Resilient Disaster Communications in the Social-Media Era

JUNO-2 Kick-off Meeting

October 25, 2018

K. K. Ramakrishnan

University of California, Riverside

Toru Hasegawa, Yuki Koizumi

Osaka University

Masakatsu Nishigaki, Tetsushi Ohki

Shizuoka University

Yoshinobu Kawabe

Aichi Institute of Technology

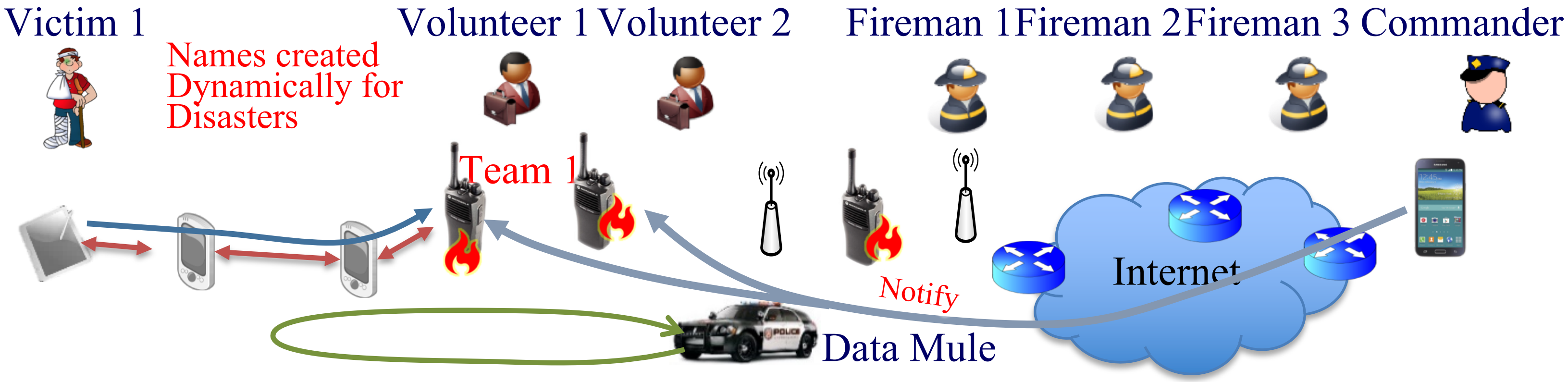
Importance of Communication for Disaster Management

- Communication is key to improving outcomes in the aftermath of a disaster
- Keys to an effective response to a catastrophic incident:
  - Effective communication within and among dynamically formed first responder teams
    - Public safety teams comprising: law enforcement, health, emergency, transport and other special services, depending on the nature and scale of the emergency
- First responders are not the only ones that can help. Increasingly, volunteers are playing a significant part in disaster management
- Lack of personnel to support emergency
- In the aftermath of a disaster, likely to face communication challenges
  - Infrastructure may be impacted
- Complement with social media with data communications: Security?

- Security and Resiliency are major concerns
- **Project Objective:** **A network architecture for information and communication resilience in disaster management that is also secure; integrate volunteers; include social media**

