Mobile Mixing

Marcin Gogolewski Mirosław Kutyłowski Tomasz Łuczak

Wrocław University of Technology, Adam Mickiewicz University

ICISC, 2-3 December 2004

Problem definition:

- encrypted messages are processed through a network

Problem definition:

- encrypted messages are processed through a network
- at each node each message is re-encrypted
  no relationship between messages before and after recoding can be detected without breaking encryption scheme

Problem definition:

- encrypted messages are processed through a network
- at each node each message is re-encrypted
  no relationship between messages before and after recoding can be detected without breaking encryption scheme
- the goal: hiding the origin of a message from an adversary monitoring the traffic

Problem definition:

- encrypted messages are processed through a network
- at each node each message is re-encrypted
  no relationship between messages before and after recoding can be detected without breaking encryption scheme
- the goal: hiding the origin of a message from an adversary monitoring the traffic

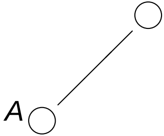
How long it takes so that traffic analysis does not provide any substantial information?

Example

single message

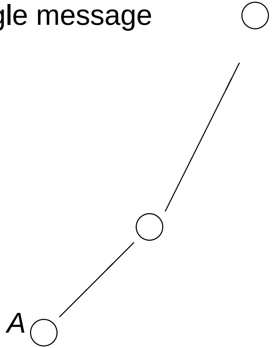
Example

single message



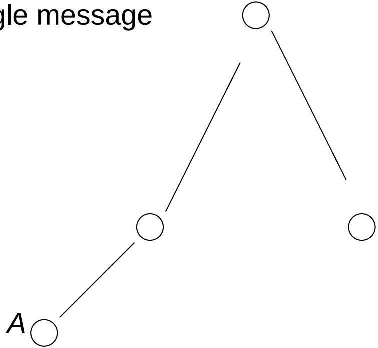
Example

single message



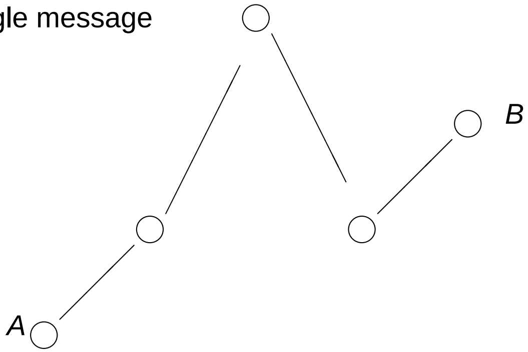
Example

single message



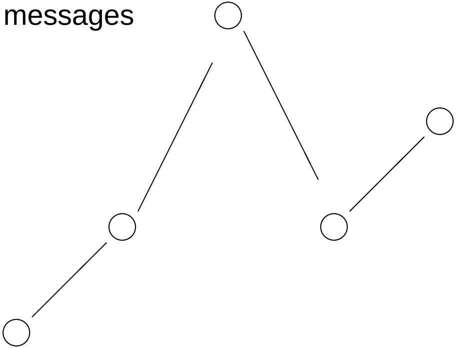
Example

single message



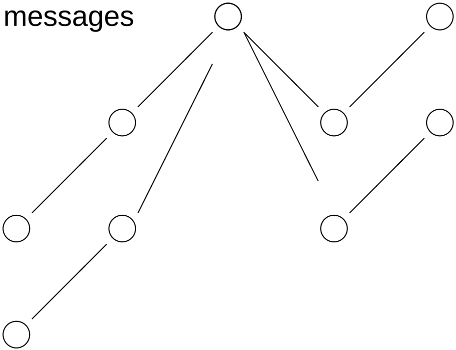
Example

many messages



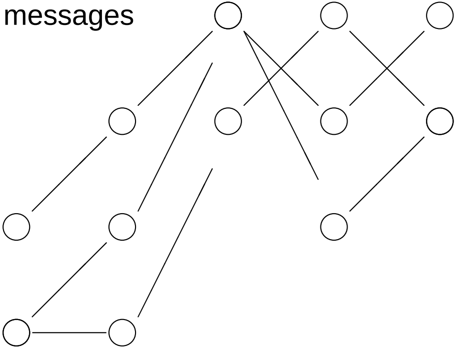
Example

many messages



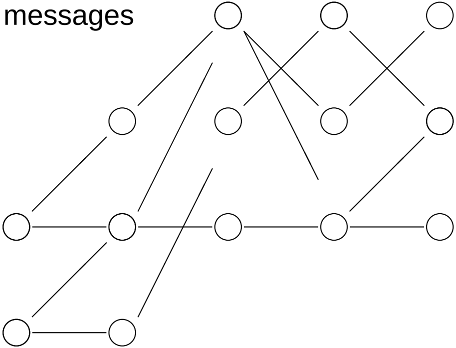
Example

many messages

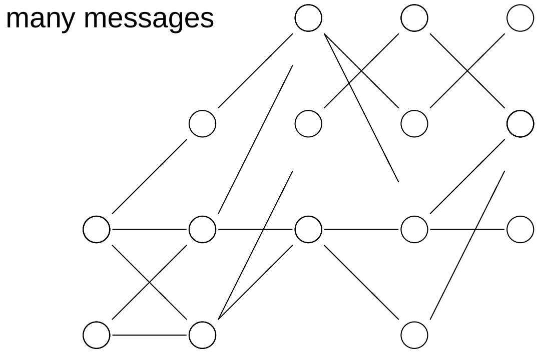


Example

many messages

