Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System

APPLAUS

Zhichao Zhu, Student Member, IEEE
Guohong Cao, Fellow, IEEE

Presentation By: Kevin Bruer
Dept. of Computer Sience
Mcmaster University

What is APPLAUS

Problem: Today's location-sensitive service relies on user's mobile device to determine the current location. This allows malicious users to access a restricted resource or provide bogus alibis by cheating on their locations.

Solution: The proposed solution is APPLAUS, where in collocated Bluetooth enabled mobile devices mutually generate location proofs and send updates to a location proof server.

Pseudonym

In order to ensure that a device is who it says it is, every device must have an encrypted Pseudonym.

Because probes are used to discover their neighbors, a neighbor can check a private key it receives against the public key for the corresponding physical identity (MAC address) of the device it is trying to authenticate.

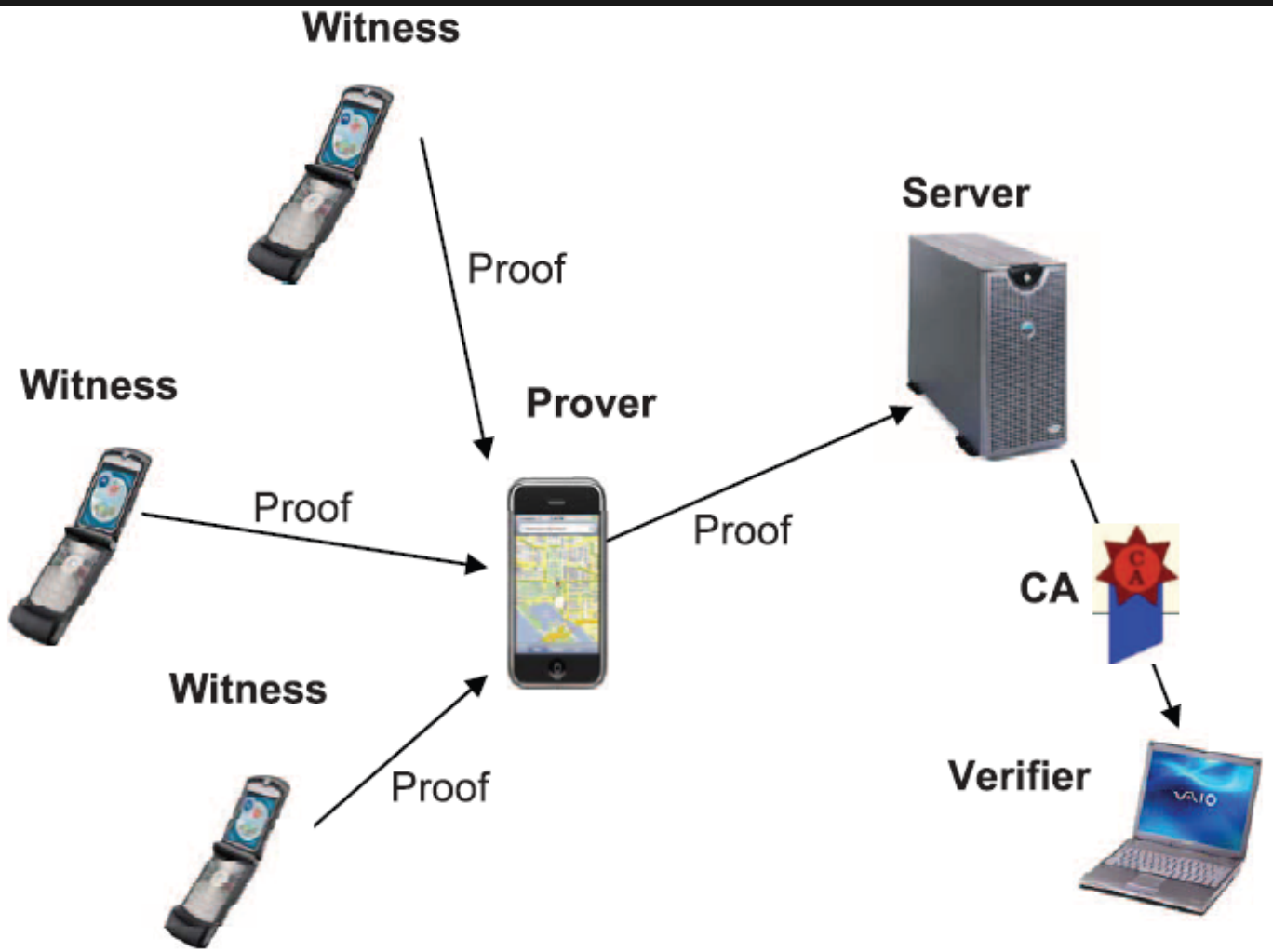
Threat Model: Internal, Passive, Global

Internal: Attacker has internal control of a device, and access to private information, as well as the ability to collude with similar devices.

Passive: Attacker cannot perform active channel jamming, mobile worm attacks or other, denial-of- service attacks.

Global: the adversary can monitor, eavesdrop, and analyze all the traffic in its neighboring area, or even monitor all the traffic around the server.