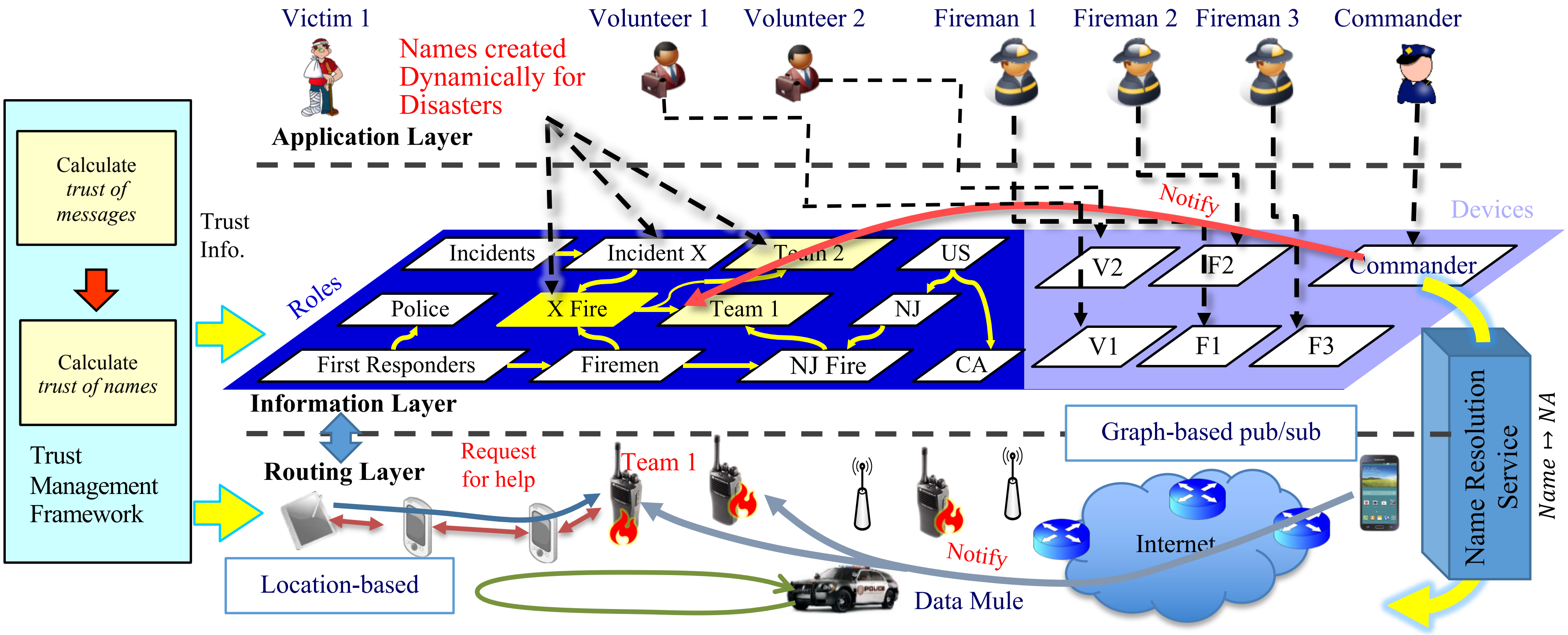
System Model and Assumptions

- Network Model
  - Enhanced Information Layer building on Information Centric Networking (ICN) concepts, with a Publish/Subscribe service
  - Multi-hop communication to allow communication even in fragmented networks, and disruptions
- Security Model
  - Honest Players: First responders and incident commander
  - Potentially Dishonest Players: Volunteers and Victims
    - No long term history/reputation available for use as basis of trust
- Safely manage information flow and support rescue efforts



Proposed System Architecture

- **Information Layer -** (Role-Based) Communication
  - Facilitate communication: dynamically formed first-responder teams
    - Communication based on dynamically created roles, not network locations
    - Include citizens, including victims and volunteers willing to help
- Secure and resilient; integrate social media communication into an Information Centric Networking (ICN) framewrork



Challenges

- Challenge 1: Designing a naming and forwarding framework in dynamic disaster environments, focusing on communication among honest first responders, and including trusted volunteers and victims

- Relationships among participants are dynamic and, often, transient

  - Task 1: Instantiation of namespace
    - Naming scheme for players in disasters
    - Graph-based naming scheme: Multi-rooted tree structure for representing multiple organizations

  - Task 2: Publish/Subscribe Framework and forwarding
    - Publish/Subscribe forwarding mechanism for graph-based name prefixes
    - Name prefix distribution to routers and participants

