HOKKAIDO UNIVERSITY

Title	Security Analysis of Anonymous Communication System 3-Mode Net Against Collaborating Nodes
Author(s)	Kono, Kazuhiro; Nakano, Shinnosuke; Ito, Yoshimichi et al.
Description	APSIPA ASC 2009: Asia-Pacific Signal and Information Processing Association, 2009 Annual Summit and Conference. 4-7 October 2009. Sapporo, Japan. Oral session: Signal Processing and Security in Communications (5 October 2009).
Citation	Proceedings : APSIPA ASC 2009 : Asia-Pacific Signal and Information Processing Association, 2009 Annual Summit and Conference, 105-110
Issue Date	2009-10-04
Doc URL	https://hdl.handle.net/2115/39650
Type	conference paper
File Information	MA-L4-4.pdf

Hokkaido University Collection of Scholarly and Academic Papers : HUSCAP

Security Analysis of Anonymous Communication System 3-Mode Net Against Collaborating Nodes

Kazuhiro Kono, Shinnosuke Nakano, Yoshimichi Ito, and Noboru Babaguchi
Graduate School of Engineering, Osaka University, Suita 565-0871 Osaka Japan
E-mail: {kono, nakano}@nanase.comm.eng.osaka-u.ac.jp, {ito, babaguchi}@comm.eng.osaka-u.ac.jp

***Abstract*—This paper analyzes the security of an anonymous communication system 3-Mode Net (3MN) against collaborating relay nodes. We evaluate the anonymity of a message sender under the situation that some relay nodes collaborate each other to find out the message sender. As in the case of Crowds, we define the measure of the anonymity of the message sender as the probability that the first immediate predecessor among the immediate predecessors of all collaborating relay nodes is in fact the message sender. This paper gives an explicit formula for this probability. Some numerical examples are also presented.**

I. Introduction

Preserving anonymity of communication on the Internet is one of the most important issues in communication engineering. Encryption protocols, such as SSL, enable users to protect their important data in a communication. However, these protocols cannot protect the sender and the receiver of a message because one can easily read the header of an IP packet, in which IP addresses of a destination and a source are included. If the sender and the receiver of a message are revealed, one can infer sender's human relationship, hobbies and diversions. Therefore, a number of anonymous communication systems, which do not only protect a message but also hide the IP addresses of the sender and the receiver of a message, have been proposed [1], [2], [11], [13], [14], [15], [18], and they are applied to electronic vote and web access.

Recently, a new anonymous communication system called 3-Mode Net (3MN) has been proposed [10], [12]. 3MN can be regarded as an extension of the Crowds-based anonymous communication system [15], [16], where each relay node in the communication path decides its action by probability, that is, whether the node sends a message to the proper receiver, or to another node. In addition to these two actions, 3MN can choose the third action, that is, to encrypt whole data set including the destination of the proper receiver and to rewrite the temporal destination. This action enables 3MN to provide anonymity to the proper receiver unlike Crowds. In [12], the expectations of the number of relay nodes as well as the number of encryption required for communication are derived, and based on the results, it is shown that 3MN has an advantage of smaller numbers of relay nodes and encryption than those of Onion Routing [5], [8], [14]. Furthermore, in [10], the probability distributions and variances of the above two numbers are obtained, and by using these results, the performance of 3MN is analyzed in more detail.

However, it is not shown how much degree of anonymity is guaranteed for the sender and the receiver of a message when the probabilities of mode selections are given. Attackers may reveal the sender and the receiver with high probability if the probabilities of mode selections are chosen inappropriately. Intuitively, when both the number of relay nodes and that of encryption are quite small, the degree of anonymity would be low. To clarify the effects of the probabilities of mode selections to the anonymity of a sender and a receiver is an important issue for evaluating the performance of anonymous communication systems.

As a first step for security analysis of 3MN, this paper evaluates the degree of sender anonymity against collaborating nodes who collaborate each other in order to identify the message sender. We refer to a node who forwards a message to a collaborating node as an immediate predecessor, and consider the probability that the first immediate predecessor among the immediate predecessors of all the collaborating nodes on the communication path coincides with the message sender. The conditional probability was first employed in [15] for the analysis of the sender anonymity of Crowds. The evaluation method is very simple because it only uses the probabilities of mode selections, the number of collaborating nodes, and the number of 3MN members, and it does not consider other attacks such as eavesdropping and timing attacks [9]. The conditional probability has been introduced in the literature (*e.g.*, [7], [11], [13], [17]) as a standard measure for the anonymity of anonymous communication systems. We also employ this measure for analyzing sender anonymity in 3MN.

As shown in [12], 3MN can be regarded as a generalization of Onion Routing and Crowds, and we can analyze these anonymous communication systems in a unified framework. By choosing the probabilities of mode selections appropriately so that 3MN behaves in the same way as Crowds, we show that this probability is equal to the one obtained in [15]. In addition, we derive a formula for sender anonymity in Onion Routing. Furthermore, by using these results, we present numerical examples with the several probabilities of mode selections, and discuss sender anonymity in 3MN through these examples.

