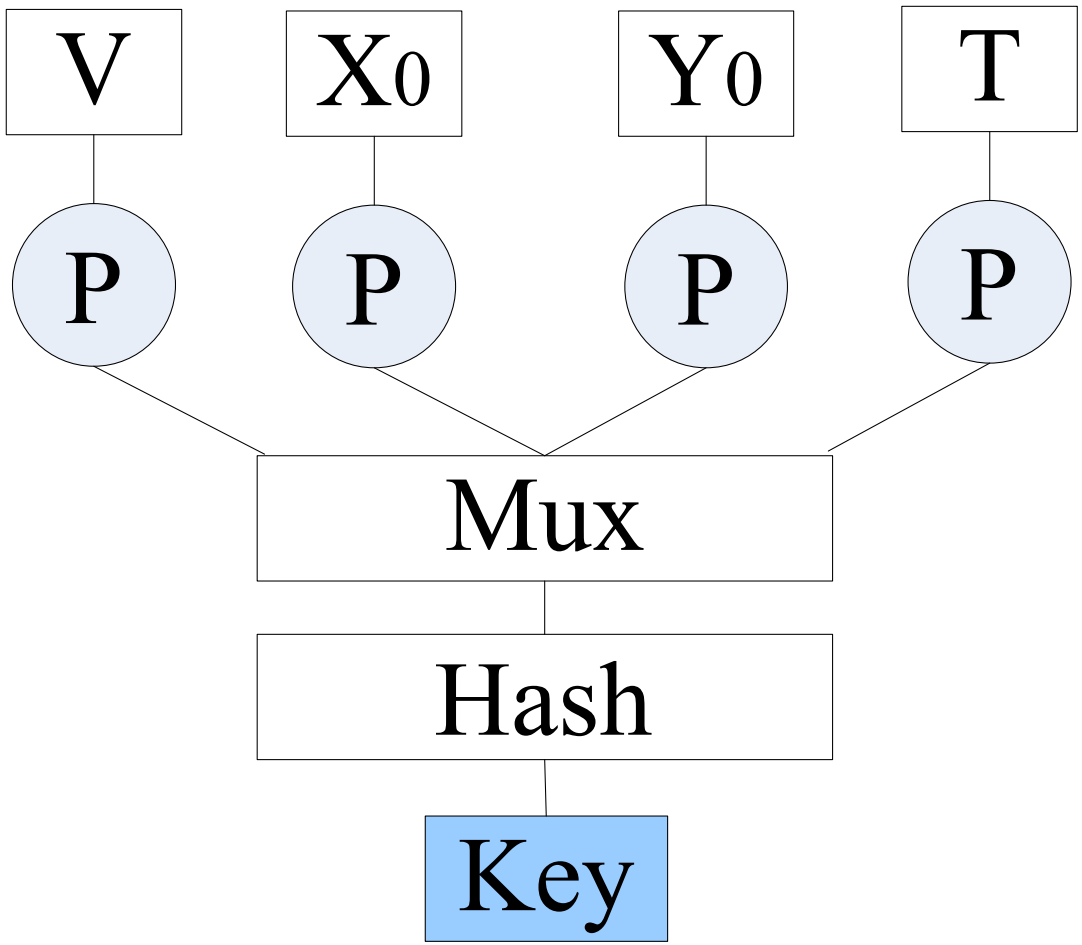
[3] [Denning & MacDoran(1996)]

Confidentiality: Our Method



To crack this scheme, attackers must have both location and private key.

