2005－ＱＡＩ－15（３）
2005／5／25

マルチ結合チェーンモデルにおけるストリームの認証確率

Qusai ABUEIN† 渋沢 進††

† 茨城大学大学院理工学研究科 〒316－8511 日立市中成沢町 4－12－1
†† 茨城大学工学部 〒316－8511 日立市中成沢町 4－12－1
E-mail: †{abueinq,sibusawa}@cis.ibaraki.ac.jp

あらまし マルチキャストストリームの認証において，データパケットごとに署名することによるオーバーヘッドを軽減する方法として，署名とハッシュチェーンを用いた署名補償法が有効である．ストリームの認証確率は，ストリーミング方式の性能を評価する上で重要な評価基準である．本報告では，これまで提案してきたマルチ結合チェーン(MC)方式の有効性を示すために，2状態マルコフモデルを用いたストリームの認証確率を求めている．また，本方式の性能を評価するためにいくつかのパラメータ要因に対する多くのシミュレーションを実施した．MCモデルにおいて，署名パケットへのハッシュ数と各パケットあたりのハッシュ数は，認証確率を決定する重要なファクタである．
キーワード 認証確率，2状態マルコフモデル，ハッシュチェーン，署名補償法，マルチキャストストリーミング，インターネットセキュリティ

Authentication Probability of Multiple Connected Chains Model for Signature Amortization

Qusai ABUEIN† and Susumu SHIBUSAWA††

† Graduate School of Science and Engineering, Ibaraki University, Hitachi, Ibaraki 316－8511, Japan
†† Department of Computer and Information Sciences, Ibaraki University, Hitachi, Ibaraki 316－8511, Japan
E-mail: †{abueinq,sibusawa}@cis.ibaraki.ac.jp

Abstract Signature amortization schemes for multicast streams authentication is introduced as a solution to reduce the high overhead that sign-each schemes suffer from. The authentication probability is an important metric to measure the performance of signature amortization schemes since packet loss seriously affects the authentication probability for multicast application. In this paper we derive the authentication probability of MC model using 2-state Markov model to achieve longer resistance to packet loss and to reduce the overhead. Several simulation studies of the authentication probability in terms of several factors have been carried out to measure our scheme performance and to determine the effect of these factors on the authentication scheme. The number of hashes appended to a signature packet and number of packets containing the hash of a previous packet have the highest influence on the authentication probability.

Key words Authentication probability, 2-state Markov model, hash chain, signature amortization, multicast streaming, Internet security.

1. Introduction

Several amortization schemes [1], [2], [3] have been introduced as a solution for authenticating multicast streams to reduce the high cost of sign-each schemes. In amortization schemes a single signature is amortized over multiple packets by using a multiple hash links called hash chains to achieve robustness against packet loss. Since The authentication of any packet in amortization schemes is dependent on other packets and is affected by packets loss, the authentication probability is an important metric for evaluating the efficiency of the authentication scheme. The EMSS [2] and Augmented Chain [3] schemes append the hash of a packet to several other packets in order to increase robustness against packet loss and achieve higher authentication probability, moreover they solved the weak robustness against packet loss of Rohatgi's scheme [1].

Finding an exact formula to characterize the authentication probability of a model in amortization schemes remains an open problem [2], and the difficulty of finding an exact for-

表 1 Notation.

symbol	representation
ν	number of packets appended with the hash of P_i
μ	number of hashes appended to the signature
β	number of hashes appended to the packets of the stream
h	hash size (SHA-1 is 20, MD5 is 16 bytes)
H	total size of all hashes in the stream
γ	number of signatures in the stream
N	number of packets in the stream
k	number of slices in a block
c	number of chains in the stream
δ	communication overhead per packet in byte
s	signature size (RSA is 128 bytes)
ℓ	loss resistance

mula is due to the hash chain topology [2], [4]. A recurrence authentication probability formula of EMSS is introduced using a specific hash chain in case of independent packet loss in [5]. Sara, et al. [6] introduced the authentication probability for their graph-based model, while Chan [4] provided a potential analytical solution of EMSS and Augmented Chain using graph theory. Park, et al. [7] introduced asymptotic authentication probability of their scheme that uses erasure codes to reduce the overhead. Sanneck, et al. [8] and Jiang, et al. [9] recommend the use of 2-state Markov model, also known as Gilbert model, to characterize burst packet loss.

