Keio University
1858
CALAMVS
GLADIO
FORTIOR

Anonymous Authentication Scheme Considering Privacy for Probe data collection

Masaaki SATO, PhD
Assistant Professor, KEIO University
Graduate school of Media and Governance

Rie Shigetomi, Michiko Izumi,

Keisuke Uehara, and Jun Murai

Contents

This research is a summary of the result of the project done by the support of the Ministry of Economy, Trade and Industry.

METI 経済産業省 Ministry of Economy, Trade and Industry

Background

- Since 1996, the InternetCAR Project have worked on connecting vehicles to the Internet and building a communication infrastructure.

- InternetCAR is not only test bed, “Give and Take” basis helps society, ITS new application.
  - ➔ Automobile has more than one hundred sensors.
  - ➔ If we can collect those data, useful information can be provided.
  - ➔ This kind of application is called as Probe Vehicle/Probe Car/Floating Car system(PVS)

- Frontline base is necessary in emergency situation.
  - ➔ Automobile can move, has battery, can bring heavy/large equipments/luggage.
  - ➔ “Communication” is most important capability.
  - ➔ InternetCAR become a “final home” in emergency/disaster situation.

What is Probe Vehicle Systems？

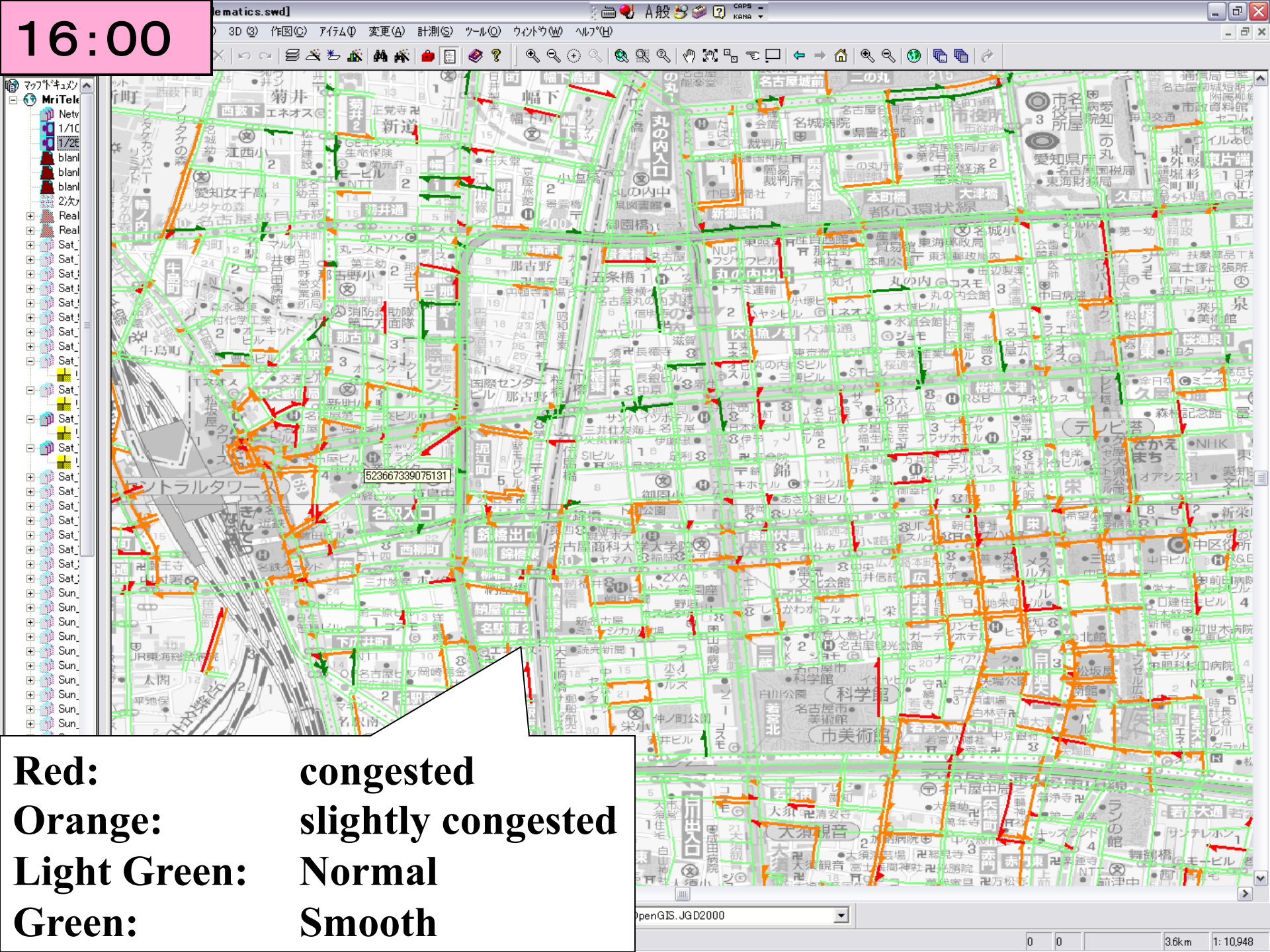
- Probe Vehicle Systems
  - Collects drivers' behavior and electronics signals which is normally used for vehicle control.

- The characteristic of Probe Information System is the two-way communication between centers and vehicles.
- Vehicles not only gains the information from centers but also provides the information from their own sensors.