New GeoLock



An Example: New GeoLock

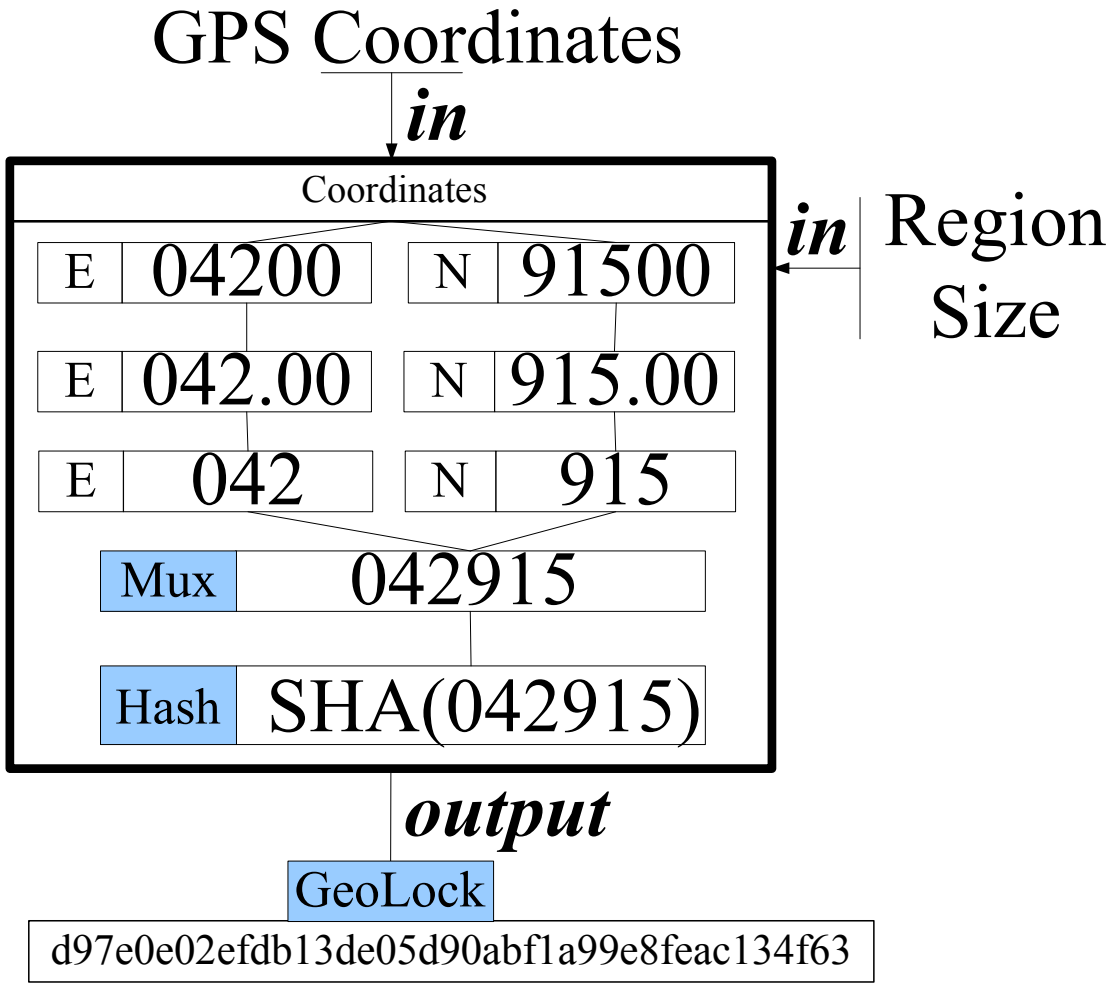


Figure: *An example of GeoLock.*

Simulation Scenario

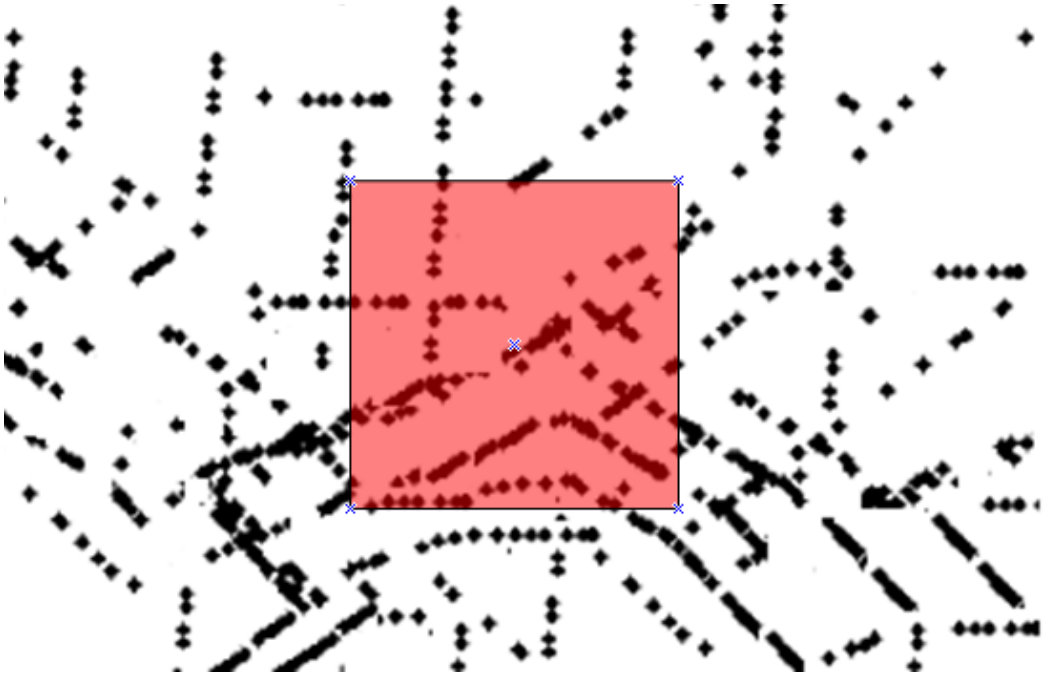


Figure: Decryption region snapshot (Decryption region is not proportionally drawn)

- Comparing our extension with a geoencryption extension: Al-Fuqaha [Al-Fuqaha & Al-Ibrahim(2007)].
- Al-Fuqaha added decryption region prediction algorithm to geoencryption in mobile networks.

