LinkDroid: Reducing Unregulated Aggregation of App-Usage Behaviors

Huan Feng, Kassem Fawaz, Kang G. Shin

Real-Time Computing Laboratory, University of Michigan

24th USENIX Security Symposium
August 14th, 2015 • Washington DC

An Emerging Threat

An Emerging Threat

Unregulated Aggregation of App-Usage Behaviors

A Novel Perspective

Dynamic Linkability Graph (DLG)

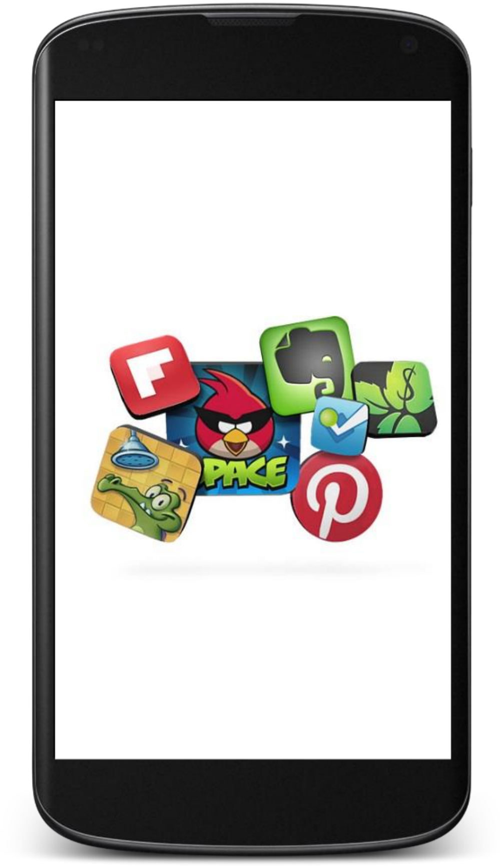
Real-world Evidence

DLG in the real-world

Proposed Solution

LinkDroid: Runtime Monitoring & Mediation

An Emerging Threat

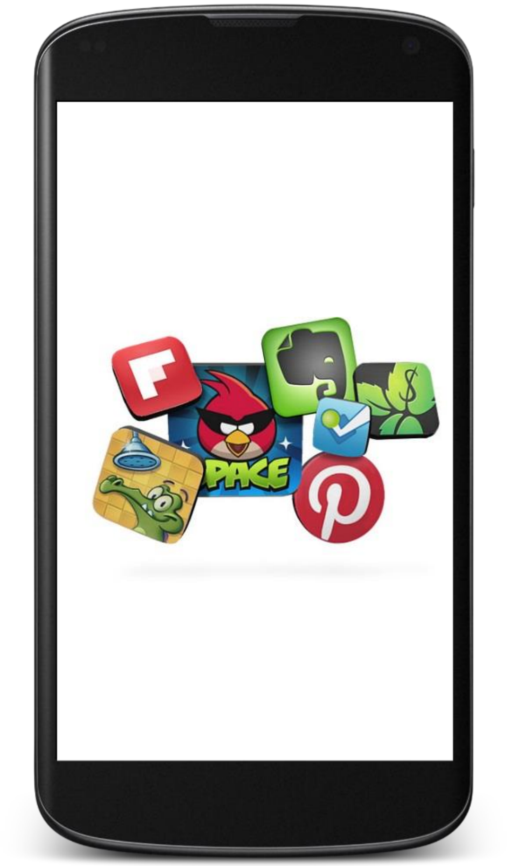


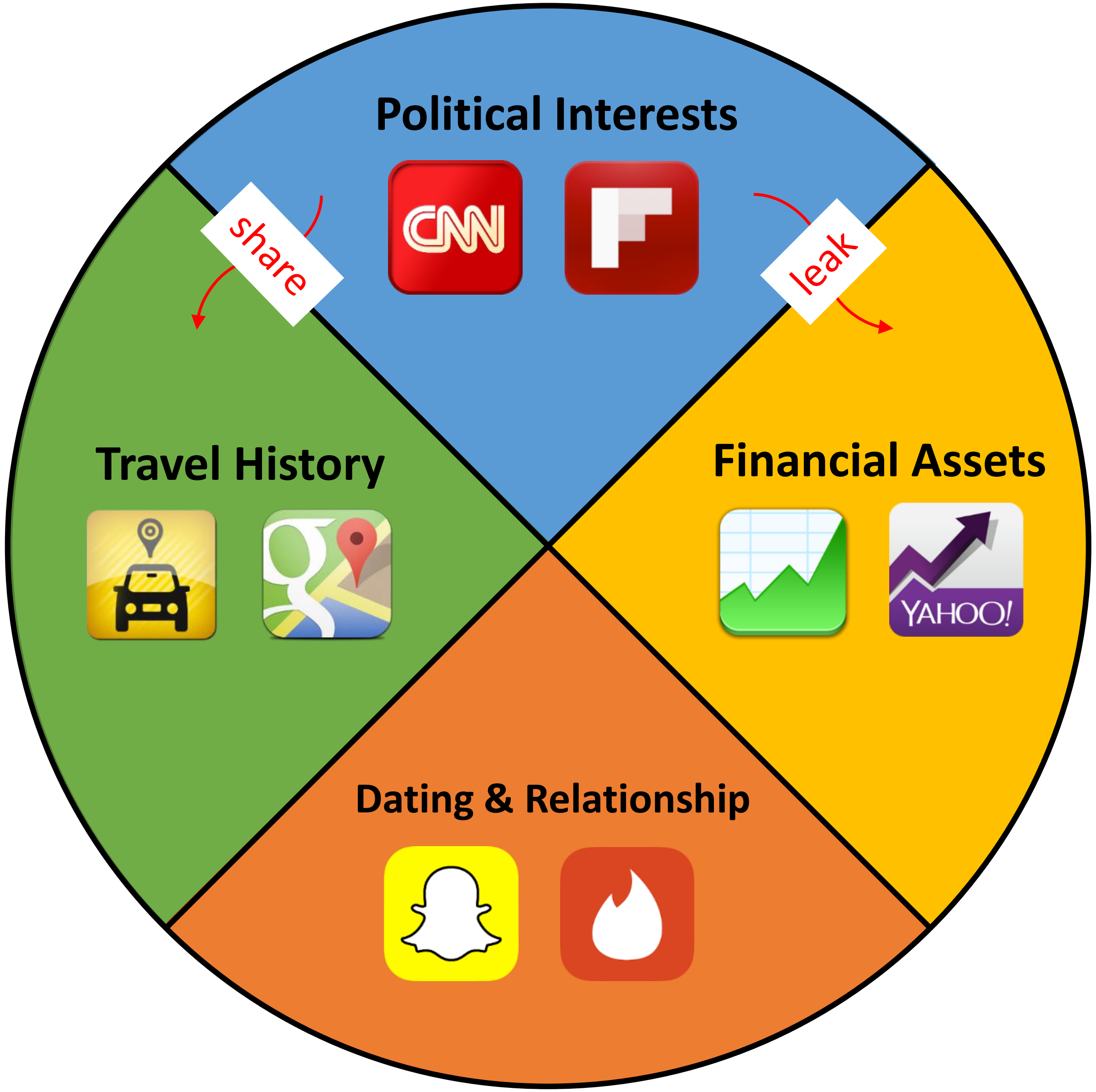
Political Interests

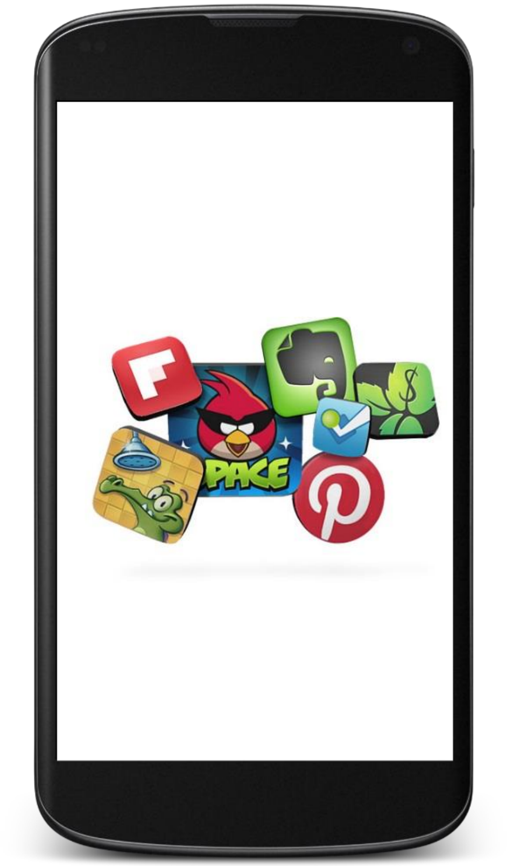
Travel History

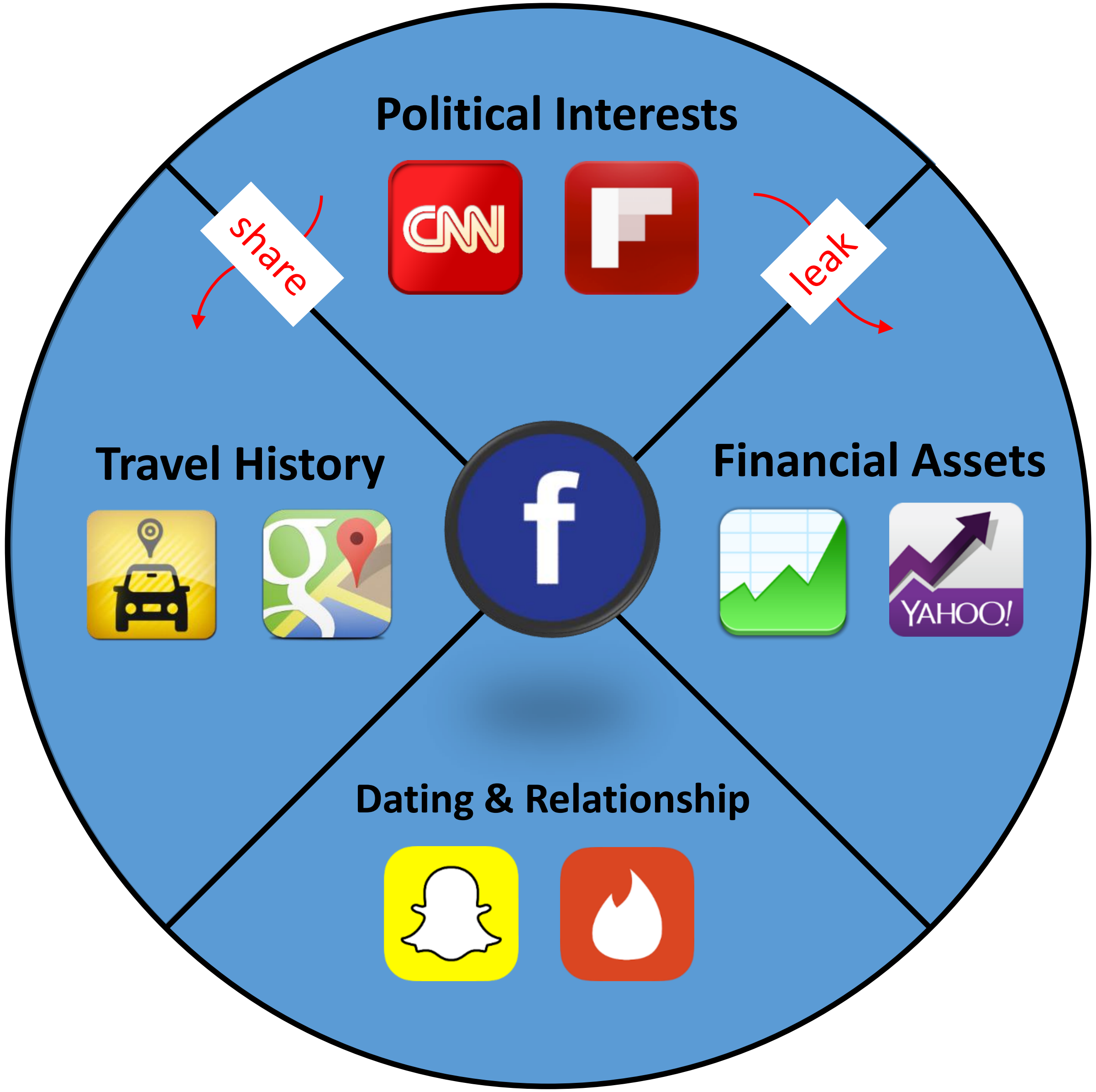
Financial Assets

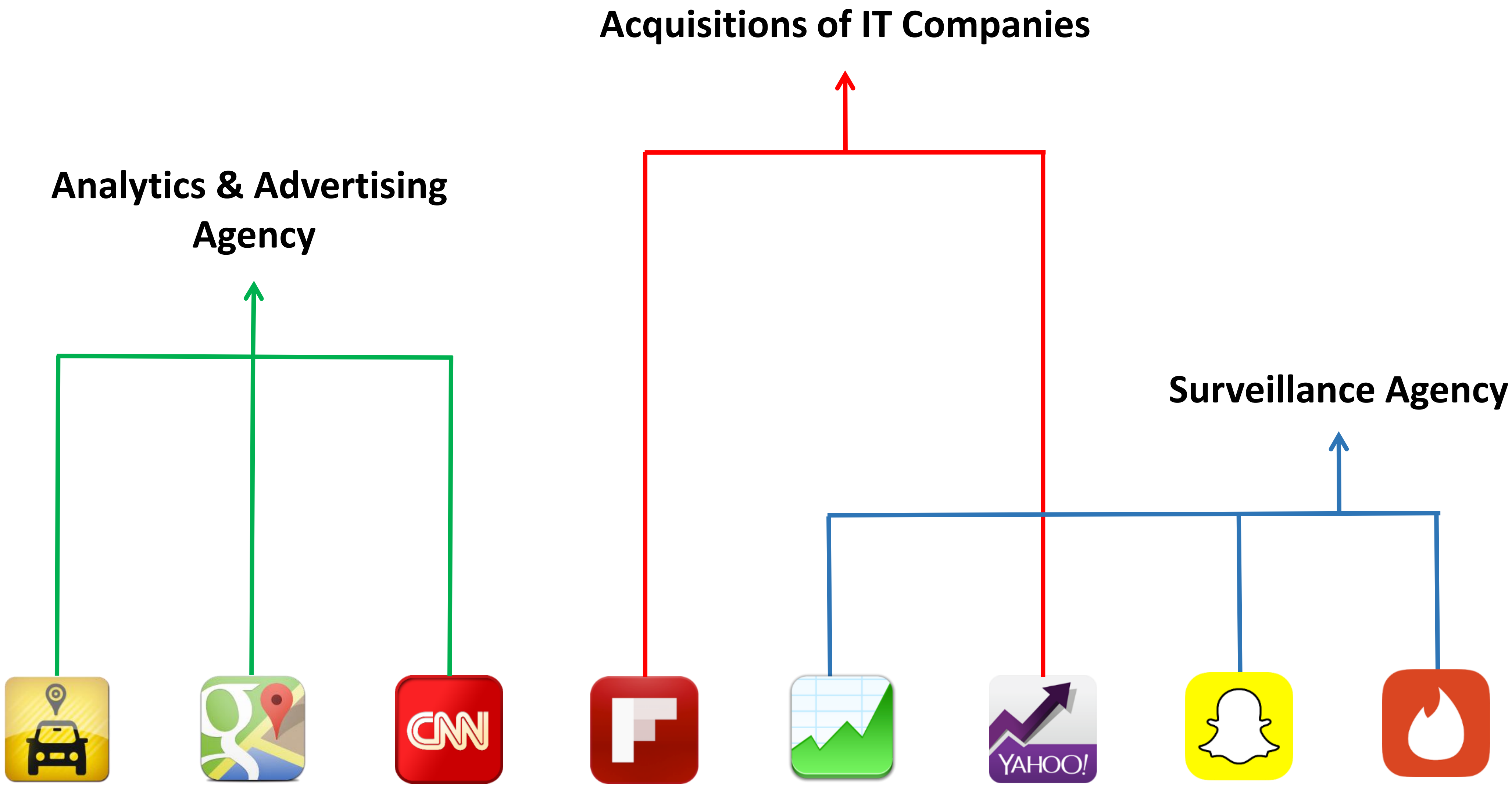
Dating & Relationship




Political Interests
share
leak
Travel History
Financial Assets
Dating & Relationship
CNN
YAHOO!