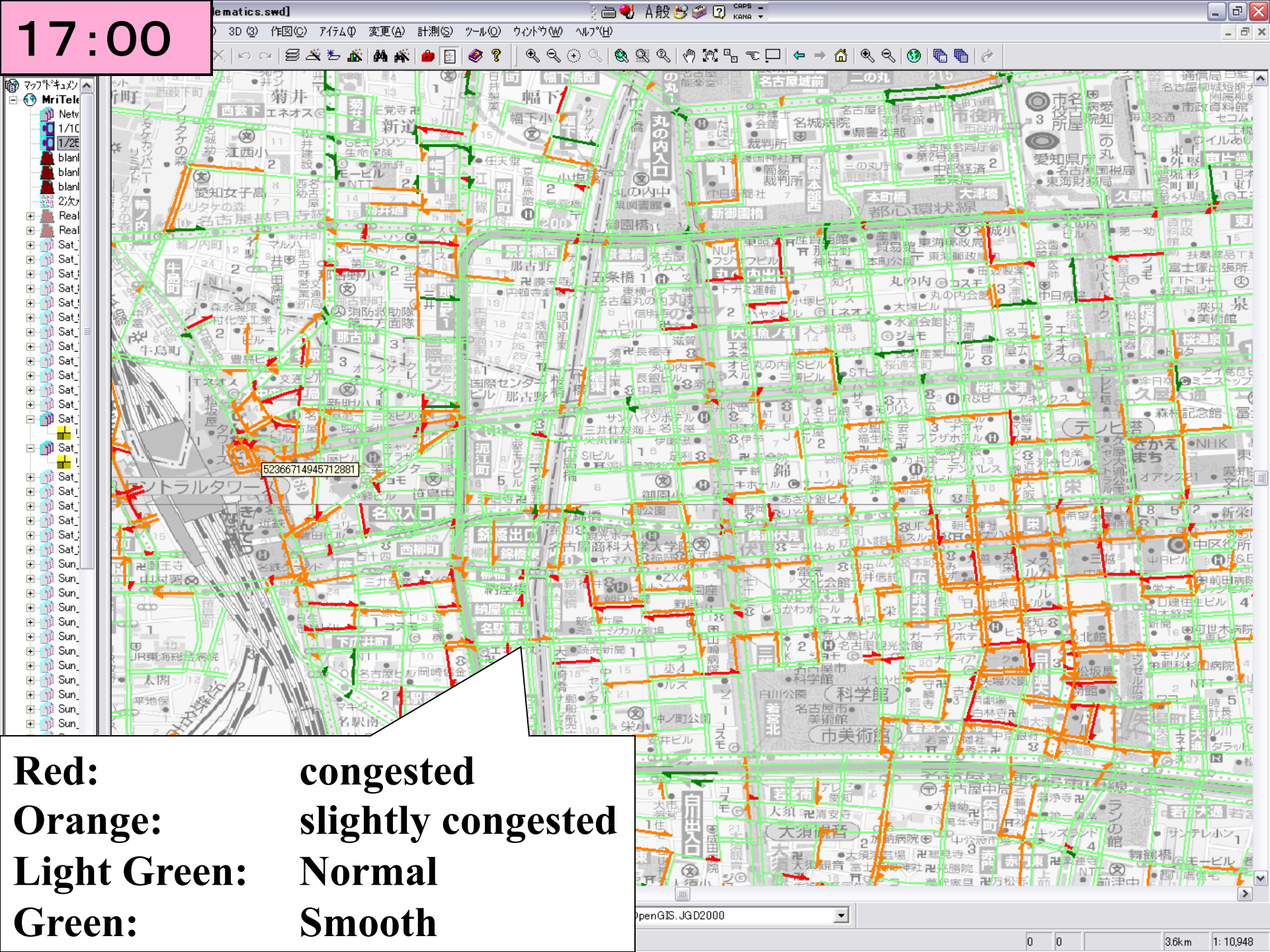
Service domain in PVS

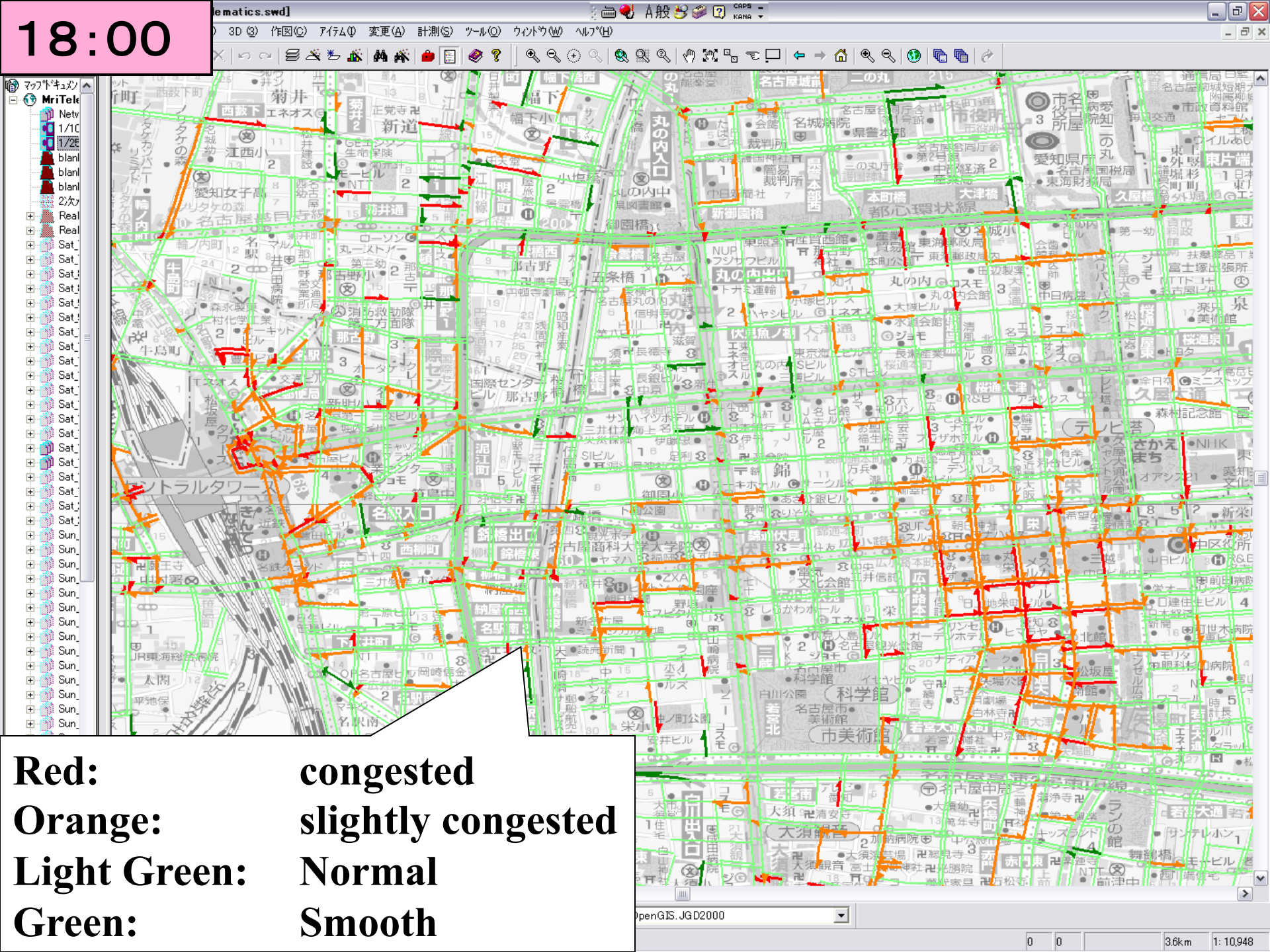
- **Various Services, Various Value**
  - **Driver/Passenger**
    - Driving Assist（Safety, Routing)
      - notification
        - » Congestion
        - » Road construction, detours
        - » Traffic accident
    - Contents download
      - Music, Movie, group Communication
    - Toll Management（Toll Gate, Drive-through）
    - Remote Diagnosis
      - Periodic Maintenance
      - Data is utilizable Vehicle development
  - **Traffic manager/Society**
    - Road maintenance
    - Taxi/bus management（location service）

