Approaching Privacy in ITS

Caitlin Cottrill
IGERT Seminar
21 March 2007
Overview

• Background
• Emerging Issues
• Current Practice
• Recent Approaches
• Next Steps
Approaches to Traffic Forecasting/Modeling

• Static:
  – Travel surveys (on-boards and household)
  – Historical data

• Dynamic:
  – GPS
  – Road sensors (inductive loop detectors, etc.)
Emerging Method

• Combined Static/Dynamic approach:
  – More consistent and accurate trip reporting;
  – More accurate reporting of non-auto trips;
  – Data gathered on specific routes; and
  – Ability to compare real-time data to historic data to ensure reliability.
Emerging Privacy Issues

• Though privacy may be maintained at the individual levels (survey or GPS) in the combined approach, this does not ensure that combined data will maintain expected levels of confidentiality.
• With additional data mining and data linkages (ex. Census), it may be possible to more clearly identify individual travelers or households.
Current Practices in Privacy Protection

• Census: Title 13
  – Requires that “any information collected from the public under the authority of Title 13 be maintained as confidential”
  • Suppression
  • Data swapping
  • Protection of microdata files
Current Practices in Privacy Protection (cont.)

• ITSA Fair Information and Privacy Principles
  – Advisory policy adopted in 2001
  – Some key requirements:
    • Individual Centered
    • Relevant
    • Anonymity
    • Commercial or other secondary use
Some Recent Approaches to Addressing Privacy in ITS

• Traffic monitoring with probe vehicles (Hoh, et al.):
  – Issue:
    • Maintain both data integrity and privacy
  – Proposed solution:
    • Architecture assigns authentication of data and filtering to one entity and actual data analysis to a separate entity.
  – Remaining issues:
    • Depending upon the frequency of probe updates, a clustering analysis may still allow an individual’s home or other destination location to be determined.
Some Recent Approaches to Addressing Privacy in ITS

• Privacy Issues in Vehicular Ad Hoc Networks (Dötzer):
  – Issue:
    • Is identification necessary in VANETS, or only a guarantee that the sender is valid/trustworthy?
  – Proposed solution:
    • Utilize a trusted third party to store identities and map one or more pseudonyms and related credentials to each identity. When sending messages, the vehicle will send a pseudonym and credentials to be verified by the receiving entity.
  – Remaining issues:
    • How often would pseudonyms need to be changed to maintain privacy?
    • What are the data use restrictions on the trusted third party?
Some Recent Approaches to Addressing Privacy in ITS

• Adaptive privacy preserving authentication in vehicular networks (Sha, et al.):
  – Issue:
    • How can the level of privacy desired be specified by the user?
  – Proposed solution:
    • Utilization of an adaptive group-based protocol that is able to trade off the degree of privacy desired with necessary resource usage.
  – Remaining issues:
    • Accurately identifying the group size needed to ensure privacy.
    • Maintaining a reasonable balance between privacy and resource usage.
However…

• The methods explored above focus their efforts primarily on maintaining privacy within the mobile network.

• This still leaves the need to ensure that data archives will maintain privacy standards, even when linked with data from travel surveys or the Census.
Next Steps for Future Research

• Work towards developing methods for ensuring that privacy is maintained when linking data sources through a combined approach to travel modeling and forecasting.

• Work towards establishing a data model that addresses privacy needs at the user, technology, and policy/political levels.
“If ITS systems are developed and deployed which do not respect the privacy of the American driver, there is a good chance that Americans will demand that the system be shut off. Without strong privacy provisions, ITS will not succeed.”

– S. Garfinkel. “Why driver privacy must be a part of ITS.” 1996.