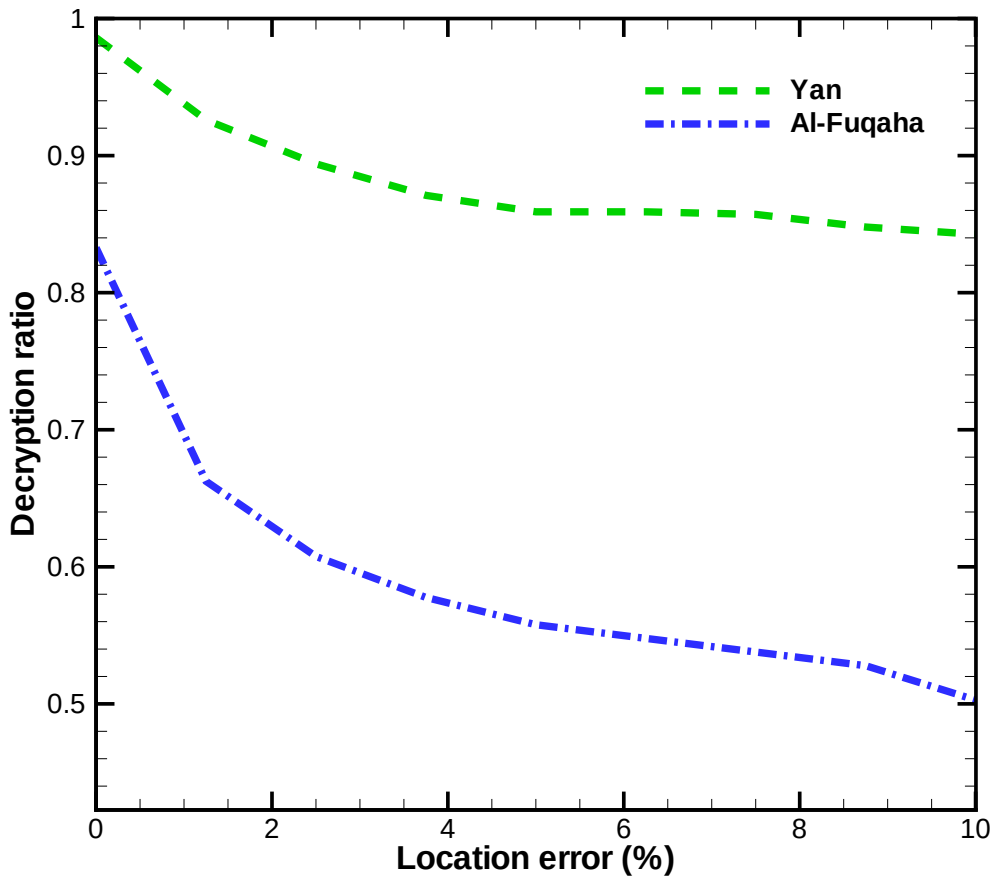
Simulation Settings

Table: The selected environment configuration

Name	Value
Transmission range	300m
Simulation map	Urban
Map area	3.2*3.2 Km^2
Decryption area	100*100 m^2
Traffic density	1500 vehicles/hour
Average speed	28 m/s
Acceleration range	[0,2] m/s^2
Initial acceleration	0 m/s^2
Initial speed	25 m/s
Mobility model	IDM [Treiber et al.(2000)]