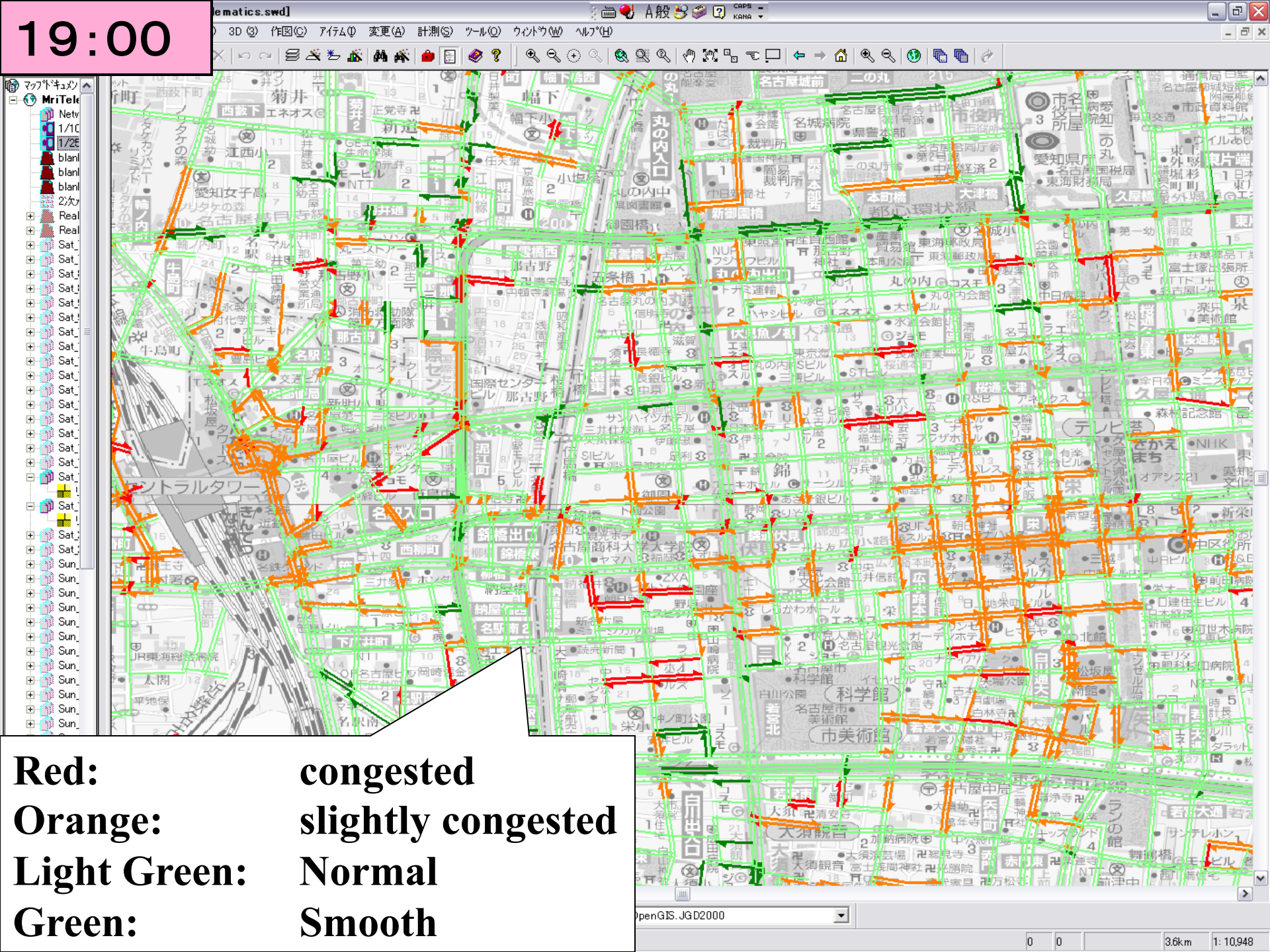
16:00

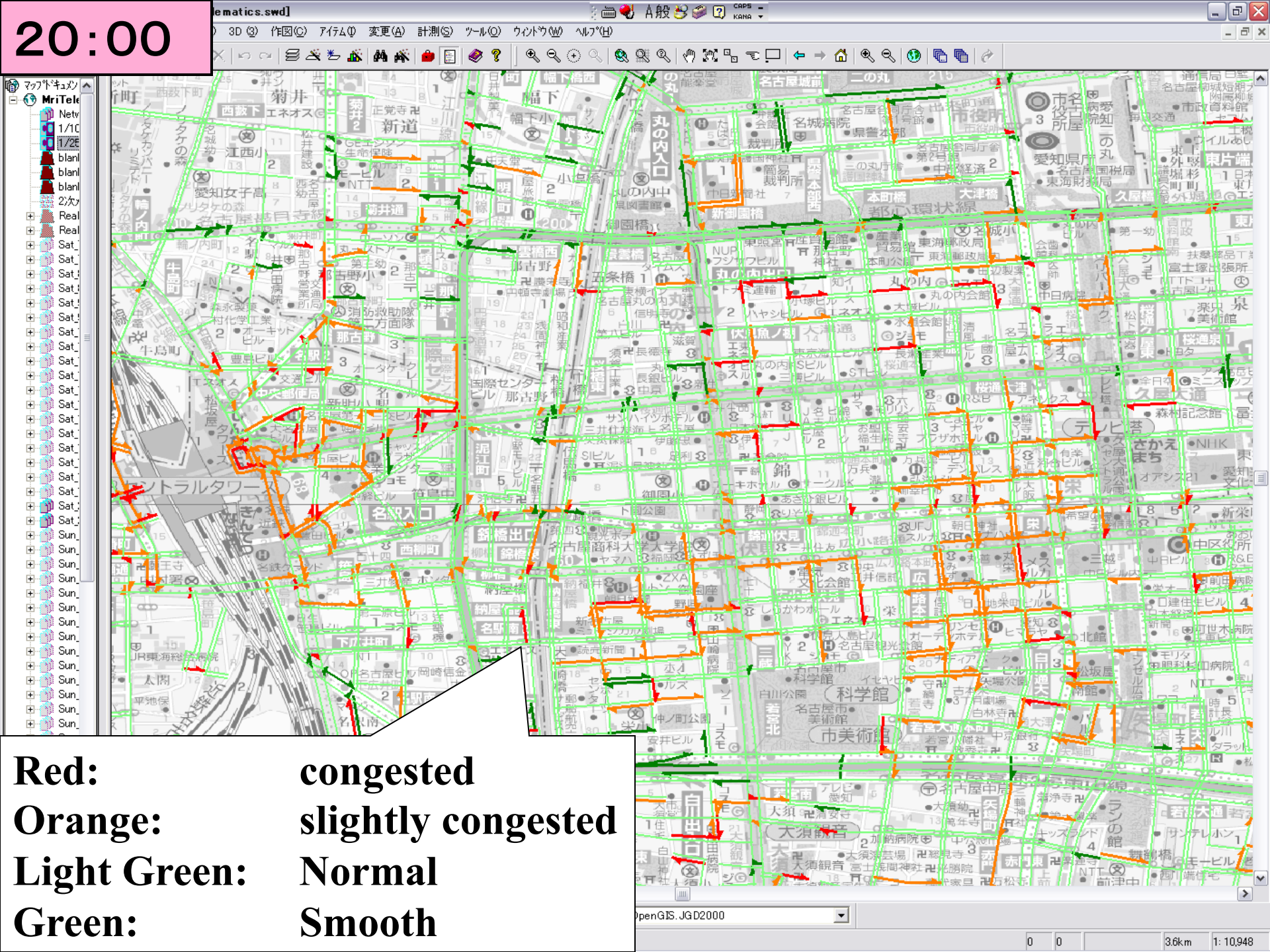


Red: congested
Orange: slightly congested
Light Green: Normal
Green: Smooth


17:00
Red: congested
Orange: slightly congested
Light Green: Normal
Green: Smooth

