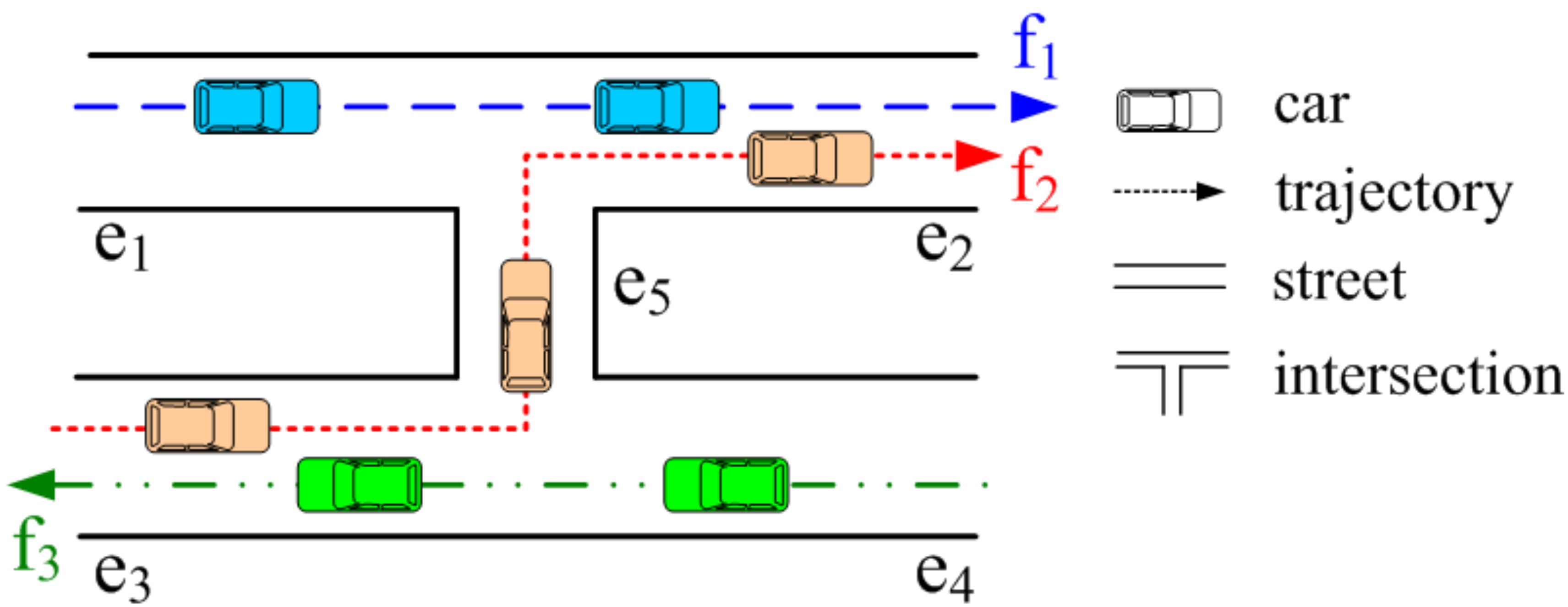
On the RSU-based Secure Distinguishability Among Vehicular Flows

Wei Chang*, Huanyang Zheng[Δ], and Jie Wu[Δ]
* Department of Computer Science, Saint Joseph's University, USA
[Δ] Department of CIS, Temple University, USA

Introduction

- Future Smart Cities
  - Static roadside sensors
  - Moving vehicles
- Vehicular data is a continuous observation along the vehicle's trajectory.
- Multiple Applications:
  - Crime scene reconstruction
  - Smart traffic flow monitoring
  - Environmental monitoring