GeoEncryption Decryption Ratio

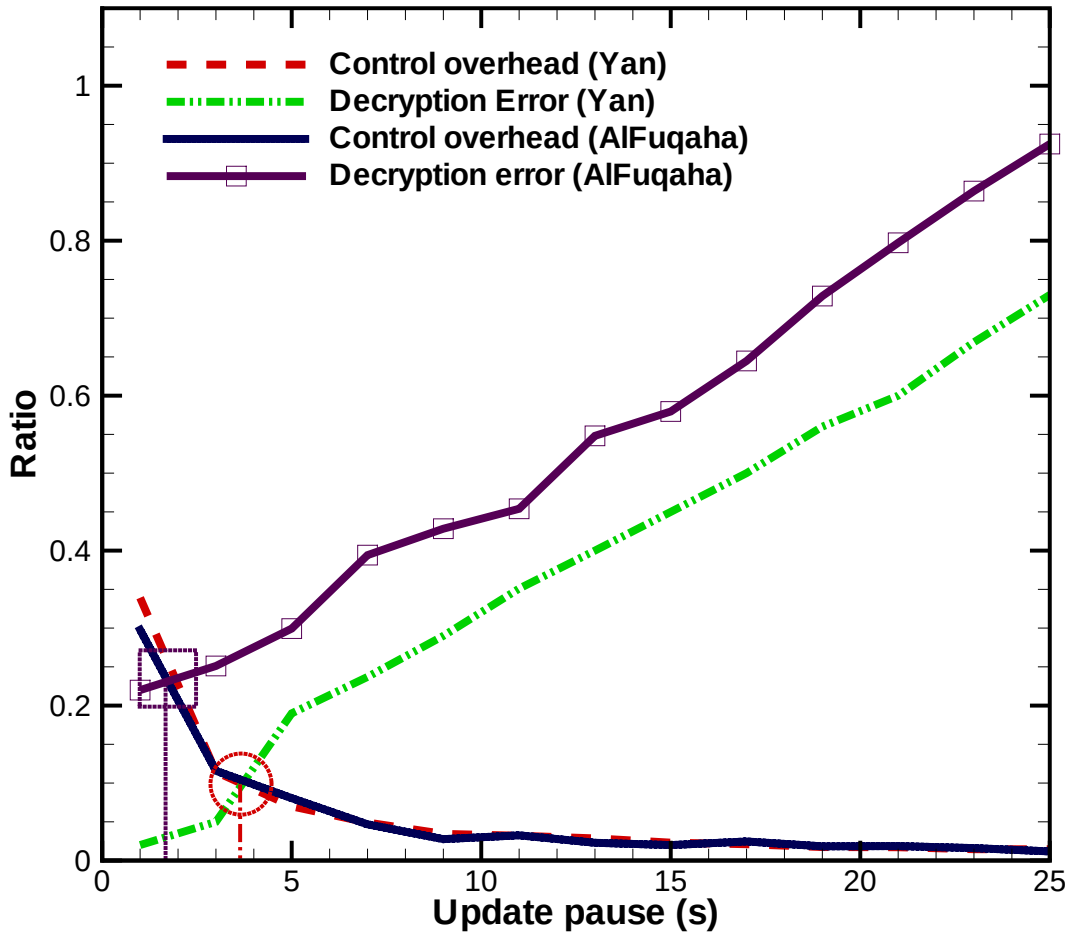
As expected, our algorithm can tolerate larger location errors. $DecryptionRatio = \frac{\text{No. of successful decryption}}{\text{No. of received ciphertext}}$



GeoEncryption Decryption Ratio Vs. Overhead

As expected, our algorithm

- Has smaller decryption error.
- Has fewer control message.



