



Anonymous
communica-
tion

M. Kutylowski

Onion Routing

Model &
attacks

Anonymity &
Traffic

Rackoff-Simon

Hobbits

Realistic
adversary

Traffic Analysis and Complexity of Anonymous Communication

Mirosław Kutylowski

Wrocław University of Technology
Institute of Mathematics and Computer Science

Dagstuhl, 18.09.2008



Communication systems

Anonymous
communica-
tion

M. Kutylowski

Onion Routing

Model &
attacks

Anonymity &
Traffic

Rackoff-Simon

Hobbits

Realistic
adversary

Anonymity in communication

- contents of a message can be kept secret easily (except its length)
- but how to hide that two parties are communicating??
- in most technical solutions the link between the sender and the recipient is shown



Onions

Anonymous
communica-
tion

M. Kutylowski

Onion Routing

Model &
attacks

Anonymity &
Traffic

Rackoff-Simon

Hobbits

Realistic
adversary

General framework

- messages are sent along (random) paths chosen by the sender
- a message is encapsulated cryptographically in an onion
- each server on the path peels of an onion obtained, learns the successor on the path and sends there the internal onion,
- retrieving any other information (final destination, source,...) from the onion is infeasible



Assumptions about an adversary

Anonymous
communica-
tion

M. Kutylowski

Onion Routing

Model &
attacks

Anonymity &
Traffic

Rackoff-Simon

Hobbitts

Realistic
adversary

Models

- **passive**
 - adversary can eavesdrop the whole traffic
 - adversary can eavesdrop a some fraction of traffic
- **active – adversary can insert, delete and modify messages**
 - everywhere
 - at some chosen locations



Replay attack

Anonymous communication

M. Kutylowski

Onion Routing

Model & attacks

Anonymity & Traffic

Rackoff-Simon

Hobbits

Realistic adversary

Mechanism of a replay attack

- a server re-sends an old packet
- the adversary looks for packets in the network that have been already sent previously



Replay attack

Anonymous communication

M. Kutylowski

Onion Routing

Model & attacks

Anonymity & Traffic

Rackoff-Simon

Hobbits

Realistic adversary

Mechanism of a replay attack

- a server re-sends an old packet
- the adversary looks for packets in the network that have been already sent previously

Re-encryption?

Does not help much:

- one can re-encrypt a ciphertext (produce a different ciphertext with the same contents inside) without knowing the key used to encrypt
- **but no method known to re-encrypt a ciphertext hidden in a ciphertext**



Replay attack-solution idea

Anonymous
communica-
tion

M. Kutylowski

Onion Routing

Model &
attacks

Anonymity &
Traffic

Rackoff-Simon

Hobbits

Realistic
adversary

minimal information protocols

design a scheme for encoding the route so that:

- the information gained by an intermediate node is only what a node must learn anyway: i.e. the next node and the previous node



Replay attack-solution idea

Anonymous
communica-
tion

M. Kutyłowski

Onion Routing

Model &
attacks

Anonymity &
Traffic

Rackoff-Simon

Hobbits

Realistic
adversary

minimal information protocols

design a scheme for encoding the route so that:

- the information gained by an intermediate node is only what a node must learn anyway: i.e. the next node and the previous node
- in particular a node cannot learn any information bit about contents of the ciphertexts that the node is forwarding



Replay attack-solution idea

minimal information protocols

design a scheme for encoding the route so that:

- the information gained by an intermediate node is only what a node must learn anyway: i.e. the next node and the previous node
- in particular a node cannot learn any information bit about contents of the ciphertexts that the node is forwarding
- any manipulation of the contents of ciphertexts and changing the route results in revealing the attacker with a fair probability (e.g. $\frac{1}{2}$)

a promising direction at the moment, in this way an active adversary will be no more powerful than a passive adversary



Time and traffic

Anonymous
communica-
tion

M. Kutylowski

Onion Routing

Model &
attacks

Anonymity &
Traffic

Rackoff-Simon

Hobbits

Realistic
adversary

Connection protocols

- for each connection an *anonymous path* is established,
- even if it is perfectly secure from a static point of view,
...



Time and traffic

Anonymous
communication

M. Kutylowski

Onion Routing

Model &
attacks

Anonymity &
Traffic

Rackoff-Simon

Hobbits

Realistic
adversary

Connection protocols

- for each connection an *anonymous path* is established,
- even if it is perfectly secure from a static point of view,
...
- when a connection is closed the traffic is reduced along the anonymous path, while it remains unchanged elsewhere



Anonymity

Anonymous communication

M. Kutylowski

Onion Routing

Model & attacks

Anonymity & Traffic

Rackoff-Simon

Hobbits

Realistic adversary

What does *anonymity* mean?

