

# Anonymous DTN routing

September 12, 2013

## 1 Experimental Result

### 1.1 Overview

#### 1.1.1 Simulation model

- ONE simulator, modified default scenario/setting
- Map: Helsinki (4500m \* 3500m)
- Simulation running time: 12 hours
- Nodes: 246 (160 humans, 80 cars, 6 trams)
  - Packet buffer: Humans and cars (50MB), trams (500MB).
  - Contact interval: Humans (2 mins 30 secs), cars (1 min), trams ( 40 secs)
- Packet(message) generation
  - Packet size: 500KB - 1MB
  - Packet generation interval: 35sec - 50sec
  - TTL: 5 hours
  - Packet generation stopped when 5 hours (packet TTL) are left.
  - Total number of packets generated: about 575
- Movement: Random way point, map-based movement.
- Network interface: bluetooth, wlan (determine communication distance and bandwidth)
  - Humans, cars: Bluetooth (Bandwidth: 2Mbps, Communication range: 10m)
  - Trams: WLAN (Bandwidth: 10Mbps, Communication range: 100m)

### 1.1.2 Anonymous DTN routing setup

- # group: 1
- # nodes in a group: [5%, 10%, 15%, 20%, 25%]
- Epoch: [10mins, 20mins, 30mins, 60mins]
- Ephemeral ID duration: [3 epochs, 6 epochs]
- Base routing protocol: epidemic (flooding)

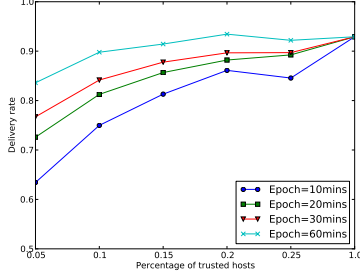
### 1.1.3 Assumptions & simplification

- Communication within a group  
Only nodes belong to any “group” can send packets to other nodes it trusts. Nodes that don’t belong to any group cannot generate packets.
- Strict time sync  
Epoch starts exactly at the same time in all nodes
- No “beacon”, “hello”, “pull” messages  
Once two nodes are located within a specific distance, they know ephemeral addresses, packet digest, pulling list of each other without any message exchange.
- Forwarding policy  
On contact, a node first forwards packets whose destinations are either trusted by the next-hop node or in neighbor list of the next-hop node. Then it tries to forward remaining packets in FIFO manner.

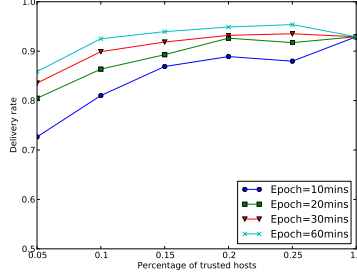
## 1.2 Results

Ephemeral ID duration	Trusted nodes %	Epoch
3 epochs	10%	60 mins
6 epochs	10%	30 mins
	20%	20 mins

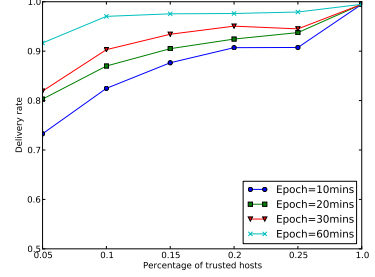
Table 1: **Example settings with delivery rate of about 90% (Flooding: 92.91%).**



(a) Ephemeral ID valid for 3 epochs

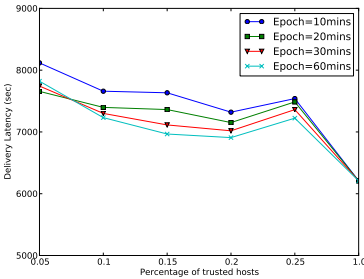


(b) Ephemeral ID valid for 6 epochs

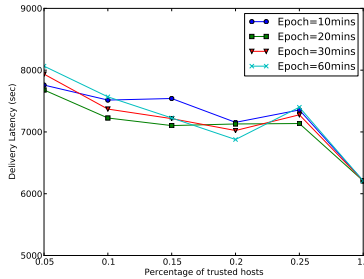


(c) Ephemeral ID valid for 6 epochs. Infinite packet buffer.