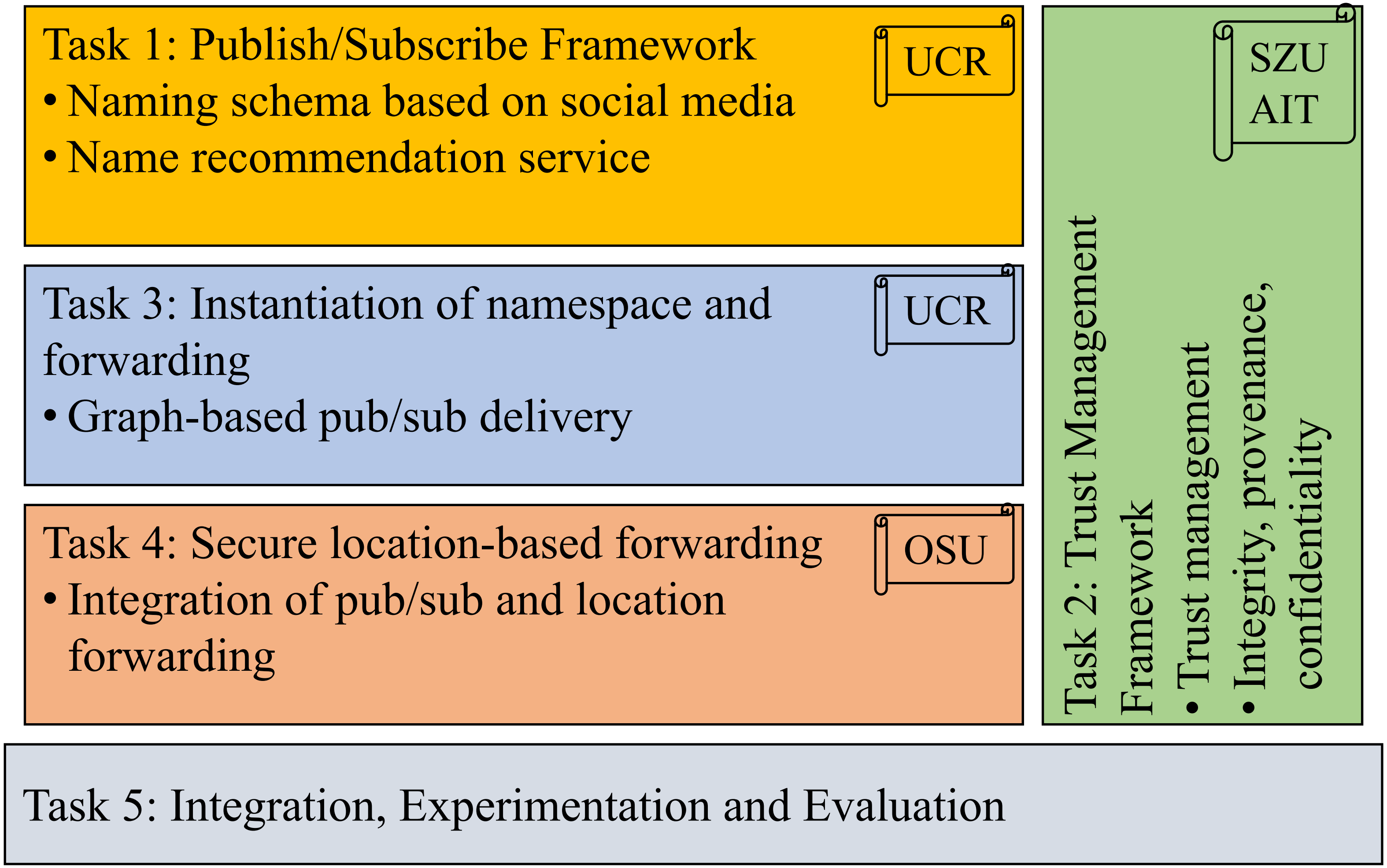
Challenges - continued

- Challenge 2: Security and resiliency against dishonest volunteers when the root of trust is lost

  - Task 3: Trust management
    - Managing trust of volunteers and victims without using any certification authority
    - Providing trust information, with first-responders choosing the method for secure communication

  - Task 4: Secure location-based forwarding
    - Protecting privacy (names) of first responders from volunteers
    - Extending the forwarding framework against malicious forwarders (volunteers) in ad-hoc and disruptive environments

Project Management



Task 1: Publish/Subscribe Framework

- Naming schema based on social media
- Name recommendation service

UCR

Task 3: Instantiation of namespace and forwarding

- Graph-based pub/sub delivery

UCR

Task 4: Secure location-based forwarding

- Integration of pub/sub and location forwarding

OSU

Task 2: Trust Management Framework

- Trust management
- Integrity, provenance, confidentiality

SZU
AIT

Task 5: Integration, Experimentation and Evaluation

UCR: University California, Riverside   OSU: Osaka University
SZU: Shizuoka University   AIT: Aichi Institute of Technology

Collaboration and Joint Research Efforts

- Build on long (6-7 year) history of collaboration among several members of the team
- Expect to have bi-weekly or monthly calls between PIs
  - Include students as and when progress is being shared and ensure all are in synch.
- Relatively frequent face-face meetings
  - Already had one face-face kick-off meeting in UC Riverside in Aug. 2018
  - Will meet here in Tokyo during this visit
- Where possible, have students from participating institutions visit for an extended period of time to enable closer sharing of artifacts, development of prototype.

Publish/Subscribe Framework

- Overview and Motivation
  - Delivering the messages to the right people (i.e., first responders dealing with the particular incident, and/or volunteers nearby that can help)

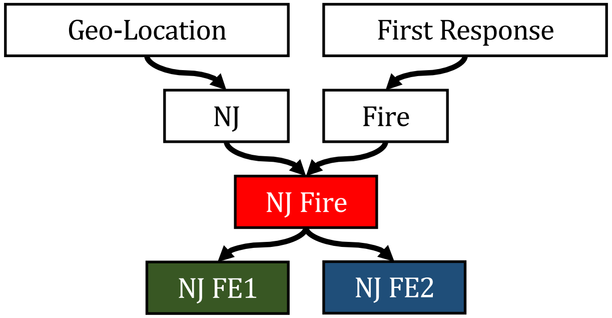
- Objective and Intellectual Merit
  - An information layer for disaster management and clearly integrating social media information so we can automate the dynamic matching among victims, first responders and volunteers in a secure and timely manner

- Research Challenge
  - A graph-based naming framework, so that the relationships come automatically from the social media data generated in calls for help in a real disaster
    - An acyclic directed graph that has multiple roots

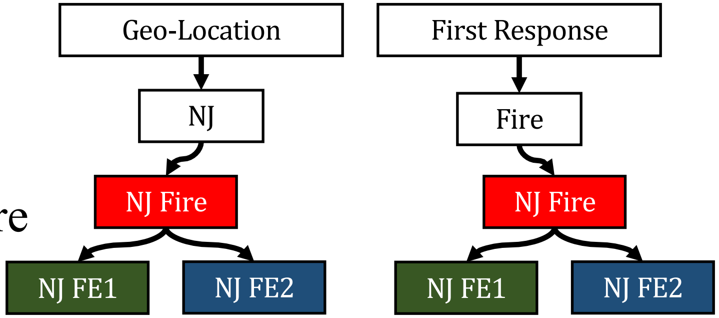
Namespace Design

- **Multi-dimensional**
  - E.g. `FireEngine1` has Time, Location and Department attributes (dimensions)
- **Graph structure**
  - More efficient than NDN-style strict hierarchy
- **Dynamic**
  - Edges (relations) pop in and out of existence
- **Publish/Subscribe service interface**
  - Support a publish/subscribe capability for users to share information
  - Multiple entities can publish to a name
  - Uses a shared multicast structure in network, using rendezvous points (RPs)