This paper is organized as follows. Section II gives an overview of 3MN. In Section III, we derive the probability that the first immediate predecessor among the immediate predecessors of all the collaborating nodes is a message sender. Also, we derive these probabilities in Crowds and Onion Routing. In Section IV, we consider the influence of the probabilities of mode selections on sender anonymity through numerical examples. We conclude this paper in Section V.

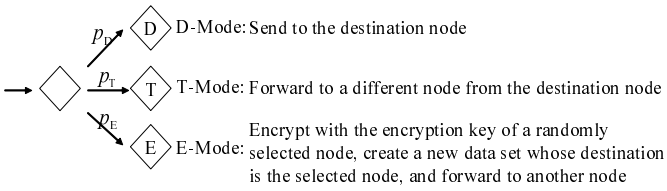

Fig. 1. Actions of a node in 3MN

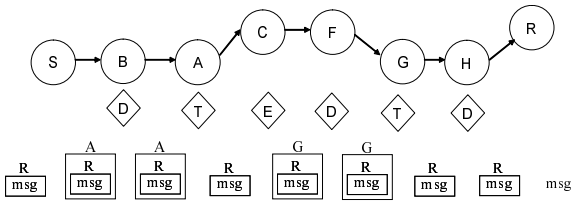

Fig. 2. An example of the behavior of 3MN

II. Overview of 3-Mode Net

3MN [12] is one of the anonymous communication systems where a message sender forwards a multi-encrypted data set to a message receiver through several relay nodes, where we refer to the data set as the set of data composed of the address of the next destination and the multi-encrypted data set.

A. Three modes in 3MN

3MN has three modes as shown in Figure 1, *i.e.*, Decryption Mode (D-Mode), Transmission Mode (T-Mode), and Encryption Mode (E-Mode). Each relay node selects one of the three modes based on probability.

In Figure 1, the first mode is the mode where a node transmits a received data set to its destination directly. In this case, after the destination node receives the data set, the node decrypts the data set with his decryption key, and produces a new data set, which is similar to the case of Onion Routing [14]. This mode is called Decryption Mode (D-Mode).

The second mode is the mode where a node forwards a received data set to other node than the destination. This mode is called Transmission Mode (T-Mode).

The third mode consists of the following two processes: first, create a new data set whose destination is a newly-selected node except for the destination of a received data set and whose data is created by encrypting the received data set with the encryption key of the newly-selected node; second, forward the new data set to other node except for the destination specified in the new data set. This mode is called Encryption Mode (E-Mode).

By introducing E-Mode, the destination of a data set does not always indicate the proper receiver of a message, and thus, 3MN has the anonymity of the proper receiver. This is sharp contrast with the case of Crowds [15], [16]. In addition, since each node cannot understand whether the immediate predecessor of the node is a message sender or one of relay nodes, sender anonymity is also preserved. This situation is similar to the case of Onion Routing.

Each relay node selects one of the three modes based on probability. Here, let the probabilities to choose D-Mode, T-Mode, and E-Mode be p_{D}, p_{T}, and p_{E}, respectively, and suppose that $p_{\mathrm{D}} + p_{\mathrm{T}} + p_{\mathrm{E}} = 1$ and $p_{\mathrm{D}} > p_{\mathrm{E}}$.

B. Behavior of 3MN

We explain the behavior of 3MN by showing the action of each relay node in Figure 2. In Figure 2, square frames indicate multi-encrypted data composed of multi-encrypted message and the address of the next destinations. Characters on square frames indicate the next destination. We refer to the set of these two data as a data set.

A sender S first creates a data set $\mathrm{R}||K_{\mathrm{R}}(\mathrm{msg})$ which consists of the address of a proper receiver R and an encrypted message $K_{\mathrm{R}}(\mathrm{msg})$ with R's encryption key K_{R} ($||$ represents the combination of data). Next, S creates a data set $\mathrm{A}||K_{\mathrm{A}}(\mathrm{R}||K_{\mathrm{R}}(\mathrm{msg}))$ (A and K_{A} represent the destination of a node selected randomly and A's encryption key, respectively). After that, S forwards the data set $\mathrm{A}||K_{\mathrm{A}}(\mathrm{R}||K_{\mathrm{R}}(\mathrm{msg}))$ to other node B. In this case, the number of multiplicity of encryption is 2. We refer to the number as the *initial multiplicity of encryption* and denote it by k in general.

When a relay node has received a data set, the node first checks its destination. If the destination is the address of the node, the node decrypts the multi-encrypted data and produces a new data set, and selects one mode based on probability. If the destination is not the address of the node, the node only selects one mode based on probability. In this example, B selects one action according to probability, and suppose that B selects D-Mode. In this case, B forwards this data set to a node A.