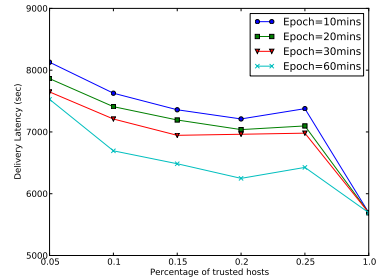
**Figure 1: Packet delivery rate.** Delivery rate of pure epidemic routing: 92.91%. Delivery rate of pure epidemic routing with infinite packet buffer: 99.48%. Increasing ephemeral ID duration from 3 epochs to 6 epochs enhances the delivery rate significantly. In Figure 1c, ephemeral ID expiry does not occur when epoch is 60 mins. [TTL (5 hours) < Epoch (1 hour) \* Ephemeral ID duration (6 epochs)] In this case, packet drop occurs only when TTL expires, and the delivery rate is almost as high as that of epidemic (flooding) routing



(a) Ephemeral ID valid for 3 epoch

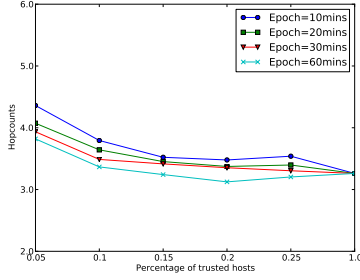


(b) Ephemeral ID valid for 6 epochs

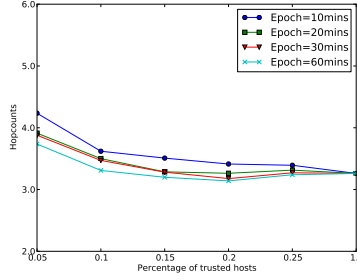


(c) Ephemeral ID valid for 6 epochs. Infinite packet buffer.

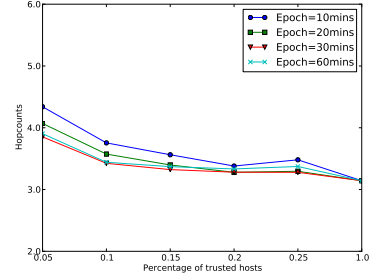
**Figure 2: Packet delivery latency.** With finite packet buffer, delivery latency of our protocol is 1000 - 2000 secs longer than that of flooding protocol.



(a) Ephemeral ID valid for 3 epochs

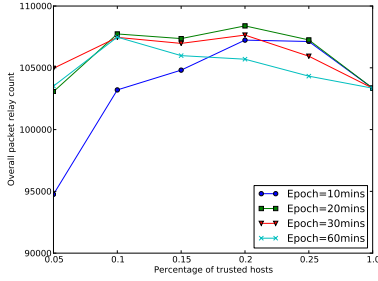


(b) Ephemeral ID valid for 6 epochs

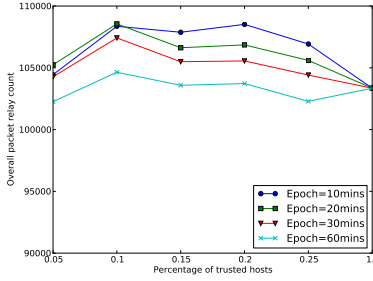


(c) Ephemeral ID valid for 6 epochs. Infinite packet buffer.

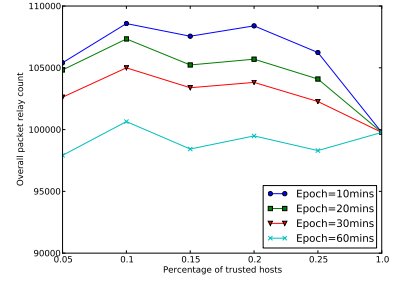
Figure 3: **Packet delivery hop count.** In general, delivery hop count is increased by less than 1 hop.



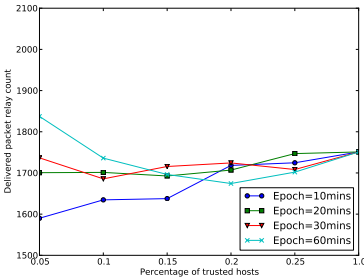
(a) Overall packets. Ephemeral ID valid for 3 epochs.