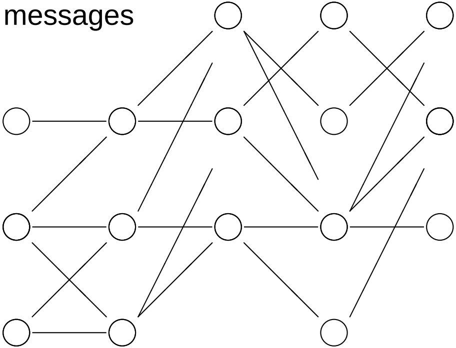


Example



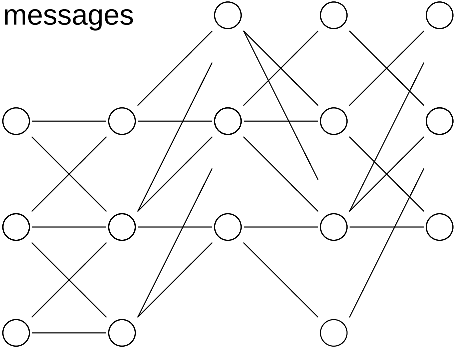
Example

many messages



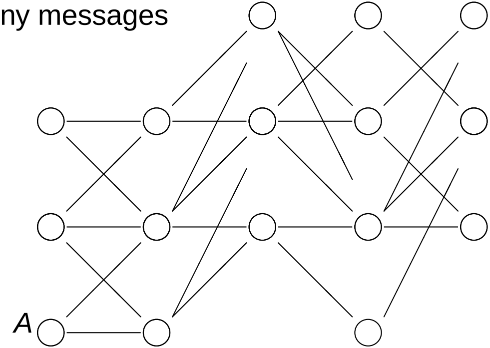
Example

many messages



Example

many messages



destination of the message starting at *A*?

State of the art

1. intuition: *after a sufficiently long time the origins are hidden*
2. no proofs, case-by-case proof or artificial assumptions
3. no reasonable bounds

Related problems - mixes and onions

Mixes:

1. several messages enters a mix
2. the messages are recoded cryptographically
3. the *next mix* is chosen by the current mix
4. the messages leave the mix in a random order

Related problems - mixes and onions

Mixes:

1. several messages enters a mix
2. the messages are recoded cryptographically
3. the *next mix* is chosen by the current mix
4. the messages leave the mix in a random order

Onions:

1. several messages enters a server
2. they are recoded cryptographically
3. the *next server* is chosen by the sender and encoded in each onion
4. the messages leave the server in a random order

Related problems - mixes and onions

Mixes:

1. several messages enters a mix
2. the messages are recoded cryptographically
3. the *next mix* is chosen by the current mix
4. the messages leave the mix in a random order

Onions:

1. several messages enters a server
2. they are recoded cryptographically
3. the *next server* is chosen by the sender and encoded in each onion
4. the messages leave the server in a random order

Adversary model

Different adversary models:

- whole traffic can be observed (strong model)
- only a constant fraction of traffic can be observerd (sometimes more realistic)

In each case we assume: adversary cannot break encoding scheme but they can analyze the traffic.