The hash chains introduced for signature amortization until now do not have a clear and fixed structures and it do not specify clearly what packets have their hashes appended to the signature. Those make it hard to study the effect of some factors on the authentication probability. The hash chain construction for most schemes has been determined by simulation.

In previous papers [10], [11], [12], [13], we introduced a multiple connected chains MC model that consists of multiple chains to achieve longer resistance to packet loss and to reduce the overhead. The number of chains plays a main role in the efficiency of MC model, where each chain connects some packets together; that is, increasing the number of chains leads to longer loss resistance and reduces overhead. The definite expression of authentication probability remains unsolved in the previous studies.

Using 2-state Markov model, this paper presents the authentication probability of MC model to measure its performance and robustness against packet loss. So as to authenticate any packet of MC model, there should be a link from that packet to the signature one. Since the hash of any packet is appended to several other packets and the signature packet is appended with several hashes of previous packets, there can be several links from any packet to the signature one. The multiplication of the transition states from any packet to the signature one through any link authenticates that packet. We perform simulation studies to determine the main effective factors on the performance of the authentication scheme.

This paper is organized as follows: in Section 2. we give a brief discussion of MC model. In Section 3. we give an efficiency and authentication probability of MC model. Section 4. describes the simulation study, and in Section 5. we give the conclusion of our study.

2. Chain Construction

Table 1 shows the notation used in MC model. When a

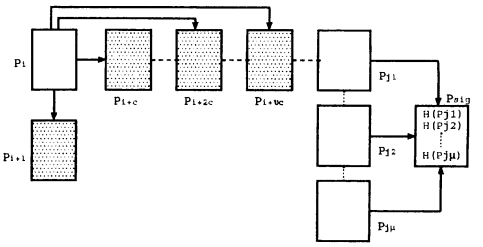

図 1 The packets of the sets $A(c,\nu)$ and $E(\mu)$.

stream S consists of N contiguous packets we represent S as:

$$S = \{P_1, P_2, \ldots, P_N\}.$$

We introduce a multiple connected chains (MC) model for multicast stream authentication using signature amortization in which a stream is divided into a number of blocks and each block consists of some packets. A single packet in each block is digitally signed and the rest of the packets are concatenated to the signed one through hash chains in a way that allows the receiver to authenticate the received packets.

A block of MC model consists of c chains, where each chain consists of some number of packets and the hash $H(P_i)$ of each packet P_i is appended to packet P_{i+1} in addition to ν other packets as P_{i+jc} where $j = 1, 2, \ldots, \nu$. For example, when $\nu = 3$, $H(P_i)$ is appended to P_{i+c}, P_{i+2c} and P_{i+3c}. Let $A(c,\nu)$ denotes a set of the packets that contain $H(P_i)$, then

$$A(c,\nu) = \{P_{i+1}, P_{i+c}, P_{i+2c}, \cdots, P_{i+\nu c}\}.$$

The set $A(c,\nu)$ is depicted as shaded cells in Figure 1. So as for MC model to be constructed and robust against packet loss, we choose the value of ν as $\nu \geq 1$.

A signature packet P_{sig} is appended with μ hashes of non-contiguous packets. We mean by non-contiguous packets that the next packet to P_i is P_{i+j} where $j > i+1$. Empty cells in Figure 2 are an example of non-contiguous packets. On the other hand contiguous packets mean that the next packet to P_i is P_{i+1}. Shaded cells in Figure 2 are an example of contiguous packets.

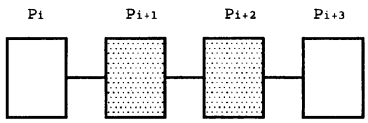

図 2 Non-contiguous and contiguous packets.

The packets that have their μ hashes appended to P_{sig} are chosen from the last c packets preceding the signature one. Let E denotes a set of the last c packets preceding the signature one, then the set $E = \{P_{(k-1)c+1}, P_{(k-1)c+2}, \cdots, P_{kc}\}$ belongs to the first signature packet P_{sig_1}. Let the first packet of those that have their μ hashes appended to P_{sig_1} chosen from E be $P_{(k-1)c+1} = P_{j_1}$, the last one be $P_{kc} = P_{j_\mu}$. So the set of the packets that have their μ hashes appended to P_{sig_1} is as:

$$E(\mu) = \{P_{j_1}, P_{j_2}, \cdots, P_{j_\mu}\},$$

where $j_1 < j_2 \cdots < j_\mu$, depicted in Figure 1. The reason to choose these packets as non-contiguous is that Internet packet loss is burst in nature, and if a packet P_i is lost, packet P_{i+1} is likely to be lost [8], [9], [14].