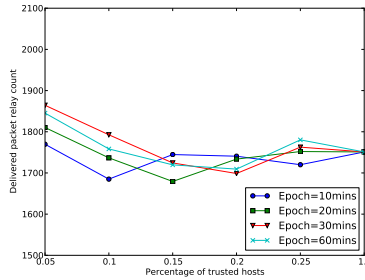
(b) Overall packets. Ephemeral ID valid for 6 epochs.



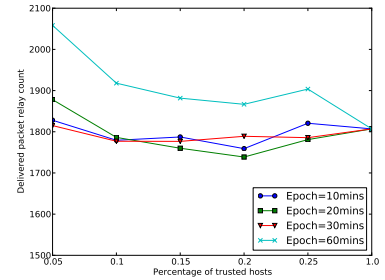
(c) Overall packets. Ephemeral ID valid for 6 epochs. Infinite packet buffer.



(d) Delivered packets. Ephemeral ID valid for 3 epochs.

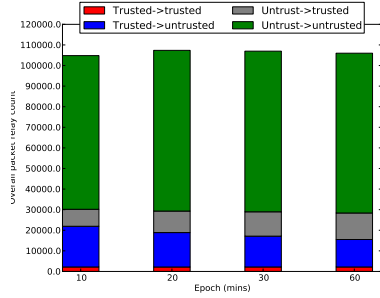


(e) Delivered packets. Ephemeral ID valid for 6 epochs.

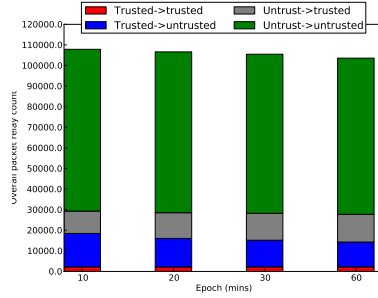


(f) Delivered packets. Ephemeral ID valid for 6 epochs. Infinite packet buffer.

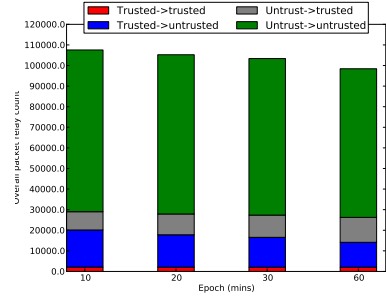
Figure 4: **Packet relay count.** Only about 2% of packet relays are used for actual packet deliveries.



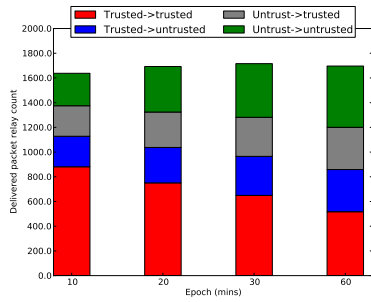
(a) Overall packets. Ephemeral ID valid for 3 epochs



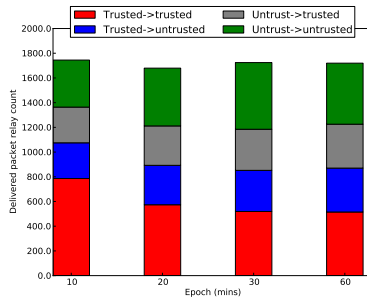
(b) Overall packets. Ephemeral ID valid for 6 epochs



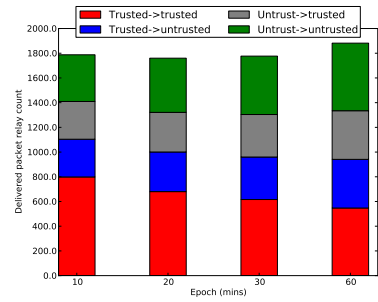
(c) Overall packets. Ephemeral ID valid for 6 epochs. Infinite packet buffer.