- one cannot deduce a destination of a message sent by a single user



Anonymity

Anonymous
communica-
tion

M. Kutylowski

Onion Routing

Model &
attacks

Anonymity &
Traffic

Rackoff-Simon

Hobbits

Realistic
adversary

What does *anonymity* mean?

- one cannot deduce a destination of a message sent by a single user
- OR



Anonymity

Anonymous communication

M. Kutylowski

Onion Routing

Model & attacks

Anonymity & Traffic

Rackoff-Simon

Hobbits

Realistic adversary

What does *anonymity* mean?

- one cannot deduce a destination of a message sent by a single user
- OR
- any significant data on the protocol participants cannot be deduced



Anonymity and traffic analysis

Anonymous communication

M. Kutylowski

Onion Routing

Model & attacks

Anonymity & Traffic

Rackoff-Simon

Hobbits

Realistic adversary

Modeling

- n messages
- source positions S_1, \dots, S_n
- destination positions D_1, \dots, D_n
- for each 1-1 mapping π from $\{S_1, \dots, S_n\}$ to $\{D_1, \dots, D_n\}$

$$\Pr(\pi)$$

is the probability that π describes correctly the links between the senders and the receivers

- $\Pr(\pi)$ is computed based on the protocol description and conditioned by the traffic information available for the adversary



Goal

Anonymous communication

M. Kutylowski

Onion Routing

Model & attacks

Anonymity & Traffic

Rackoff-Simon

Hobbits

Realistic adversary

Good protocol

probability distribution linking the senders and the recipients are almost the same for two cases:

- when conditioned by the traffic information
- when not conditioned by the traffic information

Closeness of distributions

- variation distance

$$\|\mu_1 - \mu_2\| = \frac{1}{2} \sum_{\omega \in \Omega} |\mu_1(\omega) - \mu_2(\omega)|.$$

- maximal probability
- ...



Smaller anonymity sets

Anonymous
communication

M. Kutyłowski

Onion Routing

Model &
attacks

Anonymity &
Traffic

Rackoff-Simon

Hobbits

Realistic
adversary

Reduced version

- consider a subset of senders $S \subseteq \{S_1, \dots, S_n\}$
- consider mappings from S to $\{D_1, \dots, D_n\}$

- extreme case: $|S| = 1$
- for practical point of view we might be satisfied with $|S| = n/2$ instead of $|S| = n$



Limitations

Anonymous
communica-
tion

M. Kutylowski

Onion Routing

Model &
attacks

Anonymity &
Traffic

Rackoff-Simon

Hobbits

Realistic
adversary

Costs

- the traffic overhead:
 - the length of the paths
 - the number of dummy messages (if used)
- computational power of the adversary - ignored



Extreme case

n messages, n nodes, all traffic information available

- a typical approach to show that the items get well permuted is to permute in subgroups and then shuffle the groups, but a reasonable protocol is different!

Anonymous communication

M. Kutylowski

Onion Routing

Model & attacks

Anonymity & Traffic

Rackoff-Simon

Hobbits

Realistic adversary



Extreme case

n messages, n nodes, all traffic information available

- a typical approach to show that the items get well permuted is to permute in subgroups and then shuffle the groups, but a reasonable protocol is different!
- Rackoff & Simon: some bounds on the length of the paths polylogarithmic in n (something like $\log^{12} n$) for the modified model
for $n = 2^{10}$, about 10^{12} hops required; if one hop takes 1ms , then $10^{12}\text{ms} \approx 317$ years
- the results hold with a high probability: it is possible (wsp) that the paths do not meet anywhere

Anonymous communication

M. Kutylowski

Onion Routing

Model & attacks

Anonymity & Traffic

Rackoff-Simon

Hobbits

Realistic adversary



Extreme case

n messages, n nodes, all traffic information available

- a typical approach to show that the items get well permuted is to permute in subgroups and then shuffle the groups, but a reasonable protocol is different!
- Rackoff & Simon: some bounds on the length of the paths polylogarithmic in n (something like $\log^{12} n$) for the modified model
for $n = 2^{10}$, about 10^{12} hops required; if one hop takes $1ms$, then $10^{12}ms \approx 317$ years
- Czumaj & K.: hoping to have reduced to $O(\log^2 n)$ - still practically not much convincing
- the results hold with a high probability: it is possible (wsp) that the paths do not meet anywhere

Anonymous communication

M. Kutylowski

Onion Routing

Model & attacks

Anonymity & Traffic

Rackoff-Simon

Hobbits

Realistic adversary



Local view problems

Gogolewski, Klonowski, K.