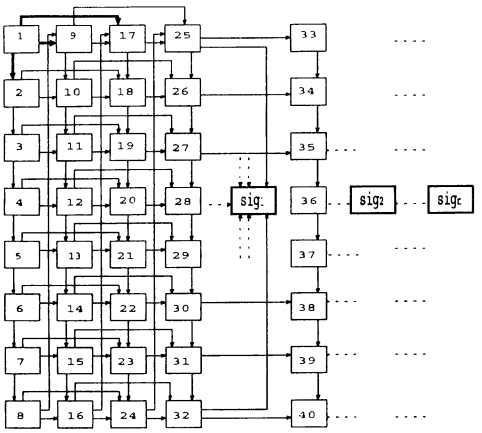

図 3 A construction of MC model when $c = 8, k = 4$ and $\nu = 2$.

Each signature packet is sent after every kc packets which determines the block size, where k denotes the number of slices in MC model. The group of the first c packets $\{P_1, P_2, \cdots, P_c\}$ is the first slice in MC model, the group of the second c packets $\{P_{c+1}, P_{c+2}, \cdots, P_{2c}\}$ is the second slice, and so on. Figure 3 depicts a construction of MC model when $c = 8$, the signature is sent after every $4c$ packet, and $\nu = 2$.

3. The Efficiency of MC Model

In this section we introduce factors that affect the performance of the authentication scheme, equations to measure these factors and the authentication probability of MC model.

3.1 Communication Overhead

The communication overhead means the total size of the information added to a packet to authenticate it, such as hashes and digital signature. The number of packets ν, number of hashes μ and number of chains c influence the performance of the authentication scheme and the authentication probability. Also the communication overhead δ and the authentication probability are dependent on each other.

Since in MC model the packets that have their μ hashes appended to a signature packet are chosen as non-contiguous to each other from the last c packets preceding the signature one, the value of μ is computed as

$$\mu \leqq \lceil \frac{c}{2} \rceil, \tag{1}$$

where $c \geqq 2$.

Since each packet P_i in MC model is appended with hashes of previous packets, P_1 contains no additional hashes. While each of the rest packets of the first slice $\{P_2, P_3, \cdots, P_c\}$ is appended with only a single hash, that is, in total there are $c-1$ hashes. Each packet of the second slice $\{P_{c+1}, P_{c+2}, \cdots, P_{2c}\}$ is appended with 2 hashes of the previous packets, so that in total there are $2c$ hashes. Each packet of the ith slice is appended with i hashes of previous packets where $i \leqq \nu$ except for P_1. In total we have $c-1+2c+3c+\ldots+\nu c$ hashes in the first ν slices; that is, $(\frac{\nu^2+\nu}{2})c-1$. Each packet of the remaining packets $\{P_{\nu c+1}, P_{\nu c+2}, \cdots, P_N\}$ is appended with $\nu+1$ hashes of previous packets. In total we have $(\nu+1)(N-\nu c)$ hashes. Accordingly, the total number of hashes β appended in the packets of stream S is computed as

$$\beta = (\frac{\nu^2+\nu}{2})c + (\nu+1)(N-\nu c) - 1. \tag{2}$$

The total size of all hashes H in the stream depends on the hash value the algorithm uses. In general H is computed as

$$H = h\beta. \tag{3}$$

Since there are kc packets in each block, the number of signatures γ in the stream is expressed as

$$\gamma = \lceil \frac{N}{kc} \rceil. \tag{4}$$

Dividing the overhead by the total number of packets in the stream gives the overhead per packet.