(d) Delivered packets. Ephemeral ID valid for 3 epochs

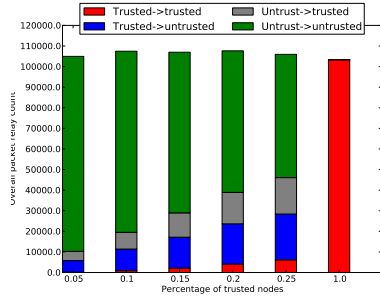


(e) Delivered packets. Ephemeral ID valid for 6 epochs

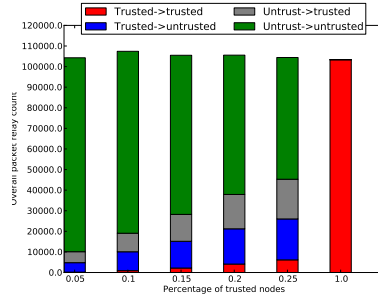


(f) Delivered packets. Ephemeral ID valid for 6 epochs. Infinite packet buffer

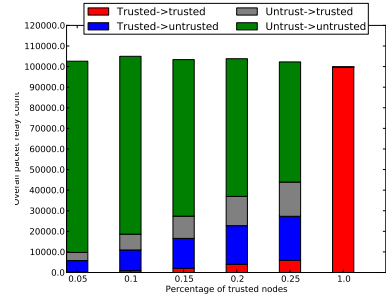
Figure 5: **Packet relay classification over varying epoch. Percentage of trusted nodes is 15%.** Ephemeral ID duration does not affect overall packet relay classification, but it affects delivered packet relay classification. When ephemeral ID duration is 6 epochs, packet relays between two trusted nodes are slightly decreased while other types of relays are increased.



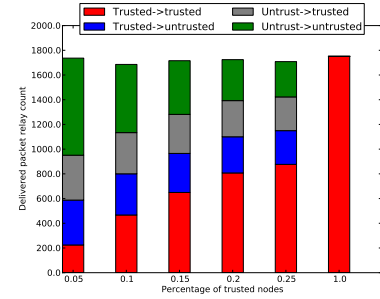
(a) Overall packets. Ephemeral ID valid for 3 epochs.



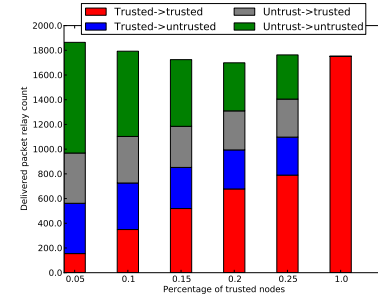
(b) Overall packets. Ephemeral ID valid for 6 epochs.



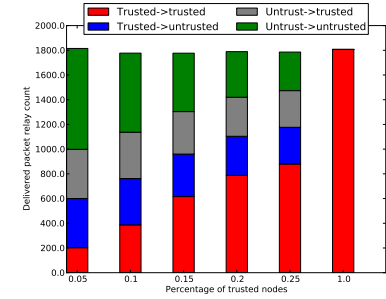
(c) Overall packets. Ephemeral ID valid for 6 epochs. Infinite packet buffer.



(d) Delivered packets. Ephemeral ID valid for 3 epochs.



(e) Delivered packets. Ephemeral ID valid for 6 epochs.



(f) Delivered packets. Ephemeral ID valid for 6 epochs. Infinite packet buffer.

**Figure 6: Packet relay classification over varying percentage of trusted nodes. Epoch is 30 mins.** As in Figure 5, ephemeral ID duration does not affect overall packet relay classification but affects delivered packet relay classification.