Graph Structure



Hierarchical Structure



Hierarchical names:

```
/Geo-Location/NJ/NJ Fire
/First Response/Fire/NJ Fire
/Geo-Location/NJ/NJ Fire/NJ FE1
/First Response/Fire/NJ Fire/ NJ FE1
/Geo-Location/NJ/NJ Fire/NJ FE2
/First Response/Fire/NJ Fire/ NJ FE2
```

Improve Efficiency of Disaster Management by Graph-based Namespace

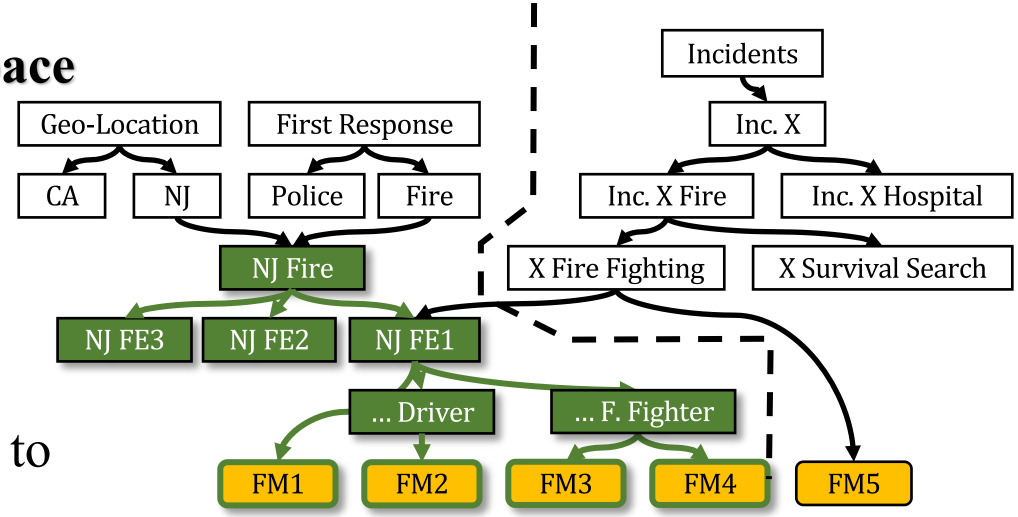
- Example namespace
  - Organizational structure: need information flow to members
    - Graph enables multiple dimensions (geo-location & functionality)
  - Incident place holder
- First responders instantiate roles
- Instantiate a disaster management template: preplanned namespaces
- Dispatch units to deal with functions in an incident
- Send messages to a role, e.g., “NJ Fire”

Need: Support a graph-based namespace in the network

Dynamic Nature of Namespace

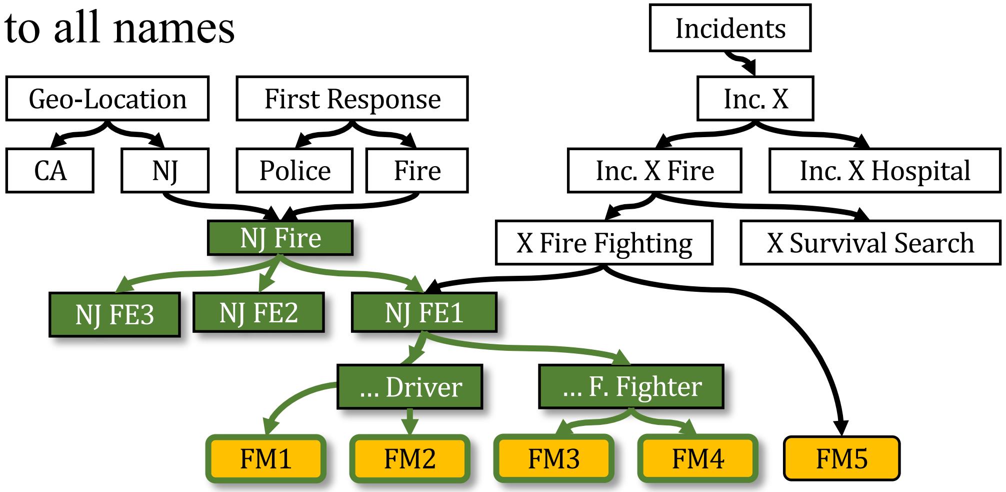
Dynamic installations of disaster namespaces

The namespace can evolve according to the situation



Supporting Graph-Pub/Sub in The Network

- Alternatives:
  - Perform BFS/DFS at each router
    - Benefit: fewer messages to be delivered
    - Issue: computation and storage cost at each router, infeasible, inefficient
  - Network only deals with flat names/ids (e.g., IP multicast, MF multicast & COPSS with flat names)
    - Subscribers subscribe to all names & publish to one
    - Subscribers subscribe to one & publish to all names



Solution: information layer to do the name expansion

Trust Management

- **Overview and Motivation**

  It is essential to introduce trust value in both the pub/sub forwarding framework (network layer) and the location-based forwarding framework (routing layer) to achieve completely trustful networking. Thus, the outcome of this task constitutes the basis of all the other tasks.

- **Objective and Intellectual Merit**

  An objective of this task is to add **"ephemeral trust"** to untrusted parties such as victims and volunteers and establish a trust chain originating from a first-responder.