Architecture and Message Flow



Prover: Node who needs to prove it's location.

Witness: a neighboring node that agrees to provide location proof for the prover.

Location proof server: Server that stores all location data, in Pseudonym form to ensure security of data.

Certificate Authority: The third party server that maps Pseudonyms to real names.

Verifier: The service that needs to verify the Prover's location.

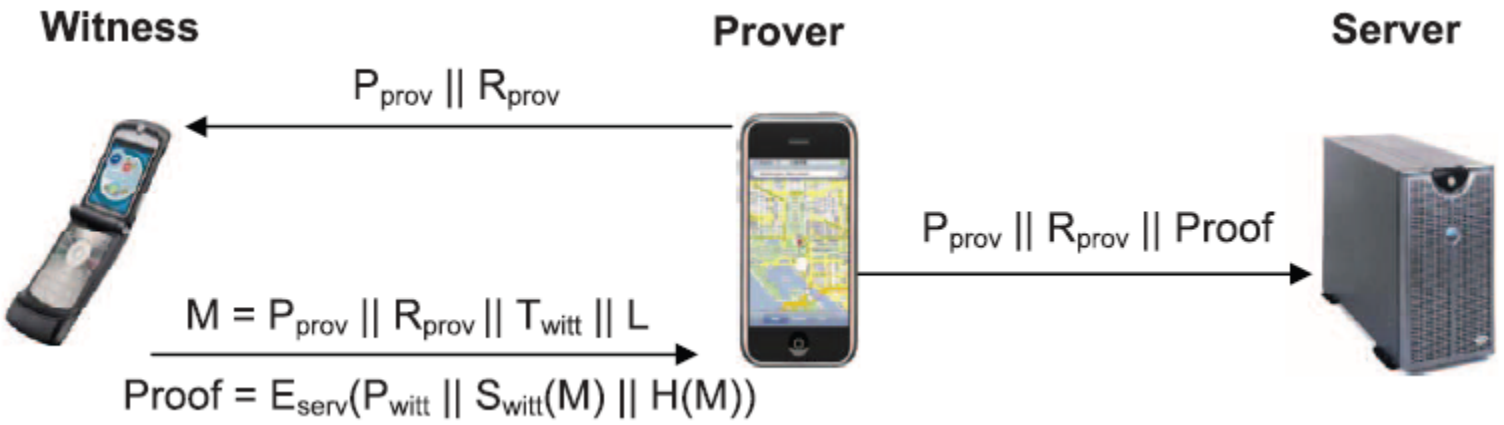
Location Proof Updating Protocol

P = Psudonym

R = Random number

T = Timestamp

L = Location



Separation of privacy knowledge

The knowledge of the privacy information is separately distributed to the location proof server, the CA, and the verifier. Thus, each party only has partial knowledge.

Scheduling Location Proof Updates

Algorithm 1. Location Proof Update Scheduling for the prover

Input: updating parameter λ;

1: generate M distinct parameter $\lambda_1, \lambda_2, \cdots, \lambda_M$ such that $\lambda_1 + \lambda_2 + \cdots + \lambda_M = \lambda$
2: **for** each pseudonym i **do**
3: **while** current timestamp t follows Poisson distribution with λ_i **do**
4: send location proof request
5: **if** request is accepted **then**
6: submit location proof
7: **else**
8: generate and submit dummy proof
9: **end if**
10: **end while**
11: **end for**

Scheduling Location Proof Updates

Algorithm 2. Scheduling Location Proof Updates at Witnesses

Input: time t of incoming location proof request;

1: calculate location privacy loss Δ assuming the incoming request is accepted
2: **if** $\Delta > \epsilon$, ϵ is pre-defined location privacy loss threshold **then**
3: deny location proof request
4: **else**
5: accept location proof request
6: **end if**

$$\Delta = \frac{E_i(t') - E_i(t)}{E_i(t)}$$

Source Location Privacy Analysis

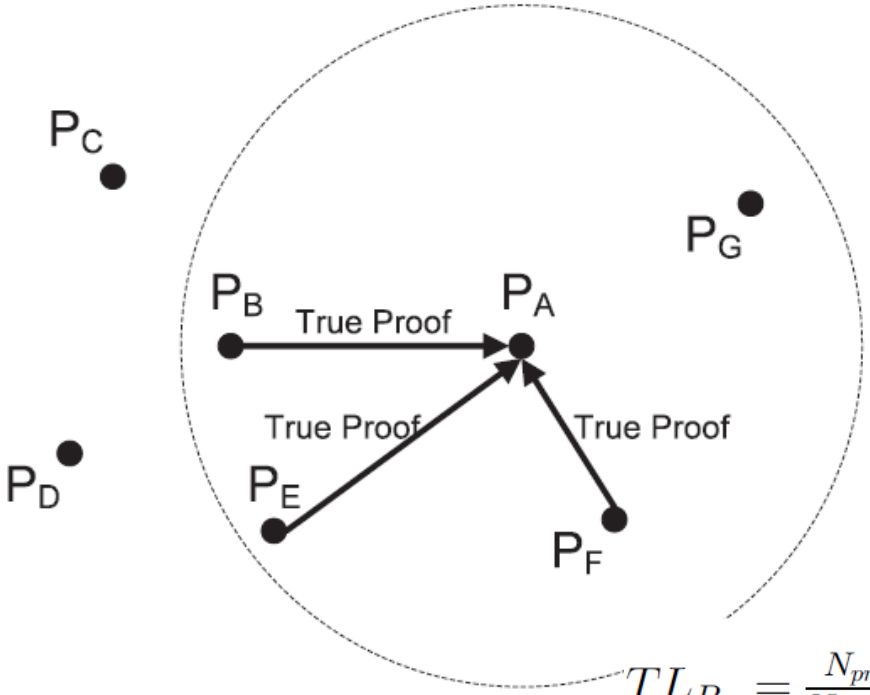
In order for the location data stored by this system to remain private, the server that contains the location data must have 2 things:

