p2p e privacy in rete con OneSwarm

OneSwarm

Privacy preserving peer-to-peer data sharing

Jan Reister

18 dicembre 2009 @ Dipartimento di Informatica e Comunicazione – Università di Milano

Come sorvegliare gli utenti p2p?

Per LAN,ISP,Carrier:

- Analisi e ispezione del traffico

Per tutti gli altri:

- partecipazione dinamica
- connessioni dirette peer to peer
- quali dati esaminare?

Come sorvegliare BitTorrent?

Tramite le informazioni sui peer e sui contenuti disponibili:

- Tracker – coordinamento centrale
- DHT – distributed hash table (trackerless)
- PEX – peer exchange (gossip)

Con le connessioni dirette peer to peer

WANTED!

–FOR COPYRIGHT INFRINGEMENT–

U.WASHINGTON PRINTER

LAST SEEN DOWNLOADING INDIANA JONES, IRON MAN

HTTP://DMCA.CS.WASHINGTON.EDU

18/12/2009

Guarda, una notifica DMCA!

Michael Piatek, Arvind Krishnamurthy et al:

Why My Printer Received a DMCA Takedown Notice (2008)

http://dmca.cs.washington.edu

Mark Freedman, (11-12/2009)

Inaccurate Copyright Enforcement: Questionable "best" practices and BitTorrent specification flaws

Erroneous DMCA notices and copyright enforcement, part deux

http://www.freedom-to-tinker.com/blog/mfreed

I sistemi p2p oggi

Accettabile efficienza tecnica

- Scalabilità, controllo di congestione, incentivi

Scarsa o nulla privacy

Modello di condivisione pubblica “tutto o niente”

Sorveglianza e manipolazione del traffico:

- Denial of service
- Profilazione
- Censura
- Abusi legali (DMCA, 3-strikes)