[Lemma 1] The communication overhead δ in bytes per packet is

$$\delta = \frac{H + \gamma(s+\mu h)}{N}. \tag{5}$$

Proof: Since the packets in the stream contain hashes and signatures in addition to data, the total of all hashes in the stream is given as H, while every signature packet contains a signature and μ hashes of other packets. Therefore, we have $s + \mu h$ overhead per signature packet. Since we have γ signatures in the stream, the overhead of all signature packets is $\gamma(s + \mu h)$. The overhead per packet is given by dividing $H + \gamma(s + \mu h)$ over N, which is δ. □

Loss resistance ℓ is the maximum number of lost packets the scheme can sustain and still able to authenticate received packets. To resist burst loss of packets, the distance from P_i to the last packet that contains $H(P_i)$ must be longer than the expected burst packet loss length. In MC model since $P_{i+\nu c}$ is the farthest packet that contains $H(P_i)$, resistance ℓ to burst loss is achieved by

$$\ell = \nu c - 1 \ . \tag{6}$$

The number of chains plays an important role in the efficiency of MC model in terms of loss resistance and overhead. The model must resist the expected burst loss b, otherwise the authentication of the received packets preceding the start of the loss becomes not possible. Accordingly, $\nu c - 1 \geqq b$; then,

$$c \geqq \lceil \frac{b+1}{\nu} \rceil. \tag{7}$$

Increasing the number of slices k decreases communication overhead δ as depicted in Figure 4 for different streams when $c = 16$, $\mu = 3$, $\nu = 2$, $s = 128$ bytes, and $h = 16$ bytes. For streams of size $N = 320$, 1000, 2000 and 5000, the overhead per packet δ decreases 6.7%, 5.9%, 6.0% and 6.0%, respectively, when increasing k from 3 to 20.

The number of the chains c plays a main role in the efficiency of MC model; that is, increasing c decreases δ and achieves longer loss resistance. The decrease of δ in terms of c is depicted in Figure 5 for different streams, where the number of slices k is 3. The overhead per packet δ decreases 27.5%, 16.6%, 14.1% and 12.5% for the streams of size $N = 320$, 1000, 2000 and 5000, respectively, when increasing c from 8 to 64.

3.2 Authentication Probability

In this section we present the authentication probability of MC model using 2-state Markov model, where the hash of packet P_i is appended to $\nu+1$ other packets and signature packet P_{sig} is appended with μ hashes of previous packets chosen as non-contiguous to each other. According to MC model, packet P_i is authenticated if signature packet P_{sig}, at least one packet of $E(\mu)$ and at least one packet of $A(c,\nu)$ are received. Note that for P_i to be authenticable, all the whole packets of $E(\mu)$ or $A(c,\nu)$ cannot be lost.

For the purpose of deriving the authentication probability

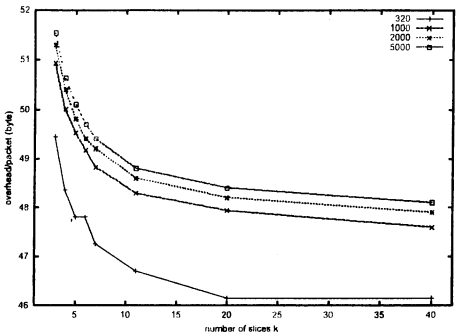

図 4 Overhead per packet in terms of number of slices k for different streams when $c = 16$, $\nu = 2$, and $\mu = 3$.

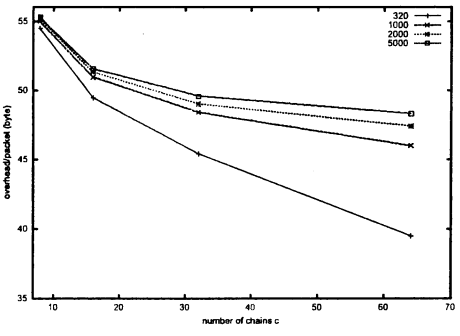

図 5 Overhead per packet in terms of number of chains c for different streams where $k = 3$, $\nu = 2$ and $\mu = 3$.

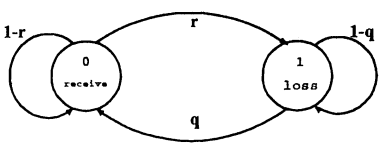

図 6 2-state Markov model for burst packet loss.

of P_i, we assume the followings:

- the derivation applies to a single block.
- packets P_i and P_{sig_1} are received.
- $i + \nu c < j_1$. Since packet P_{j_1} is chosen from the packets that are preceding P_{sig}, this condition means that the packet $P_{i+\nu c}$ lies before P_{sig}.