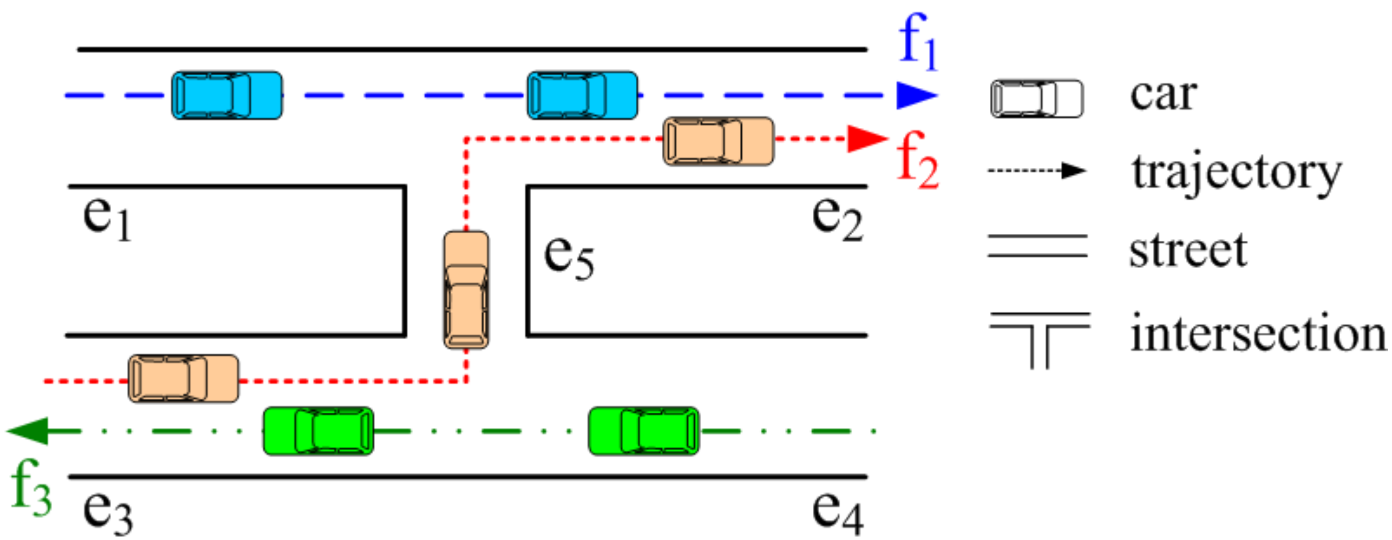
Introduction: motivation example



- How can we guarantee that the claimed data indeed comes from a car in vehicular flow f2 rather than flows f1 or f3?

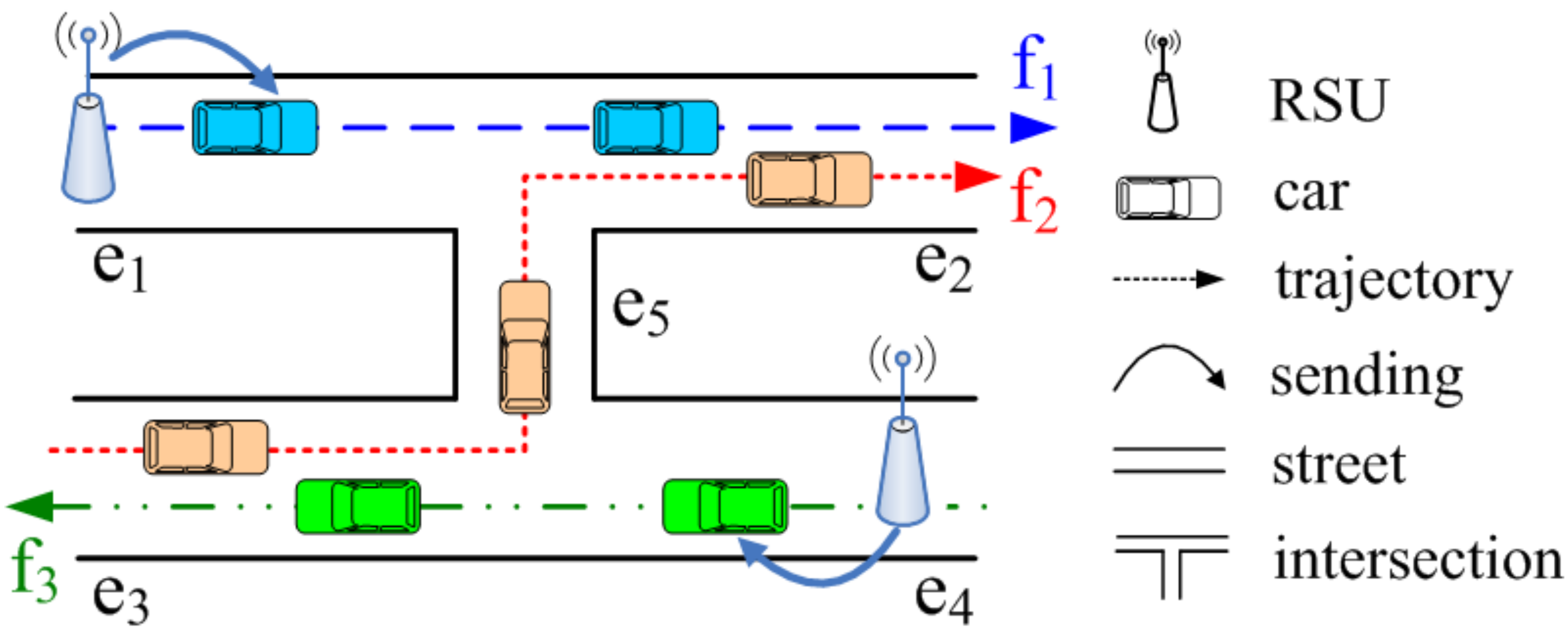
Attack Model

- Attackers are non-cooperative.
- Attacking goal:
  - An attacker, who was driving along vehicular flow *f'*, tries to pretend that he was in flow *f*.