Political Interests
share
leak
Travel History
Financial Assets
Dating & Relationship



Acquisitions of IT Companies

Analytics & Advertising Agency

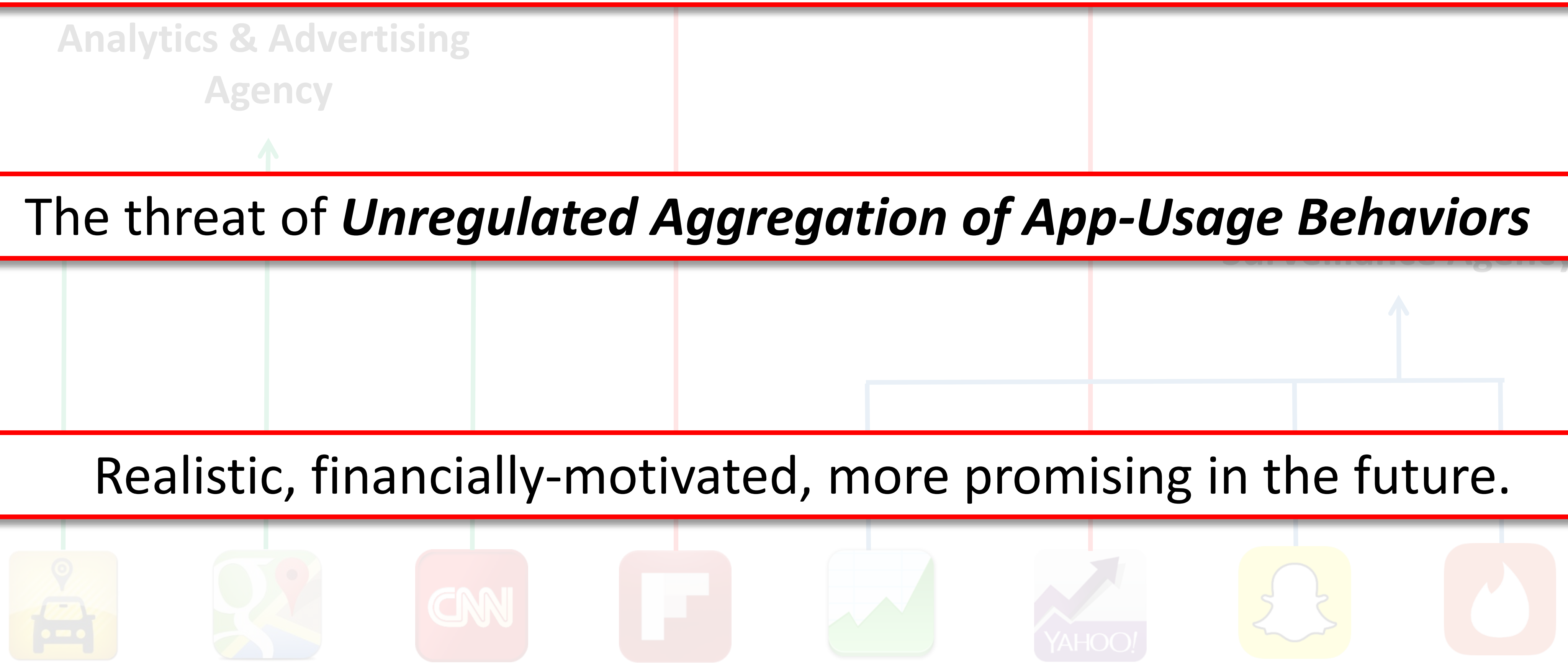
Surveillance Agency

An Emerging Threat

A curious adversary is able to aggregate usage behaviors of the same user across multiple apps without his knowledge or consent.

The threat of ***Unregulated Aggregation of App-Usage Behaviors***

Realistic, financially-motivated, more promising in the future.



A Novel Perspective

An Emerging Threat

Unregulated Aggregation of App-Usage Behaviors

A Novel Perspective

Dynamic Linkability Graph (DLG)