1. Pseudonym unlinkability

2. Statistically strong source location unobservability

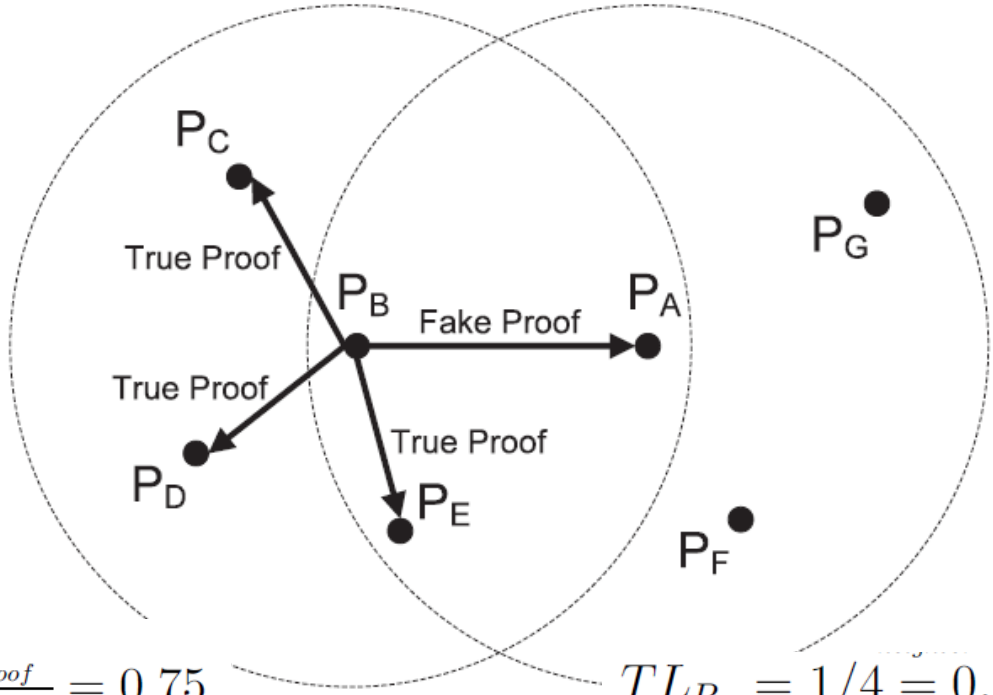
Colluding Attacks and Countermeasures

Problem: users might attempt to thwart the system by making false location proofs.



(a) Normal case

$$TL_{P_A} = \frac{N_{proof}}{N_{neighbor}} = 0.75.$$



(b) Colluding case

$$TL_{P_A} = 1/4 = 0.2$$

Colluding Attacks and Countermeasures

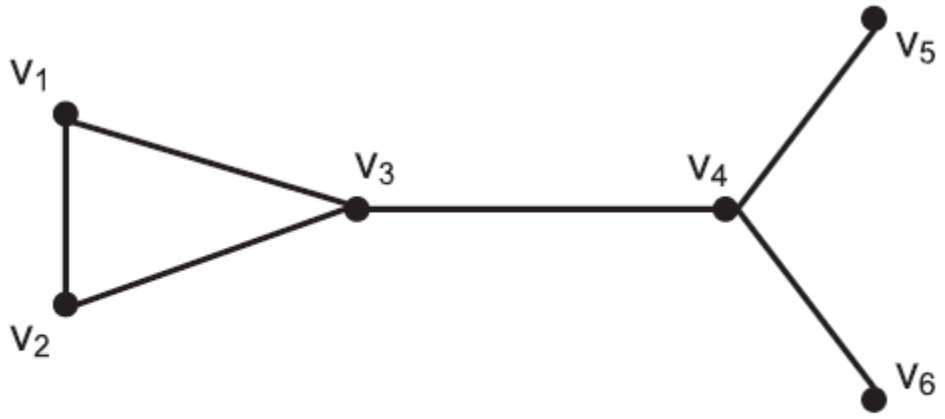
In addition to calculating the Trust Level of each node, two other methods are employed to detect Collusion:

1. Betweenness Ranking

2. Correlation Clustering

Colluding Attacks and Countermeasures

Betweenness is defined as the number of shortest paths from all vertices to all others that pass through node v.