- **Research Challenges**

  Our research challenge is to ensure the ephemeral trust of messages/participants in disaster situations.

  A key idea is to employ two types of information sources:

  - Verify consistency of multiple-messages in social media communications from volunteers/victims, and
  - A deterrence capability emphasized by their biometric information.

Solution

- **(i1) Assignment of ephemeral trust:**
  Social media messages reported from volunteers/victims may have some degree of uncertainty. Some volunteers/victims may even send false messages or non-urgent messages deliberately. We develop a scheme to evaluate the veracity of messages in a disaster situation.

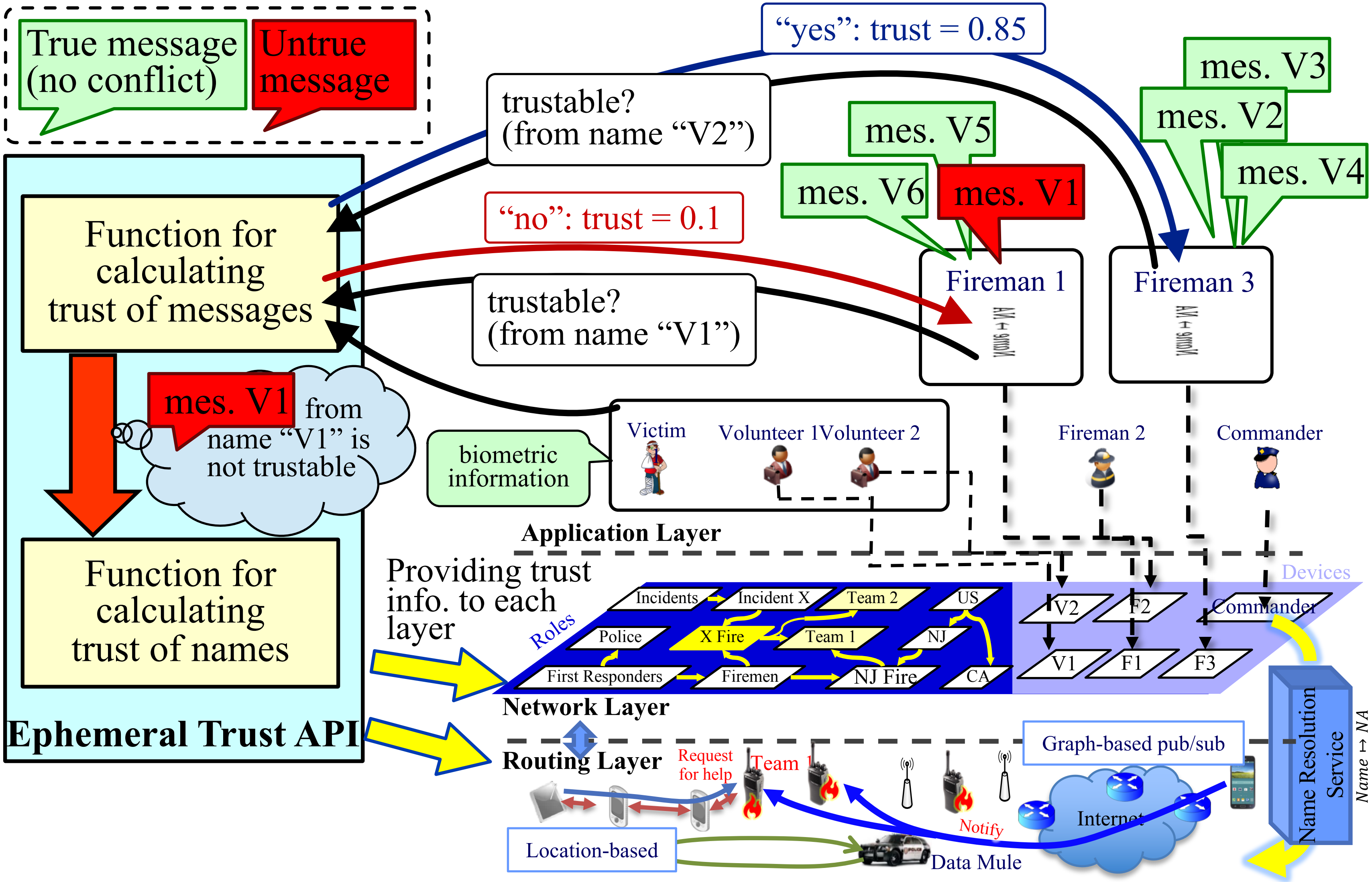
- **(i2) Trust value management of ephemeral trust:**
  A possible way to formulate the veracity of messages is a game-theoretic approach. The trust value of a participant/message is formalized by a utility function, and the sender of true messages is assigned a trust value as a reward.

- **(i3) Deterrence provided by biometrics:**
  We introduce a concept of **"deterrence-based trust"** in our ephemeral trust model. By using biometric signature, even when participants are completely alone and isolated, they can leave evidence (biometric signature) linked to their actions.

- **(i4) Development of trust API:**
  We develop a **"trust API"** which can be used not only for trustful/effective name resolution in pub/sub forwarding framework but also for trustful/effective route determiniation in location-based forwarding framework.