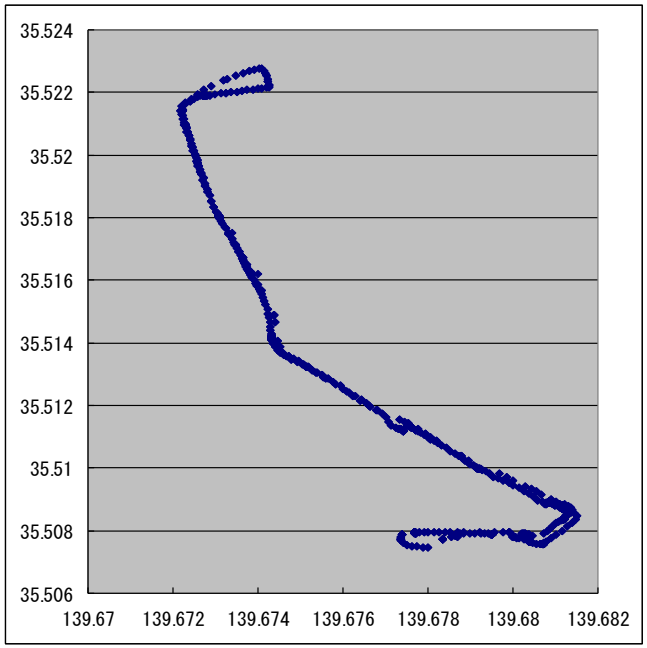

18:00
Red: congested
Orange: slightly congested
Light Green: Normal
Green: Smooth


19:00
Red: congested
Orange: slightly congested
Light Green: Normal
Green: Smooth


20:00
Red: congested
Orange: slightly congested
Light Green: Normal
Green: Smooth

Probe vehicle systems and personal data

- Probe data surely contains “Location” and “time” of transmitted vehicles.
- It may become personal data where the vehicle “existed”.
  - vehicle has a close relation to owner
  - excursion of Automobile as an activity history of owner
- It is necessary to relieve (owner’s) Uneasiness for deploy of probe vehicle information services.

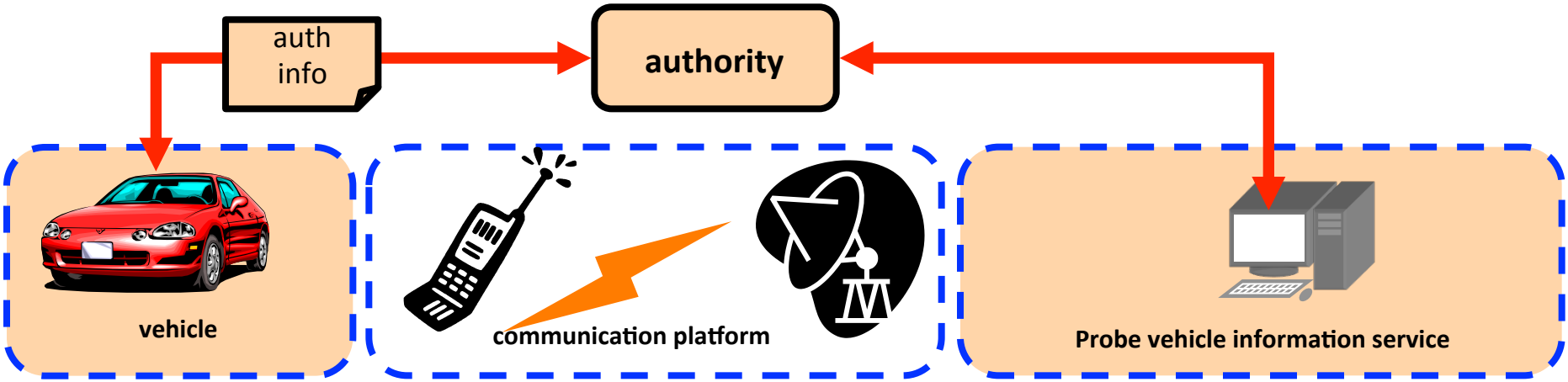


Issues :
Connection of the personal data and probe data

- Probe vehicle information service doesn't need the vehicle identification.
- Personal data might be handled in many different ways in probe vehicle information services.

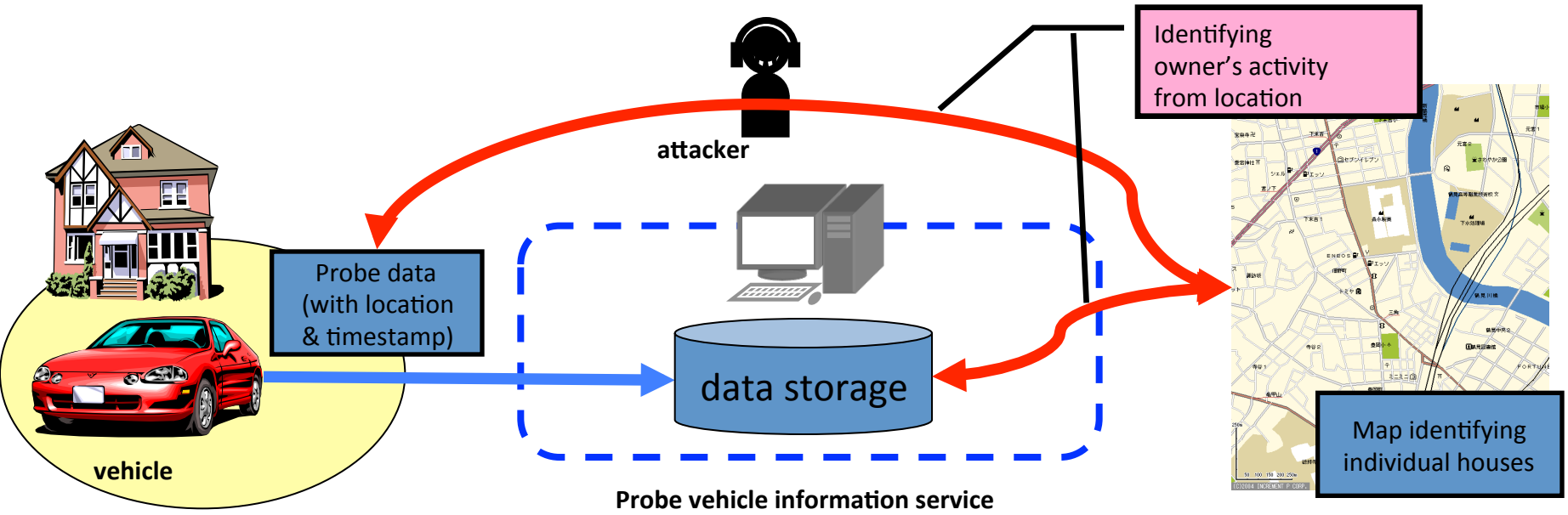
- When collecting probe data, probe vehicle service often uses personal data.
  - unique communication address
  - authentication information