Location Confidentiality: Summary

- Main points:
  - Encrypt/decrypt location information
  - Location is part of the key: GeoLock
  - Key exchange is secured by GeoLock + private key
- Contributions:
  - New Geoencryption can operate with only one PKI peer
  - New Geolock can compute key dynamically.
  - New Geolock can tolerate larger location errors.
  - New Geoencryption has lower control overhead.

Location Confidentiality: Summary

- Main points:
  - Encrypt/decrypt location information
  - Location is part of the key: GeoLock
  - Key exchange is secured by GeoLock + private key
- Contributions:
  - New Geoencryption can operate with only one PKI peer
  - New Geolock can compute key dynamically.
  - New Geolock can tolerate larger location errors.
  - New Geoencryption has lower control overhead.

Location Confidentiality: Summary

- Main points:
  - Encrypt/decrypt location information
  - Location is part of the key: GeoLock
  - Key exchange is secured by GeoLock + private key
- Contributions:
  - New Geoencryption can operate with only one PKI peer
  - New Geolock can compute key dynamically.
  - New Geolock can tolerate larger location errors.
  - New Geoencryption has lower control overhead.

Location Confidentiality: Summary

- Main points:
  - Encrypt/decrypt location information
  - Location is part of the key: GeoLock
  - Key exchange is secured by GeoLock + private key
- Contributions:
  - New Geoencryption can operate with only one PKI peer
  - New Geolock can compute key dynamically.
  - New Geolock can tolerate larger location errors.
  - New Geoencryption has lower control overhead.

Location Confidentiality: Summary

- Main points:
  - Encrypt/decrypt location information
  - Location is part of the key: GeoLock
  - Key exchange is secured by GeoLock + private key
- Contributions:
  - New Geoencryption can operate with only one PKI peer
  - New Geolock can compute key dynamically.
  - New Geolock can tolerate larger location errors.
  - New Geoencryption has lower control overhead.

Location Confidentiality: Summary

- Main points:
  - Encrypt/decrypt location information
  - Location is part of the key: GeoLock
  - Key exchange is secured by GeoLock + private key
- Contributions:
  - New Geoencryption can operate with only one PKI peer
  - New Geolock can compute key dynamically.
  - New Geolock can tolerate larger location errors.
  - New Geoencryption has lower control overhead.

Location Confidentiality: Summary

- Main points:
  - Encrypt/decrypt location information
  - Location is part of the key: GeoLock
  - Key exchange is secured by GeoLock + private key
- Contributions:
  - New Geoencryption can operate with only one PKI peer
  - New Geolock can compute key dynamically.
  - New Geolock can tolerate larger location errors.
  - New Geoencryption has lower control overhead.

Location Confidentiality: Summary

- Main points:
  - Encrypt/decrypt location information
  - Location is part of the key: GeoLock
  - Key exchange is secured by GeoLock + private key
- Contributions:
  - New Geoencryption can operate with only one PKI peer
  - New Geolock can compute key dynamically.
  - New Geolock can tolerate larger location errors.
  - New Geoencryption has lower control overhead.

Location Confidentiality: Summary

- Main points:
  - Encrypt/decrypt location information
  - Location is part of the key: GeoLock
  - Key exchange is secured by GeoLock + private key
- Contributions:
  - New Geoencryption can operate with only one PKI peer
  - New Geolock can compute key dynamically.
  - New Geolock can tolerate larger location errors.
  - New Geoencryption has lower control overhead.