Let $P_r\{P_i\}$ denote the authentication probability of packet P_i when P_i is received, then $P_r\{P_i\}$ is expressed as:

$$P_r\{P_i\} = P_r\{P_i \textit{ is verifiable} \mid P_i \textit{ is received}\} \quad (8)$$

Figure 6 shows the 2-state Markov model that is used for characterizing burst packet loss. In the figure, r represents the probability that the next packet is lost, provided the previous one has arrived. q is the transition probability from loss state to received state, and it is opposite to r. The transition matrix P of the 2-state Markov model is expressed as

$$P = \begin{bmatrix} p_{00} & p_{01} \\ p_{10} & p_{11} \end{bmatrix} = \begin{bmatrix} 1-r & r \\ q & 1-q \end{bmatrix}, \quad (9)$$

where p_{ij} is the transition probability from state i to state j.

Packet P_i can be authenticated by multiplying the transition probabilities from P_i to one of the packets of $A(c,\nu)$, then to one of the packets of $E(\mu)$. The authentication probability of P_i in MC model is influenced by two factors ν and μ. According to 2-state Markov model depicted in Figure 6, receive and loss states are denoted 0 and 1, respectively. We give an example when $\nu = 1$, $\mu = 2$, and both packets P_{i+c} and P_{j_2} are lost, a case to authenticate P_i is through P_{i+1}, P_{j_1} and P_{sig}, and its transition probability is denoted as $p_{00}p_{01}^{(c-1)}p_{10}^{(j_1-i-c)}p_{01}^{(j_2-j_1)}$. The only case that cannot authenticate P_i is that all the whole packets of $E(\mu)$ or $A(c,\nu)$ are lost, while the combination of lost and receive of these packets are cases to authenticate P_i.

Table 2 shows the combination of the transition states when $\nu = 1$, $\mu = 2$ and the cases of transition probabilities to authenticate P_i, where P_{rec} means the receive probability.

表 2 Transition states and probabilities to authenticate P_i when $\nu = 1$ and $\mu = 2$.

P_i	P_{i+1}	P_{i+c}	P_{j_1}	P_{j_2}	P_{rec}
0	0	1	0	1	$p_{00}p_{01}^{(c-1)}p_{10}^{(j_1-i-c)}p_{01}^{(j_2-j_1)}$
0	1	0	0	1	$p_{01}p_{10}^{(c-1)}p_{00}^{(j_1-i-c)}p_{01}^{(j_2-j_1)}$
0	0	1	1	0	$p_{00}p_{01}^{(c-1)}p_{11}^{(j_1-i-c)}p_{10}^{(j_2-j_1)}$
0	1	0	1	0	$p_{01}p_{10}^{(c-1)}p_{01}^{(j_1-i-c)}p_{10}^{(j_2-j_1)}$
0	0	1	0	0	$p_{00}p_{01}^{(c-1)}p_{10}^{(j_1-i-c)}p_{00}^{(j_2-j_1)}$
0	1	0	0	0	$p_{01}p_{10}^{(c-1)}p_{00}^{(j_1-i-c)}p_{00}^{(j_2-j_1)}$
0	0	0	0	1	$p_{00}p_{00}^{(c-1)}p_{00}^{(j_1-i-c)}p_{01}^{(j_2-j_1)}$
0	0	0	1	0	$p_{00}p_{00}^{(c-1)}p_{01}^{(j_1-i-c)}p_{10}^{(j_2-j_1)}$
0	0	0	0	0	$p_{00}p_{00}^{(c-1)}p_{00}^{(j_1-i-c)}p_{00}^{(j_2-j_1)}$

[Lemma 2] The hash of a packet P_i is appended to ν other packets as P_{i+jc}, $j = 1, 2, \cdots, \nu$, in addition to P_{i+1}. A signature packet is appended with μ hashes of previous packets. Based on 2-state Markov model the number of cases m of transition probability to authenticate P_i is:

$$m = (2^{\nu+1} - 1) * (2^{\mu} - 1) \quad (10)$$

Proof: The hash of P_i is appended to the $\nu + 1$ packets of $A(c,\nu)$, also μ hashes of the packets of $E(\mu)$ are appended to signature packet. So as to authenticate P_i, at least one of the packets of $A(c,\nu)$ should be received. All the whole packets of $A(c,\nu)$ cannot be lost and the other cases are the combination of lost or receive states, so we have $(2^{\nu+1} - 1)$ cases. On the other hand, at least one of the packets of $E(\mu)$ should be received. All the whole packets of $E(\mu)$ cannot be lost and the other cases are the combination of lost or receive states, so we have $(2^{\mu} - 1)$ cases. In total we have $(2^{\nu+1} - 1) * (2^{\mu} - 1)$ cases to authenticate P_i. □

Since packet P_i is assumed to be received, its authentication probability $P_r\{P_i\}$ is the total of the transition probabilities from P_i to $A(c,\nu)$, then to $E(\mu)$, all the whole packets of $E(\mu)$ or $A(c,\nu)$ cannot be lost.