- Probe data sender (Vehicle) cannot furnish probe data with complete peace of mind unless there is a rule to protect their personal data



Issues:
Probe data it is guessed that is personal data

- **All probe data has a timestamp and a location in probe data.**
- **There is possibility of identifying a particular vehicle on the basis of the nature of probe data and where it is collected.**
  - When probe data is collected from a vehicle on private property（ex. home）
  - When probe data is collected from a vehicle driving in an area where the number of vehicles is not sufficient to avoid identification.
- **Identifying a vehicle means the possibility of disclosure of personal data.**



Our objectives

- Probe vehicle systems **should be secure（from attack)**
- Probe vehicle systems **should protect personal data /privacy**

- We need…
  - Balance of Security and Privacy
  - Compatible method
  - Operational method
    - PDCA cicle
    - Security is a process, not a product (Bruce Schneier)

- The standard which can clarify the characteristic of a system is required.
  - Be measured (privacy/security metrics)

MOTIVATIONS

- In order to protect the privacy, a vehicle should not be identified by the collected data.
- for a measurement of the link travel time, the consecutive vehicle data are necessary.
- Therefore, it is necessary to have three following requirements for collection of probe data in consideration of privacy.

- **R-1: The data sender has can be confirmed without identifying the data sender.**
- **R-2: When a data sender sends multiplex probe data, the right of the data sender can be stopped by some kind of methods.**
- **R-3: The data sender's sameness is verified within the period permitted by the data sender without identifying the data sender.**

“Basic principles for personal data protection in probe vehicle information services”（ISO 24100）

- **Basic rules to be observed by service providers who handle personal data in probe vehicle information services.**
  - **This rule is aimed at protecting the personal data of probe data senders.**

- **The definition of the Basic principles in alignment with the framework of the OECD guideline for personal data protection.**
  - the OECD Council in 1980 concerning guidelines governing the protection of privacy and trans-border flows of personal data