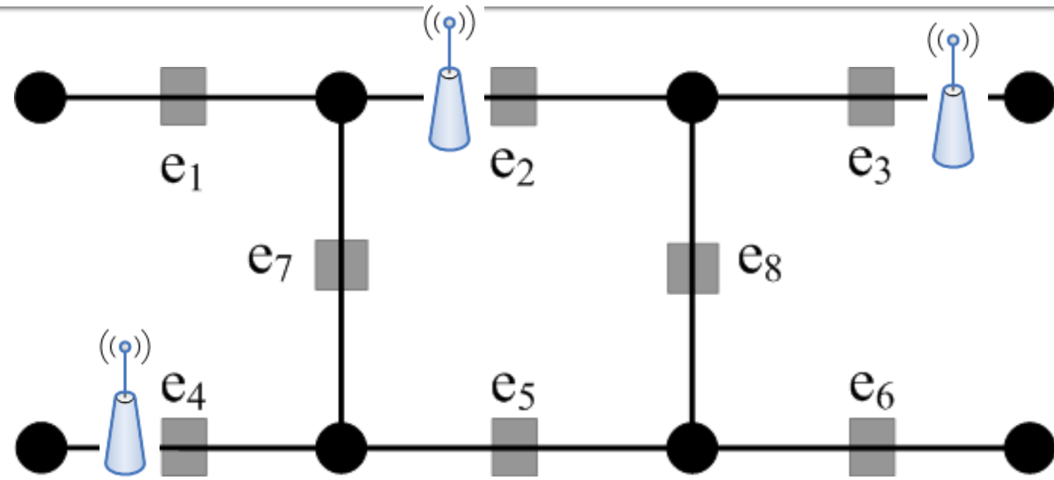
Introduction: RSU-based location proofs for vehicular trajectory data

- A RoadSide Unit (RSU) is a typical infrastructure widely adopted in smart cities.



RSU Placement Requirements

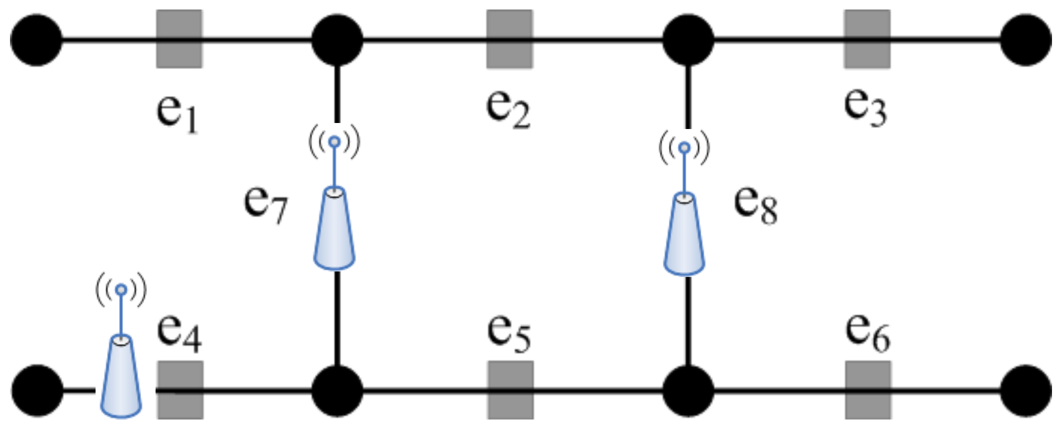
- Distinguishability: the set of bypassed RSUs is unique for each flow



ID	six given vehicle flows	S_1
f_1	$e_1 \to e_7 \to e_5 \to e_6$	$\emptyset$
f_2	$e_4 \to e_5 \to e_6$	e_4
f_3	$e_4 \to e_5 \to e_8 \to e_3$	e_3, e_4
f_4	$e_1 \to e_2 \to e_8 \to e_6$	e_2
f_5	$e_1 \to e_7 \to e_5 \to e_8 \to e_3$	e_3
f_6	$e_4 \to e_7 \to e_2 \to e_3$	e_2, e_3

RSU Placement Requirements

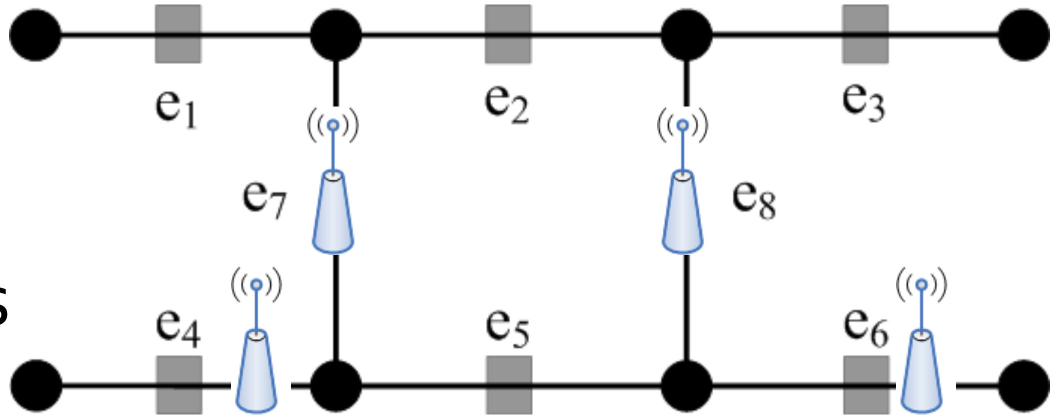
- Distinguishability
- Coverage: Each flow goes through at least one RSU