Adversary model

Different adversary models:

- whole traffic can be observed (strong model)
- only a constant fraction of traffic can be observerd (sometimes more realistic)

In each case we assume: adversary cannot break encoding scheme but they can analyze the traffic.

Related problems – results on mixes

- many attacks and countermeasures for a dynamic adversary
- no security proofs except: a cascade of pairs of mixes, passive adversary – processing through $O(1)$ pairs is enough,
  Gomułkiewicz, Klonowski, Kutyłowski (ESORICS'2003)

Related problems – results on onions

- many attacks and countermeasures for a dynamic adversary
- strong adversary:
  - Rackoff, Simon (ACM STOC'93): polylogarithmic time (degree 11), special assumption: at stage i the messages stay inside groups of cardinality 2^i
  - Czumaj, Kanarek, Kutyłowski, Loryś (ACM SODA'99): under the same assumptions - time $O(\log^2 n)$
- passive adversary:
  - Berman, Fiat, Ta-Shma (FC'2004) – $O(\log^4 n)$ steps for n messages,
  - Gomułkiewicz, Klonowski, Kutyłowski (ISC'2004) – $O(\log n)$ steps

Our model

- **A message cannot be sent to any other node in a network in one step.**
- It can be sent only to the neighbor nodes.

Application – RFID-tags

RFID-tags:

- small, powerless, low-cost devices
- communication through a radio channel
- can be used as identity tags, bar code replacement,...

Application – RFID-tags

RFID-tags:

- small, powerless, low-cost devices
- communication through a radio channel
- can be used as identity tags, bar code replacement,. . .

Problem: Anyone in range can contact an RFID-tag. Even if they cannot write any information, they can trace the tag!

Re-encryption of the RFID-tags does not automatically protect against traffic analysis.

Application – Mobile Agents

Mobile agents:

- program and data migrating through a network
- used for diverse perpuses: processing and search of information in a distributed information system
- Problems: privacy (if agents are searching information anonymously) and security issues (if agents used for diagnostics)

Application – Mobile Agents

Mobile agents:

- program and data migrating through a network
- used for diverse perpuses: processing and search of information in a distributed information system
- Problems: privacy (if agents are searching information anonymously) and security issues (if agents used for diagnostics)

Goal: routes of the agents should remain hidden.

Application – Distributed Timestamping

Timestamping with Boomerang Onions:

- A time-stamping requests encoded in an onion.
- the onion is processed through an anonymous path which returns to the sender.
- Each server on a path attaches encoded timestamp.

Application – Distributed Timestamping

Timestamping with Boomerang Onions:

- A time-stamping requests encoded in an onion.
- the onion is processed through an anonymous path which returns to the sender.
- Each server on a path attaches encoded timestamp.

Advantages

- privacy
- randomly chosen *witnesses*
- scalability
- no special hardware/servers required

Application – Distributed Timestamping

Timestamping with Boomerang Onions:

- A time-stamping requests encoded in an onion.
- the onion is processed through an anonymous path which returns to the sender.
- Each server on a path attaches encoded timestamp.

Advantages

- privacy
- randomly chosen *witnesses*
- scalability
- no special hardware/servers required

Security problem: if traffic analysis suceeds, then an adversary can block timestamping requests of particular users and observe who is issuing timestamps

Process description – adversary view - On hobbits and the rings

The following process well describes our scenario:

- There are m *hobbits*.
- Each hobbit is holding one *ring*. Some of them are magic rings.