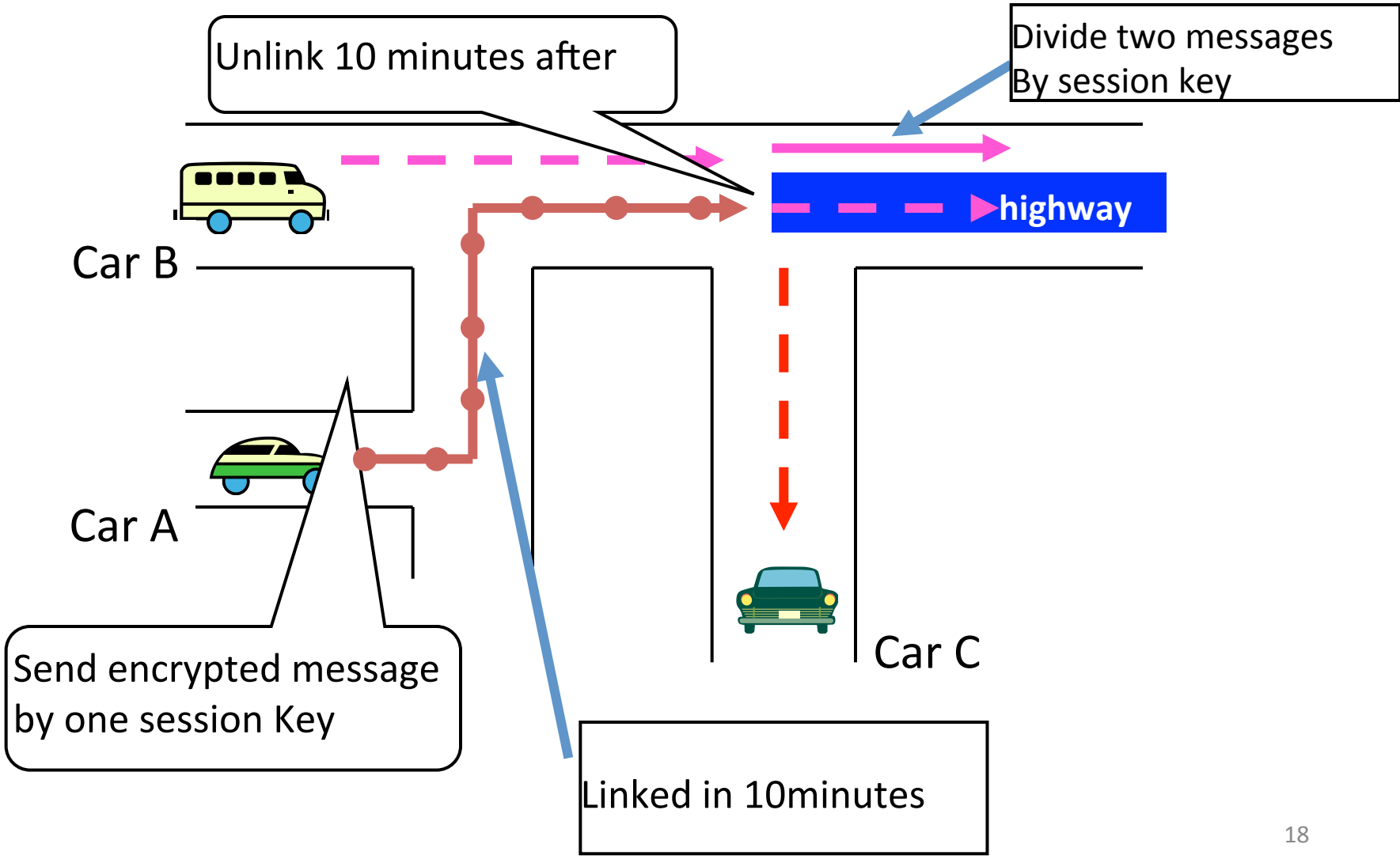
Approach : Anonymous Authentication

- Anonymity & Traceability
  - For privacy protection, one solution is to use a kind of random code.
  - The driver's privacy is protected using random code, therefore could not be "traced".
  - the driver could never be traced, even if it is required.
  - As a method to satisfy "Traceability", there is a proposed an Anonymous Authentication scheme such as various anonymous credential schemes based on cryptography.