2009: nasce OneSwarm

Privacy-preserving p2p data sharing with OneSwarm

Thomas Isdal, Michael Piatek, Arvind Krishnamurthy, Thomas Anderson

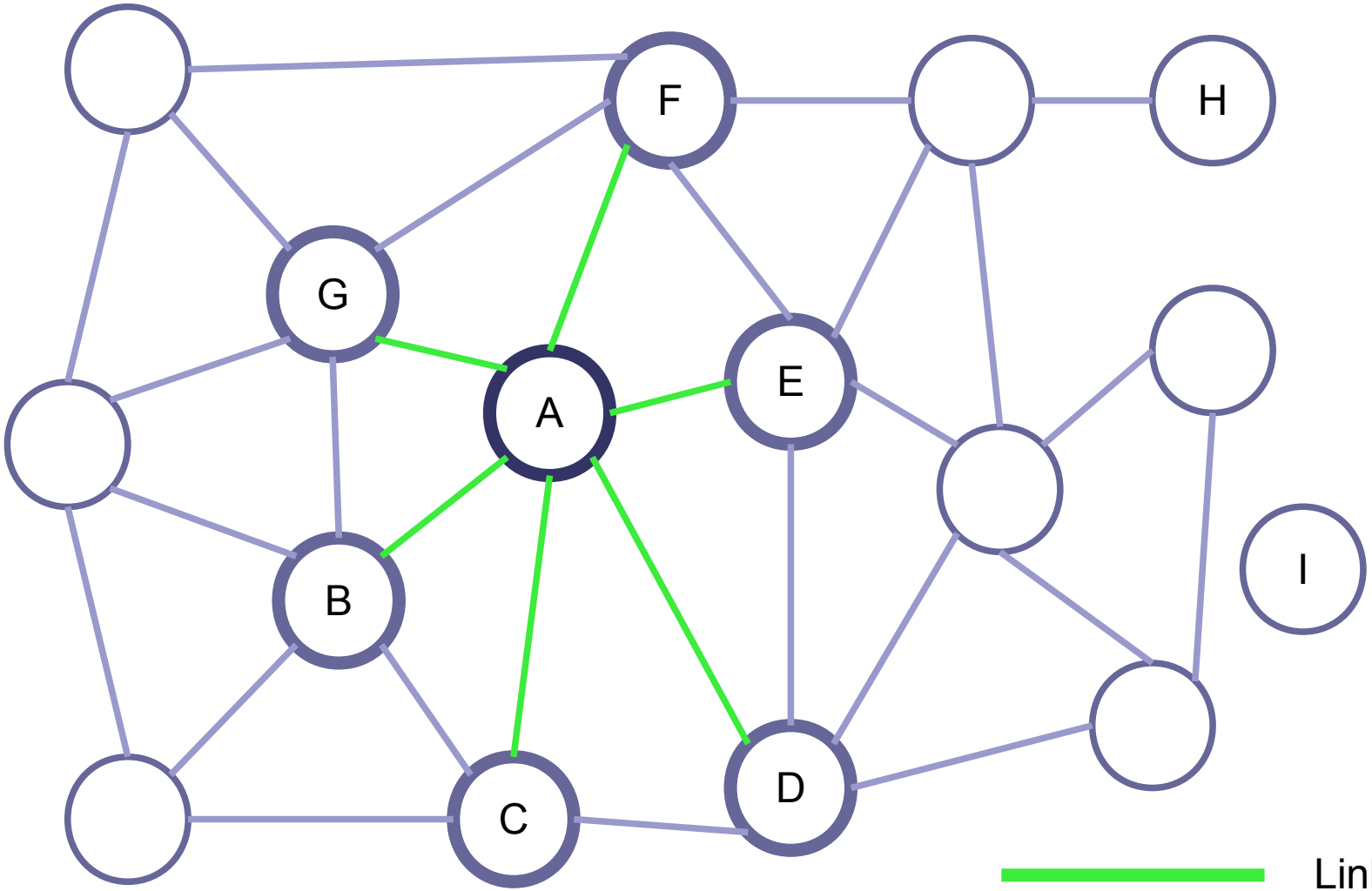
http://oneswarm.cs.washington.edu

- Nasce da una lunga competenza teorica e pratica sulle reti p2p BitTorrent
- Basato su una particolare mix-net
- Usa idee e componenti di BitTorrent (Azureus/Vuze)
- Obiettivi: privacy, usabilità, adozione, prestazioni

OneSwarm in 3 minuti

- È un software p2p che permette all'utente sceglie **cosa** condividere, con **chi**, **come**
- Impedisce l'analisi del traffico (cifrato, mix-net)
- Ha prestazioni elevate (400KB/s in lab.)
- In Java, GUI multilingue
- progetto attivo, con vasta base utenti
- Open source (GPL(v2), Apache, CPL, CC)
- Oggi alla versione 0.6.9

I peer diretti



I peer diretti (2)

identità persistente:

- ogni peer ha una coppia di chiavi RSA

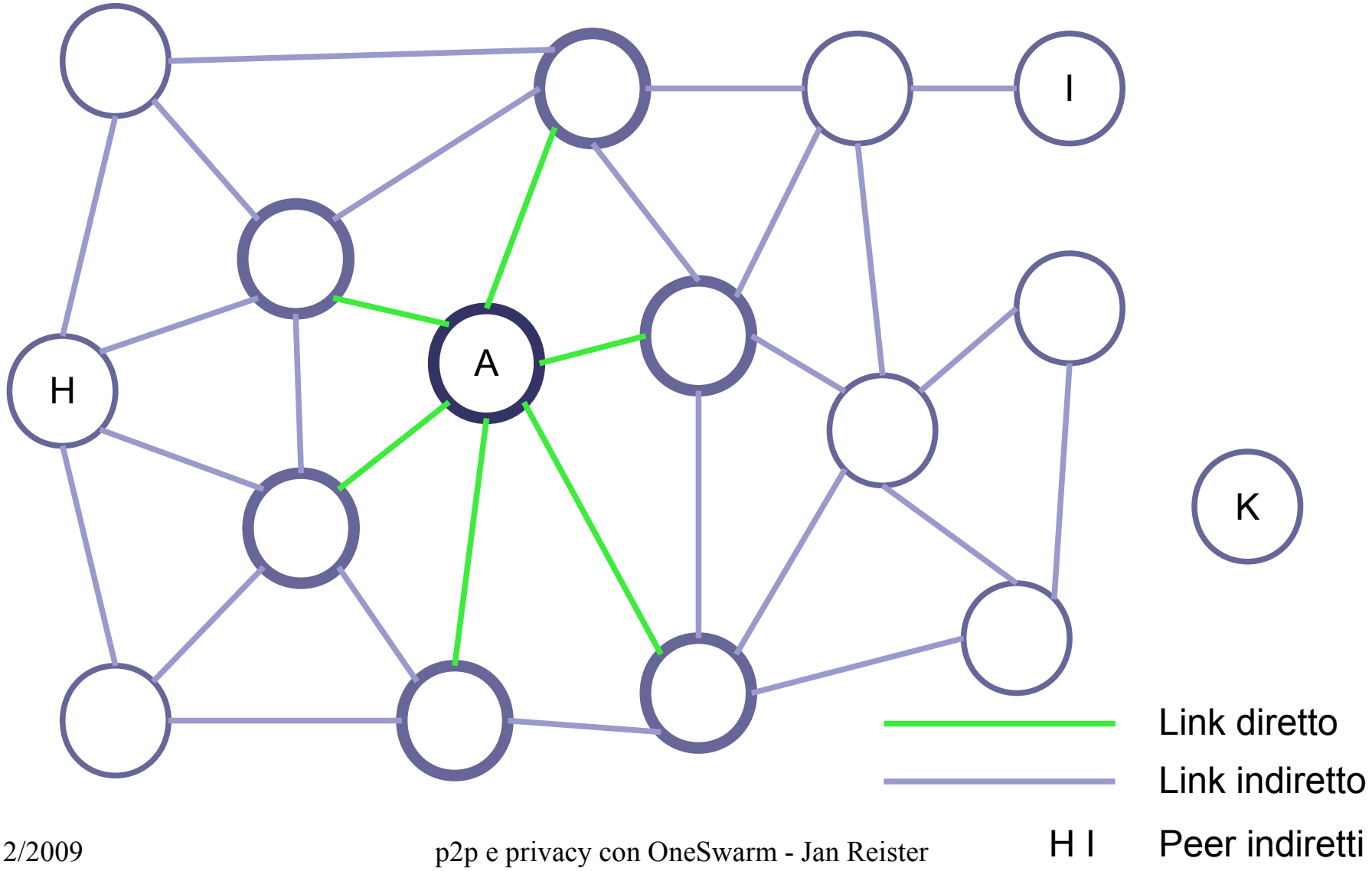
Posizione (indirizzo IP):

- informazioni distribuite con una DHT
- IP:porta cifrati **per peer**
- resistenza a monitoraggio sistematico nella DHT

Ricerca dei peer:

- amici = chiavi pubbliche, importate via LAN, social network (Google Talk), inviti via email, community server

I peer indiretti



I peer indiretti (2)

ogni peer conosce :

- direttamente, i peer di cui ha la chiave (amici e limitati)
- indirettamente, i peer collegati nella rete f2f

L'overlay network (f2f) distribuisce le informazioni sulla topologia della rete OneSwarm

un attaccante non può esplorarlo sitematicamente

- È limitato dalla posizione di rete (DHT) e dalle chiavi dei peer di cui dispone

La ricerca dei dati

Identificare un file:

- hash dei dati e generazione di coppie peer-dati

Cercare un file:

- flood di ricerche nell'overlay network
- nessun server centrale, nessuna DHT contenuti
- search, reply, cancel