Trust Management - continued

- API



True message (no conflict)

Untrue message

Function for calculating trust of messages

mes. V1 from name "V1" is not trustable

Function for calculating trust of names

Ephemeral Trust API

trustable? (from name "V2")

"yes": trust = 0.85

"no": trust = 0.1

trustable? (from name "V1")

biometric information

Application Layer

Providing trust info. to each layer

Network Layer

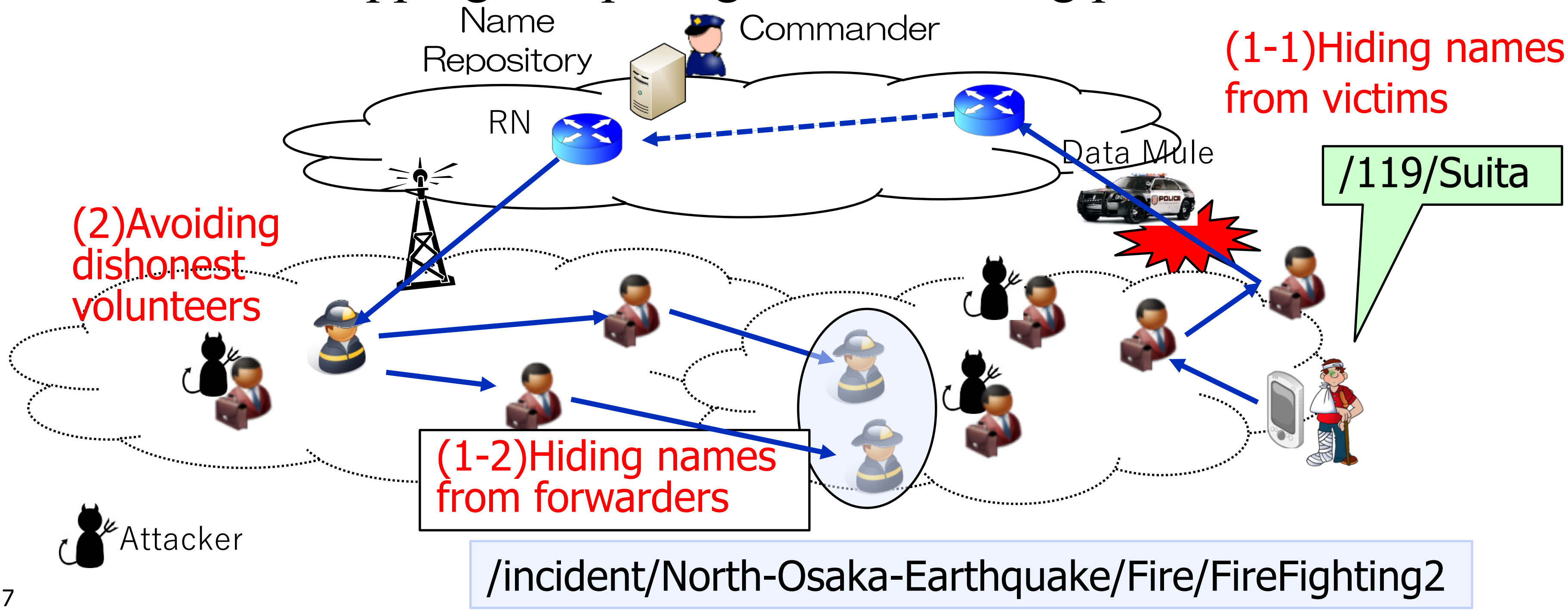
Routing Layer

Secure Location Based Forwarding

- Overview and Motivation
  - Secure and resilient forwarding between honest first responders and between honest first responders and a volunteer/victim in multi-hop environments, assuming that
    - Security
      - No certificate authority is reachable from first responders
      - Some volunteers as forwarders may be dishonest
    - Reachability
      - Network is fragmented, thus the Internet backbone may not be available
- Objective and Intellectual Merit
  - Securely deliver urgent messages from a victim to one of the nearest first-responders when central emergency offices are not reachable

Secure Location Based Forwarding - continued

- Research Challenges
  - (1)Privacy: Hiding first responders' names from victims and volunteers
  - (2)Security: Resiliency against dishonest volunteers: eavesdropping, tampering and discarding packets