Summary

"Art is never finished, only abandoned." (Leonardo da Vinci)

- Focused on studying location information security
- *CIA* model
  - Location availability: A mobility and probability model in VANET communication
  - Location integrity: The active, passive and general models
  - Location confidentiality: The location-based encryption and decryption

Summary

"Art is never finished, only abandoned." (Leonardo da Vinci)

- Focused on studying location information security
- *CIA* model
  - Location availability: A mobility and probability model in VANET communication
  - Location integrity: The active, passive and general models
  - Location confidentiality: The location-based encryption and decryption

Summary

"Art is never finished, only abandoned." (Leonardo da Vinci)

- Focused on studying location information security
- *CIA* model
  - Location availability: A mobility and probability model in VANET communication
  - Location integrity: The active, passive and general models
  - Location confidentiality: The location-based encryption and decryption

Summary

"Art is never finished, only abandoned." (Leonardo da Vinci)

- Focused on studying location information security
- *CIA* model
  - Location availability: A mobility and probability model in VANET communication
  - Location integrity: The active, passive and general models
  - Location confidentiality: The location-based encryption and decryption

Summary

"Art is never finished, only abandoned." (Leonardo da Vinci)

- Focused on studying location information security
- *CIA* model
  - Location availability: A mobility and probability model in VANET communication
  - Location integrity: The active, passive and general models
  - Location confidentiality: The location-based encryption and decryption

Putting The Work In Perspective

What remains to be done:

- Cross layer issues
- Extensive simulation
- Integrate to other research, e.g. privacy
- Optimization of the algorithm
- Real traffic data import
- Test bed implementation
- Prototype design
- Applying the research in real applications
- Theory analysis of the transportation issues
- Disaster evacuation
- Data storage in VANET

VANET Applications

VANET Applications		
I. Active safety	1. Dangerous road features	1. Curve speed warning, 2 low bridge warning, 3. traffic lights violation warning
	2. Abnormal conditions	1. Vehicle-based road condition warning, 2. infrastructure-based road condition warning, 3. visibility enhancer, 4. work zone warning.
	3. Danger of collision	1. Blind spot warning, 2. lane change warning, 3. intersection collision warning, 4. forward/rear collision warning, 5. emergency electronic brake lights, 6. rail collision warning, 7. warning about pedestrians crossing
	4. Incident occurred	1. Post-crash warning, 2. incident recovery (insurance), 3. SOS service, 4. evacuate people
II. Public service	1.Support for authorities	1. Electronic license plate, 2. electronic drivers license, 3. vehicle safety inspection, 4. stolen vehicles tracking, 5. Emergency vehicle warning,
III. Improved driving	1. Enhanced Driving	1. Highway merge assistant, 2. left turn assistant, 3. cooperative adaptive cruise control, 4. cooperative glare reduction, 5. in-vehicle signage, 6. adaptive drivetrain management
	2. Traffic Efficiency	1. Notification of crash, 2. intelligent traffic flow control, 3. enhanced route guidance and navigation, 4. map download/update, 5. parking spot locator service
IV. Entertainment	1. Mobile Services	1. Internet service provisioning, 2. instant messaging, 3. point-of-interest notification
	2. E-Commerce	1. Fleet management, 2. rental car processing, 3. area access control, 4. cargo tracking; 5. toll collection, 6. parking/gas payment

1. E. Schoch, at el, "Communication Patterns in VANETs," IEEE Communications Magazine, Vol.46

Selected Publication Lists

Journal

1. **G Yan**, S. Olariu, "An Efficient Geographic Location-based Security Mechanism for Vehicular Ad hoc Networks", *IEEE Transactions on Intelligent Transportation System*, 2010. Accepted with minor revision **(Impact factor: 2.844)**.
2. **G Yan**, S. Olariu, S. Salleh, "A Probabilistic Routing Protocol in VANET," *International Journal of Mobile Computing and Multimedia Communication*, IGI-Global, 2010.
3. **G. Yan**, S. Olariu, M. C. Weigle, "Providing Location Security in Vehicular Ad hoc Networks ", *IEEE Wireless Communication Magazine Special Issue On-The-Road Communications*, 16(6), pp. 48-53, 2009. **(Impact factor: 2.0)**.
4. **G. Yan**, S. Olariu, M. C. Weigle, "Providing VANET Security through Active Position Detection", *Computer Communications - Elsevier, Special Issue on Mobility Protocols for ITS/VANET*, 31(12):2883-2897, 2008. **(Impact factor: 0.884)**

Refereed Conference Publication Lists

Refereed Conference

5. **G. Yan**, S. Olariu, D. B. Rawat, "Provisioning Vehicular Ad hoc Networks with Quality of Service", in *Proceedings of The International Workshop on Wireless Sensor, Actuator and Robot Networks (WiSARN)*. Montreal, Canada, June 17, 2010.