Ostacoli all'analisi del traffico

- ritardo e casualità determinata nelle risposte
- ottimizzazione dei percorsi

Link e path

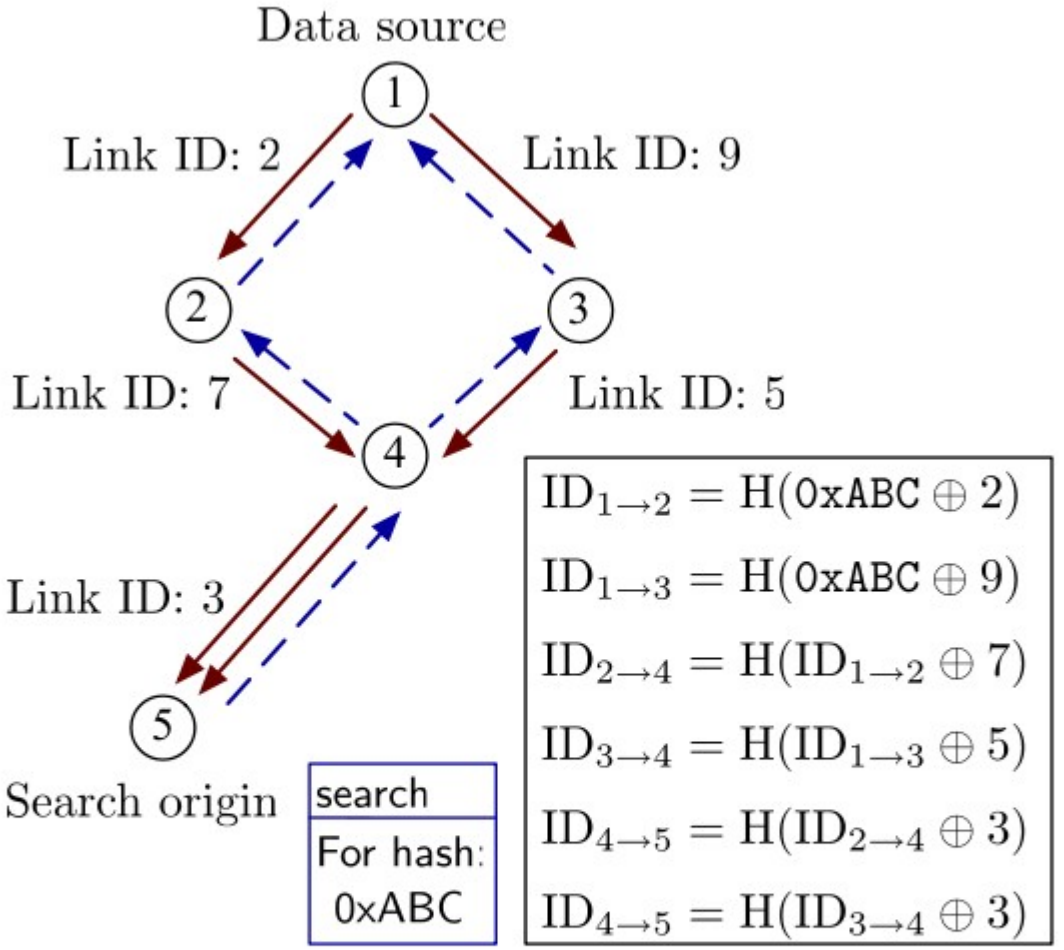


Figure 2: An example of end-to-end path ID computation. Client 5 searches for peers with file ID 0xABC and queries are forwarded along the dashed links.

Link e path (2)