ID	six given vehicle flows	S_1	S_2
f_1	$e_1 \rightarrow e_7 \rightarrow e_5 \rightarrow e_6$	$\emptyset$	e_7
f_2	$e_4 \rightarrow e_5 \rightarrow e_6$	e_4	e_4
f_3	$e_4 \rightarrow e_5 \rightarrow e_8 \rightarrow e_3$	e_3, e_4	e_4, e_8
f_4	$e_1 \rightarrow e_2 \rightarrow e_8 \rightarrow e_6$	e_2	e_8
f_5	$e_1 \rightarrow e_7 \rightarrow e_5 \rightarrow e_8 \rightarrow e_3$	e_3	e_7, e_8
f_6	$e_4 \rightarrow e_7 \rightarrow e_2 \rightarrow e_3$	e_2, e_3	e_4, e_7

RSU Placement Requirements

- Securely distinguishable: the set of bypassed RSUs is not the subset of others



ID	six given vehicle flows	S_1	S_2	S_3
f_1	$e_1 \to e_7 \to e_5 \to e_6$	$\emptyset$	e_7	e_6, e_7
f_2	$e_4 \to e_5 \to e_6$	e_4	e_4	e_4, e_6
f_3	$e_4 \to e_5 \to e_8 \to e_3$	e_3, e_4	e_4, e_8	e_4, e_8
f_4	$e_1 \to e_2 \to e_8 \to e_6$	e_2	e_8	e_6, e_8
f_5	$e_1 \to e_7 \to e_5 \to e_8 \to e_3$	e_3	e_7, e_8	e_7, e_8
f_6	$e_4 \to e_7 \to e_2 \to e_3$	e_2, e_3	e_4, e_7	e_4, e_7

Model and Formulation

- Graph G = (V, E)
- V: street intersections, and E: streets
- F = $\{f_1, f_2, \ldots, f_n\}$ is a set of n known traffic flows on G (assume no sub-flow relation)
- S is a subset of E on which RSUs are placed
- S(f) is a subset of S that covers f

- Objective is minimizing the number of RSUs
  Secure Distinguishability

Formulation

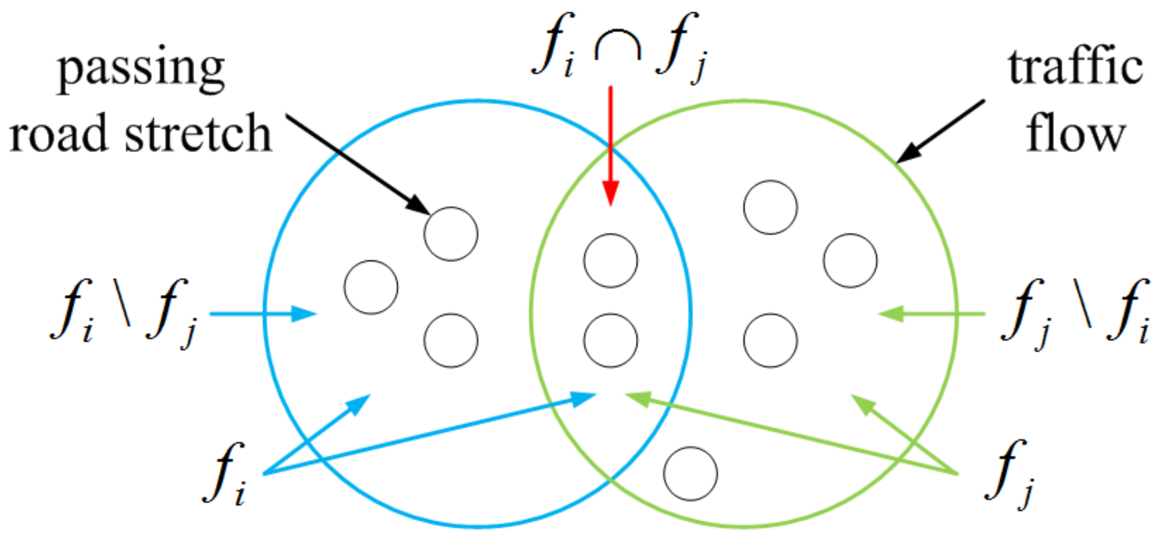
- Objective is minimizing the number of RSUs
  Secure Distinguishability (SD)

- minimize $|S|$ (# of RSUs)
- s.t. $S(f) \not\subseteq S(f')$ for $\forall f, f' \in F$ (SD)

- $S(f) \not\subseteq S(f')$ for $\forall f, f' \in F$ also guarantees:
  - $S(f) \neq S(f')$ for $f \neq f'$ (full distinguishability)
  - $S(f) \neq \emptyset$ for $\forall f \in F$ (full coverage)

Problem Analysis

- minimize $|S|$
- s.t. $S(f) \not\subseteq S(f')$ for $\forall f, f' \in F$



- To securely distinguish an arbitrary pair of traffic flows (f_i and f_j), two RSUs should be placed on street from two subsets of $f_i \setminus f_j$ and $f_j \setminus f_i$, respectively.
- The optimal RSU placement is NP-hard and monotonic, but non-submodular.