Anonymous
communica-
tion

M. Kutylowski

Onion Routing

Model &
attacks

Anonymity &
Traffic

Rackoff-Simon

Hobbits

Realistic
adversary

local view

- it may happen that a sender (say Alice) does not know all servers and designs the path through a subset of possible nodes,
- practical attack: one can compute the candidate locations for a message sent by Alice. The size of this set fluctuates but sometimes does not grow much.

Lesson to be learned: rethink all assumptions



Local view problems

Gogolewski, Klonowski, K.

Anonymous communication

M. Kutylowski

Onion Routing

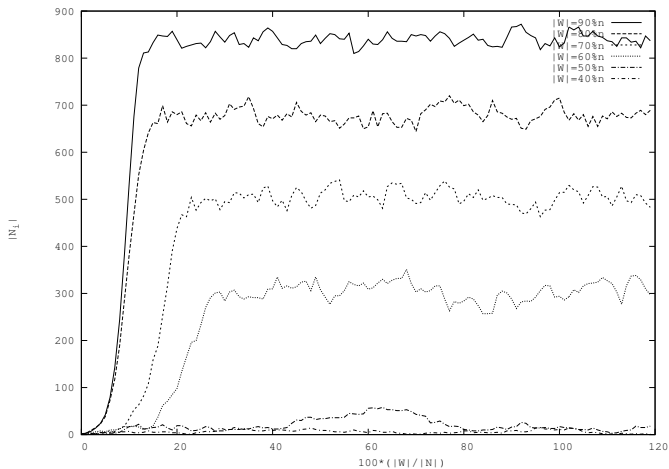
Model & attacks

Anonymity & Traffic

Rackoff-Simon

Hobbits

Realistic adversary





Local view problems

Gogolewski, Klonowski, K.

Anonymous
communication

M. Kutylowski

Onion Routing

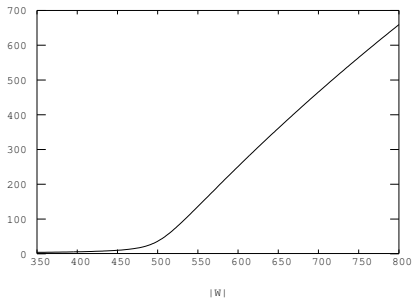
Model &
attacks

Anonymity &
Traffic

Rackoff-Simon

Hobbits

Realistic
adversary



equilibrium point for the anonymity set for different sizes of
local view



Mobile mixing

Łuczak, Gogolewski, K.

Anonymous
communication

M. Kutylowski

Onion Routing

Model &
attacks

Anonymity &
Traffic

Rackoff-Simon

Hobbitts

Realistic
adversary

n messages, n nodes, $|S| = n/2$, all traffic information available, messages transmitted over a d -regular graph

anonymity achieved whp in time for

$$t = \Omega(\tau_G^3 \cdot \log^6 n \cdot \log k),$$

where $k = |S|$, n is the number of nodes and τ_G is the mixing time of graph G .

... the bound only theoretical:

- $\log^6 n$ too high
- regularity is a strange assumption



Moderate case

Berman, Fiat, Ta-Shma

Anonymous
communica-
tion

M. Kutylowski

Onion Routing

Model &
attacks

Anonymity &
Traffic

Rackoff-Simon

Hobbitts

Realistic
adversary

number of messages arbitrary, a fraction of traffic
information available

- intuition: adversary loses control completely if messages do not go through monitored links
- the number of messages need not to be high for the adversary to lose a message from his eyes
this is not possible if we relay on mixing messages by the nodes: if the number of messages is small, they are unlikely to meet



Moderate case

Berman, Fiat, Ta-Shma

Anonymous
communica-
tion

M. Kutylowski

Onion Routing

Model &
attacks

Anonymity &
Traffic

Rackoff-Simon

Hobbitts

Realistic
adversary

Prior distribution

it is assumed that each sender has some probability distribution of destination places,

Trick

- Use mutual information instead of statistical distance.
- Mutual information does not grow if the perform additional mixing of the messages (even in a correlated way)
- concern the configuration of messages after time $T/2$ for paths of length T .



Moderate case

Berman, Fiat, Ta-Shma

Anonymous
communication

M. Kutyłowski

Onion Routing

Model &
attacks

Anonymity &
Traffic

Rackoff-Simon

Hobbitts

Realistic
adversary

Path length

- paths of length $O(\log^4 n)$ are sufficiently long to guarantee anonymity whp (BFT).
- $O(\log n)$ should be enough (via a path coupling argument)



Anonymous
communica-
tion

M. Kutylowski

Onion Routing

Model &
attacks

Anonymity &
Traffic

Rackoff-Simon

Hobbits

Realistic
adversary

Thanks for your attention