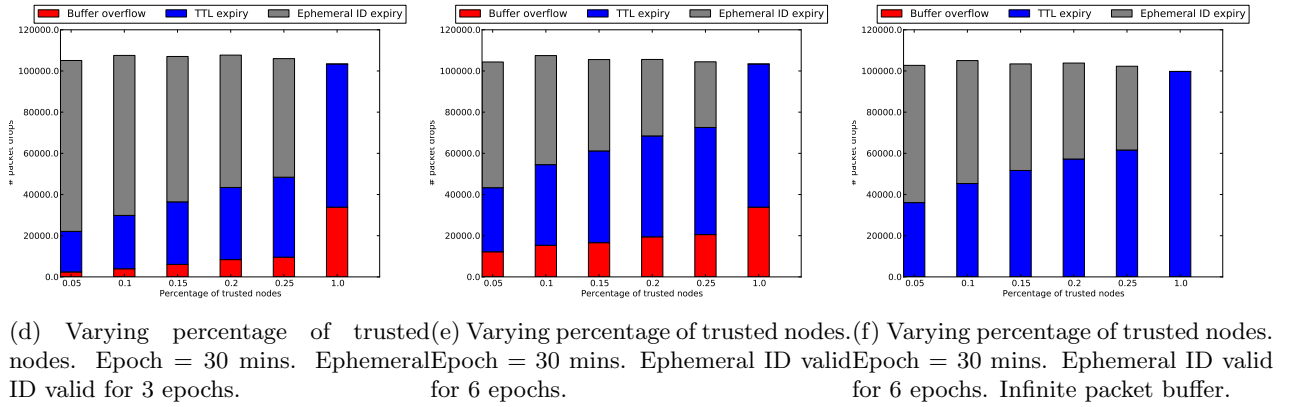
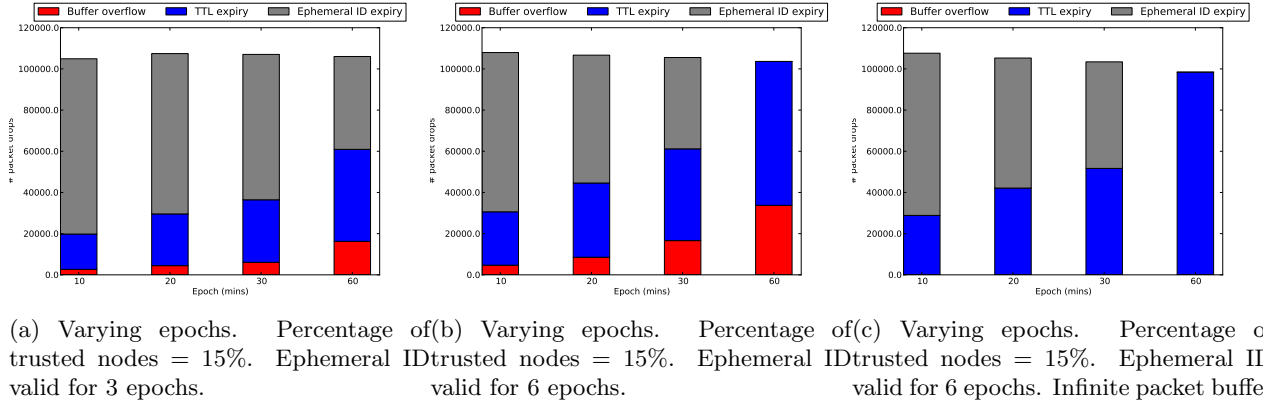


Figure 7: **Packet drop classification.** With ephemeral ID valid for 6 epochs (Figures 7b and 7e), packet drops due to ephemeral ID expiry are decreased significantly. Note that packet drop due to ephemeral ID expiry does not occur when epoch is 60 mins and ephemeral ID duration is 6 epochs. [TTL (5 hours) < Epoch (1 hour) \* Ephemeral ID duration (6 epochs)]

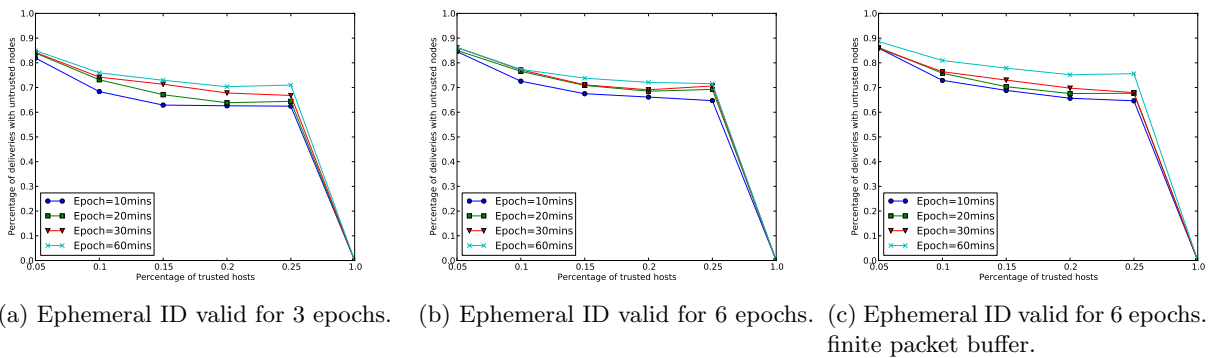


Figure 8: **Packet deliveries with untrusted nodes.** Percentage of packet delivery routes containing at least one untrusted node.