Greedy Algorithm

- Initialize S = ∅
- **for** each pair of traffic flows, f_i and f_j do
  - Generate distinguishing sets, $f_i \backslash f_j$ and $f_j \backslash f_i$
- **while** there exists a distinguishing set **do**
  - Update *S* to place an RSU that hits max # of distinguishing sets, remove corresponding sets
- **Return S**

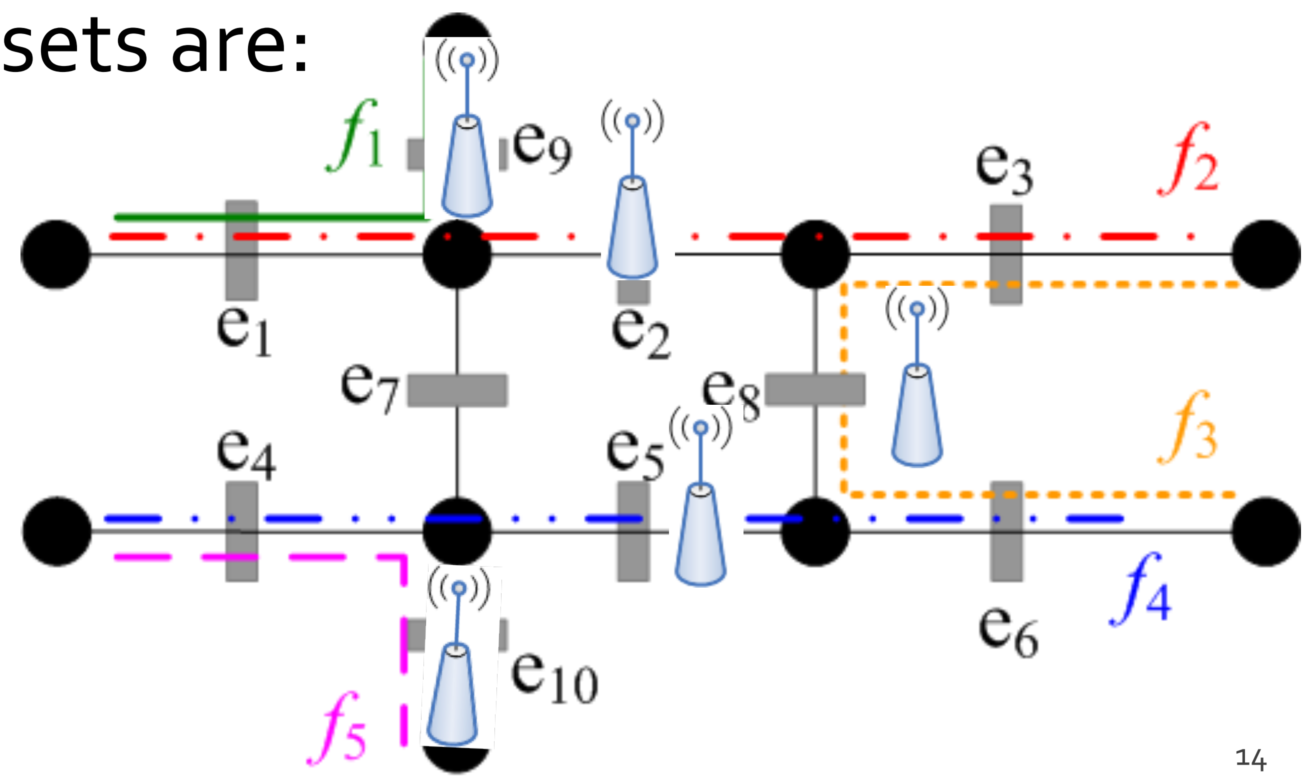
- It achieves a ratio of O(ln *n*) to the optimal algorithm for the number of placed RSUs.

Advanced Model: Propagated RSU Tags

- Some flows are less-important.
- Idea: propagate RSU tags from high-priority flows to low-priority flows, and use the propagated tags to achieve secure distinguishability.
- Let l denote the priority level of a flow f, and we require that the secure distinguishability of flows with priority l must be provided by the RSU-based credentials within l-hop.