When the node A has received the data set, A acquires a new data set $\mathrm{R}||K_{\mathrm{R}}(\mathrm{msg})$ since A has the decryption key of $K_{\mathrm{A}}(\mathrm{R}||K_{\mathrm{R}}(\mathrm{msg}))$. After that, suppose that A chooses T-mode, A forwards $\mathrm{R}||K_{\mathrm{R}}(\mathrm{msg})$ to other node C.

In the similar manner, the node C and the following nodes forward a data set with encryption and decryption by selecting one mode. Finally, the receiver R receives a data set $\mathrm{R}||K_{\mathrm{R}}(\mathrm{msg})$. Then, R obtains the message msg by decrypting the data set, and the transmission of a message finishes.

Notice that 3MN provides a unified framework which can deal with Onion Routing and Crowds as a special case by selecting the probabilities of the three modes and the initial multiplicity of encryption appropriately. The relationships among Onion Routing, Crowds, and 3MN are shown in Table I. In Table I, p_f represents the probability of forwarding a received message to another randomly chosen node in Crowds.

TABLE I
Relationships among Onion Routing, Crowds, and 3MN

	Initial multiplicity	Probability of mode selections		
		D-Mode	E-Mode	T-Mode
3MN	k	p_{D}	p_{E}	p_{T}
Onion Routing	k	1	0	0
Crowds	1	$1 - p_f$	0	p_f

III. Anonymity of a message sender against collaborating nodes

In this section, we evaluate the degree of sender anonymity against collaborating nodes who attempt to identify a message sender by collaborating each other. To simplify the discussion, we assume that the number of 3MN members is constant. In addition, suppose that collaborating nodes do not perform other attacks, *e.g.*, eavesdropping, timing attacks [9], and so on.

It should be noted that, in order to argue the sender anonymity of 3MN in a similar way to the case of Crowds, we assume that both a message sender and a message receiver are not collaborating nodes.

A. Derivation of the formula on sender anonymity against collaborating nodes

In order to measure the degree of sender anonymity, we derive the probability that the first immediate predecessor among the immediate predecessors of all the collaborating nodes on the communication path is indeed a message sender. Our approach is the same as the approach of Crowds [15]. Therefore, we derive the probability in a similar way to Crowds case.

Let H_i, $i \geq 1$, denote the event that the first collaborating node on the communication path appears at i-th node on the path, and define $H_{i+} = H_i \vee H_{i+1} \vee H_{i+2} \vee \cdots$. Also, let I denote the event that the first immediate predecessor among the immediate predecessors on the communication path is the message sender.

Now, we consider the conditional probability $P(I|H_{1+})$ that the first immediate predecessor among the immediate predecessors of the collaborating nodes is the message sender, under the condition that one of the collaborating nodes receives a data set. However, unlike the simple situation such as Crowds, it is rather hard to derive the probability because we must compute infinite series concerning H_{1+} which is very complicated for 3MN case. In order to avoid the computation of the infinite series, we introduce "probability generating function" and its properties [6]. By using the function, we can obtain the following theorem that concerns this probability.

Theorem 1: Let n and c denote the number of all members and that of collaborating nodes in 3MN, respectively. Then, the probability $P(I|H_{1+})$ is given by the following equation:

$$P(I|H_{1+}) = \frac{(n-c)(c+1) - n \times g_{\tau_k}(\frac{n-c}{n})}{n(n-c)\{1 - g_{\tau_k}(\frac{n-c}{n})\}}, \quad (1)$$

where $g_{\tau_k}(\lambda)$ is a probability generating function for a random variable τ_k representing the number of the relay nodes, until the message reaches the proper receiver under the condition that the initial multiplicity of encryption is k, and is given by the following equation:

$$g_{\tau_k}(\lambda) = \begin{cases} \left(\frac{1-p_{\mathrm{T}}\lambda - \sqrt{(1-p_{\mathrm{T}}\lambda)^2 - 4p_{\mathrm{D}}p_{\mathrm{E}}\lambda^2}}{2p_{\mathrm{E}}\lambda}\right)^k & (p_{\mathrm{E}} \neq 0) \\ \left(\frac{p_{\mathrm{D}}\lambda}{1-p_{\mathrm{T}}\lambda}\right)^k & (p_{\mathrm{E}} = 0) \end{cases}. \quad (2)$$

Proof: The conditional probability $P(I|H_{1+})$ is obtained by the following equation:

$$\begin{aligned} P(I|H_{1+}) &= \frac{P(I \wedge H_{1+})}{P(H_{1+})} = \frac{P(I)}{P(H_{1+})} \\ &= \frac{P(I|H_1)P(H_1) + P(I|H_{2+})P(H_{2+})}{P(H_{1+})}. \end{aligned} \quad (3)$$

Here, we use $P(I \wedge H_{1+}) = P(I)$ since $I \Rightarrow H_{1+}$. Here, note that $P(H_1) = c/n$, $P(I|H_1) = 1$, $P(I|H_{2+}) = 1/(n-c)$. The third equation indicates that if the first collaborating node receives a data set through several relay nodes, then the immediate predecessor of the collaborating node is one of the any non-collaborating nodes with equal likelihood [15].