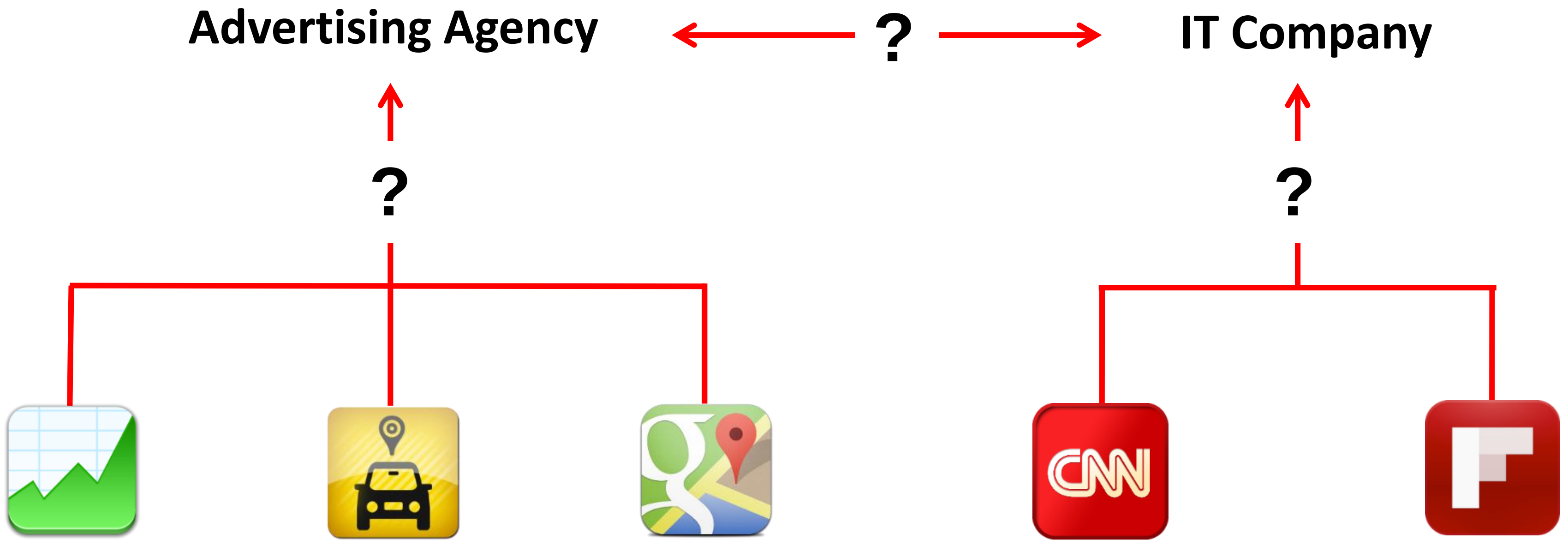
Real-world Evidence

DLG in the real-world

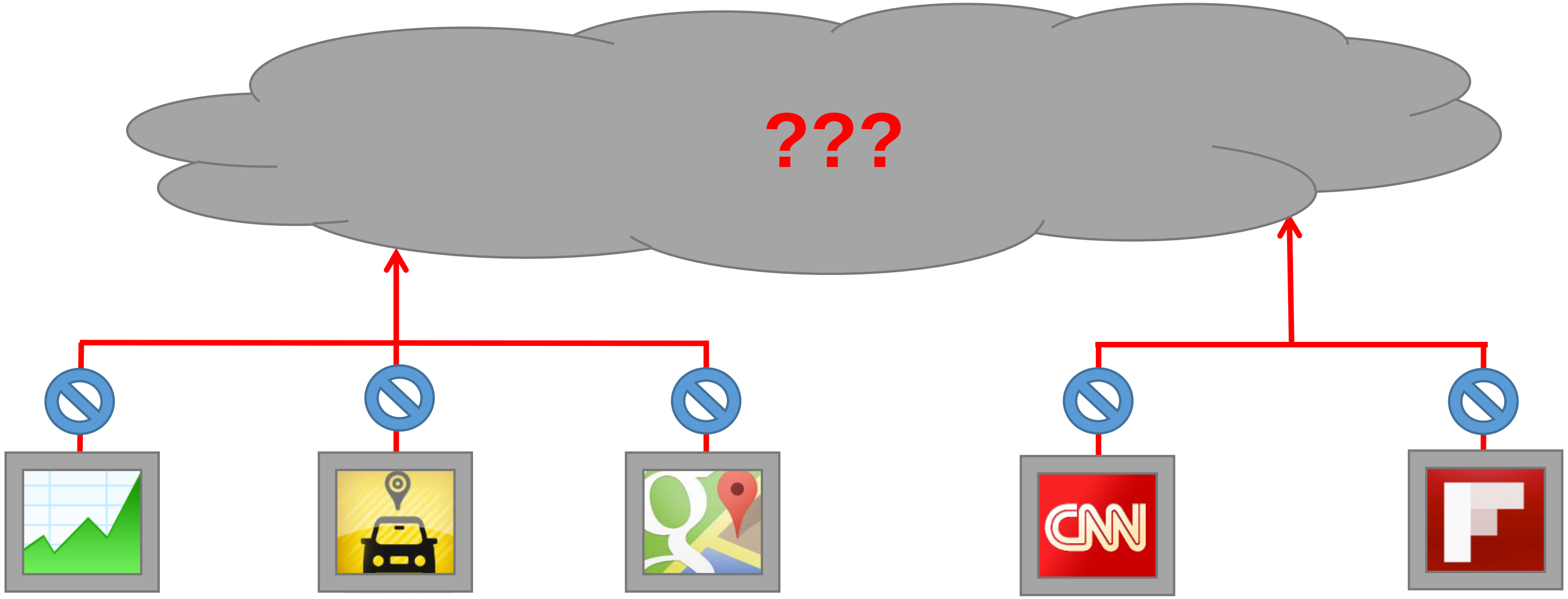
Proposed Solution

LinkDroid: Runtime Monitoring & Mediation

Challenges



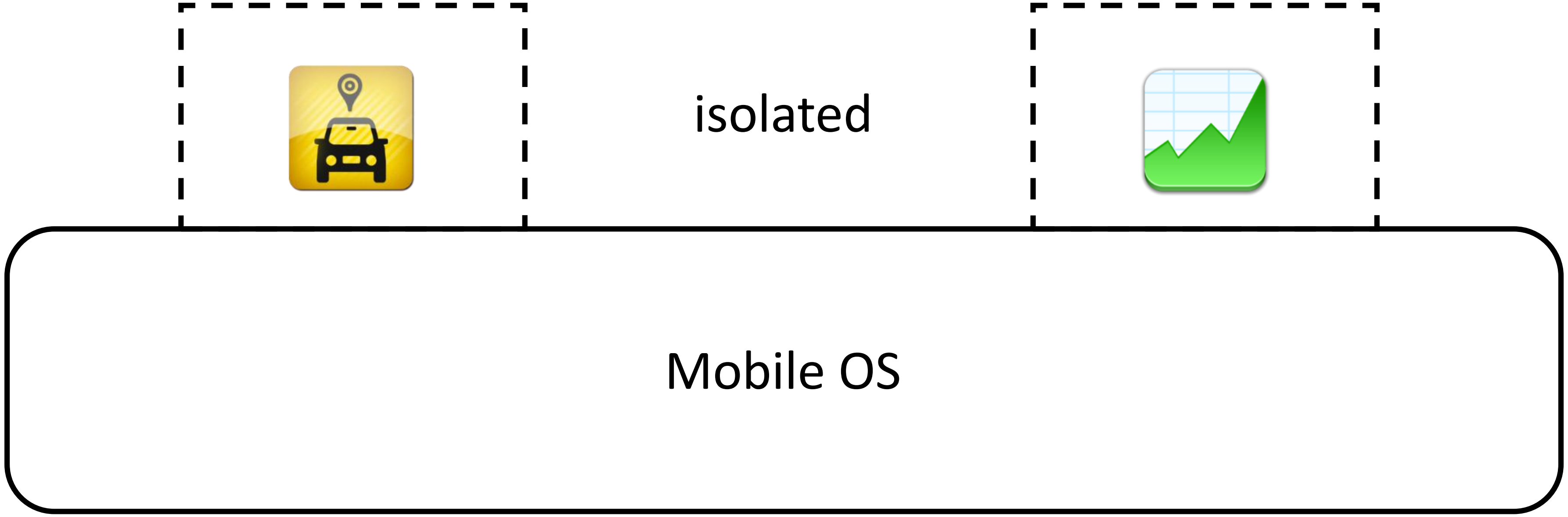
Challenges



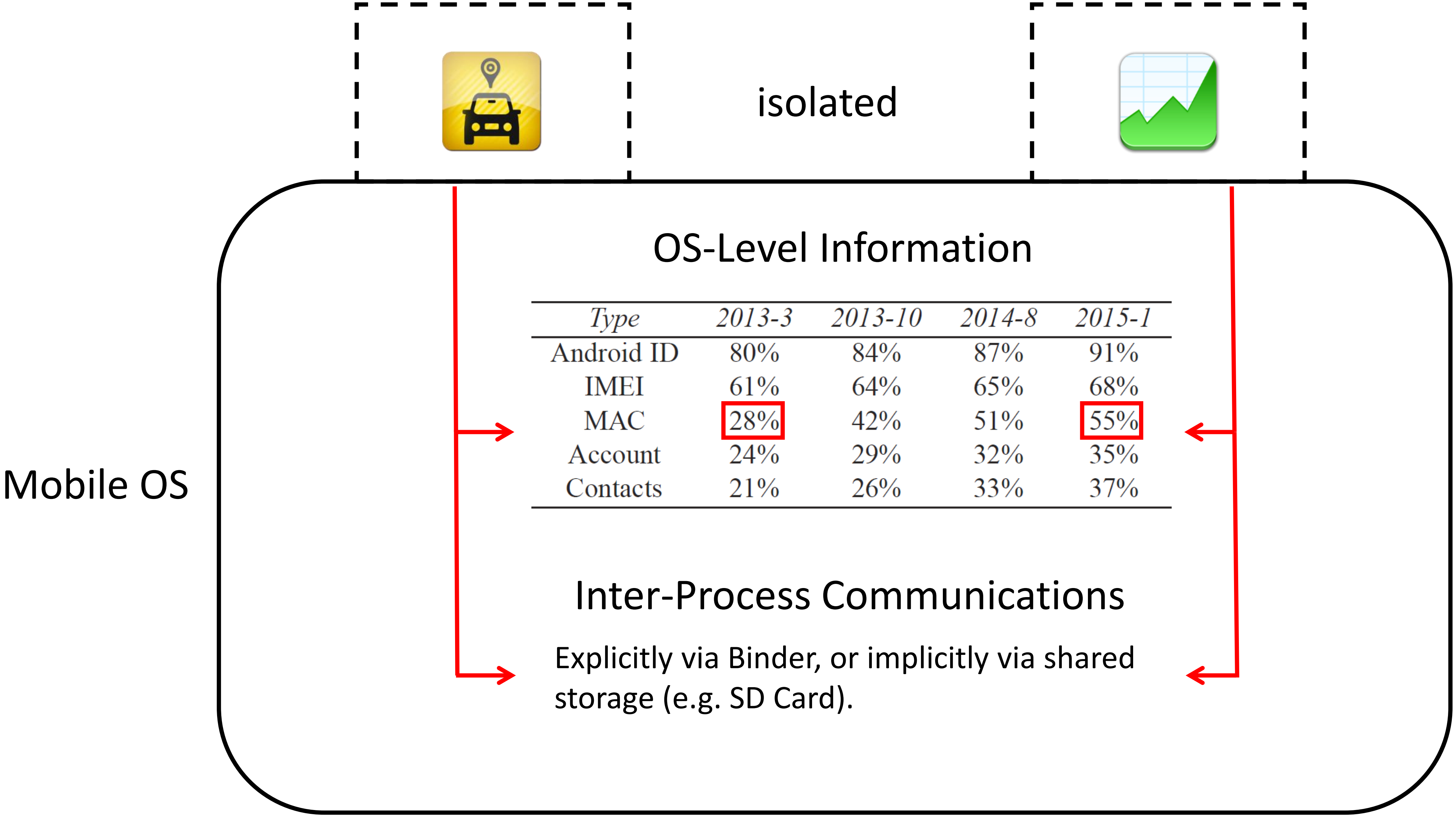
New paradigms (πBox, MoRePriv) ---> modify app & ecosystem

A Different Perspective

- Characterize & monitor the linkability across mobile apps
  - Two apps are *linkable* if can associate behaviors of the same user
  - Pre-requisites of conducting aggregation



A Novel Perspective



isolated

Mobile OS

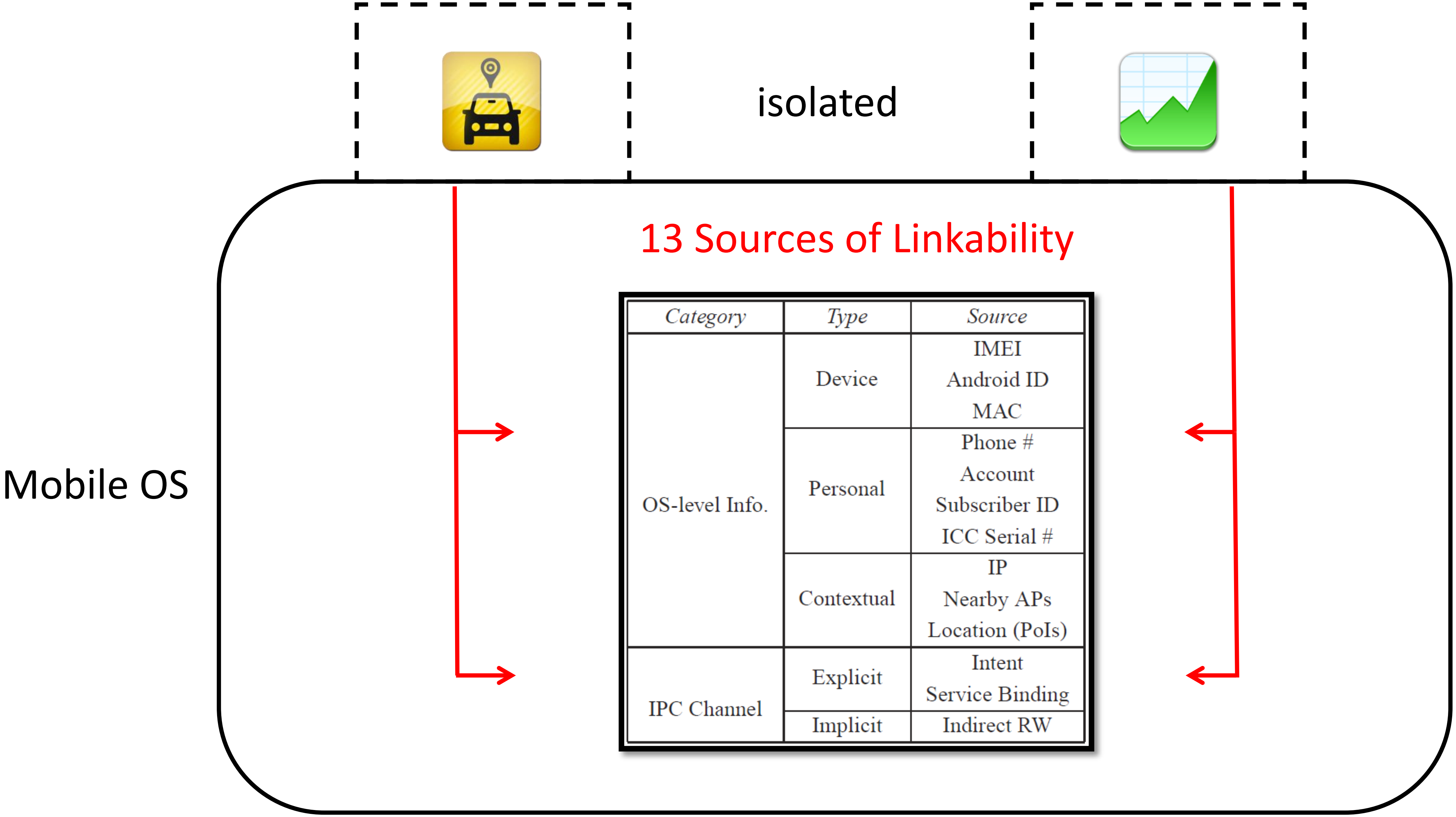
OS-Level Information

Type	*2013-3*	*2013-10*	*2014-8*	*2015-1*
Android ID	80%	84%	87%	91%
IMEI	61%	64%	65%	68%
MAC	28%	42%	51%	55%
Account	24%	29%	32%	35%
Contacts	21%	26%	33%	37%

Inter-Process Communications

Explicitly via Binder, or implicitly via shared storage (e.g. SD Card).

A Novel Perspective

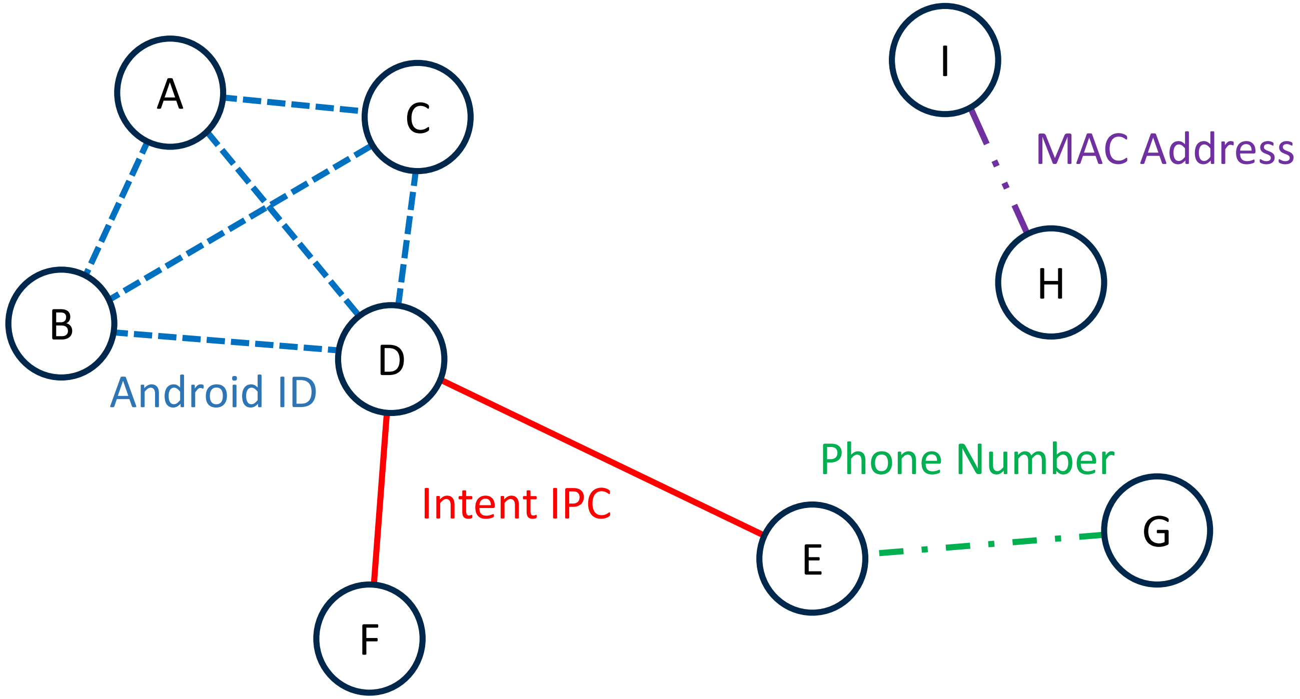


13 Sources of Linkability

Category	*Type*	*Source*
OS-level Info.	Device	IMEI Android ID MAC
	Personal	Phone # Account Subscriber ID ICC Serial #
	Contextual	IP Nearby APs Location (PoIs)
IPC Channel	Explicit	Intent Service Binding
	Implicit	Indirect RW