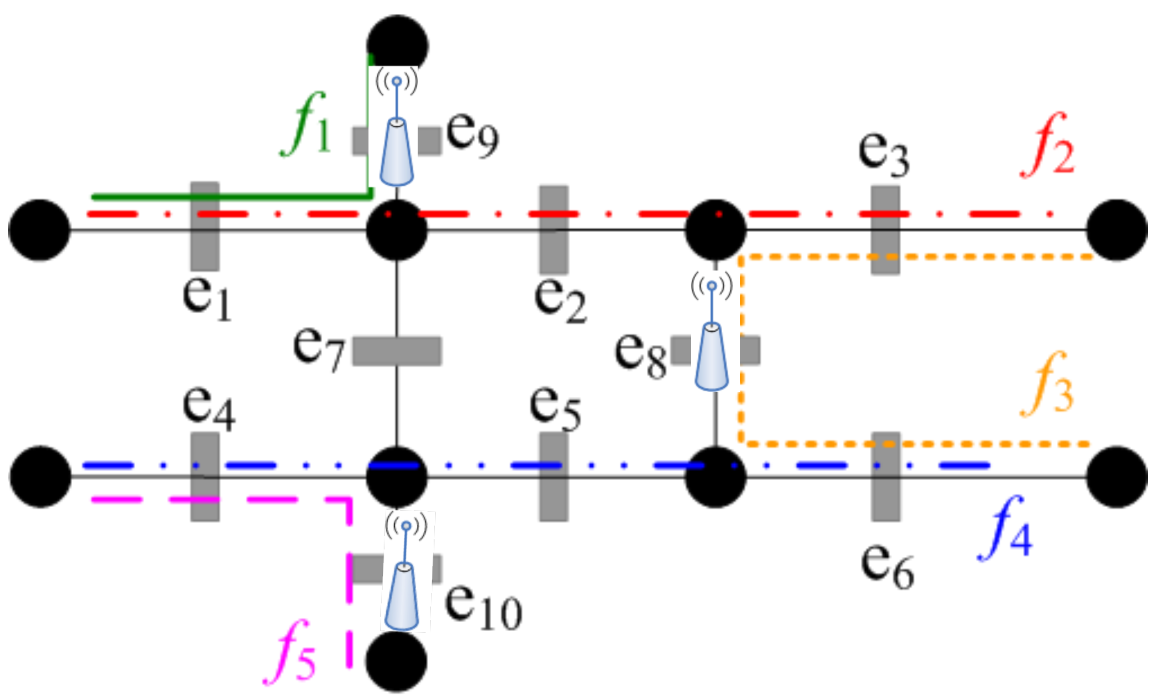
Advanced Model: Example

- According to the requirements of secure distinguishability, at least 5 RSUs are needed: $S = \{e_2, e_5, e_8, e_9, e_{10}\}$.
- Received tag sets are:
- $f1$: e_9
- $f2$: e_2
- $f3$: e_8
- $f4$: e_5
- $f5$: e_{10}