In order to calculate Equation (3), we need to compute $P(H_{1+})$ because $P(H_{2+}) = P(H_{1+}) - P(H_1)$. This value is calculated as follows:

$$P(H_{1+}) = 1 - g_{\tau_k}\Big(\frac{n-c}{n}\Big). \quad (4)$$

The proof of this equation is given in Appendix A. Equation (2) is proved in Appendix B.

From Equations (3) and (4), $P(I)$ and $P(I|H_{1+})$ are calculated as follows, respectively:

$$P(I) = \frac{c}{n} + \frac{1}{n-c}\Big\{1 - \frac{c}{n} - g_{\tau_k}\Big(\frac{n-c}{n}\Big)\Big\}, \quad (5)$$

$$P(I|H_{1+}) = \frac{(n-c)(c+1) - n \times g_{\tau_k}(\frac{n-c}{n})}{n(n-c)\{1 - g_{\tau_k}(\frac{n-c}{n})\}}. \quad (6)$$

This completes the proof. ■

B. Sender anonymity in Crowds and Onion Routing

We show that the above conditional probability is equal to that of Crowds as a special case. In addition, we give a formula for sender anonymity in Onion Routing.

First, we drive the equation in [15] from Equation (1). Since Crowds can be regarded as the special case of 3MN by selecting the probabilities of the three modes and the initial multiplicity of encryption appropriately, Equation (1) must be equal to the equation in Crowds. From Table I, the initial multiplicity of encryption and the probabilities of D-Mode, E-Mode, and T-Mode are 1, $1 - p_f$, 0, and p_f, respectively. Also, Equation (2) is calculated as follows:

$$g_{\tau_k}(\lambda) = \frac{(1-p_f)\lambda}{1 - p_f\lambda}. \quad (7)$$

Therefore, from Equation (1), we obtain:

$$P(I|H_{1+}) = \frac{\{n - p_f(n-c-1)\}}{n}. \quad (8)$$

This result coincides with the equation obtained in [15].

Next, we compute a conditional probability that the first immediate predecessor among the immediate predecessors of all collaborating nodes is a message sender in Onion Routing. From Table I, the initial multiplicity of encryption, the probabilities of D-Mode, E-Mode, and T-Mode are k, 1, 0, and 0, respectively. Also, Equation (2) is calculated as follows:

$$g_{\tau_k}(\lambda) = \lambda^k. \quad (9)$$

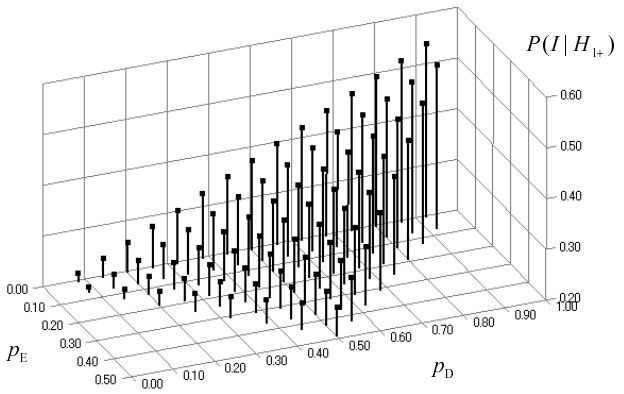

Fig. 3. Sender anonymity under the various probabilities of mode selections

Therefore, from Equation (1), we obtain:

$$P(I|H_{1+}) = \frac{(c+1)n^{k-1} - (n-c)^{k-1}}{n^k - (n-c)^k}. \qquad (10)$$

IV. Numerical Examples

A. Effects of the probabilities of mode selections

In this section, we consider the influence of the probabilities of mode selections on sender anonymity against collaborating nodes through numerical examples.

First, we illustrate the degree of sender anonymity under the condition that $k = 2$, $n = 10$, and $c = 1$. Figure 3 shows the degree of sender anonymity under the various probabilities of mode selections in the region satisfying $0 < p_{\rm D} < 1$, $0 < p_{\rm E} < 1$, $0 < p_{\rm D} + p_{\rm E} < 1$ (this corresponds to $0 < p_{\rm T} < 1$), and $p_{\rm D} > p_{\rm E}$. From Figure 3, we show that when $p_{\rm D}$ becomes large, $P(I|H_{1+})$ becomes large under the condition that $p_{\rm E}$ is constant. Also, we show that when $p_{\rm E}$ becomes small, $P(I|H_{1+})$ becomes large under the condition that $p_{\rm D}$ is constant. These results show that the degree of sender anonymity degrades when we set $p_{\rm D}$ to be large and $p_{\rm E}$ to be small. In order to provide high anonymity, we must set $p_{\rm D}$ to be small and $p_{\rm E}$ to be large. However, in such a situation, it is shown in [10] that the number of relay nodes becomes large. Therefore, there is a performance trade-off between sender anonymity and the number of relay nodes required for communication.