Process description – adversary view - On hobbits and the rings

The following process well describes our scenario:

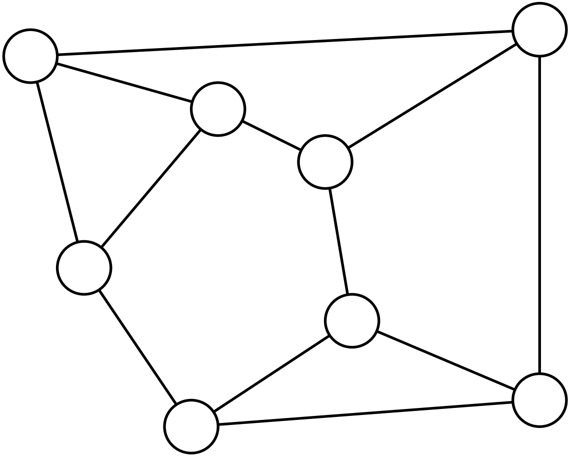
- There are m *hobbits*.
- Each hobbit is holding one *ring*. Some of them are magic rings.
- The hobbits perform (independently) a random walk on a graph G.
- If some hobbits meet in a node they exchange their rings at random.

Process description – adversary view - On hobbits and the rings

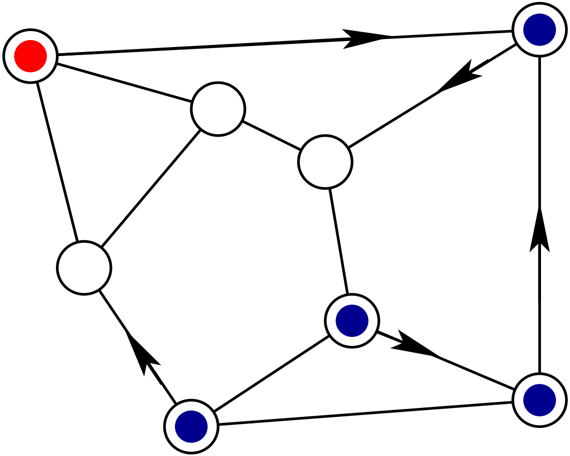
The following process well describes our scenario:

- There are m *hobbits*.
- Each hobbit is holding one *ring*. Some of them are magic rings.
- The hobbits perform (independently) a random walk on a graph G.
- If some hobbits meet in a node they exchange their rings at random.
- An adversary observes the movements of the hobbits (but not how they exchange the rings) and tries to locate the magic ring(s).