La ricerca dati si propaga lungo i link

Il recupero dati avviene lungo i path

- indiretto, address rewriting

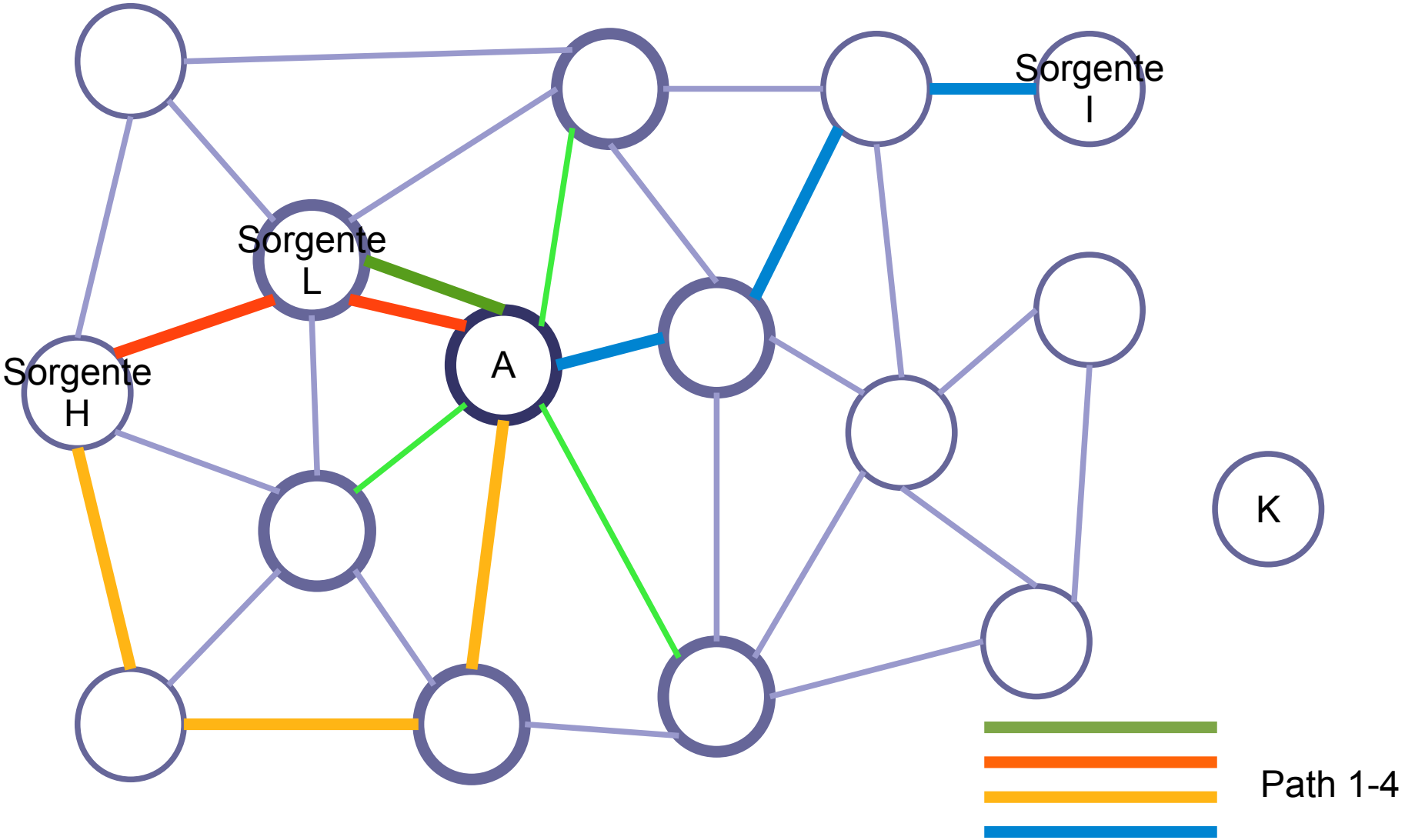
link ID e path ID:

- calcolato da hash XOR tra file e link ID,
- per ogni link nel path

path multipli aggiungibili successivamente

keepalive

Link e path (3)



Il trasferimento dei dati

tunnel del protocollo BitTorrent (Azureus) sui path individuati nella ricerca

- ottimizzazione,
- download parziali,
- ridondanza,
- load balance e congestioni

Partecipazione dinamica

- cadute path, ingressi e uscite nodi,

Sistema di incentivi:

- rapporto upload/download

Gli amici

Installo OneSwarm ed aggiungo nuovi amici:

- amici amici: possono vedere tutti i miei file condivisi
- amici limitati: possono solo fare ricerche

- A mano, per email, da Gtalk, dalla LAN, da un community server
- casi d'uso particolari
  - Attraversamento NAT
  - Nodi in LAN

I contenuti condivisi

Aggiungo contenuti e ne definisco la condivisione:

- ad amici,
- ad amici limitati,
- a gruppi ad hoc

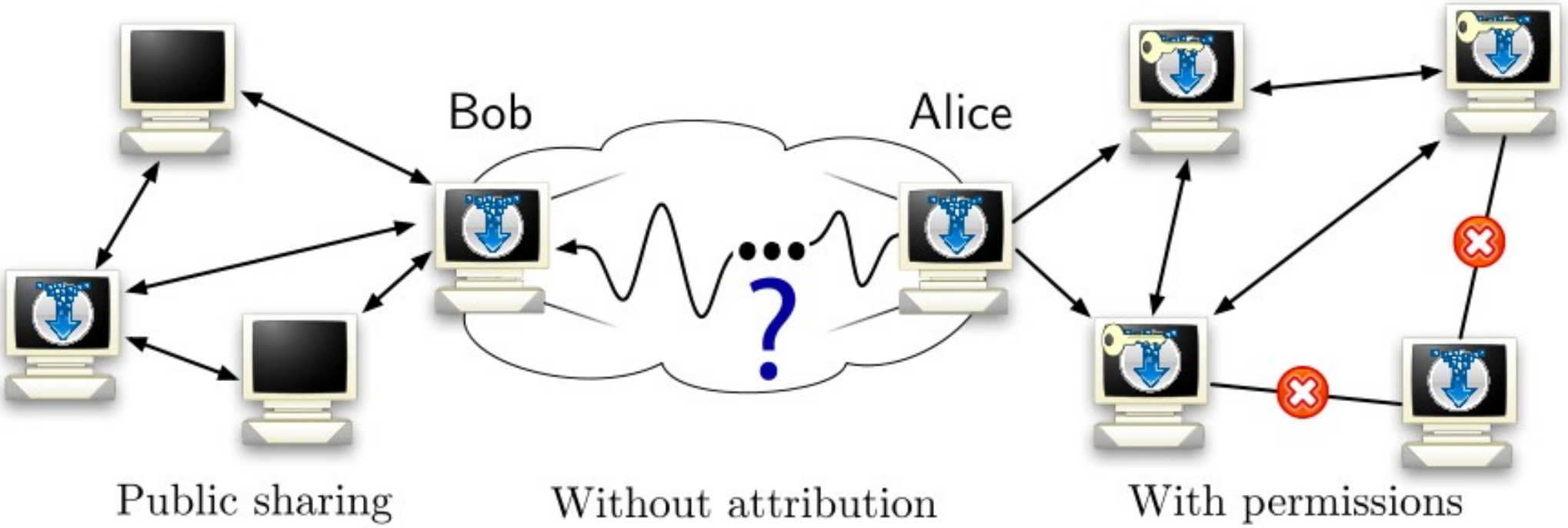
- Per singoli file, per cartelle
- Controllo granulare
- Revocabile in ogni momento

I contenuti condivisi (2)

3 diversi modelli di condivisione informazioni

- distribuzione pubblica universale:
  - Funziona come un normale client BitTorrent
- accesso controllato per file/utente
  - Definizione di gruppi e visibilità,
  - protocollo OneSwarm
- diffusione anonima
  - Nessuna attribuzione (chi condivide quel file?)
  - Identificazione file tramite ricerche o link (magnet, edk)
  - (Analogie con Freenet, Tor)

scenari di condivisione



Prestazioni

- Gli sviluppatori dichiarano velocità di 400 KB/s in laboratorio
- L'obiettivo principale è ridurre il “costo” della privacy in termini di prestazioni
- Esperienze sul campo danno velocità paragonabili a normali collegamenti BitTorrent

Quale privacy si ottiene?

La rete f2f non è esplorabile a piacere

- L'osservazione è limitata a un sottoinsieme definito

I link sono cifrati

- Intercettazione del traffico LAN/ISP

Lo scambio dati nella rete f2f offre **plausible deniability**

La privacy coi nodi amici “amici” dipende da fattori sociali

- Cfr social engineering

Community server

offre l'iscrizione a un servizio di distribuzione di chiavi

permette il controllo delle relazioni di fiducia

- Amici limitati di default
- gestione avanzata utenti

resistenza al crawling

- registrazione 3-step dei client

topologia mista OneSwarm

I community server sperimentali

https://community.oneswarm.org

Pagine web pubbliche

Gestione utenti e autorizzazioni

- Chi pubblica cosa e come

Pubblicazione di link ai contenuti nella rete f2f

Funzioni sociali (tag, categorie, commenti)

Secondo voi cosa sono?