Second, in order to consider from the viewpoints of sender anonymity as well as the number of relay nodes and that of encryption, we consider the following three cases under the condition $k = 1$: Case A: ($p_{\rm D}$, $p_{\rm E}$, $p_{\rm T}$)=(0.50, 0.43, 0.07), Case B: ($p_{\rm D}$, $p_{\rm E}$, $p_{\rm T}$)=(0.10, 0.03, 0.87), Case C: ($p_{\rm D}$, $p_{\rm E}$, $p_{\rm T}$)=(0.75, 0.05, 0.20). The reason why $k = 1$ is to see the influence of mode probabilities for sender anonymity more clearly. The numerical results of the expectations and variances of the numbers of relay nodes and encryption, and the conditional probabilities $P(I|H_{1+})$ are shown in Table II. In Table II, $M_{\rm N}$, $V_{\rm N}$, $M_{\rm E}$, and $V_{\rm E}$ are the expectation and variance of the number of relay nodes, and the expectation and variance of the number of encryption, respectively. From Table II, we observe that $P(I|H_{1+}) = 0.3728$ in Case A and $P(I|H_{1+}) = 0.2695$ in Case B, respectively. If collaborating nodes tried to identify a message sender without any information other than the number of 3MN members and that of the collaborating nodes, all the non-collaborating nodes would seem to be the message sender with equal likelihood, *i.e.*, $1/(n-c) = 1/9 = 0.1111$. Compared with this value, these results of $P(I|H_{1+})$ in Table II are high, but are less than 0.5. Therefore, according to the criterion in [15], sender anonymity is maintained in these two examples.

Also, from Table II, 3MN in Case C hardly maintains sender anonymity because $P(I|H_{1+}) = 0.7564$. In Case C, in almost cases, after a message sender forwards a message to a relay node, the relay node sends the message to a message receiver, because the number of relay nodes and that of encryption are quite small. By this, we observe that when the number of relay nodes and that of encryption become small, sender anonymity becomes little. Therefore, we conclude that sender anonymity is lost under the case where the inappropriate probabilities of mode selections are chosen so that the number of relay nodes and that of encryption are quite small.

Also, we observe that the degrees of sender anonymity for Case A and Case B are different although the expectations of the number of relay nodes are the same. By this observation, it is expected that there exist the probabilities of mode selections with high performance and high anonymity for a message sender in 3MN because all the values of Case B are superior to those of Case A in Table II. However, we have to consider how much degree of anonymity is guaranteed for a message receiver because the behavior of 3MN in Case B is almost similar to that of Crowds and Crowds does not provide anonymity to a message receiver. Therefore, in order to consider the security and performance of 3MN, we need to analyze 3MN in more detail.

B. Effects of the initial multiplicity of encryption

In this section, using the three cases in the above examples, we observe influence of the initial multiplicity of encryption on sender anonymity through numerical examples.

The numerical results about the influence of the initial multiplicity of encryption on sender anonymity in 3MN are shown in Table III. Table III indicates that, in the examples, the probabilities $P(I|H_{1+})$ between $k=1$ and $k=2$ vary widely. This implies that, considering the performance of 3MN, it is appropriate to select $k = 2$ as the initial multiplicity of encryption. We also observe that $P(I|H_{1+})$ converges to one

TABLE II
Expectations and variances of the numbers of relay nodes and encryption, and degrees of sender anonymity in 3MN

	$(p_{\rm D}, p_{\rm E}, p_{\rm T})$ $(k=1,\ n=10,\ c=1)$		
	(0.50, 0.43, 0.07)	(0.10, 0.03, 0.87)	(0.75, 0.05, 0.20)
$M_{\rm N}$	14.29	14.29	1.429
$V_{\rm N}$	2697	364.7	0.9038
$M_{\rm E}$	7.143	1.426	1.071
$V_{\rm E}$	582.9	1.137	0.08746
$P(I\|H_{1+})$	0.3728	0.2695	0.7564

value whatever $p_{\rm D}$, $p_{\rm E}$, and $p_{\rm T}$ may be, when k becomes large. This value is larger than the probability $1/(n-c)=1/9$. Concerning these points, we have the following theorem.