6. **G. Yan**, S. Olariu and S. Salleh, "A Probabilistic Routing Protocol in VANET", in *Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia (MoMM2009)*, 14-16 December 2009, Kuala Lumpur, Malaysia.

7. **G. Yan**, M. C. Weigle and S. Olariu, "A Novel Parking Service Using Wireless Networks," In P*roceedings of the International 2009 IEEE International Conference on Service Operations, Logistics and Informatics (SOLI 2009)*, July 22 - 24, 2009, Chicago, IL, USA, **The Best Student Paper Award**.

8. **G. Yan**, S. Olariu, "An Efficient Geographic Location-based Security Mechanism for Vehicular Ad hoc Networks," In *Proceedings of the 2009 IEEE International Symposium on Trust, Security and Privacy for Pervasive Applications (TSP)*. Macau, October 12-14, 2009.

9. **G. Yan**, X. Chen, S. Olariu, "Providing VANET Position Integrity Through Filtering," In *Proceedings of the 12th International IEEE Conference on Intelligent Transportation Systems (ITSC2009)*. St. Louis, MO, USA. Accepted, October 3-7, 2009.

10. **G. Yan**, Y. Wang, M. C. Weigle, S. Olariu and K. Ibrahim, "WEHealth: A Secure and Privacy Preserving eHealth Using NOTICE," In *Proceedings of the IEEE International Conference on Wireless Access in Vehicular Environments (WAVE)*. Dearborn, 2008.

11. **G. Yan**, S. Olariu, M. C. Weigle and M. Abuelela, "SmartParking: A Secure and Intelligent Parking System Using NOTICE," In *Proceedings of the International IEEE Conference on Intelligent Transportation Systems (ITSC)*. Beijing, October 2008, pp. 569-574.

Selected Book Chapters

Book Chapters

12. **G. Yan**, K. Ibrahim and M. C. Weigle, "Vehicular Network Simulators," In *Vehicular Networks: From Theory to Practice*, S. Olariu and M. C. Weigle, Eds. Chapman & Hall/CRC, 2009.
13. **G. Yan**, S. El-Tawab, and D. B. Rawat, "Reliable Routing Protocols in VANETs," In *Advances in Vehicular Ad-Hoc Networks: Developments and Challenges*, Mohamed Watfa, Ed. IGI Global, 2009.
14. **G. Yan**, S. Olariu, D. B. Rawat, W. Yang, "E-Parking: A Electronic Parking Service Using Wireless Networks". in *E-Business Issues Challenges and Opportunities for SMEs: Driving Competitiveness*, M. Manuela Cruz-Cunha and João Eduardo Varajão, Eds, IGI Global, 2010.

Thank you!

References

Al-Fuqaha, A., & Al-Ibrahim, O. (2007).
Geo-encryption protocol for mobile networks.
Comput. Commun., *30*(11-12), 2510–2517.

Caussinus, H., & Ruiz, A. (1990).
Interesting projections of multidimensional data by means of generalized principal component analysis.
In X. XX (Ed.) *COMPSTAT 90*, (pp. 121–126). Physica-Verlag.

Denning, D., & MacDoran, P. (1996).
Location-based authentication: Grounding cyberspace for better security.
Computer Fraud and Security, *1996*(2), 12–16.

Douceur, J. (2002).
The sybil attack.
Lecture Notes in Computer Science: Revised Papers from the First International Workshop on Peer-to-Peer Systems, *2429*, 251–260.

Filzmoser, P. (2004).
A multivariate outlier detection method.
In *Proceedings of the Seventh International Conference on Computer Data Analysis and Modeling*, (pp. 18–22). Belarusian State University, Minsk.

Mahalanobis, P. C. (1936).
On the generalised distance in statistics.
In *Proceedings National Institute of Science, India*, vol. 2, (pp. 49–55).
URL `http://ir.isical.ac.in/dspace/handle/1/1268`