(1-1)Hiding names from victims

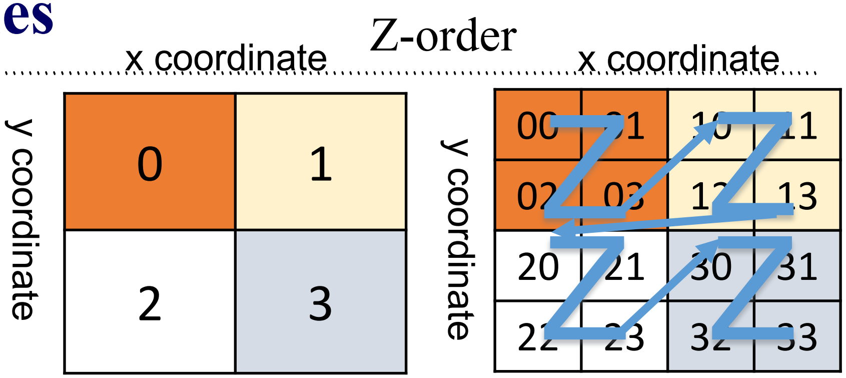
/119/Suita

(2)Avoiding dishonest volunteers

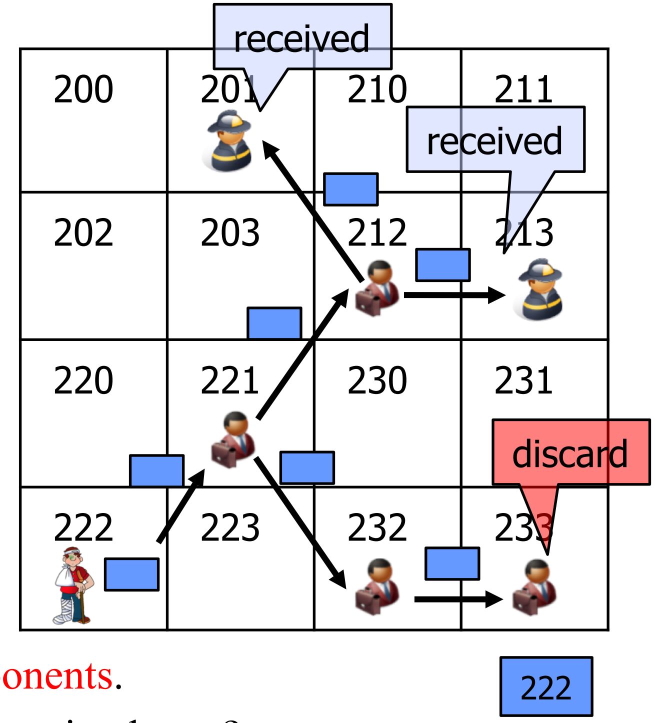
(1-2)Hiding names from forwarders

/incident/North-Osaka-Earthquake/Fire/FireFighting2

(1) Hiding First-Responders’ Names



- Against victims: Location based forwarding
  - Hide first-responders’ names by using location names according to Z-order
  - Walking scenario
    - A victim sends a message to its location name 222
    - It is delivered to first-responders who subscribe to nearby locations like 201 and 213

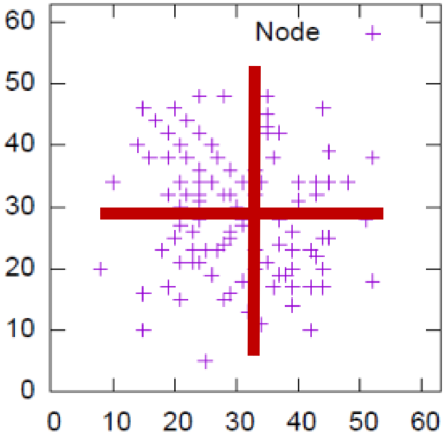


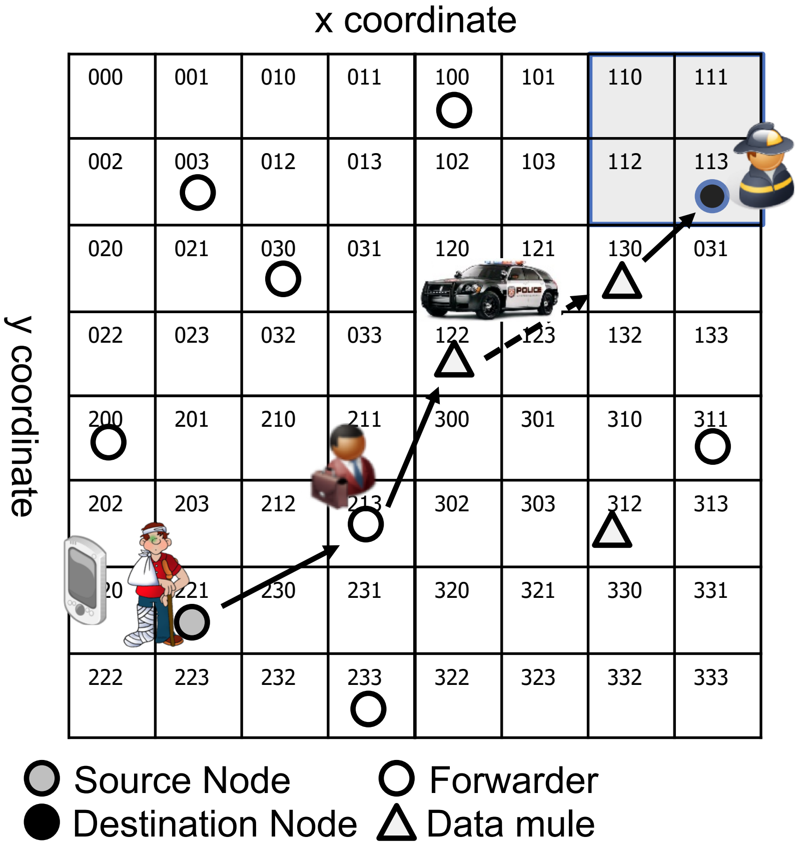
- Against forwarders: Obfuscating first-responder names
  - Names are obfuscated as keyed hashes
  - Issues
    - How to hash a name? Either a whole name or components.
    - How to aggregate hashed names in forwarding information bases?
    - How to share keys among first-responders and a commander?