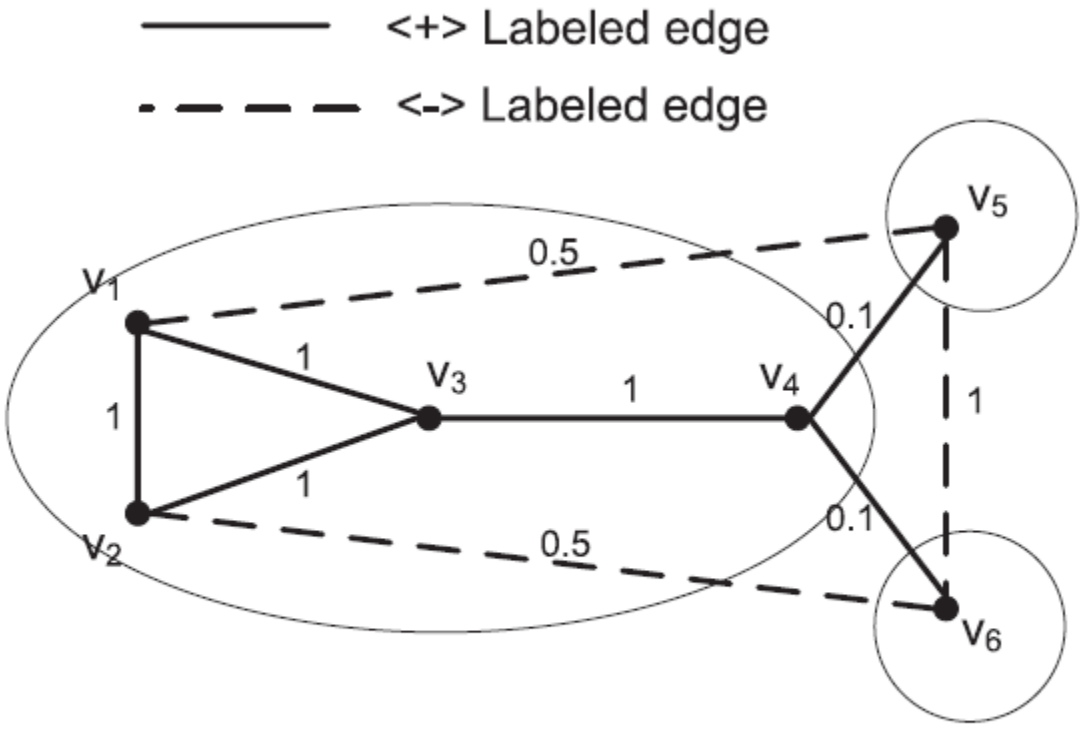


(a) Unweighted pseudonym-correlation graph

Colluding Attacks and Countermeasures

Edge weight:

$$c_{ij} = \frac{1}{1 + t_{ij}}.$$



(b) Weighted proof-correlation graph and correlation clustering

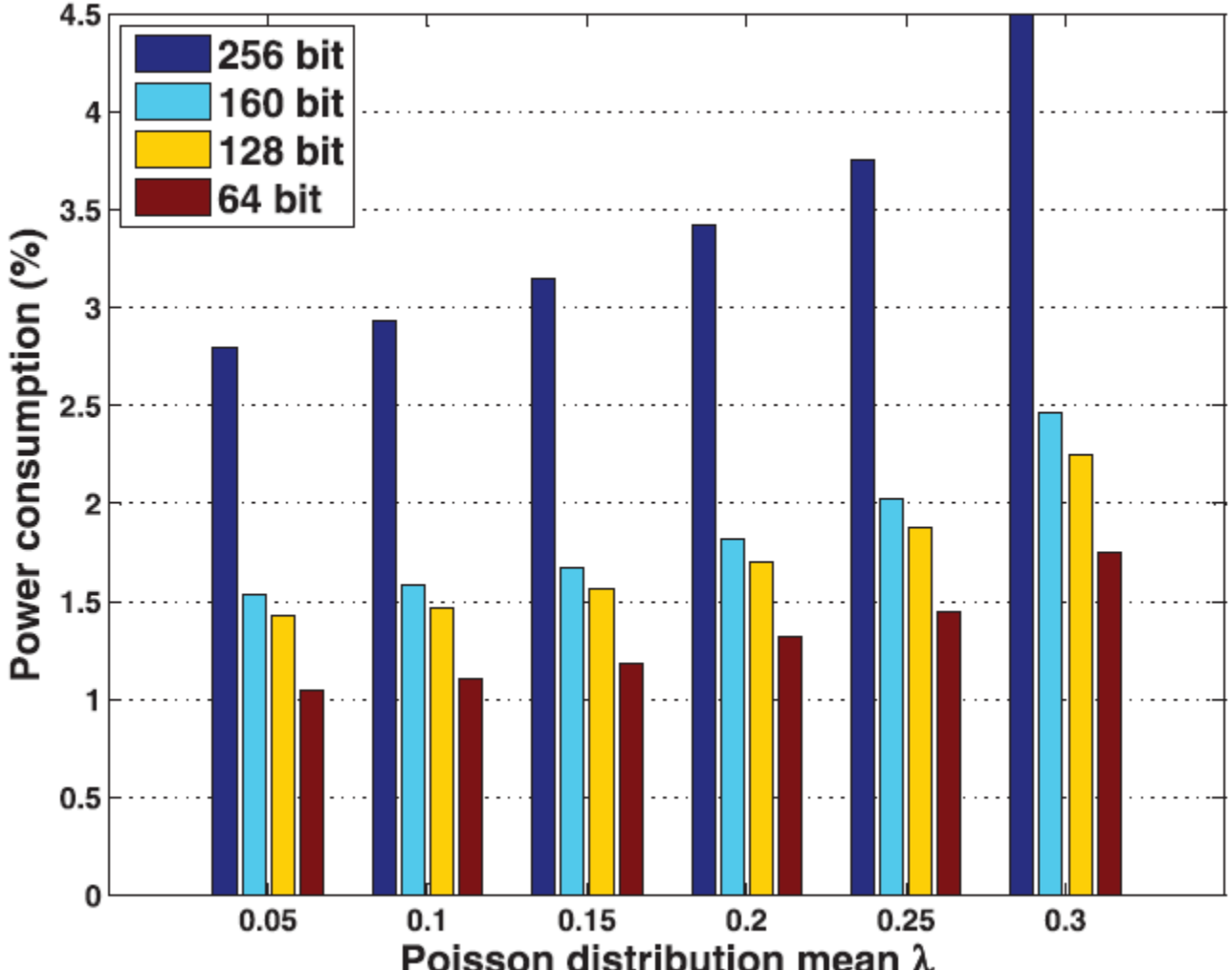
Power Consumption

The client: Android Developer Phone 2 (ADP2), which is equipped with 528 MHz chipset, 512 MB ROM, 192 MB RAM, Bluetooth, and GPS module, and running Google Android 1.6 OS.

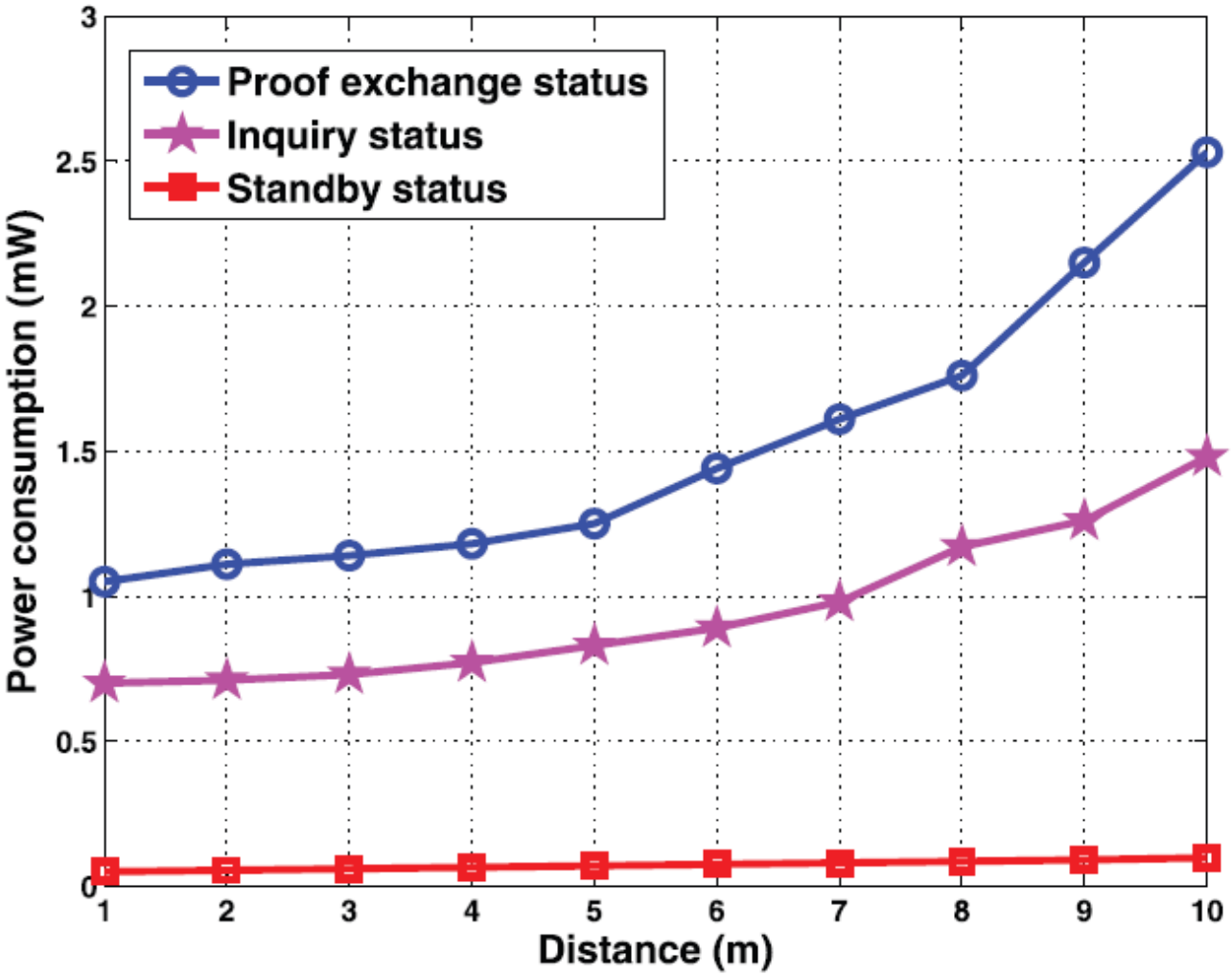
Communication: AT&T's 3G wireless data service.