Theorem 2: Let n and c be the number of all members and that of collaborating nodes in 3MN, respectively. Then, the probability $P(I|H_{1+})$ that the first immediate predecessor among the immediate predecessors of all the collaborating nodes is the message sender tends to $(c+1)/n$ whatever $p_{\rm D}$,$p_{\rm E}$, and $p_{\rm T}$ may be, when k goes to infinite. In addition, this value is larger than $1/(n-c)$.

Proof: In order to prove this theorem, we use a probability generating function for a random variable and its general property [6]. A probability generating function $g_X(\lambda)$ for a random variable X is defined as follows:

$$g_X(\lambda) = \sum_{r=0}^{\infty} P(X=r)\lambda^r, \tag{11}$$

where k and $P(X=r)$ are the initial multiplicity of encryption and a probability distribution for X, respectively. When $0<\lambda<1$, we obtain the following equation.

$$g_X(\lambda) = \sum_{r=0}^{\infty} P(X=r)\lambda^r < \sum_{r=0}^{\infty} P(X=r) = 1. \tag{12}$$

Therefore, the following property is obtained.

$$\text{if} \quad 0<\lambda<1 \quad \text{then} \quad 0<g_X(\lambda)<1. \tag{13}$$

By using this property and Equations (1) and (2), we obtain:

$$\begin{aligned} P(I|H_{1+}) &= \lim_{k\to\infty} \frac{(n-c)(c+1) - n\times g_{\tau_k}(\frac{n-c}{n})}{n(n-c)\{1-g_{\tau_k}(\frac{n-c}{n})\}} \\ &= \lim_{k\to\infty} \frac{(n-c)(c+1) - n\times (g_{\tau_1}(\frac{n-c}{n}))^k}{n(n-c)[1-\{g_{\tau_1}(\frac{n-c}{n})\}^k]} \\ &= \frac{(n-c)(c+1)}{n(n-c)} = \frac{c+1}{n}. \end{aligned} \tag{14}$$

In addition, we obtain:

$$\frac{c+1}{n} - \frac{1}{n-c} = \frac{c(n-c-1)}{n(n-c)} \geq 0 \quad (\because\ n \geq c+1).$$

This completes the proof. ■

V. Conclusion

In this paper, we have analyzed the degree of sender anonymity for an anonymous communication system 3-Mode Net (3MN) against collaborating nodes. In order to evaluate the degree of sender anonymity in 3MN, we consider collaborating nodes who attempt to identify a message sender, and derive the conditional probability that the first immediate predecessor among the immediate predecessors of all the collaborating nodes is the message sender when one of the collaborating nodes receives the message. We show that this conditional probability is represented by a probability generating function, which is different from the derivation method in Crowds [15]. Furthermore, we calculate the conditional probabilities in Crowds and Onion Routing from obtained results. By using these results, we consider the influence of the probabilities of mode selections and the initial multiplicity of encryption.

The remaining works in 3MN are mainly as follows;

1) derive receiver anonymity against collaborating nodes,
2) analyze 3MN in detail from the viewpoints of security and performance,
3) implement 3MN, like Freenet [3], Mixminion [4], and Tor [5].

Especially, the first issue would be one of the most interesting topics because we can evaluate sender-receiver anonymity by using receiver anonymity together with the results of sender anonymity obtained in this paper.

TABLE III
Sender anonymity in the several initial multiplicity of encryption of 3MN

	$(p_{\rm D}, p_{\rm E}, p_{\rm T})$ $(k=1,\ n=10,\ c=1)$		
	(0.50, 0.43, 0.07)	(0.10, 0.03, 0.87)	(0.75, 0.05, 0.20)
$k=1$	0.3728	0.2695	0.7654
$k=2$	0.2687	0.2212	0.4621
$k=3$	0.2360	0.2082	0.3617
$k=5$	0.2128	0.2015	0.2827
$k=100$	0.2000	0.2000	0.2000

References

[1] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM*, 24(2):84–88, February 1981.

[2] D. Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology*, 1:66–92, January 1988.

[3] I. Clarke, O. Sandberg, B. Wiley, and T. Hong. Freenet: A distributed anonymous information storage and retrieval system. In *Proc. International Workshop on Design Issues in Anonymity and Unobservability*, July 2000.

[4] G. Danezis, R. Dingledine, and N. Mathewson. Mixminion: Design of a type III anonymous remailer protocol. In *Proc. IEEE Symposium on Security and Privacy*, May 2003.

[5] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second-generation onion router. In *Proc. 13th USENIX Security Symposium*, pages 303–320, August 2004.

[6] W. Feller. *An Introduction to Probability Theory and Its Applications*, volume 1. John Wiley & Sons, Inc., 3rd edition, 1968.

[7] D. Figueiredo, P. Nain, and D. Towsley. On the analysis of the predecessor attack on anonymity systems. Computer Science Technical Report 04-65, July 2004. University of Massachusetts CMPSCI.

[8] M. Gomulkiewicz, M. Klonowski, and M. Kutylowski. Onions based on universal re-encryption - anonymous communication immune against repetitive attack. In *Proc. 5th International Workshop on Information Security Applications*, August 2004.