Community server search

Search

Community Server

Subscribe to this server

Login

Home | AI / Robotics | Architecture | Comp. Bio | Databases | Graphics | HCI | Programming languages | Security | Software Engineering | Systems & Networking | Theory | Video

Most recent swarms

Swarm name	Size	Category	Date
ISutherland_091027_OnDemand_100_256K_320x240.mp4	178.2 MB	Architecture	13 days ago
EBradley_091022_OnDemand_100_256K_320x240.mp4	166.7 MB	Software Engineering	13 days ago
IJacobs_091015_OnDemand_100_256K_320x240.mp4	173.7 MB	Video	13 days ago
MHind_091020_OnDemand_100_256K_320x240.mp4	170.2 MB	Video	13 days ago
GBorriello_091013_OnDemand_100_256K_320x240.mp4	164.1 MB	HCI	13 days ago
BChen_091008_OnDemand_100_256K_320x240.mp4	167.0 MB	Systems & Networking	13 days ago
CSimonyi_091001_OnDemand_100_256K_320x240.mp4	140.8 MB	Video	13 days ago
NMyhrvold_091006_OnDemand_100_256K_320x240.mp4	152.3 MB	Video	13 days ago
AAgarwala_090519_OnDemand_100_256K_320x240.mp4	127.8 MB	Graphics	13 days ago
BChess_090512_OnDemand_100_256K_320x240.mp4	171.2 MB	Security	13 days ago
JCamp_090416_OnDemand_100_256K_320x240.mp4	163.3 MB	Video	13 days ago
SPetrov_090428_OnDemand_100_256K_320x240.mp4	148.4 MB	AI / Robotics	13 days ago
IWagner_090414_OnDemand_100_256K_320x240.mp4	186.5 MB	Architecture	13 days ago
LZettlemoyer_090402_OnDemand_100_256K_320x240.mp4	152.4 MB	AI / Robotics	13 days ago
KToyama_090312_OnDemand_100_256K_320x240.mp4	151.9 MB	Video	13 days ago
AScott_090331_OnDemand_100_256K_320x240.mp4	148.8 MB	Comp. Bio	13 days ago
SKatti_090310_OnDemand_100_256K_320x240.mp4	147.4 MB	Systems & Networking	13 days ago
DDensmore_090226_OnDemand_100_256K_320x240.mp4	146.7 MB	Video	13 days ago
ARao_090217_OnDemand_100_256K_320x240.mp4	140.0 MB	Theory	13 days ago
JEstrin_090224_OnDemand_100_256K_320x240.mp4	128.4 MB	Video	13 days ago

Community server search

Search

Community Server

Subscribe to this server

Login

Home | AI / Robotics | Architecture | Comp. Bio | Databases | Graphics | HCI | Programming languages | Security | Software Engineering | Systems & Networking | Theory | Video

« Back

Download: ISutherland_091027_OnDemand_100_256K_320x240.mp4 (magnet)

Preview:

Category: Architecture

Description: This talk describes a radically different architecture for computing called Fleet. Fleet accepts the limitations to computing imposed by physics: moving data costs more energy, more delay, and more chip area than the arithmetic and logical operations ordinarily called "computing." Fleet puts the programmer firmly in charge of the most costly resource: communication. Fleet treats arithmetic and logical operations as side effects of where the programmer sends data. (October 27, 2009, 3:30 pm)

Size: 178.2 MB (1 files)

Comments

(None)

You must log in to make comments

7 ms | OneSwarm Community Server 0.7pre

grazie

http://oneswarm.org

Contatti:

- http://www.nazioneindiana.com/author/jan-reister
- jan.reister@winstonsmith.info