The server is implemented on a T4300 2.1 GHz 3 GB RAM laptop.

Power Consumption

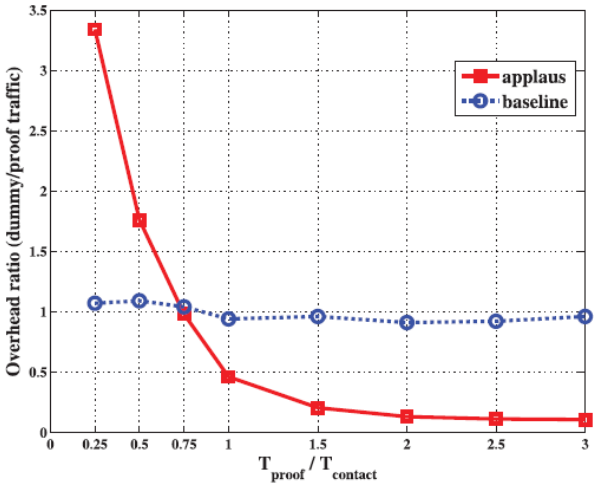


Power Consumption

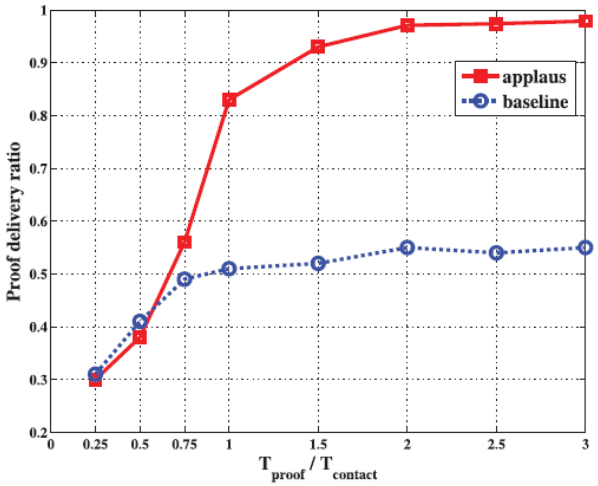


Simulation Results

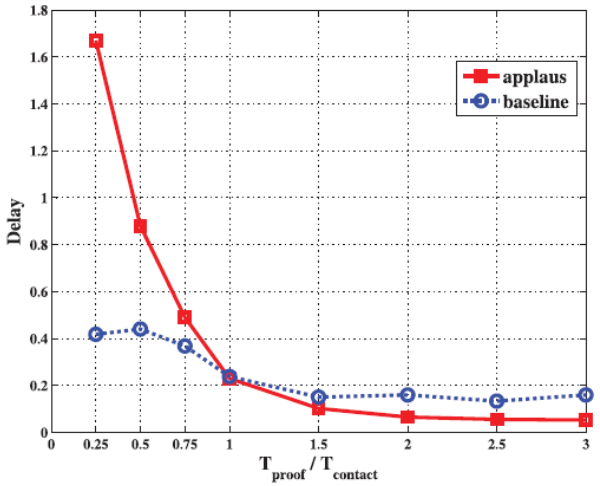
1,000 mobile nodes in a 3 km by 3 km area.