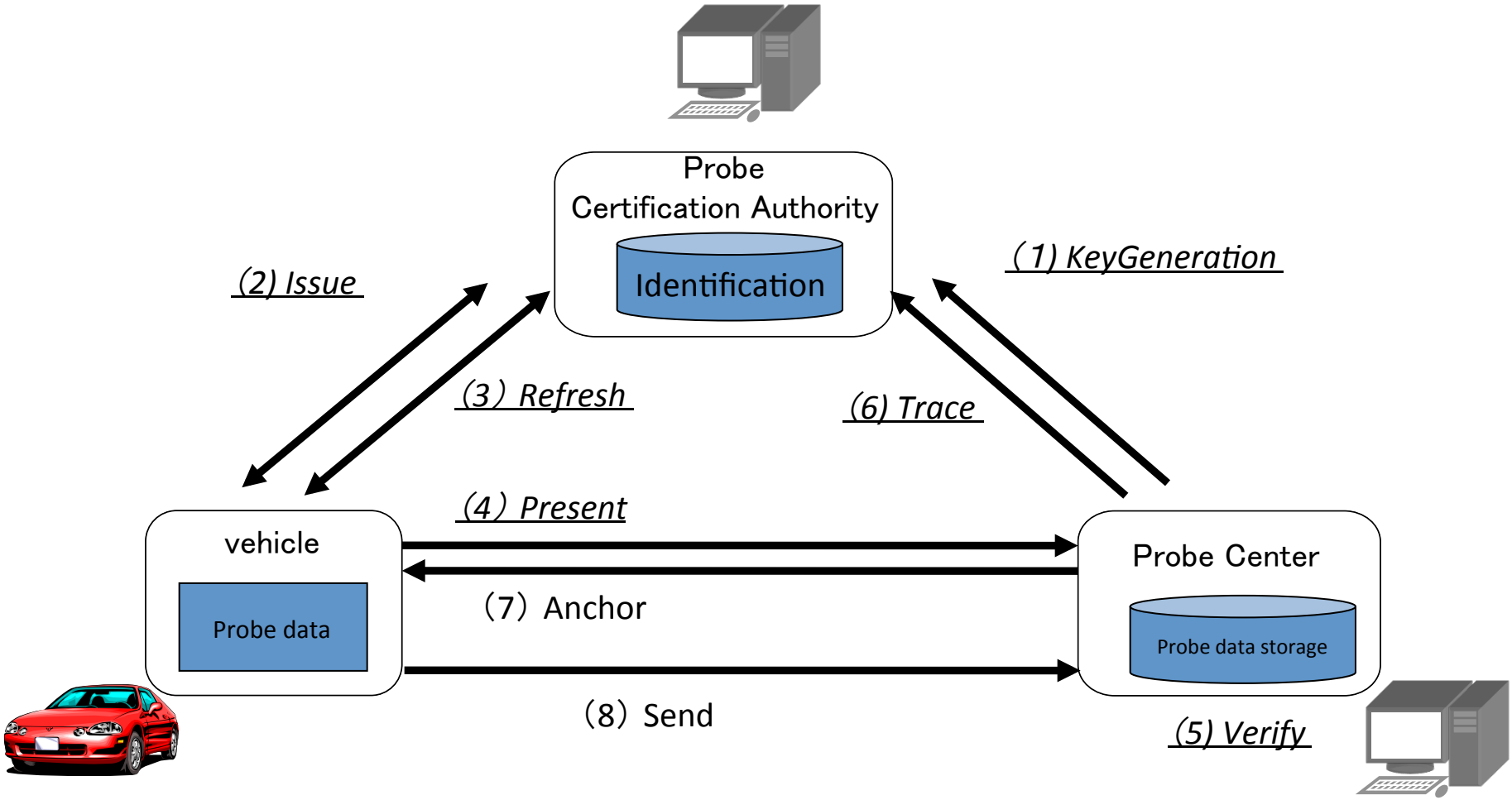
- "Unlinkability" is perfect privacy protection for drivers
  - The Probe Vehicle System needs consecutive data group for high quality service, especially measurement of the link travel time.
  - On the other hand, usual anonymous authentication protocols tend to consume both heavily for the Probe Vehicle System, because the computational and network resource on vehicle are limited.
  - The anonymity has been achieved by empirical methods based on the senses and the people.