The first transition probability starts from state 0 since P_i is received, to either 0 or 1; that is, P_{i+1} is either received or lost, this transition probability is denoted p_{0g_1}, where the value of g_1 is either 0 or 1. The second transition probability goes from state g_1 to either 0 or 1; that is, P_{i+c} is either received or lost and this transition probability is denoted $p_{g_1g_2}$. The rest transition probabilities go from state g_2 to g_3, then g_3 to $g_4, \cdots$, until $g_{\nu+1}$, where g_k is either 0 or 1. The next transition probability goes from state $g_{\nu+1}$ to either 0 or 1 which means P_{j_1} is either received or lost and this transition probability is denoted $p_{g_{\nu+1}h_1}$. The next

transition probability goes from state h_1 to h_2; that is, P_{j_2} is either received or lost, the transition probability is denoted $p_{h_1h_2}$. The rest of the transition probabilities go from h_2 to h_3, then h_3 to $h_4, \cdots$ until h_μ, where h_k is either 0 or 1. The total of all the cases of these transition probabilities gives the authentication probability of P_i.

[Theorem 1] Based on 2-state Markov model the authentication probability of the ith packet P_i in a block according to MC model is given by the following expression, when $i + \nu c < j_1$:

$$P_r\{P_i\} = \sum_{g,h} \left\{ \left[p_{0g_1} p_{g_1g_2}^{(c-1)} \prod_{k=2}^{\nu} (p_{g_kg_{k+1}}^{(c)}) \right] \left[p_{g_{\nu+1}h_1}^{(j_1-i-\nu c)} \prod_{k=1}^{\mu-1} (p_{h_kh_{k+1}}^{(j_{k+1}-j_k)}) \right] \right\} \quad (11)$$

where $g_k \in \{0,1\}$, $k = 1, 2, \cdots, \nu+1$, $g = (g_1, g_2, \cdots, g_{\nu+1})$, $g \neq (1, 1, \cdots, 1)$ and $h_k \in \{0,1\}$, $k = 1, 2, \cdots, \mu$, $h = (h_1, h_2, \cdots, h_\mu)$, $h \neq (1, 1, \cdots, 1)$.

Proof: Since P_i is received, there is one transition state from P_i to P_{i+1}, so the transition probability is denoted p_{0g_1}. There are $(c-1)$ transition states from P_{i+1} to P_{i+c}, so the transition probability is denoted $p_{g_1g_2}^{(c-1)}$. On the other hand, there are c transition states between every two adjacent packets of $A(c,\nu)$, so we have transition probability $\prod_{k=2}^{\nu}(p_{g_kg_{k+1}}^{(c)})$, and in total we have transition probability $p_{0g_1}p_{g_1g_2}^{(c-1)}\prod_{k=2}^{\nu}(p_{g_kg_{k+1}}^{(c)})$. Also a signature packet is appended with μ hashes of previous packets and is assumed to be received. Since $i+\nu c < j_1$, we have $(j_1 - i - \nu c)$ transition states from $P_{i+\nu c}$ to P_{j_1}, and the transition probability is denoted $p_{g_{\nu+1}h_1}^{(j_1-i-\nu c)}$. There are $(j_2 - j_1)$ transition states from P_{j_1} to $P_{j_2}, \cdots, (j_\mu - j_{\mu-1})$ transition states from $P_{j_{\mu-1}}$ to P_{j_μ}, so we have transition probability $\prod_{k=1}^{\mu-1}(p_{h_kh_{k+1}}^{(j_{k+1}-j_k)})$. Since all the whole elements of g or h cannot be 1, the total of the whole transition probabilities gives the desired result. □

When $i + \nu c = j_1$, it means that the same packet $P_{i+\nu c}$ that contains the hash of P_i has its hash appended to the signature packet. As a result the transition states are reduced and the authentication probability of P_i is given in the next Corollary.

