A New Anonymous Routing Scheme and its Aptitude for Recent Networks

Jin Tamura (University of Tokyo, Information and Communication Engineering)

1 Introduction

Constructing an Anonymous Network through the Internet becomes one of the most important topics recently. For instance, when we need a medical consultation, but willing not to open our individual information, even against a doctor (a receiver) or against intermediate nodes, we can use an anonymous routing scheme ([2][3][5]). A whistle-blowing activity is one of these cases that highly requires keeping anonymous even against inner administrators in sender-identifiable environments (e.g. NAT Environment). A number of protocols have been already proposed, but still there are several drawbacks when we use them especially in such kind of recent networks. In this report, I discuss about some existing major schemes (Crowds [2], Mix-net [3], Onion Routing [4]) and show their advantages and drawbacks and focus on Onion Routing Scheme and Sliced Onion Routing Scheme, which is my proposal scheme[5], and show the considerable aptitude for recent networks.

2 Main Researches

2.1 Trends of Recent Networks

Sender-Identifiable Environments:

NAT Environments or networks behind Firewalls have been widely spread these days. However in such networks, administrators can easily identify a sender who sent data from inside through the Gateway (for the reason that outside-users can't send data directly to inside-users). We call these kinds of networks as Sender-Identifiable Environments.

Dynamic Environments:

Recently, several kinds of dynamic networks are wide spread (e.g. Wireless LAN, Ad-hoc Networks). These networks strongly require high availability for routing scheme.

2.2 Requirements

I raise the following two requirements of Anonymous Routing Scheme for Recent Networks.
Unlinkability (even in Sender-Identifiable Environments)
Availability (even in Dynamic Networks)

2.3 Sliced Onion Routing Scheme (Our Scheme)

Tamura, Kobara and Imai developed Sliced Onion Routing Scheme[5][6], whose routing information is unchanged, and each node open their own block to transact the data. We don't use multiple encryption, but same as Onion Routing Scheme, our scheme achieved both Sender Anonymity and Receiver Anonymity.

2.4 Computational Analysis (Comparisons)

As mentioned above, both Onion Routing Scheme and our Sliced Onion Routing Scheme satisfy Sender Anonymity and Receiver Anonymity against a single or collusion of intermediate nodes. Therefore we discuss furthermore from our requirements' point of view (Unlinkability and Availability, see 2.2).

2.5 Definitions and Notations

Definitions

-Availability:

Availability of a Node Probability of the connectivity from the next nodes. Availability of a Scheme (i.e. one of our requirement) Probability of the reach ability of sent data using the Scheme.

-Uninkability: (i.e. one of our requirements)

We define Linkability as follows; Probability for attacker(s) to find out the link between a sender and a receiver of the data. We calculate Unlinkability as follows; Unlinkability = 1 - Linkability

Notations

N: a set of whole nodes in networks

I: a set of intermediate nodes between a sender and a receiver ($I \subset N$)

i_k ($k \in \aleph$): an intermediate node ($i_k \in I$)

$\Pr(i_k)$: Participating collision Probability of i_k

$A(i_k)$: Availability of i_k, $|N| = n$, $|I| = m$ $(n \geq m)$

2.6 Unlinkability of Both Schemes

Onion Routing Scheme The only way to identify the link is method I. Therefore,

$$\begin{aligned} &\mathit{Unlinkability} = 1 - \mathit{Linkability} \\ &= 1 - \Pr(i_1)\Pr(i_2)\cdots\Pr(i_m) \\ &= 1 - \prod_{k=1}^{m} \Pr(i_k) \end{aligned}$$

Sliced Onion Routing Scheme Attacker can use both method I and II.

$$\begin{aligned} &\mathit{Unlinkability} = 1 - \mathit{Linkability} \\ &= 1 - \prod_{k=1}^{m} \Pr(i_k) - \tfrac{1}{n} \prod_{k=2}^{m} \Pr(i_k) - \cdots \\ &= 1 - \prod_{k=1}^{m} \Pr(i_k) - \tfrac{1}{n} \sum_{j=2}^{m} \prod_{k=j}^{m} \Pr(i_k) \end{aligned}$$

2.7 Further Analyses

About Unlinkability Unlinkability of Onion Routing Scheme is always equal or slightly higher than that of Sliced Onion Routing Scheme.

The difference is $\frac{1}{n} \sum_{j=2}^{m} \prod_{k=j}^{m} \Pr(i_k) \leq \frac{m}{n}$

Usually, we can say $m << n$.

Therefore this difference is ignorable.

About Availability Availability of Sliced Onion Scheme is constantly much higher than that of Onion Routing Scheme (the more complicated a networks is, the much higher Availability in Our Scheme).

3 Conclusion

We have shown major existing anonymous routing schemes in this report, and pointed out their drawbacks when we apply them to whistle-blowing from the inside activities in recent networks. We focused on Onion Routing Scheme to compare with our scheme; Sliced Onion Routing Scheme, which are superior to others. For our results of the comparison, there is trade-off between Availability and Unlinkability, but the difference of Unlinkability is ignorable meanwhile Availability of Sliced Onion Routing Scheme has much higher Availability than Onion Routing Scheme. Therefore we believe that our scheme is superior to other schemes especially in dynamic and complicated networks with Sender-Identifiable Environments.

References

[1] Pfitzmann, A. and Waidner, M., "Networks without user observability", Comput Secur 2.6, pp. 158-166, 1987.

[2] M. Reiter and A. Rubin, "Crowds: Anonymity for Web transactions", DIMACS Technical Report, 97(15), April 1997.

[3] Chaum, "Untraceable Electronic Mail, Return Address, and Digital Pseudonyms". Communications of the ACM, vol.24 no.2, pp. 84-88, 1981.

[4] Song, R. and Korba, L. "Review of Network-based Approaches for Privacy.", Proceedings of the 14th Annual Canadian Information Technology Security Symposium, NRC44905, Ottawa, 2002.

[5] Jin Tamura, Kazukuni Kobara, Hideki Imai. "Consideration of Unlinkability among Anonymous Routing Schemes", Proceedings of the 2002 Symposium on Cryptography and Information Security (SCIS), pp.1409-1414, Japan, 2004.

[6] Jin Tamura, Kazukuni Kobara, Hideki Imai. "A New Anonymous Routing Scheme and its Application to NAT-Environment", Proceedings of the 4th International Workshop on ITS Telecommunications (ITST), Singapore, 2004.

[7] Oliver Berthold, Andreas Pfitzmann, and Ronny Standtke., "The disadvantages of free MIX routes and how to overcome them", Designing Privacy Enhancing Technologies, volume 2009 of LNCS, pp. 30-45.