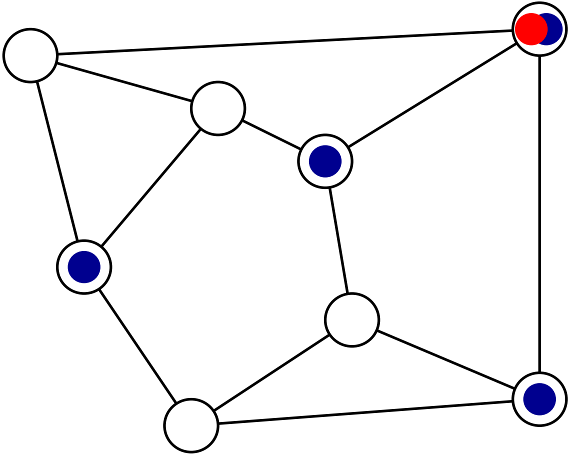
Hobbits



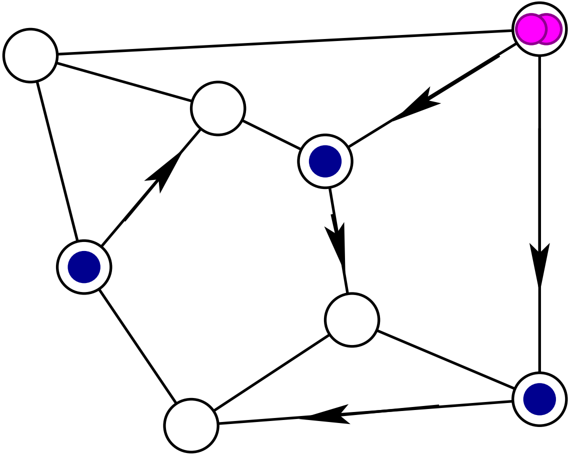
Hobbits



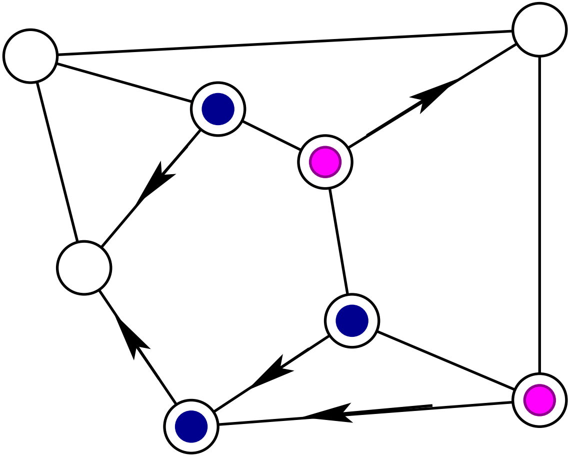
Hobbits



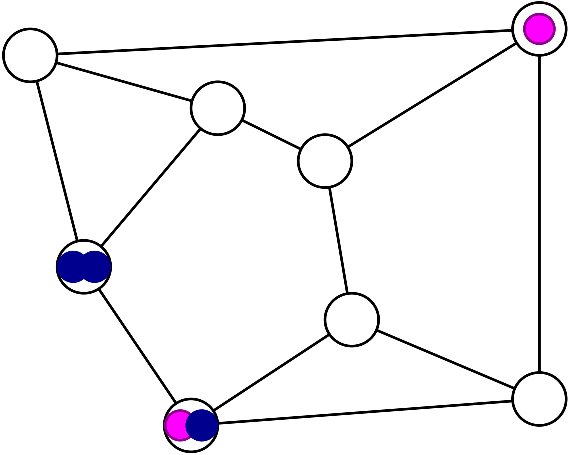
Hobbits



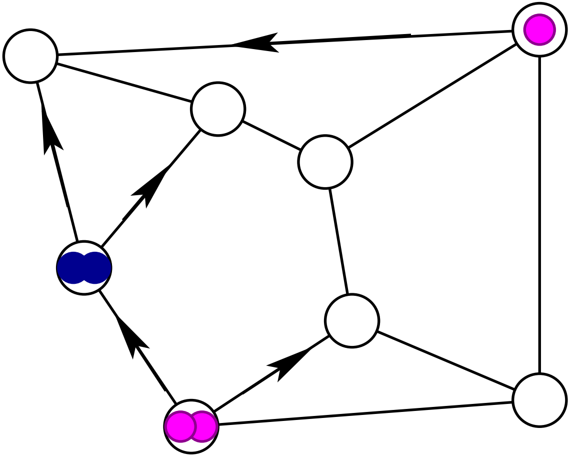
Hobbits



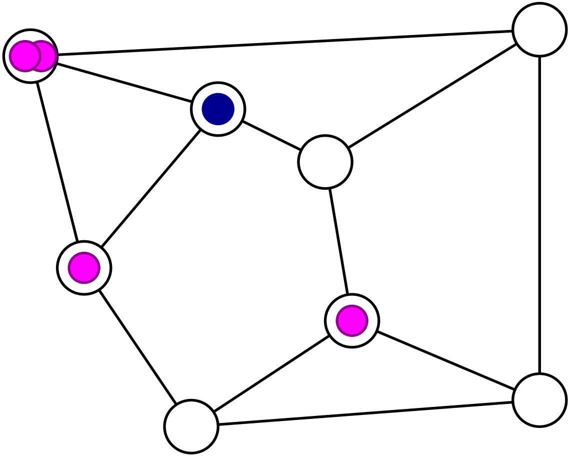
Hobbits



Hobbits



Hobbits



Main problem

How many steps of the hobbits are necessary until the adversary has no substantial advantage from observing the movements of the hobbits?

Anonymity Condition

- main parameter: **probability distribution of location of all magic rings**

Anonymity Condition

- main parameter: **probability distribution of location of all magic rings**
- considering all rings at the same time necessary since there might be strong dependencies between locations of different rings!

  i.e. revealing position of one ring would give much information about others!