(a) Overhead Ratio



(b) Proof Delivery Ratio



(c) Average Delay

Simulation Results

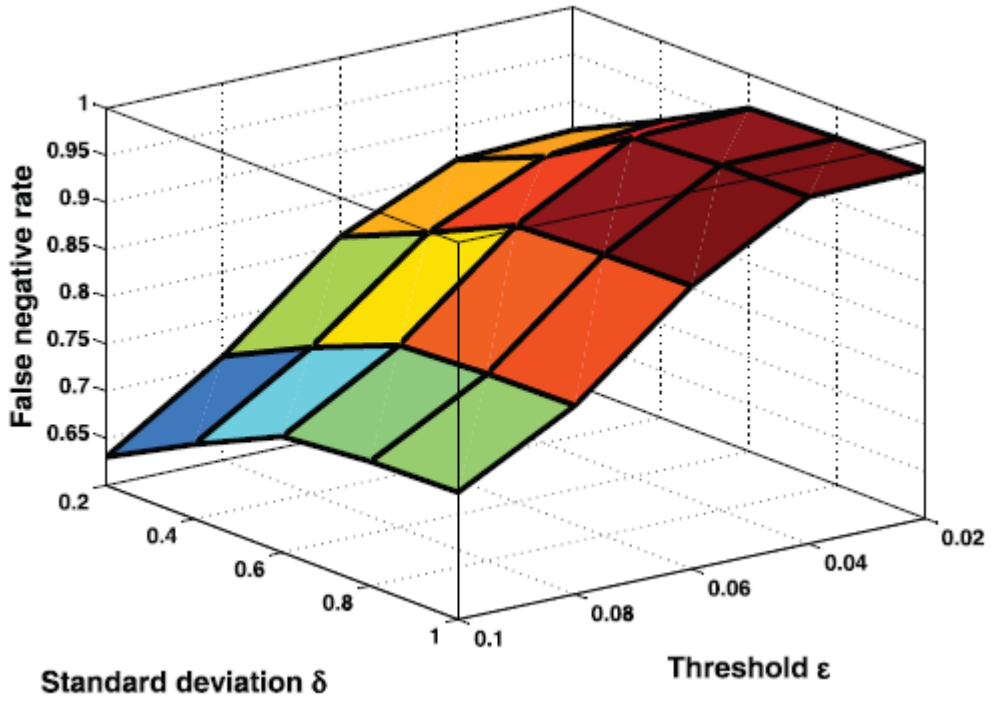
Message overhead ratio: the ratio of dummy proof traffic and real location proof traffic.

Proof delivery ratio: the percentage of location proof message that is successfully uploaded to the location proof server.

Average delay: the time difference between the time when a location proof update is needed and when the location proof message has reached the location proof server.

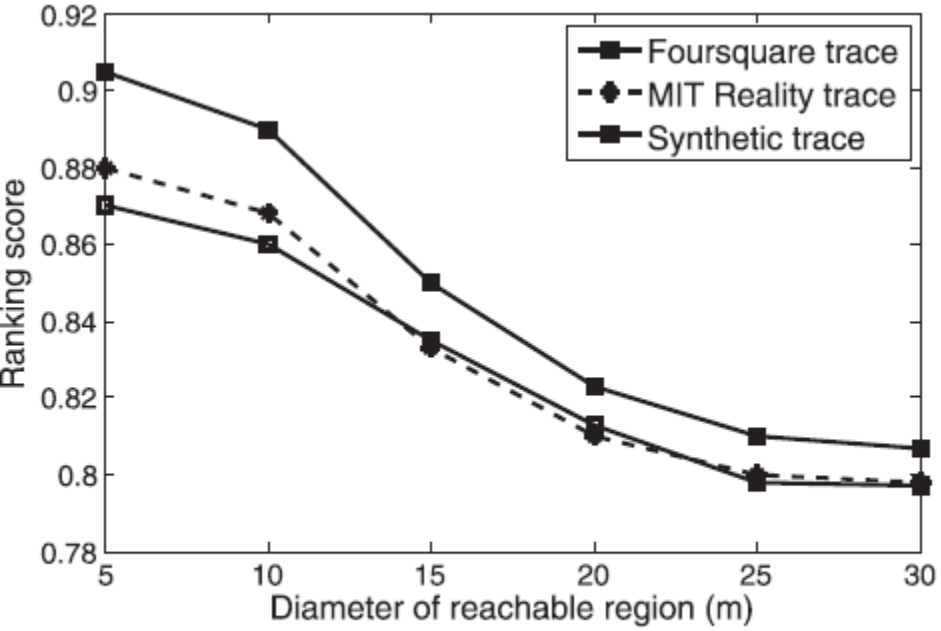
Tproof is the required interval between two location proof updates, and **Tcontact** is the mean real node contact interval.