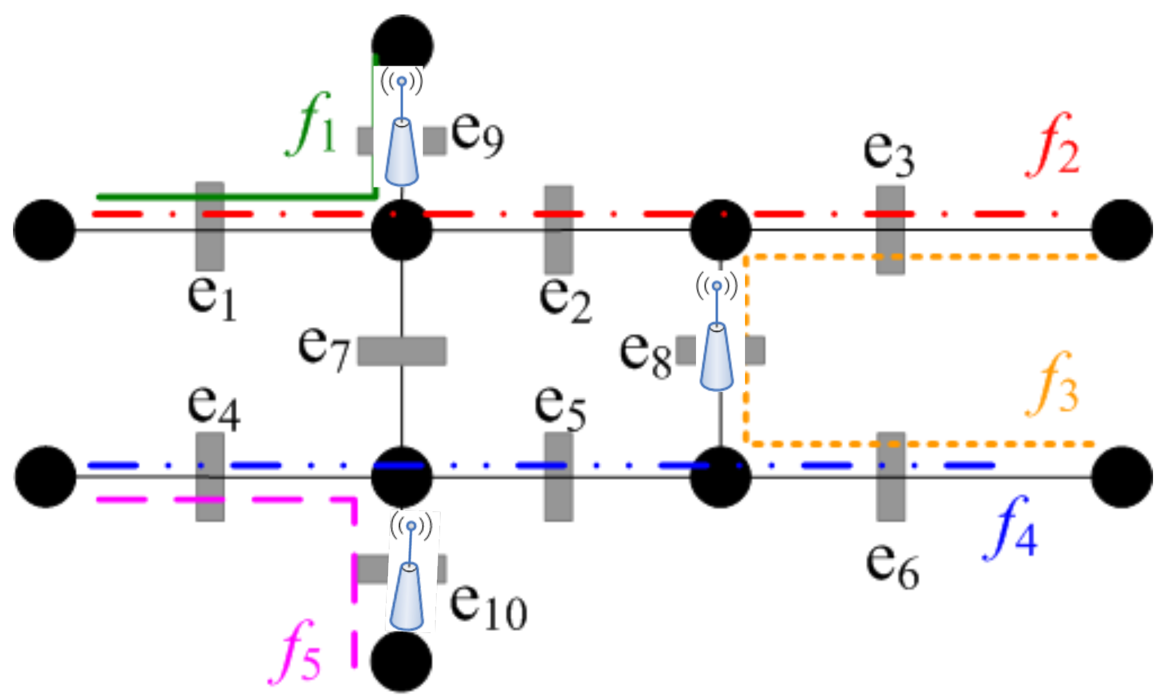
Advanced Model: Example

- Priority levels: $l_1 = l_3 = l_5 = 0$, $l_2 = l_4 = 1$, $l_{max} = 1$
- Placing 3 RSUs is enough: $S' = \{e_8, e_9, e_{10}\}$
- Received tag sets are:
- f_1: $\{e_9^{[0]}, e_9^{[1]}\}$
- f_2: $\{e_8^{[1]}, e_9^{[1]}\}$
- f_3: $\{e_8^{[0]}, e_8^{[1]}\}$
- f_4: $\{e_8^{[1]}, e_{10}^{[1]}\}$
- f_5: $\{e_{10}^{[0]}, e_{10}^{[1]}\}$



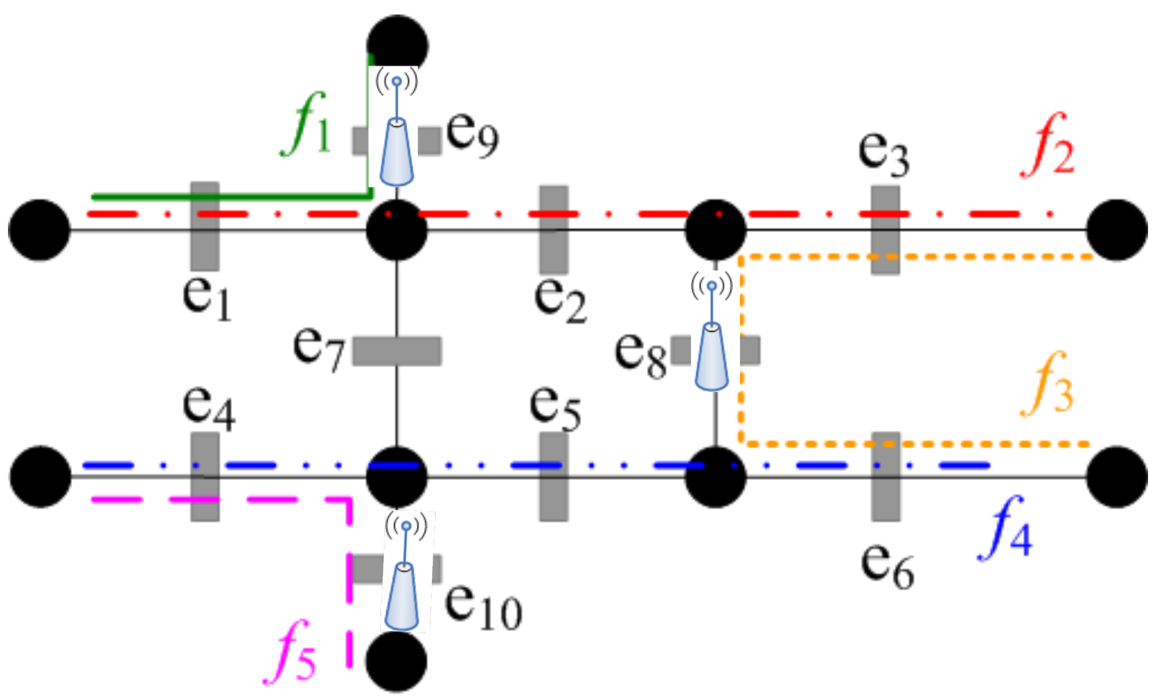
Advanced Model: Example

- Priority levels: $l_1 = l_3 = l_5 = 0$, $l_2 = l_4 = 1$, $l_{max} = 1$
- Placing 3 RSUs is enough: $S' = \{e_8, e_9, e_{10}\}$
- Received tag sets are:
- $f1$: $\{e_9^{[0]}, e_9^{[1]}\}$
- $f2$: $\{e_8^{[1]}, e_9^{[1]}\}$
- $f3$: $\{e_8^{[0]}, e_8^{[1]}\}$
- $f4$: $\{e_8^{[1]}, e_{10}^{[1]}\}$
- $f5$: $\{e_{10}^{[0]}, e_{10}^{[1]}\}$



Advanced Model: Example

- Priority levels: $l_1 = l_3 = l_5 = 0$, $l_2 = l_4 = 1$, $l_{max} = 1$
- Placing 3 RSUs is enough: $S' = \{e_8, e_9, e_{10}\}$
- Received tag sets are:
- $f1$: $\{e_9^{[0]}, e_9^{[1]}\}$
- $f2$: $\{e_8^{[1]}, e_9^{[1]}\}$
- $f3$: $\{e_8^{[0]}, e_8^{[1]}\}$
- $f4$: $\{e_8^{[1]}, e_{10}^{[1]}\}$
- $f5$: $\{e_{10}^{[0]}, e_{10}^{[1]}\}$



General Problem Formulation

- Objective is minimizing the number of RSUs the prob. of securely distinguishing f and f' is no less than a predefined threshold.