[9] P. C. Kocher. Timing attacks on implementations of die-hellman, rsa, dss, and other systems. In *Proc. Advances in Cryptology*, pages 104–113, August 1996.

[10] K. Kono, N. Nakano, Y. Ito, and N. Babaguchi. Performance analysis of anonymous communication system 3-mode net. In *Proc. 5th International Conference on Information Assurance and Security*, August 2009. Accepted.

[11] B. Levine and C. Shields. Hordes: A multicast based protocol for anonymity. *ACM Journal of Computer Security*, 10(3):213–240, September 2002.

[12] N. Miyake, Y. Ito, and N. Babaguchi. 3-mode net: A bi-directional anonymous communication system based on multiple encryption and probabilistic selections of actions. *IEICE Trans. A*, J91-A(10):949–956, October 2008. (in Japanese).

[13] A. Nambiar and M. Wright. Salsa: A structured approach to large-scale anonymity. In *Proc. ACM conference on Computer and Communication Security*, pages 17–26, October 2006.

[14] M. G. Reed, P. F. Syverson, and D. M. Goldschlag. Anonymous connections and onion routing. *IEEE Journal of Selected Areas in Communication*, 16(4):482–494, May 1988.
[15] M. Reiter and A. Rubin. Crowds: Anonymity for web transactions. *ACM Trans. Information and System Security*, 1(1):66–92, June 1998.
[16] M. Reiter and A. Rubin. Anonymous web transactions with crowds. *Commun. ACM*, 42(2):32–38, February 1999.
[17] M. Wright, M. Adler, and B. Levine. The predecessor attack: An analysis of a threat to anonymous communication systems. *Acm Trans. Information and System Security*, 7(4):489–522, November 2004.
[18] S. Yamanaka, K. Kobara, and H. Imai. Valkyrie: An anonymous routing scheme on unstable network. *Trans. Information Processing Society of Japan*, 46(8):2025–2035, August 2005. (in Japanese).

APPENDIX

A. Derivation of Equation (4)

Let τ_k be the random variable representing the number of relay nodes required for communication under the condition that the initial multiplicity of encryption is k, and $P_k(i)$ be the probability that the number of relay nodes required for communication is i, that is, $P_k(i) = P(\tau_k = i)$. If the first collaborating node on a communication path appears at i-th node on the path, the number of relay nodes required for communication is larger than or equal to i. Therefore, the probability $P(H_i)$ that the first collaborating node on the communication path appears at i-th node on the path is described as follows:

$$\begin{aligned}
P(H_i) =& P_k(i)\Big(\frac{n-c}{n}\Big)^{i-1}\Big(\frac{c}{n}\Big) + P_k(i+1)\Big(\frac{n-c}{n}\Big)^{i-1}\Big(\frac{c}{n}\Big) + \cdots \\
=& \{P_k(i) + P_k(i+1) + \cdots\}\Big(\frac{n-c}{n}\Big)^{i-1}\Big(\frac{c}{n}\Big) \\
=& \Big[1 - \big\{P_k(0) + \cdots + P_k(i-1)\big\}\Big]\Big(\frac{n-c}{n}\Big)^{i-1}\Big(\frac{c}{n}\Big) \\
=& \left\{1 - \sum_{j=0}^{i-1} P_k(j)\right\}\lambda^{i-1}(1-\lambda),
\end{aligned}$$

where $\lambda = (n-c)/n$. Therefore, we can calculate the probability $P(H_{1+})$ as follows:

$$\begin{aligned}
P(H_{1+}) =& \sum_{i=1}^{\infty} P(H_i) \\
=& (1-\lambda)\sum_{i=1}^{\infty}\Big\{1 - \sum_{j=0}^{i-1} P_k(j)\Big\}\lambda^{i-1} \\
=& (1-\lambda)\Big\{\sum_{i=1}^{\infty}\lambda^{i-1} - \sum_{i=1}^{\infty}\sum_{j=0}^{i-1} P_k(j)\lambda^{i-1}\Big\} \\
=& 1 - (1-\lambda)\sum_{j=0}^{\infty}\sum_{i=j+1}^{\infty} P_k(j)\lambda^{i-1} \\
=& 1 - (1-\lambda)\sum_{j=0}^{\infty} P_k(j)\frac{\lambda^j}{1-\lambda} \\
=& 1 - \sum_{j=0}^{\infty} P_k(j)\lambda^j = 1 - \sum_{j=0}^{\infty} P(\tau_k = j)\lambda^j \\
=& 1 - g_{\tau_k}(\lambda) = 1 - g_{\tau_k}\Big(\frac{n-c}{n}\Big).
\end{aligned}$$