Mobile OS

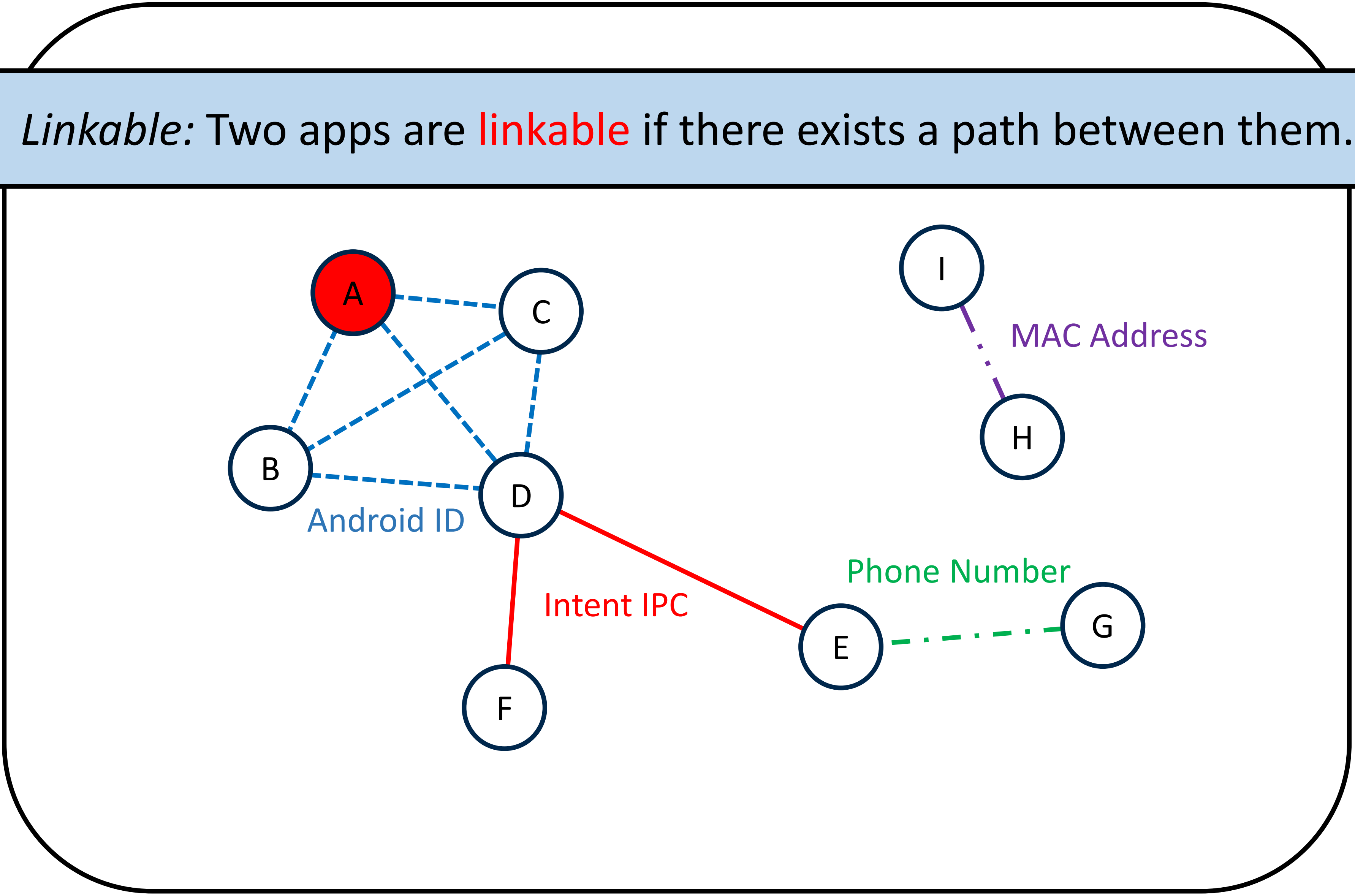
DLG: Dynamic Linkability Graph



1. Client-side information is enough
2. Quantify the privacy threat (though upper bound)

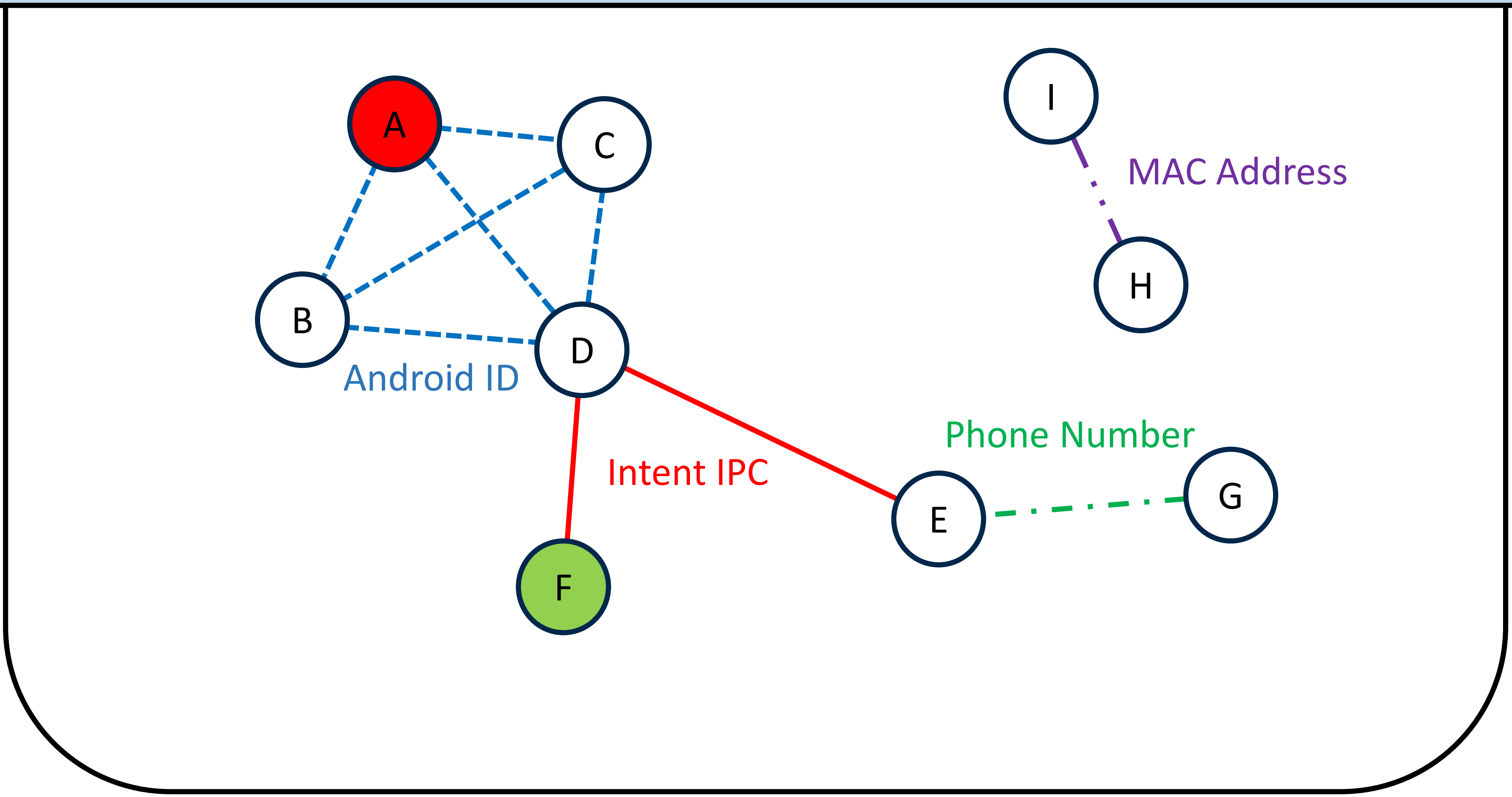
Linkable: Two apps are linkable if there exists a path between them.

Mobile OS

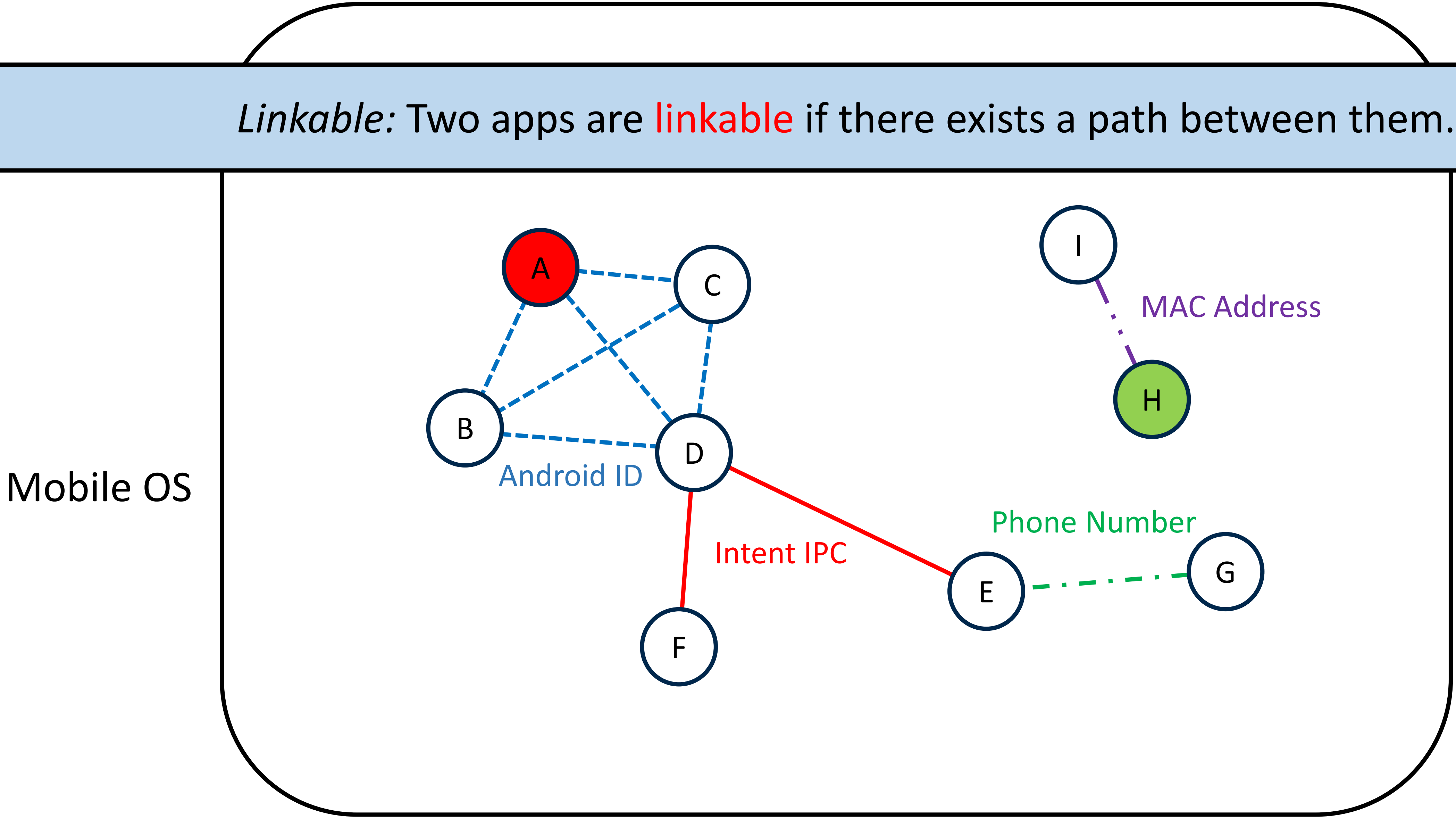


Linkable: Two apps are linkable if there exists a path between them.

Mobile OS

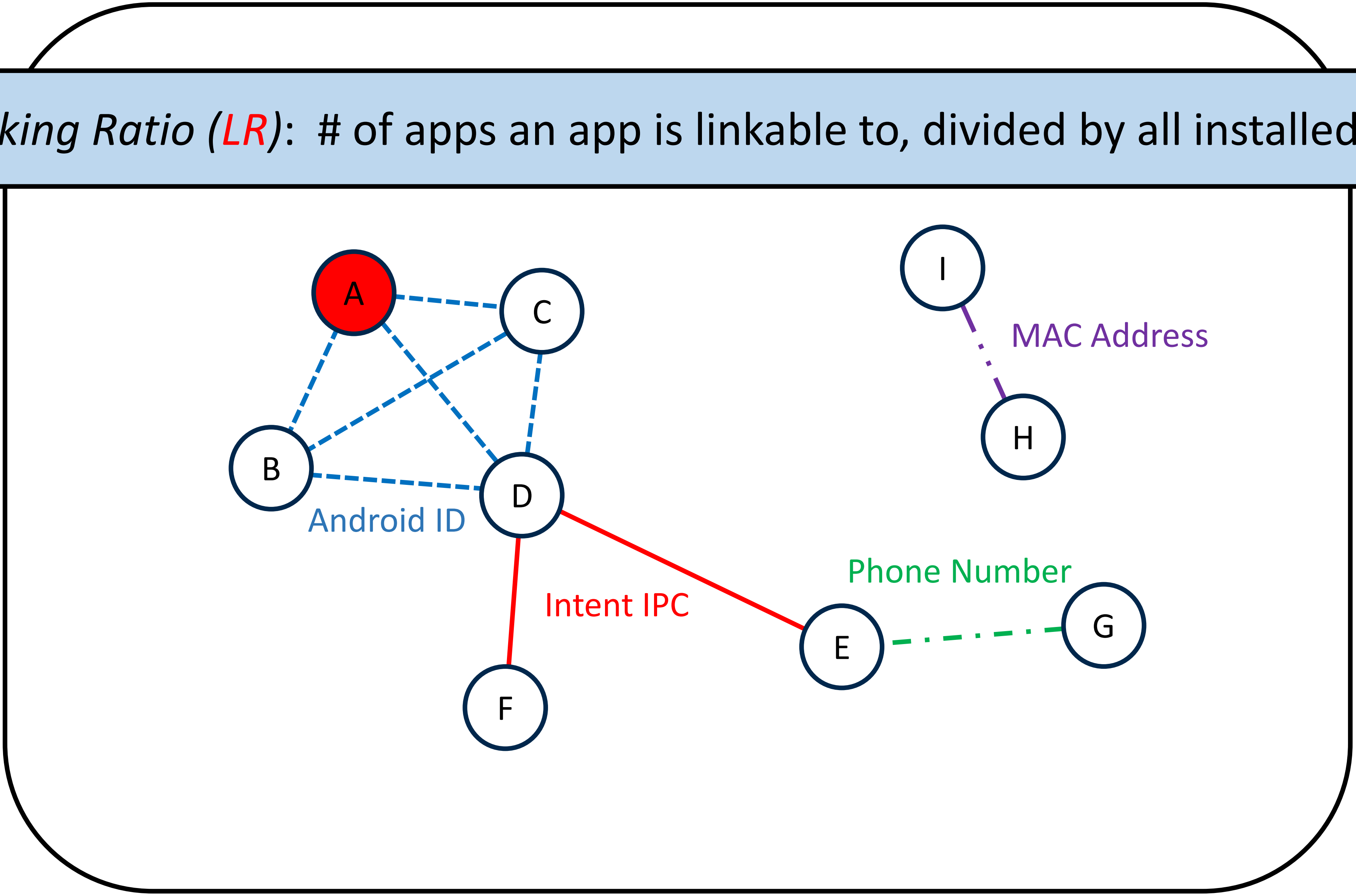


Linkable: Two apps are linkable if there exists a path between them.