Location based Forwarding

- Distance vector routing protocol
  - Routing information: Aggregation based on Plaxton
- Preliminary evaluation
  - Packets are forwarded between randomly chosen nodes on a 64 x 64 mesh network
  - Some nodes forward more packets than the others

Top 100 Nodes which forward many packets





000	001	010	011	100	101	110	111
002	003	012	013	102	103	112	113
020	021	030	031	120	121	130	031
022	023	032	033	122	123	132	133
200	201	210	211	300	301	310	311
202	203	212	213	302	303	312	313
20	221	230	231	320	321	330	331
222	223	232	233	322	323	332	333

◉ Source Node ○ Forwarder

● Destination Node △ Data mule

	0	1	2	3
1st digit	030	122 via 213	-	312
2nd digit	200	213	-	233

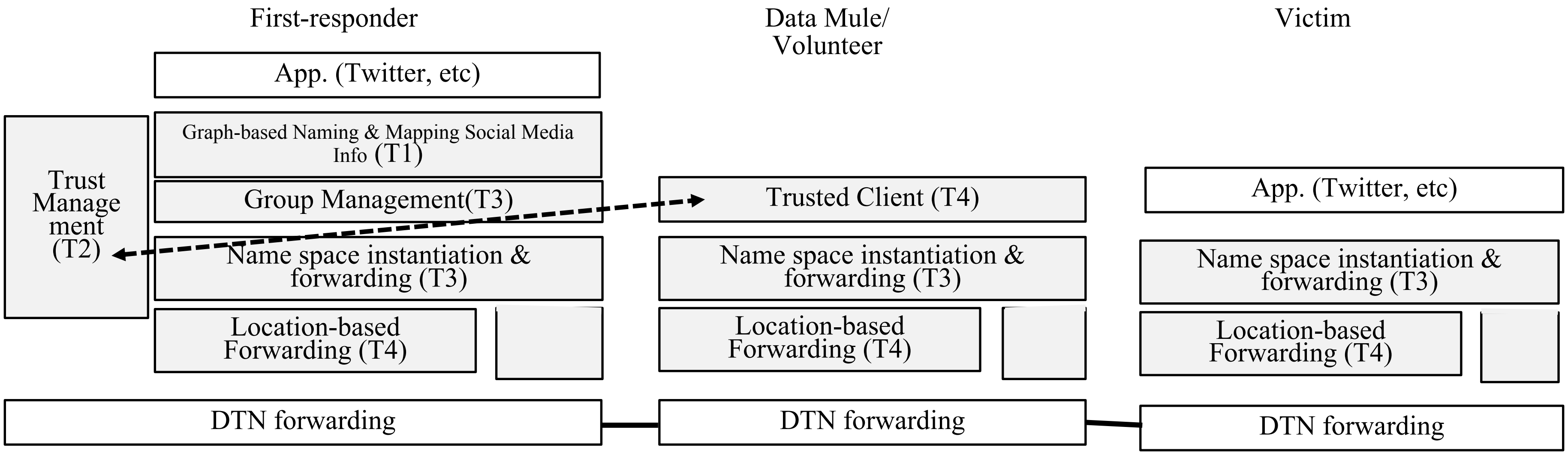
Forwarding table at 211

Resiliency against dishonest volunteers' behavior

- Approaches
  - Selecting volunteers with high trust values to avoid dishonest forwarders on forwarding paths
  - Reliably recording/sharing information (trust values and authentication information) of volunteers to prevent dishonest volunteers among volunteers by leveraging blockchain
    - Assuming that forwarding paths among them are not either secure or resilient to failures
- Research issues
  - Energy efficient byzantine fault tolerant algorithm rather than proof of work
    - Multi-hop environments where broadcasting is not available

Integration and Experiment

- Validation based on simulation and prototyping
  - Integrate graph-based namespace, pub/sub, forwarding and security functionality for design and performance evaluation
  - Integrate graph-based forwarding (T1 and T3) and location-based forwarding (T4) on a prototype
  - Integrate trust management (T2) with above (T1, T3 & T4)


First-responder
Data Mule/ Volunteer
Victim
App. (Twitter, etc)
Graph-based Naming & Mapping Social Media Info (T1)
Group Management(T3)
Trust Manage ment (T2)
Name space instantiation & forwarding (T3)
Location-based Forwarding (T4)
DTN forwarding
Trusted Client (T4)
Name space instantiation & forwarding (T3)
Location-based Forwarding (T4)
DTN forwarding
App. (Twitter, etc)
Name space instantiation & forwarding (T3)
Location-based Forwarding (T4)
DTN forwarding

Conclusion

- Secure and resilient disaster communication in the Social Media era
  - Protocol design and evaluation based on analysis, simulation and prototype experiments over testbeds like Cutei and NDN testbed
- Dissemination
  - Open source software
    - Software on open source ICN software: Cefore, NFD(NDN Forwarding Daemon)
      - Example: An emergency message delivery service like 119/911 calls
  - Publications and Standardization
    - ACM ICN, IEEE Transactions, et. al.
    - IRTF ICNRG