Privacy Evaluation

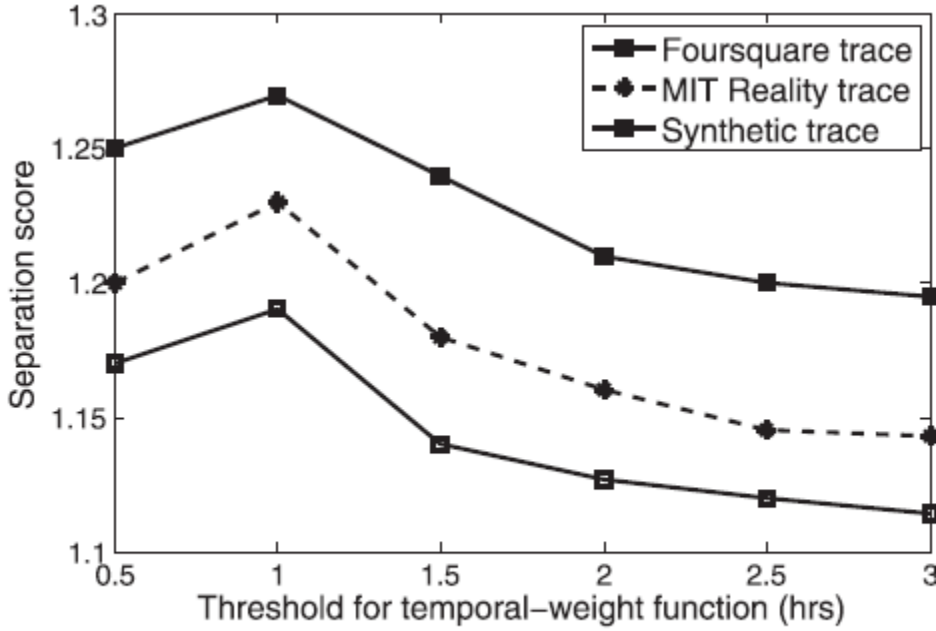


H_0—the two pseudonyms belong to the same source.
H_1—the two pseudonyms belong to different source.

Collusion Detection

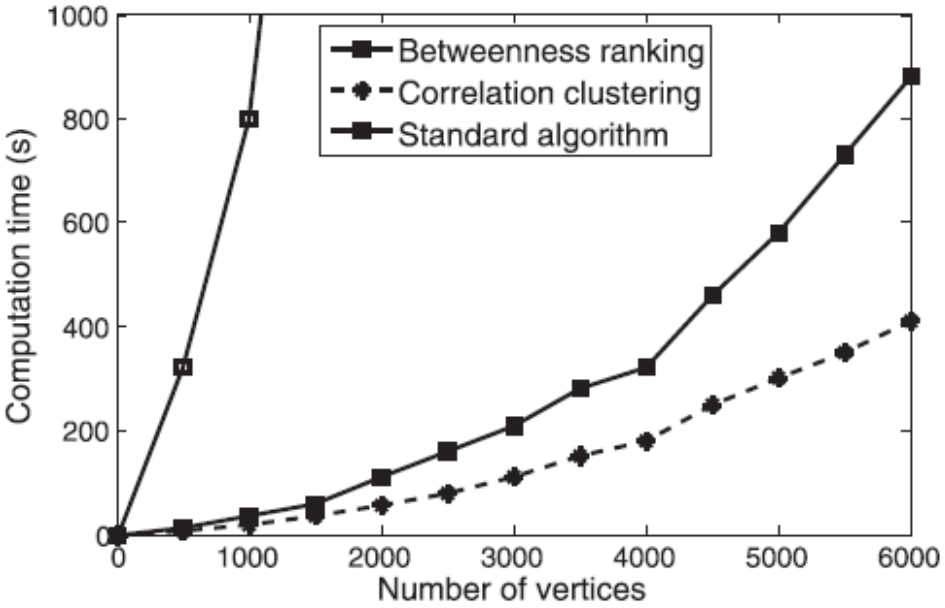


(a) Ranking score of betweenness ranking

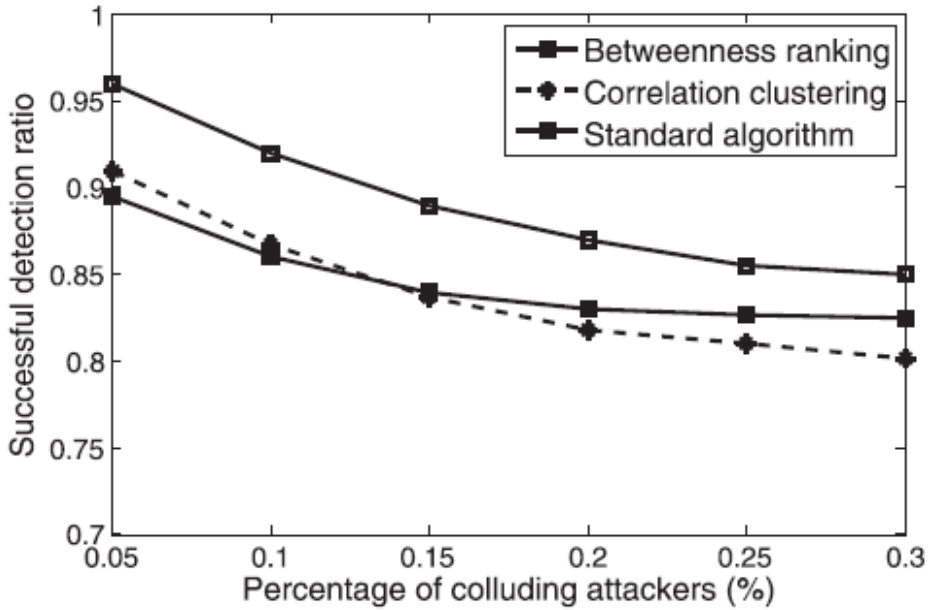


(b) Separation score of correlation clustering

Collusion Detection



(a) Computation time with number of vertices



(b) Successful detection ratio

Conclusion

APPLAUS uses colocated Bluetooth enabled mobile devices mutually generate location proofs and upload to the location proof server. This may be the first work to address the joint problem of location proof and location privacy. APPLAUS can provide real-time location proofs effectively, and it preserves source location privacy and is collusion resistant.

Thanks For Listening