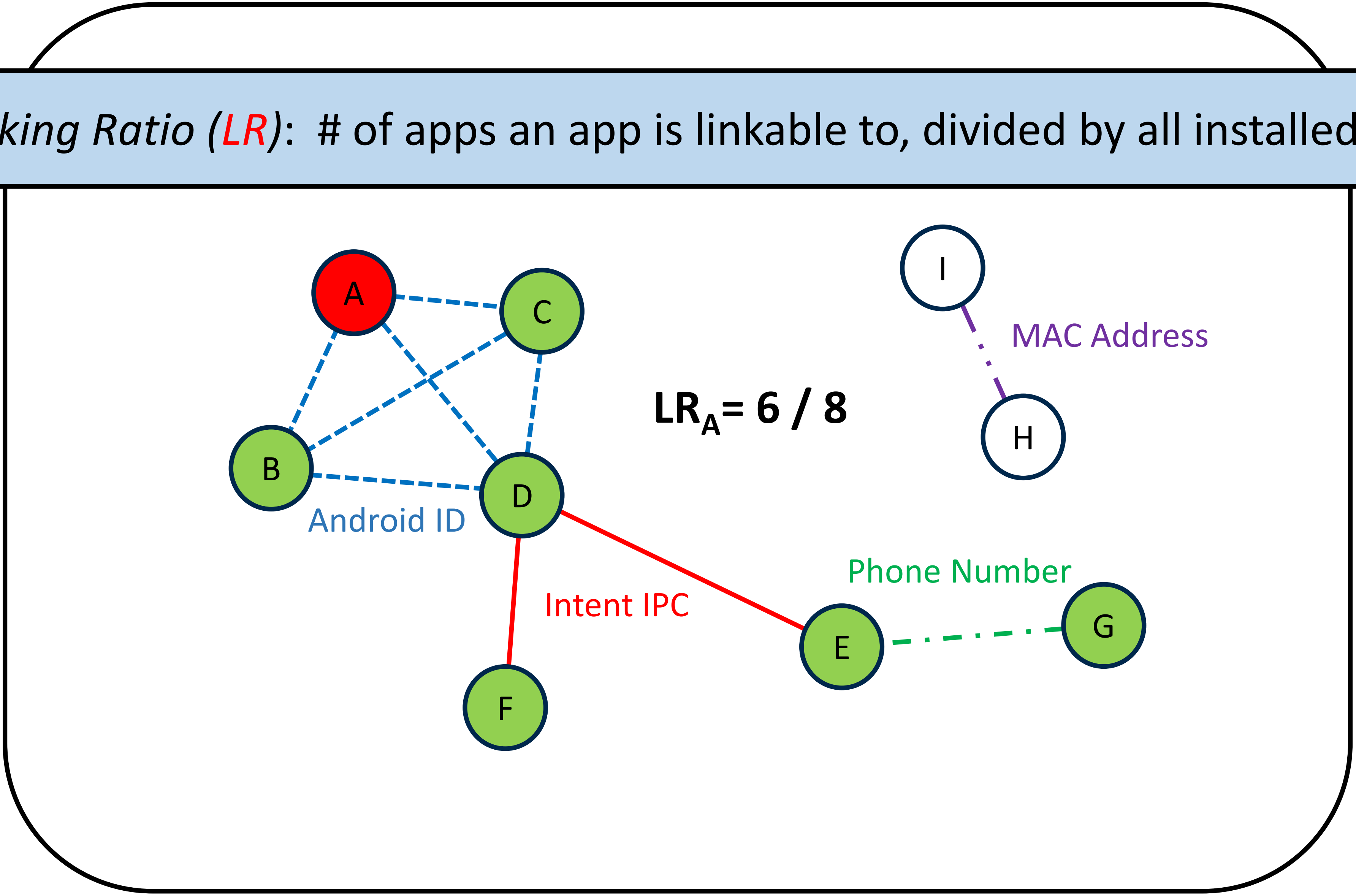
Linking Ratio (LR): # of apps an app is linkable to, divided by all installed apps

Mobile OS



Linking Ratio (LR): # of apps an app is linkable to, divided by all installed apps