Anonymity Condition

- main parameter: **probability distribution of location of all magic rings**
- considering all rings at the same time necessary since there might be strong dependencies between locations of different rings!
  i.e. revealing position of one ring would give much information about others!
- probability distribution **conditioned on the traffic information** should be almost uniform

Anonymity Condition

- main parameter: **probability distribution of location of all magic rings**
- considering all rings at the same time necessary since there might be strong dependencies between locations of different rings!
  i.e. revealing position of one ring would give much information about others!
- probability distribution **conditioned on the traffic information** should be almost uniform
- **variation distance** as a measure of closeness of two probability distributions

Main result

Let:

- G – n-node regular graph with mixing time τ_G
- $m = \Theta(n)$ – hobbits
- $k \leq \frac{1}{2}m$ – magic rings

Main result

Let:

- G – n-node regular graph with mixing time τ_G
- $m = \Theta(n)$ – hobbits
- $k \leq \frac{1}{2}m$ – magic rings

Main Theorem

After $\lambda = \Omega(\tau_G^3 \cdot \log^6 n \cdot \log k)$ steps probability distribution of magic rings is close to the uniform distribution with high probability (over traffic information).

Proof outline

- Our problem is much different from locating the hobbits on random positions in graph G.
- “mixing” occurs dynamically - therefore an analysis is becomes harder.

Proof phases

1. solve the problem for one magic ring - *potential functions*
2. generalize to many magic rings - *path coupling*

The main technical contribution is part 1.

Notation

- $\rho(P; j, t)$ – after t steps hobbit j has the magic ring
  (P – is the pattern of hobbit moves observed)

Notation

- $\rho(P;j,t)$ – after t steps hobbit j has the magic ring
  (P – is the pattern of hobbit moves observed)
- $d_H(P;t) = \frac{1}{2}\sum_{i=1}^{m} |\rho(P;i,t) - \frac{1}{m}|$ (variation distance)

Notation

- $\rho(P;j,t)$ – after t steps hobbit j has the magic ring (P – is the pattern of hobbit moves observed)
- $d_H(P;t) = \frac{1}{2}\sum_{i=1}^{m} |\rho(P;i,t) - \frac{1}{m}|$ (variation distance)
- $\tau_H(P) = \min_t\{d_H(P;t) \leq 0.1\}$

Notation

- $\rho(P;j,t)$ – after t steps hobbit j has the magic ring (*P* – is the pattern of hobbit moves observed)
- $d_H(P;t) = \frac{1}{2}\sum_{i=1}^{m} |\rho(P;i,t) - \frac{1}{m}|$ (variation distance)
- $\tau_H(P) = \min_t\{d_H(P;t) \leq 0.1\}$
- τ_G – *mixing time* of graph *G* (it describes time after which "a single hobbit is at a random location in *G*"

Key technical result

Key Theorem

Assume that the mixing time of G is $n^{o(1)}$*.*
Then with probability at least $1-\frac{1}{n}$ *over the choices of P:*

$$\tau_H(P) = O(\tau_G^3 \cdot \log^5 n)$$

Potential functions

- $g(P;t) = \sum_{i=1}^{m} \rho^2(P;i,t)$.
- $d_H(P;t) = \frac{1}{2}\sum_{i=1}^{m} |\rho(P;i,t) - \frac{1}{m}|$

Potential functions

- $g(P;t) = \sum_{i=1}^{m} \rho^2(P;i,t)$.
- $d_H(P;t) = \frac{1}{2} \sum_{i=1}^{m} |\rho(P;i,t) - \frac{1}{m}|$

Some properties:

- $g(P;t)$ is a non-increasing function of t .
- It suffices to inspect when $d_H(P;t_0) \leq 0.1$.

Main Lemma

Lemma

Let $d_H(P;t_0) \geq 0.1$ *for a pattern P. Then for certain* τ_1, τ_0*:*

$$E\left[g(P;t_0) - g(P;t_0+\tau_1+1)\right] \geq \Omega(g(P;t_0)/(\tau_G^2 \log^3 n))$$

Corollary:

By definition $g \geq \frac{1}{7}m$*, so finally* $d_H(P;t_0) < 0.1$*)*

Proof rationale:

if $d_H(P;t_0) \geq 0.1$, then there are many hobbits with high (low) probability of posessing the magic ring. When such hobbits meet, then probabilities get equal and the potential decreases substantially.

Final remarks and conclusions

- mobile mixing related to graph mixing time
- still unclear what is the **real** relationship between the convergence rate considered and the mixing time

Final remarks and conclusions

- mobile mixing related to graph mixing time
- still unclear what is the **real** relationship between the convergence rate considered and the mixing time
- what about special classes of graphs occuring in practice