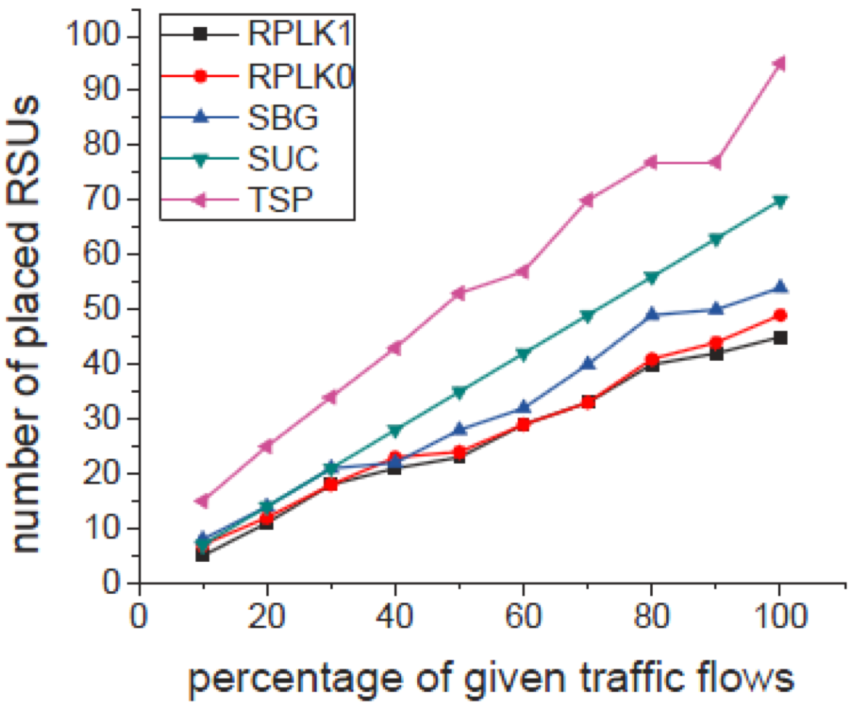
$$\begin{aligned} \min \quad & |S| \\ \text{s.t.} \quad & \mathbb{P}\{S^l(f_i) \not\subseteq S^l(f_j)\} \geq T(l_i, l_j) \text{ for } \forall f_i, f_j \in F \end{aligned}$$

Where $l = \max(l_i, l_j)$ and $S^l(f)$ represents all received tags within *l*-hop. $\mathbb{P}\{\cdot\}$ indicates the probability, and $T(l_i, l_j)$ gives the threshold.

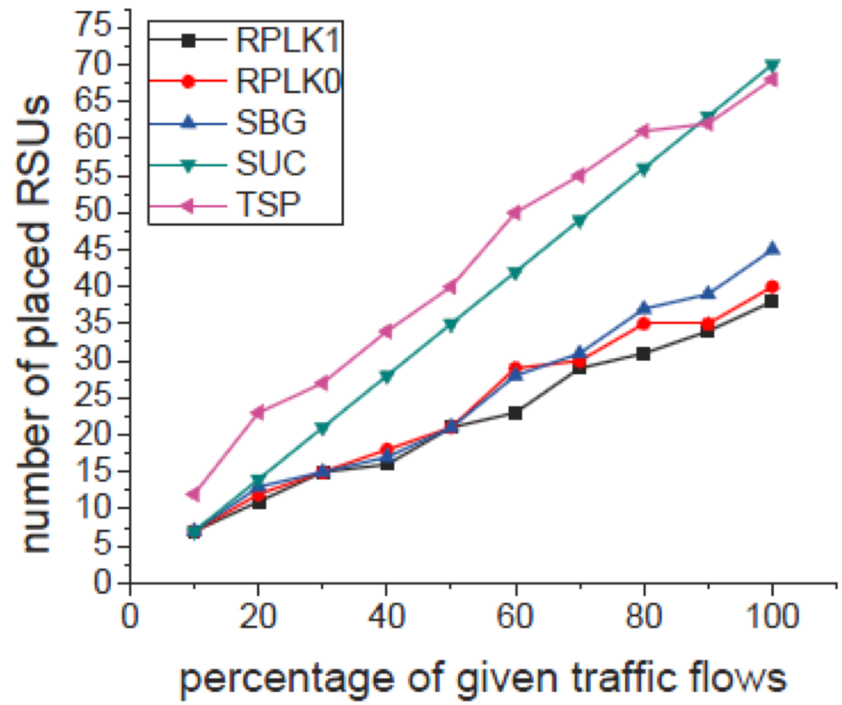
Algorithm for Advanced Model

- Initialize S = Ø
- **for** priority level l from l_{max} to l_{min}
  - **for** each pair of undistinguishable flows, f_i and f_j do
    - Generate distinguishing sets, $f_i \backslash f_j$ and $f_j \backslash f_i$ based on the potential RSU tags within l-hop
  - **while** there exists a distinguishing set **do**
    - Update S to place an RSU that hits max expected # of distinguishing sets, remove corresponding sets
- **Return S**

Experiments



Dublin bus trace



Seattle bus trace

Thank you.