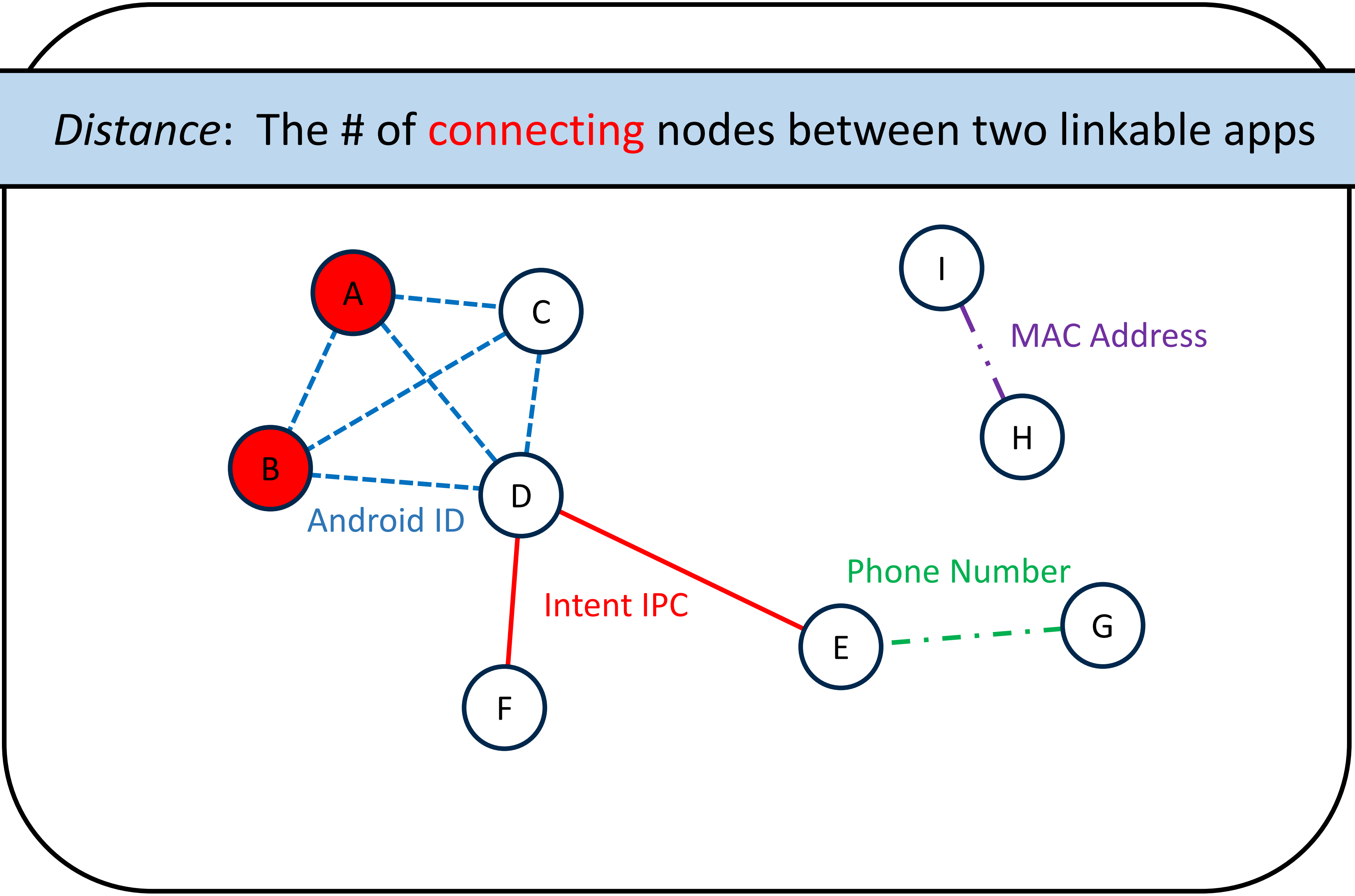
Mobile OS



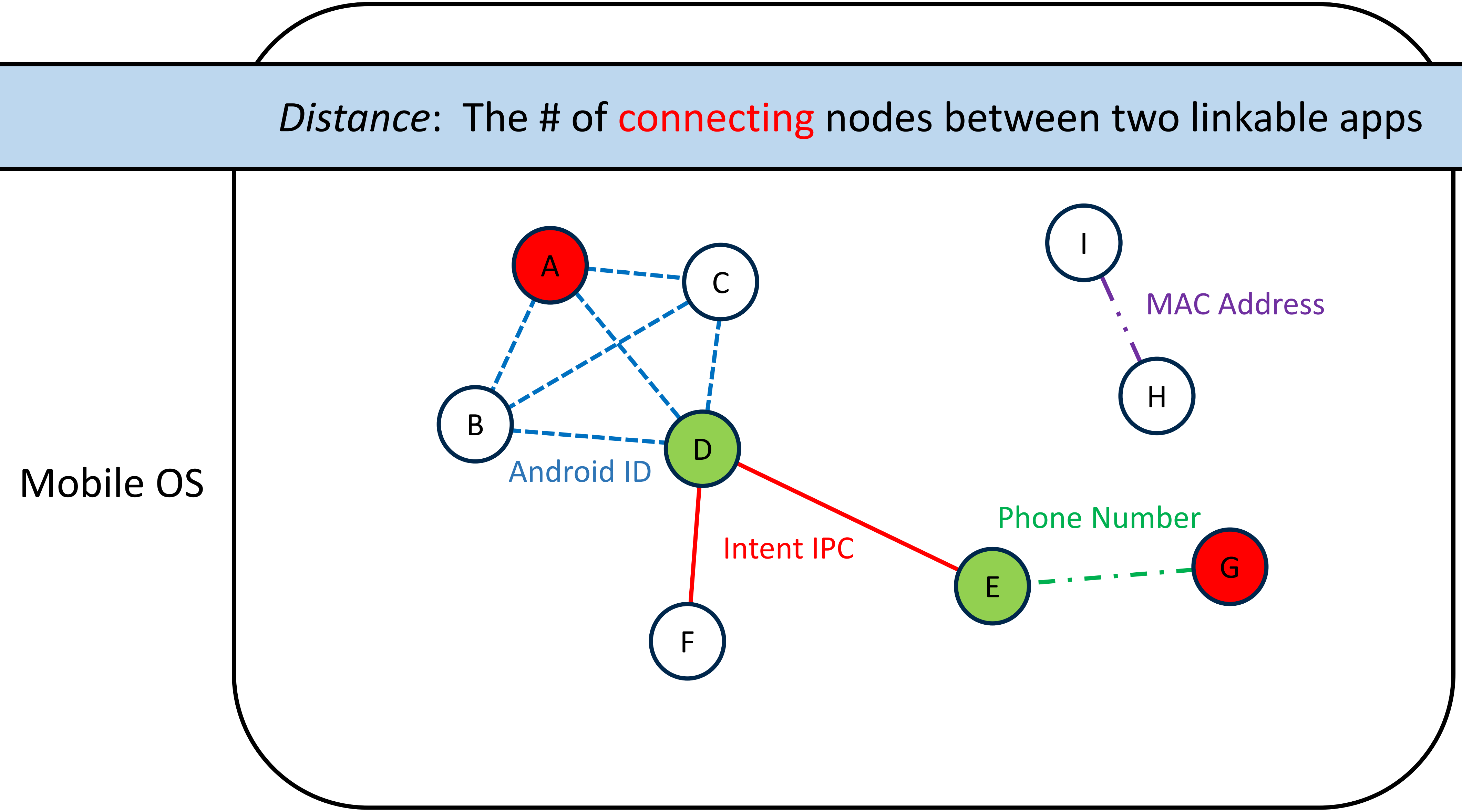
$LR_A = 6 / 8$

Distance: The # of <span>connecting</span> nodes between two linkable apps

Mobile OS

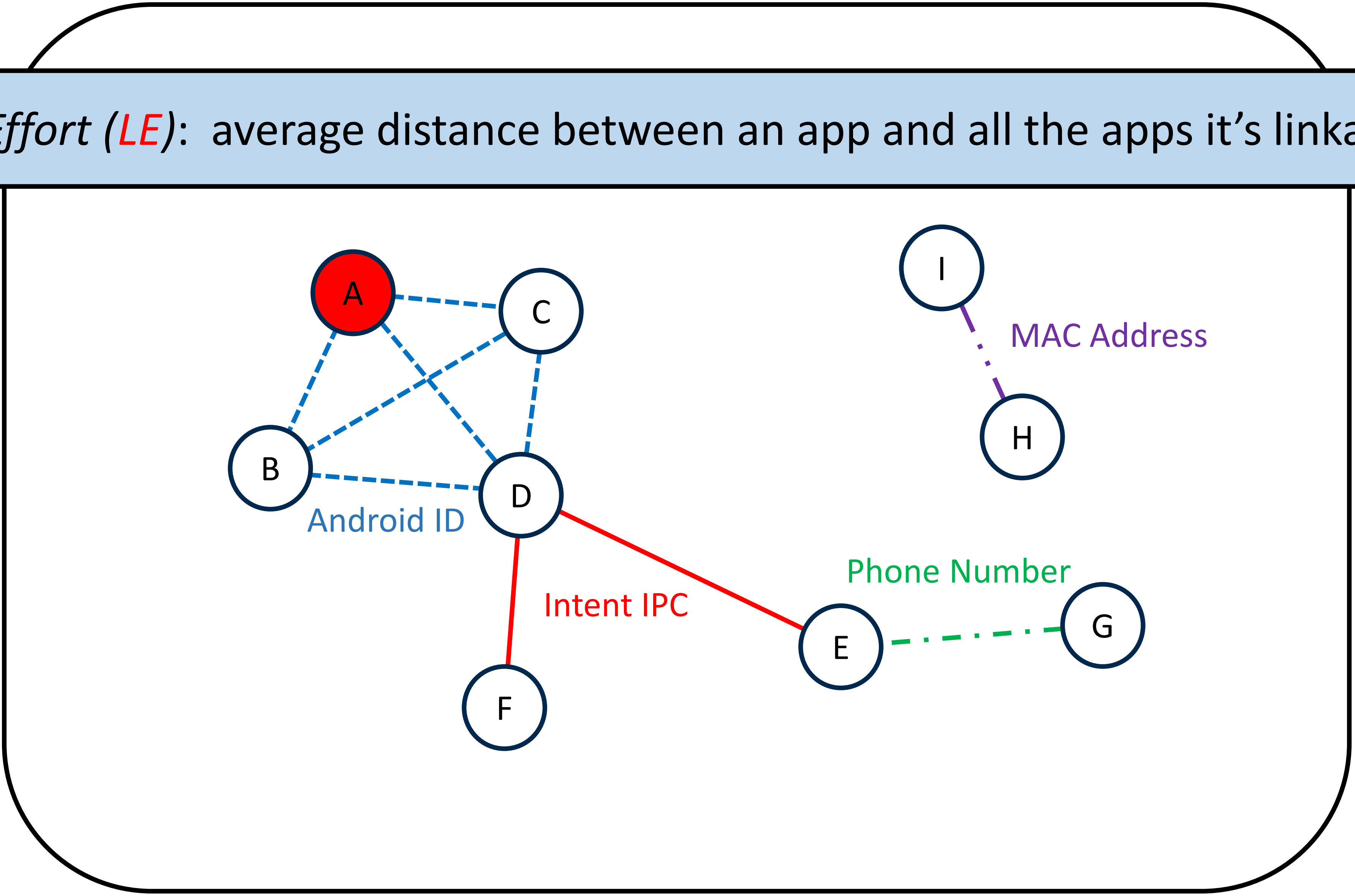


Distance: The # of connecting nodes between two linkable apps

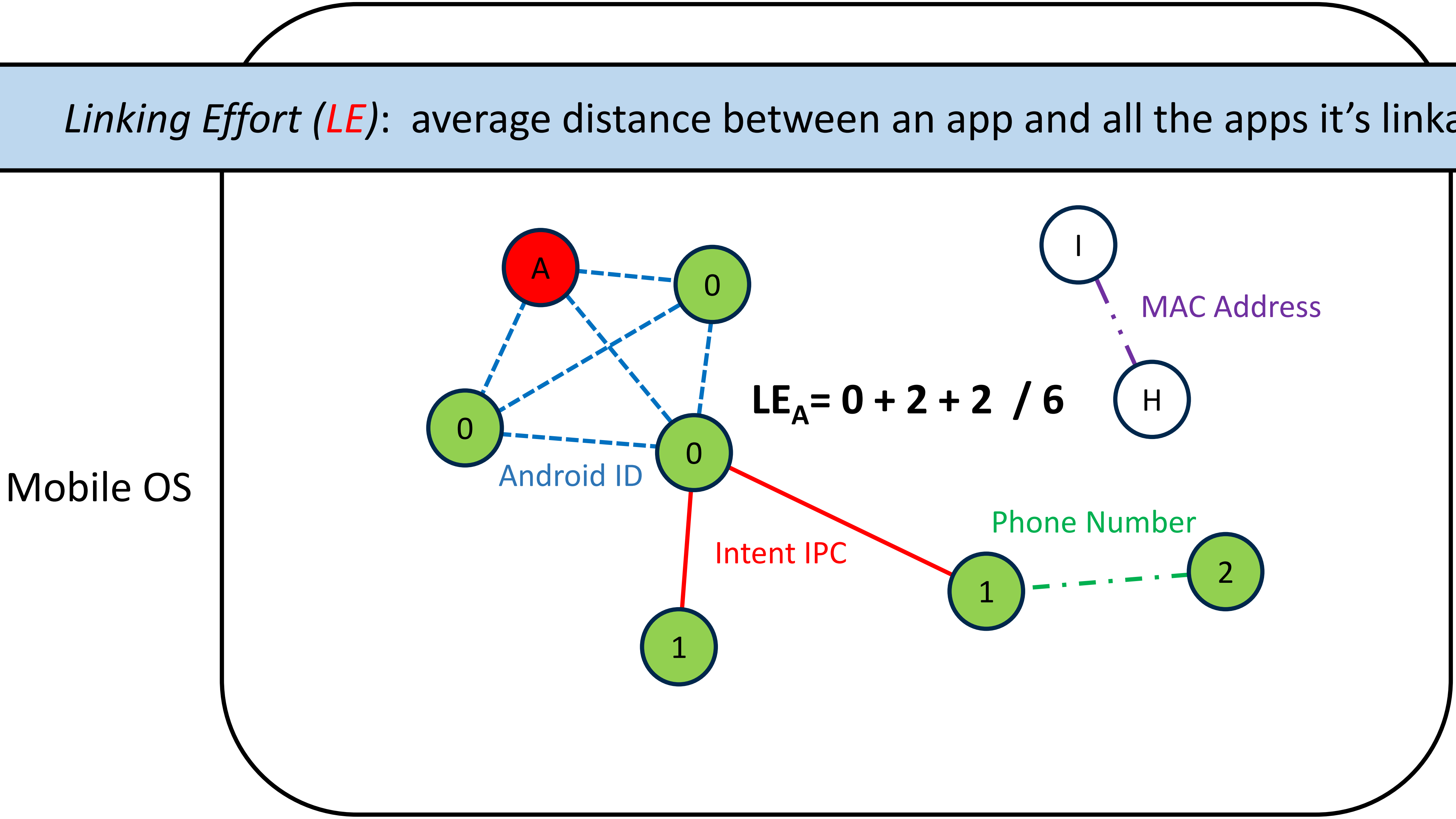


Linking Effort (LE): average distance between an app and all the apps it’s linkable to

Mobile OS

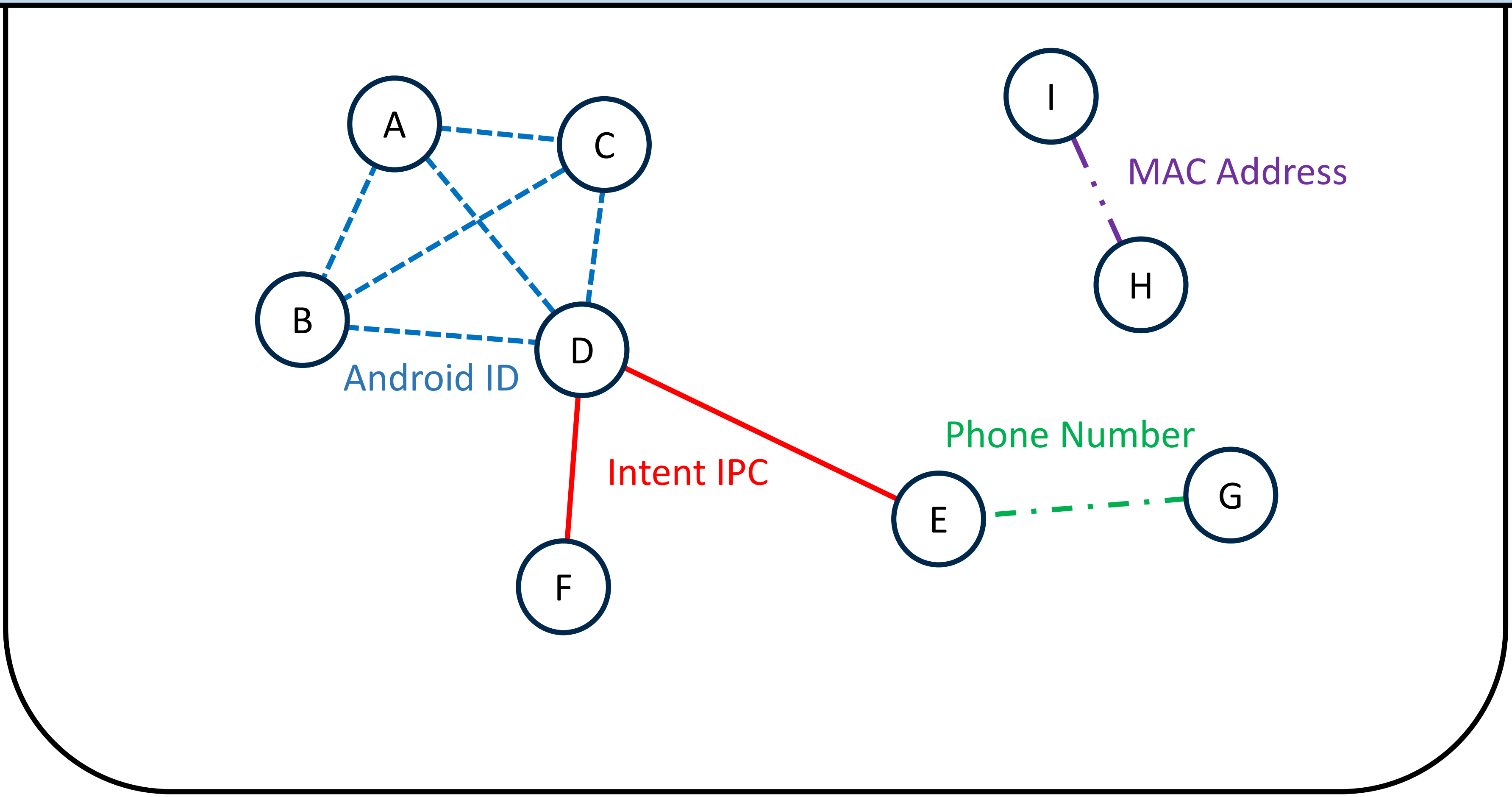


Linking Effort (LE): average distance between an app and all the apps it's linkable to

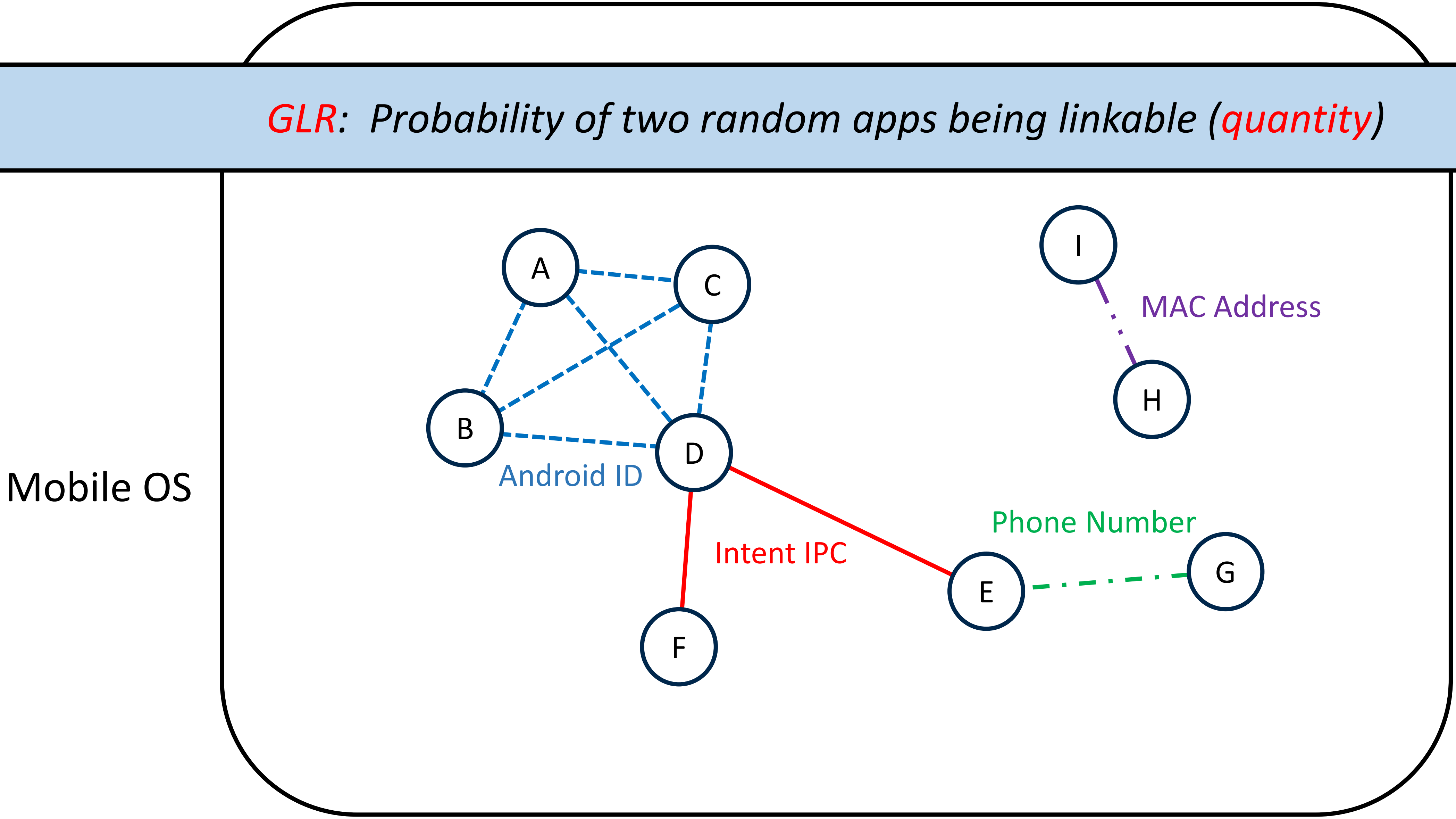


$LE_A = 0 + 2 + 2\ \ / 6$

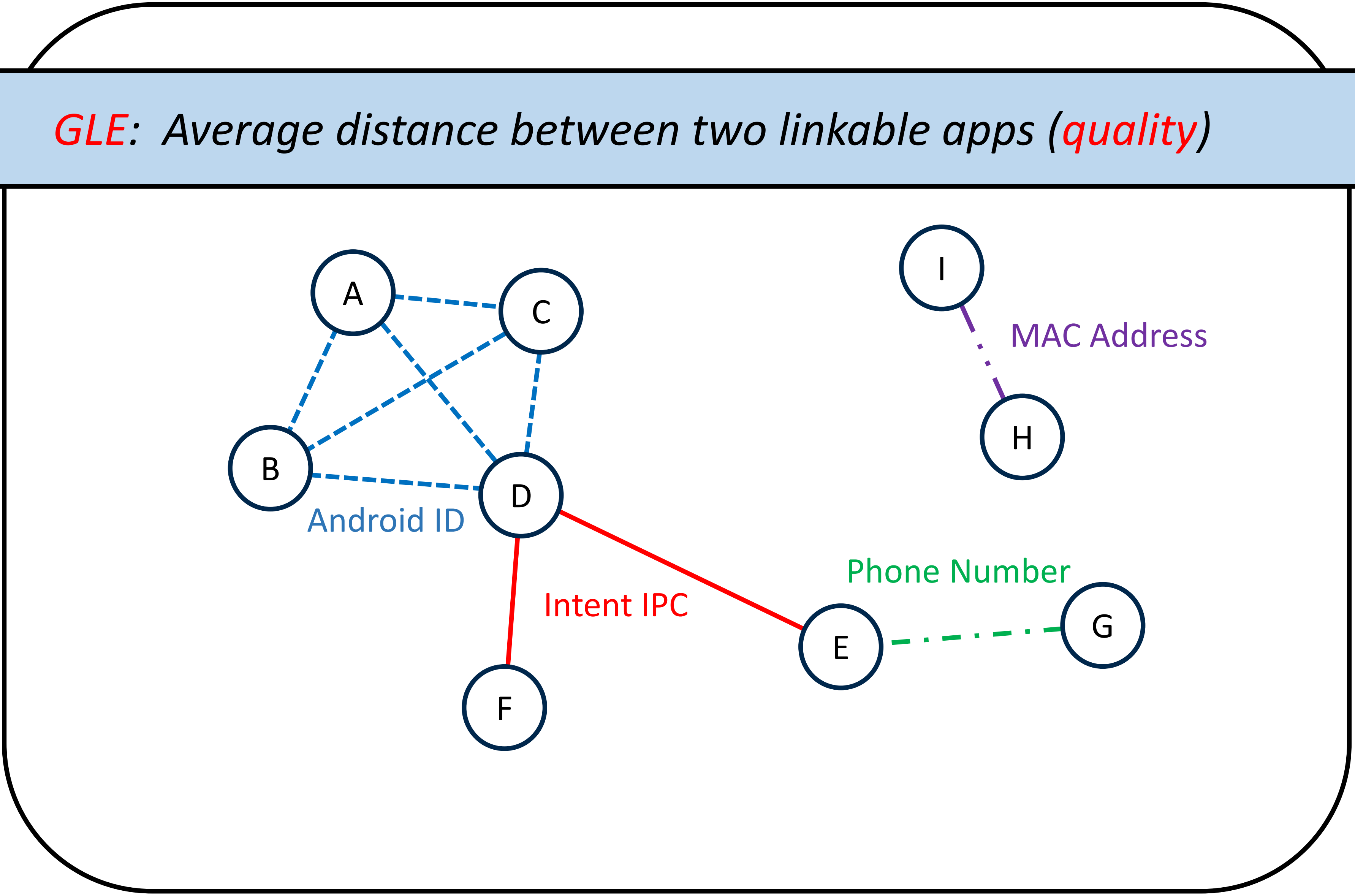
Global Linking Ratio (GLR) & Global Linking Effort (GLE)