- Anonymous Authentication Scheme for Probe Vehicle Systems
  - When the user is authenticated by anonymous authentication to the service provider, the user and the service provider share a common one-time key for these transactions. Our scheme allows also that a user and a service provider are able to choose to permit linking of transactions during a limited period or the number of times.

Over View

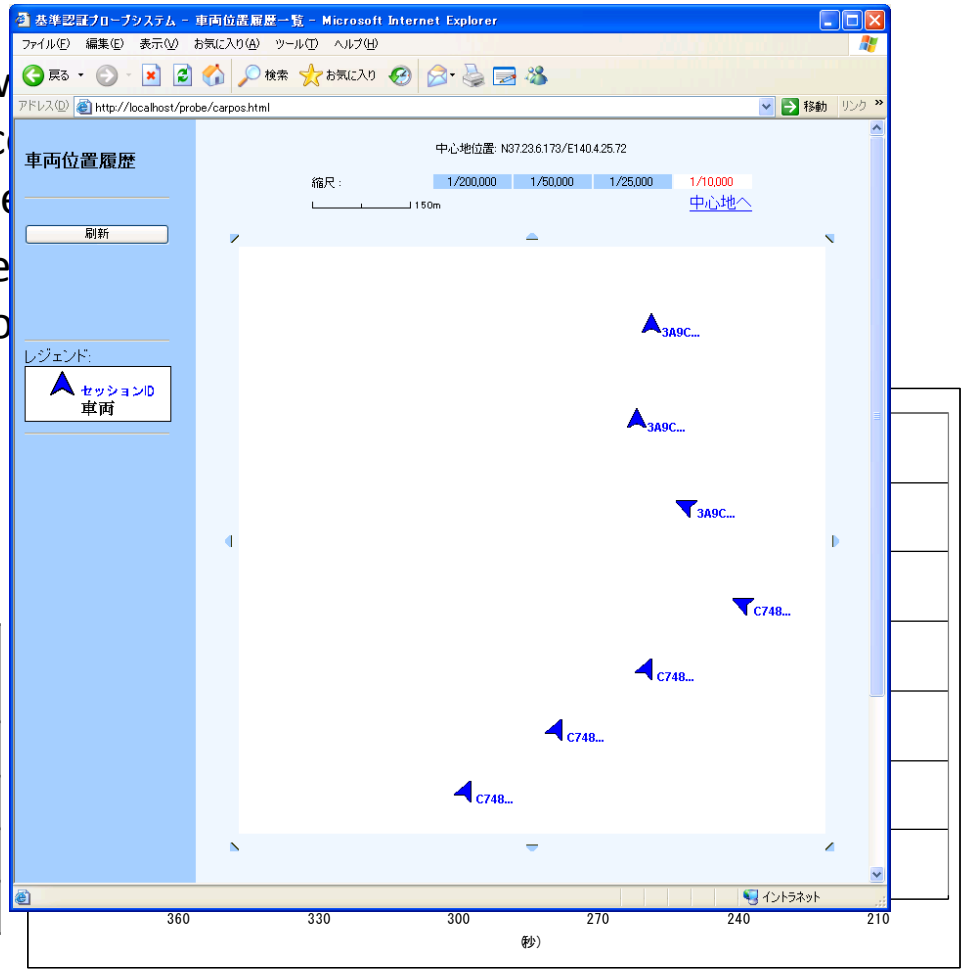

Unlink 10 minutes after
Divide two messages
By session key
highway
Car B
Car A
Car C
Send encrypted message
by one session Key
Linked in 10minutes

Solution:
Anonymous Authentication Scheme



Verification & Evaluation

- Verify testbed
  - 5,000 vehicle emulator/ Vehicle send a probe data each 1sec
- Processing cost
  - CPU utilization changed in the place v
    set at 210 seconds exceeding 90 perc
    to the Probe Certification Authority se
  - it is thought that it is one index in the
    it assumes the probe data of per seco
    seconds when the token processing



Interval (sec)	Issues (msec)	Refresh (msec)	Verify (msec)	CPU Load ave.
300	334	**999**	62	60%
270	360	**5,454**	79	75%
240	408	6,180	90	80%
210	443	6,548	113	90%

Conclusion

- proposed a new anonymous authentication scheme for developing the Probe Vehicle System considering the privacy.

- designed and implemented the proposal scheme to evaluate the effectiveness, and evaluated the proposed scheme by the experiment in the environment of 5,000 scales with a probe vehicle simulator.

- As a result, it was able to be confirmed to achieve the collection of the probe data by which the proposed scheme partially had Linkability while protecting privacy, and showed that proposed scheme is efficient enough for real deploy.

- As a future work, it is necessary to examine the following parts.
  - Optimization of token update processing
  - Decentralization/Distribution of the Probe Certification Authority function

Thank you for your kind attention