[Corollary 1] Based on 2-State Markov model the authentication probability of the ith packet P_i in a block according to MC model is given by the following expression, when $i + \nu c = j_1$:

$$P_r\{P_i\} = \sum_{g,h} \left\{ \left[p_{0g_1} p_{g_1g_2}^{(c-1)} \prod_{k=2}^{\nu} (p_{g_kg_{k+1}}^{(c)}) \right] \left[\prod_{k=1}^{\mu-1} (p_{h_kh_{k+1}}^{(j_{k+1}-j_k)}) \right] \right\} \quad (12)$$

where $g_k \in \{0,1\}$, $k = 1, 2, \cdots, \nu+1$, $g = (g_1, g_2, \cdots, g_{\nu+1})$, $g \neq (1, 1, \cdots, 1)$ and $h_k \in \{0,1\}$, $k = 1, 2, \cdots, \mu$, $h = (h_1, h_2, \cdots, h_\mu)$, $h \neq (1, 1, \cdots, 1)$ □

4. Simulation Results

Several simulation studies have been carried out to analyze the authentication probability $P_r\{P_i\}$ of MC model. We study the authentication probability in terms of the followings:

- ν, the number of packets containing the hash of a packet P_i

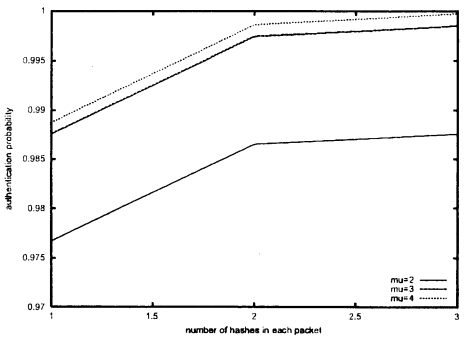

図 7 Authentication probability in terms of ν, when $c = 8$, $k = 5$, $r = 0.1$ and $q = 0.8$.

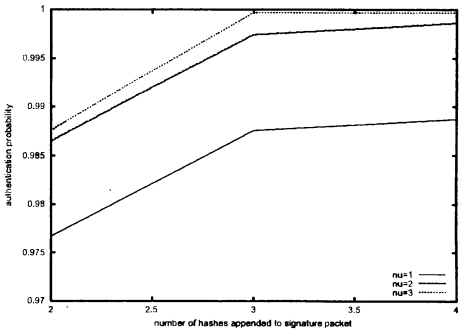

図 8 Authentication probability in terms of μ, when $c = 8$, $k = 5$, $r = 0.1$ and $q = 0.8$.

- μ, the number of hashes appended to a signature packet
- c, the number of chains in MC model
- q, the transition probability from loss to receive
- r, the transition probability from receive to loss.

Figure 7 depicts the authentication probability in terms of ν for different values of μ when $c = 8$, $k = 5$, $r = 0.1$ and $q = 0.8$, where the authentication probability increases when ν increases for all values of μ. Appending the hash of a packet to more other packets increases the authentication probability.

Figure 8 depicts the authentication probability in terms of μ for different values of ν when $c = 8$, $k = 5$, $r = 0.1$ and $q = 0.8$, where the authentication probability increases when μ increases for all values of ν. The more hashes are appended to the signature packet, the higher the authentication probability is achieved.

The authentication probability increases as the transition probability q increases for all values of ν and μ as Figure 9 depicts when $c = 8$, $k = 5$, $r = 0.1$. Also the authentication probability decreases as the transition probability r increases for all values of ν and μ as Figure 10 shows when $c = 8$, $k = 5$, $q = 0.8$. Increasing the transition probability q achieves higher authentication probability since more packets are received. The transition probability r is opposite to q; that is, increasing r achieves lower authentication probability since more packets are lost.

Figure 11 depicts the authentication probability in terms of number of chains c. The greater the value of c, the greater μ can be chosen, this in turn will increase the authentication probability. For each value of c in Figure 11, the maximum

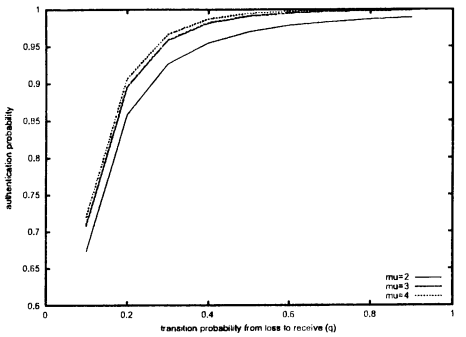

図 9 Authentication probability in terms of q, when $\nu = 2$, $c = 8$, $k = 5$ and $r = 0.1$.