GLR: Probability of two random apps being linkable (quantity)



GLE: Average distance between two linkable apps (quality)



Mobile OS

Real-world Evidence

An Emerging Threat

Unregulated Aggregation of App-Usage Behaviors

A Novel Perspective

Dynamic Linkability Graph (DLG)

Real-world Evidence

DLG in the real-world

Proposed Solution

LinkDroid: Runtime Monitoring & Mediation

DLG: A Mobile Extension

- Alternative approaches
  - User-level Interception (Aurasium)
  - Dynamic OS Instrumentation (Xposed Framework)

- Monitor various access to OS-level Info & IPC Channels
  - System Services (Wifi, Telephony, etc)
  - Content Provider
  - Intent Firewall
  - FUSE Daemon

The Alarming Findings

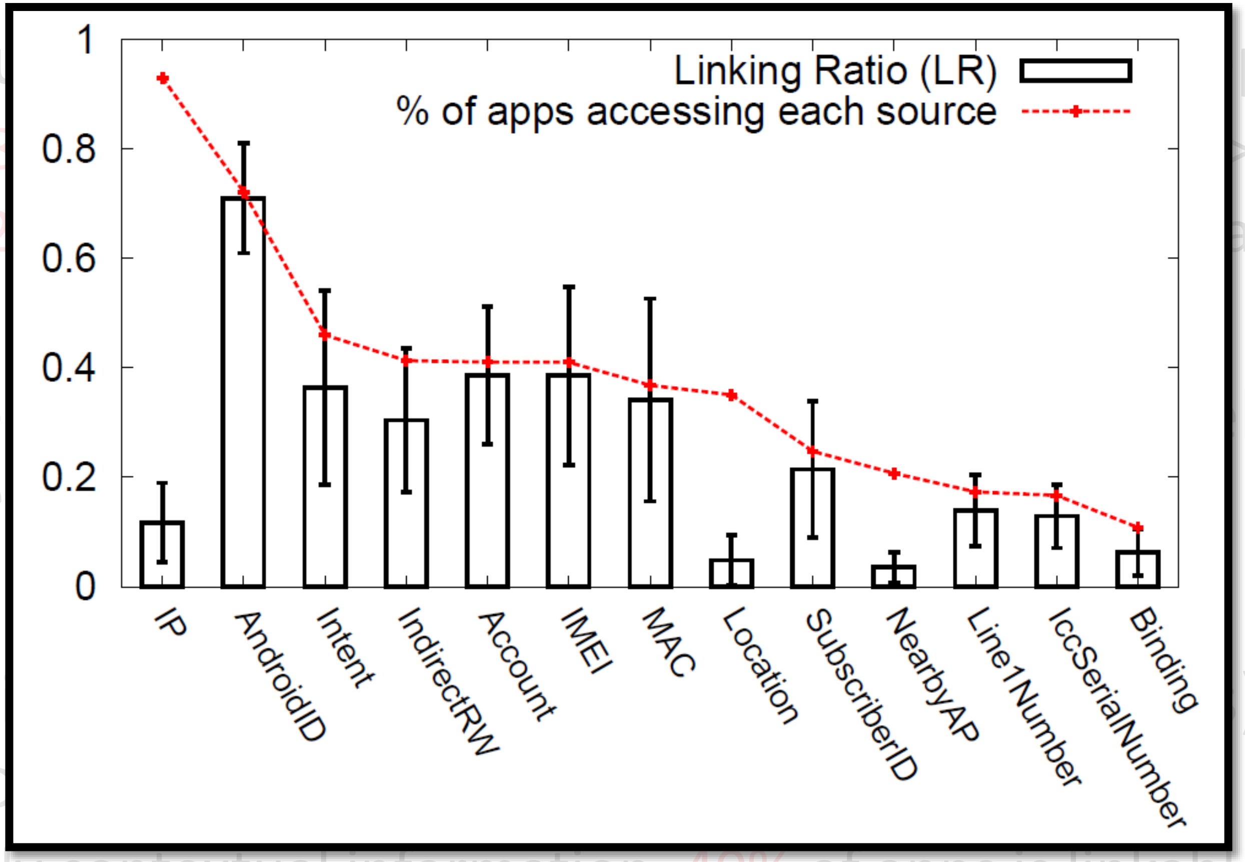
- DLG of 13 users during 47 days using 215 unique apps
  - GLR = 0.81 (two random apps are linkable -> 81%)
  - GLE = 0.2 (control 0.2 additional apps, on average)

- 86% of the apps a user installed are linkable to Facebook, namely his real identity

- Linkability is contributed by various factors (sources)
  - Device ID leads, with others following closely behind
  - Using only contextual information, 40% of apps is linkable to Facebook

Linkability contributed by different sources are proportional to the % of apps accessing each source, except for quasi-identifiers.

- DLG of 13 u ps
  - GLR = 0.8 > 81%)
  - GLE = 0.2 average)
- 86% of the book, namely his real ide



- Linkability)
  - Device ID
  - Using only contextual information, 40% of apps is linkable to Facebook

Functional Analysis

- *OS-level Information*

• *Device ID*	no need for the actual identifiers
• *Personal ID*	*abuse user accounts & phone #*
• *Contextual ID*	exploit Location & nearby AP

- *IPC Communications*
  - Apps report their installation using Intents (WeChat)
  - Apps bind to service & exchange user IDs (Facebook, AdMob)
  - Apps read identifiers written by other apps (Qingting Radio)
- Subject to personal preference and application context

Proposed Solution

An Emerging Threat

Unregulated Aggregation of App-Usage Behaviors

A Novel Perspective

Dynamic Linkability Graph (DLG)

Real-world Evidence

DLG in the real-world

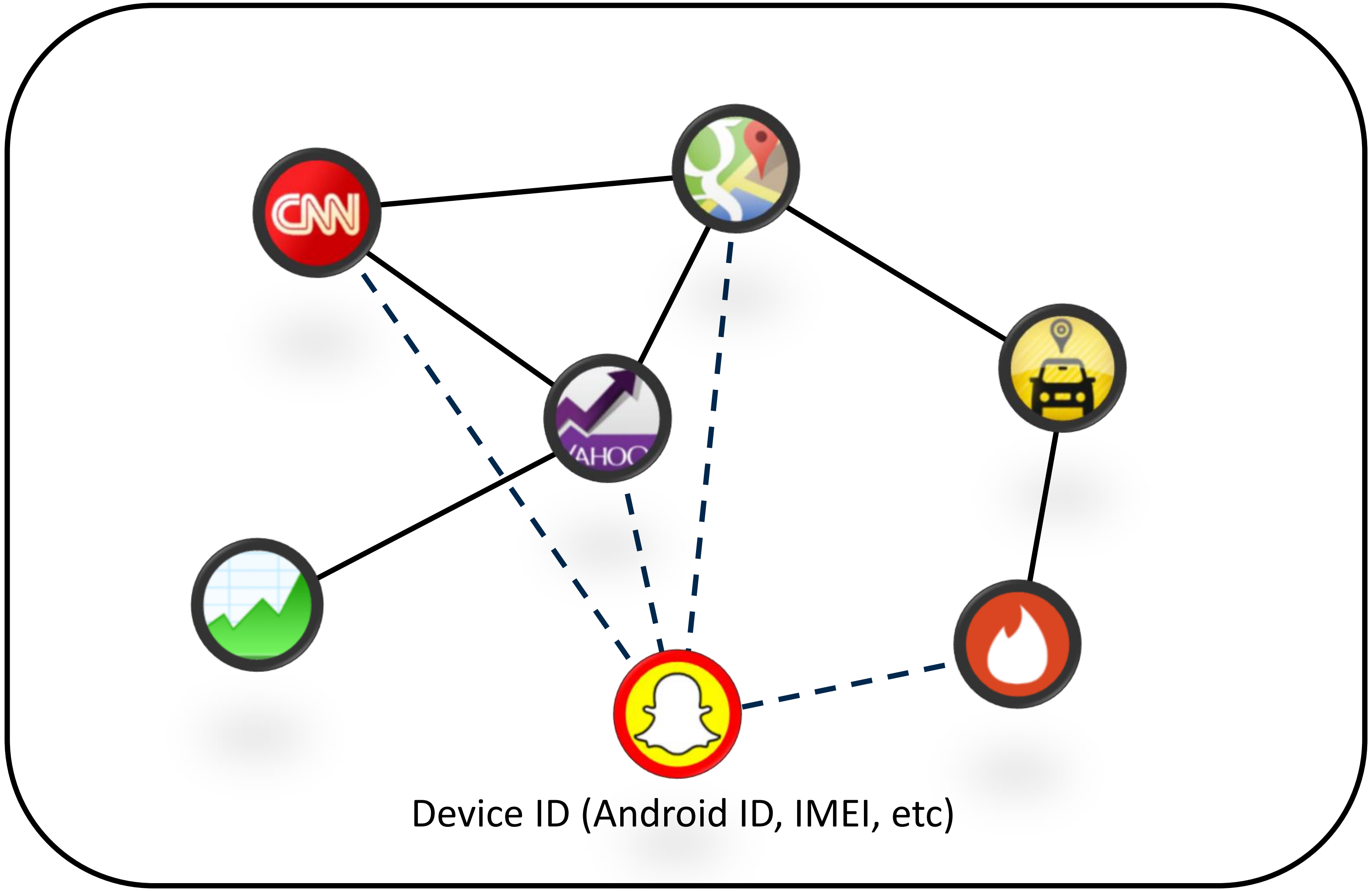
Proposed Solution

LinkDroid: Runtime Monitoring & Mediation

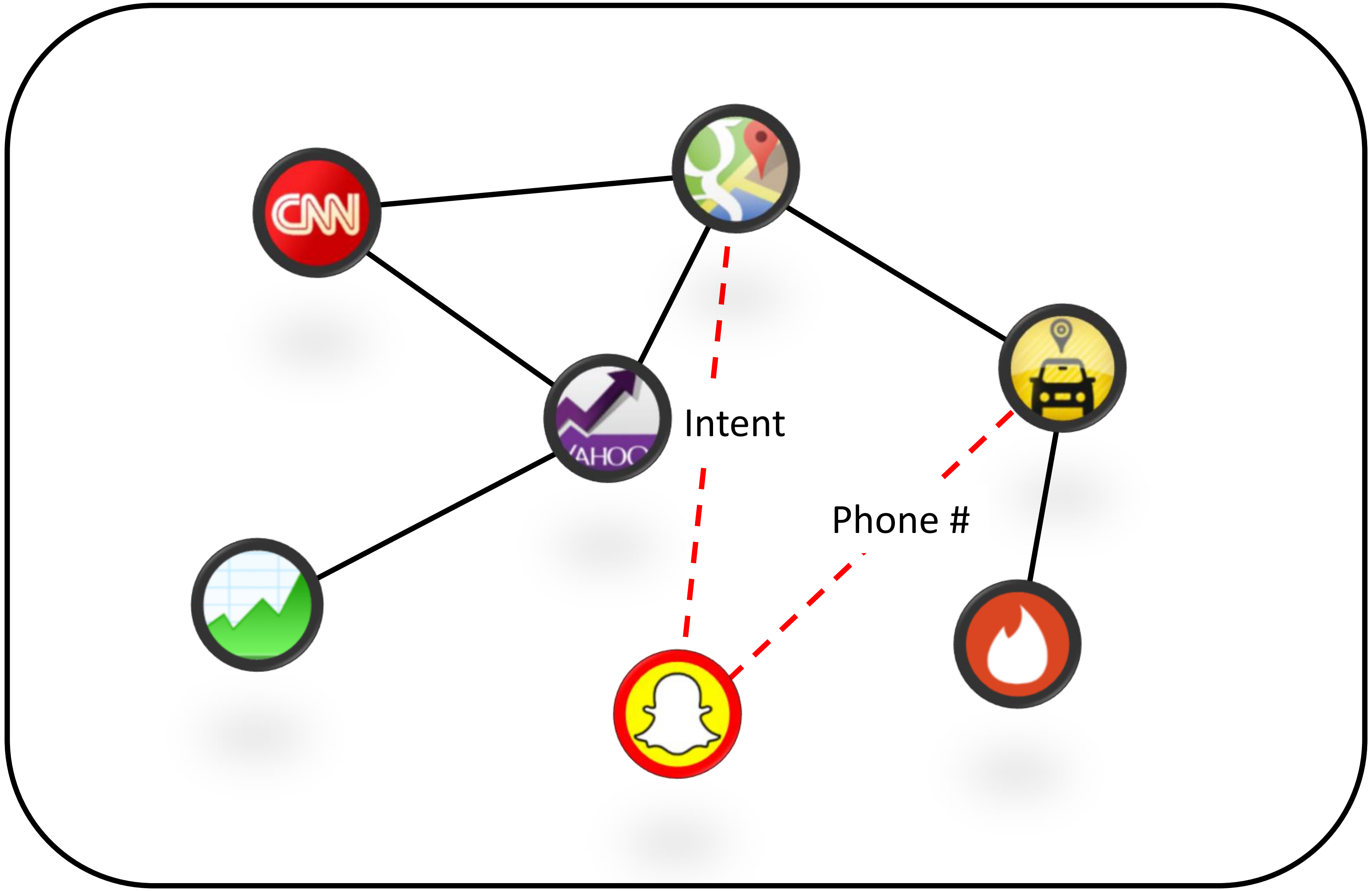
LinkDroid

- Designed with practicality in mind
    - No modification of apps, no additional trusted parties
    - Works purely on the client-side
- A new dimension to privacy protection on mobile OS
    - How app behaviors implicitly affect linkability
    - Opt-out & reduce unnecessary links
- Features provided by LinkDroid
    - Install-time Obfuscation
    - DLG-powered Runtime Monitoring
    - Unlinkable Mode