In the above derivation, we used the definition of a probability generating function:

$$g_{\tau_k}(\lambda) = \sum_{j=0}^{\infty} P(\tau_k = j)\lambda^j. \tag{15}$$

This completes the proof. ■

B. Derivation of Equation (2)

From Equation (15), $g_{\tau_k}(\lambda)$ can be written by

$$g_{\tau_k}(\lambda) = E(\lambda^{\tau_k}),$$

where $E(\cdot)$ is the expectation operator. Since τ_k is the sum of k copies of an independent random variable τ_1, the probability generating function $g_{\tau_k}(\lambda)$ is calculated as follows:

$$g_{\tau_k}(\lambda) = E(\lambda^{\tau_k}) = E(\lambda^{k\tau_1}) = E(\lambda^{\tau_1})^k = g_{\tau_1}(\lambda)^k.$$

This is derived from the relation $E(\lambda^{X+Y}) = E(\lambda^X)E(\lambda^Y)$ when random variables X and Y are independent. In order to drive $g_{\tau_k}(\lambda)$, we consider $g_{\tau_1}(\lambda)$.

Considering the property of 3MN, we derive several conditions about $g_{\tau_1}(\lambda)$. First, since the events selecting D-Mode, E-Mode, and T-Mode are mutually exclusive, we obtain:

$$g_{\tau_1}(\lambda) = E(\lambda^{\tau_1}) = E(\lambda^{\tau_1}|\mathrm{D}) + E(\lambda^{\tau_1}|\mathrm{E}) + E(\lambda^{\tau_1}|\mathrm{T}),$$

where $E(\lambda^{\tau_1}|\mathrm{X})$ represents the conditional expectation of λ^{τ_1} under the condition that X-mode is selected.

Next, we consider the above conditional expectations $E(\lambda^{\tau_1}|\mathrm{D})$, $E(\lambda^{\tau_1}|\mathrm{E})$, and $E(\lambda^{\tau_1}|\mathrm{T})$. When D-Mode, E-Mode, and T-Mode are selected, the multiplicities of encryption become 0, 2, and 1 by one step, respectively. Therefore, the random variables of the conditional expectations in D-Mode, E-Mode, and T-Mode become 1, $1+\tau_2$, $1+\tau_1$, respectively. Since the probabilities of mode selections are p_{D}, p_{E}, and p_{T}, the conditional expectations are as follows:

$$\begin{aligned}
E(\lambda^{\tau_1}|\mathrm{D}) =& p_{\mathrm{D}}E(\lambda^1) = p_{\mathrm{D}}\lambda, \\
E(\lambda^{\tau_1}|\mathrm{E}) =& p_{\mathrm{E}}E(\lambda^{1+\tau_2}) = p_{\mathrm{E}}\lambda E(\lambda^{\tau_2}) = p_{\mathrm{E}}\lambda(g_{\tau_1}(\lambda))^2, \\
E(\lambda^{\tau_1}|\mathrm{T}) =& p_{\mathrm{T}}E(\lambda^{1+\tau_1}) = p_{\mathrm{T}}\lambda E(\lambda^{\tau_1}) = p_{\mathrm{T}}\lambda(g_{\tau_1}(\lambda)).
\end{aligned}$$

From these results, we obtain:

$$g_{\tau_1}(\lambda) = p_{\mathrm{D}}\lambda + p_{\mathrm{E}}\lambda(g_{\tau_1}(\lambda))^2 + p_{\mathrm{T}}\lambda g_{\tau_1}(\lambda).$$

By solving the above quadratic equation, $g_{\tau_1}(\lambda)$ is given as follows:

$$g_{\tau_1}(\lambda) = \frac{1 - p_{\mathrm{T}}\lambda - \sqrt{(1-p_{\mathrm{T}}\lambda)^2 - 4p_{\mathrm{D}}p_{\mathrm{E}}\lambda^2}}{2p_{\mathrm{E}}\lambda},$$

where we use two conditions that $g_{\tau_1}(\lambda)$ have to be finite when $\lambda \to 0$ and that $p_{\mathrm{E}} \neq 0$. Therefore, when $p_{\mathrm{E}} \neq 0$, we obtain:

$$g_{\tau_k}(\lambda) = \left(\frac{1 - p_{\mathrm{T}}\lambda - \sqrt{(1-p_{\mathrm{T}}\lambda)^2 - 4p_{\mathrm{D}}p_{\mathrm{E}}\lambda^2}}{2p_{\mathrm{E}}\lambda}\right)^k.$$

Also, in the case $p_{\mathrm{E}} = 0$, by solving the linear equation $(1 - p_{\mathrm{T}}\lambda)g_{\tau_1}(\lambda) - p_{\mathrm{D}}\lambda = 0$, we obtain:

$$g_{\tau_k}(\lambda) = \Big(\frac{p_{\mathrm{D}}\lambda}{1 - p_{\mathrm{T}}\lambda}\Big)^k.$$

This completes the proof. ■