Install-time Obfuscation



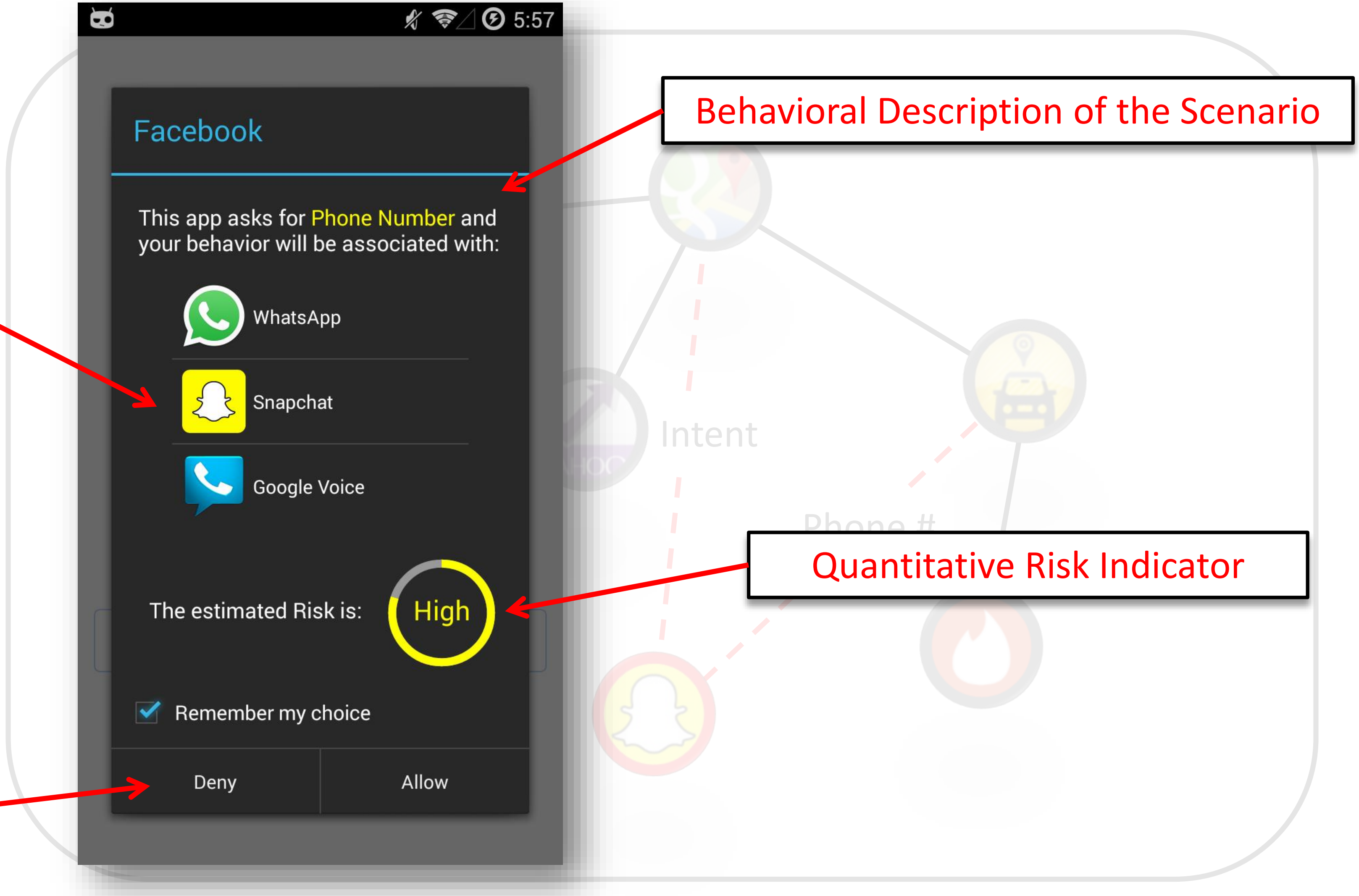
Runtime Monitoring



Runtime Monitoring

Descriptive Risk Indicator

Opt-out Options



5:57

Facebook

This app asks for Phone Number and your behavior will be associated with:

- WhatsApp
- Snapchat
- Google Voice

The estimated Risk is: High

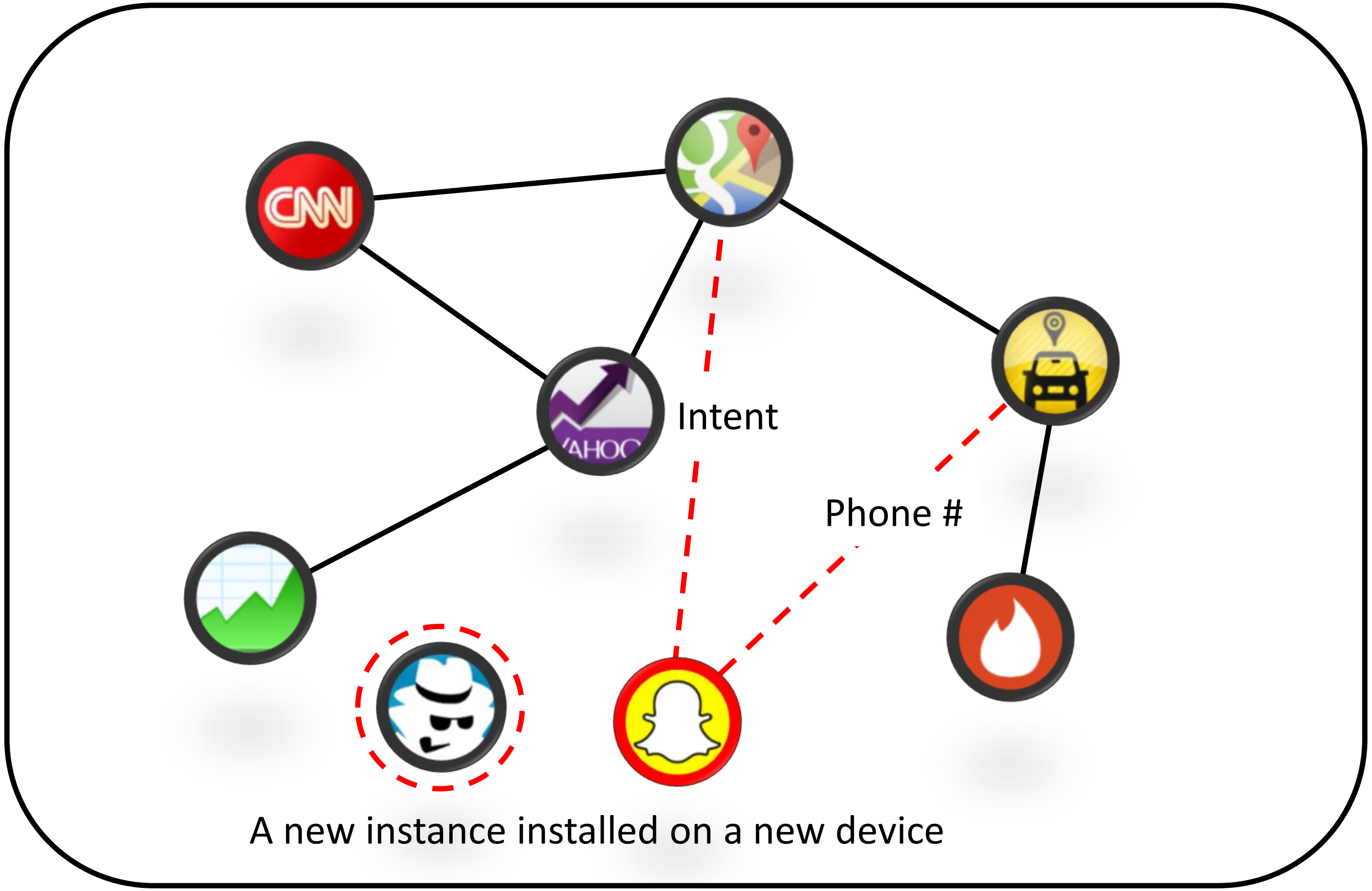
☑ Remember my choice

Deny | Allow

Behavioral Description of the Scenario

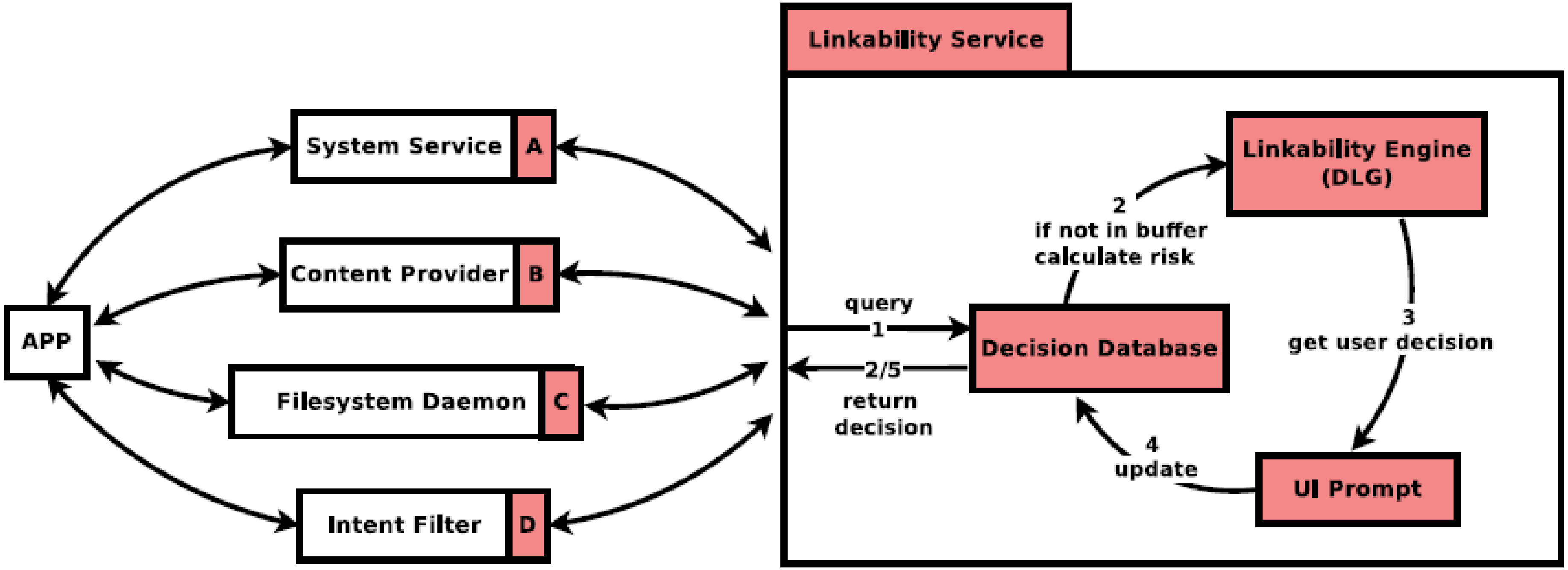
Quantitative Risk Indicator

Unlinkable Mode



A new instance installed on a new device

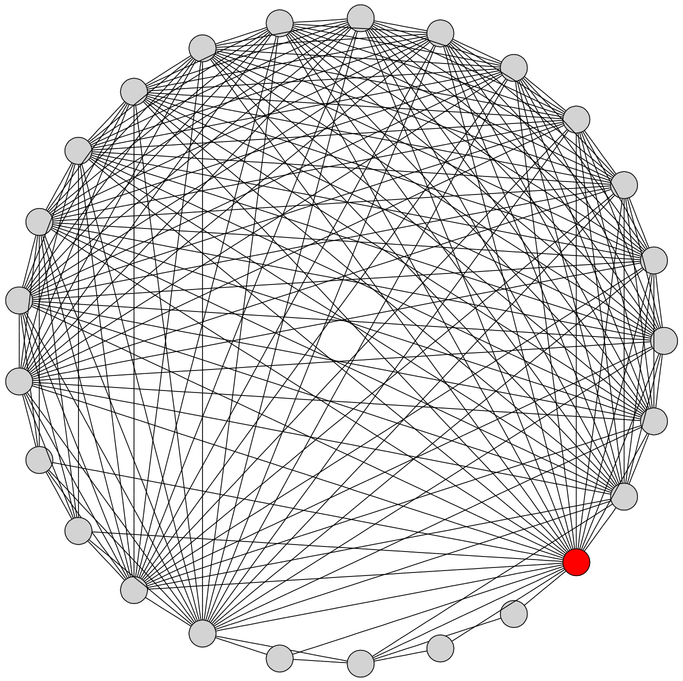
Design of LinkDroid



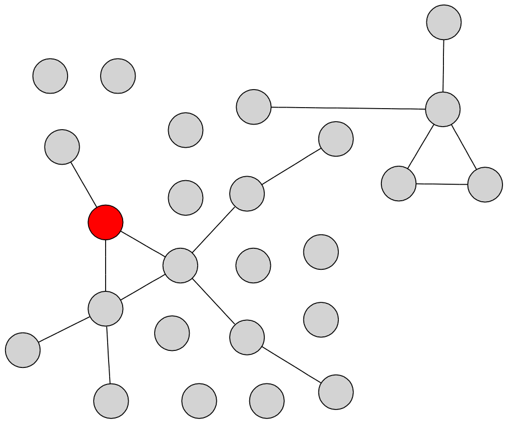
Evaluation

- Evaluated on the same set of 13 participants as in the measurement
  - Replay traces collected in the measurement with LinkDroid features
- GLR (*two random apps being linkable*): 81% to 21%
- GLE (*additional apps required to link two apps*): 0.22 to 0.68
  - Under most scenarios, at least one additional app is required
- Apps directly linkable to Facebook dropped from 86% to 18%

DLG of a representative user *before* and *after* applying LinkDroid.
(Red circle is the Facebook app)



(a) before



(b) after

Takeaway

Leaked (shared) information should NOT be linkable unless REALLY necessary

Linkability: a useful but MISSING notion in the mobile ecosystem

Anonymous (unlinkable) in-app behaviors should be a BASIC right

Questions?

LinkDroid: Reducing Unregulated Aggregation of App-Usage Behaviors

Huan Feng

huanfeng@umich.edu