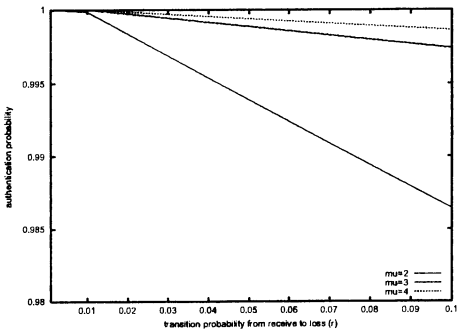

図 10 Authentication probability in terms of r, when $\nu = 2$, $c = 8$, $k = 5$ and $q = 0.8$.

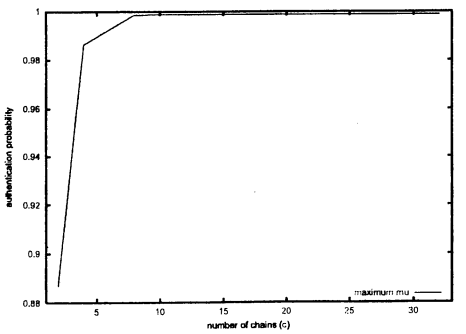

図 11 Authentication probability in terms of c, when $\nu = 2$, $k = 5$ $r = 0.1$ and $q = 0.8$.

value of μ is chosen using equation (1); that is, when $c = 4$, the value of $\mu = 2$ while when $c = 8$, the value of $\mu = 4$ and so on.

5. Conclusion

We introduced a multiple connected chains MC model for signature amortization to authenticate multicast streams. We also presented the authentication probability of MC model using 2-state Markov model and equations to measure the factors that influence the performance of the authentication scheme. The authentication probability is derived as a multiplication of the transition states from any packet to the signature one.

Simulation studies of the authentication probability in terms of several factors such as the number of packets containing the hash of a previous packet, the number of hashes appended to the signature packet, number of chains and the transition probabilities have been carried out. The authentication probability increases as the number of hashes appended to the signature packet increases and also increases as the number of packets that contain the hash of a previous packet increases. Increasing the number of chains makes it possible to append more hashes to the signature packet, that in turn achieve higher authentication probability.

More studies and derivation of the authentication probability using different statistical model is needed. Empirical study to compare the theoretical results to the experimental ones is our next research.

文　献

[1] R. Gennaro, and P. Rohatgi, "How to sign digital streams," *Advances in Cryptology - CRYPTO'97*, pp.180 – 197, 1997.

[2] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," *IEEE Symposium on Security and Privacy*, pp.56 – 73, May 2000.

[3] P. Golle and N. Modadugu. "Authenticating streamed data in the presence of random packet loss," *Proc. of ISOC Network and Distributed System Security Symposium*, pp.13 – 22, 2001.

[4] A. Chan, "A graph-theoretical analysis of multicast authentication," *Proc. of the 23rd Int. Conf. on Distributed Computing Systems*, 2003.

[5] A. Perrig and J. D. Tygar, *Secure Broadcast Communication in Wired and Wireless Networks*, Kluwer Academic Publishers, 2003.

[6] S. Miner and J. Staddon, "Graph-based authentication of digital streams," *Proc. of the IEEE Symposium on Research in Security and Privacy*, pp.232 – 246, May 2001.

[7] J. Park, E. Chong and H. Siegel, "Efficient multicast stream authentication using erasure codes," *ACM Trans. on Information and System Security*, Vol. 6, No. 2, pp.258 – 258, May 2003.

[8] H. Sanneck, G. Carle, and R. Koodli, "A framework model for packet loss metrics based on loss runlengths," *SPIE/ACM SIGMM Multimedia Computing and Networking Conf.*, Jan. 2000.

[9] W. Jiang and H. Schulzrinne, "Modeling of packet loss and delay and their effect on real-time multimedia service quality," *Proc. of 10th Int. Workshop on Network and Operations System Support for Digital Audio and Video*, June 2000.

[10] Q. Abuein and S. Shibusawa, "Efficient loss resistance multicast stream authentication," *Proc. of the Internet Conference* 2004, Tsukuba, Japan, Oct.. 2004.

[11] Q. Abuein and S. Shibusawa, "Efficient multicast authentication scheme using signature amortization," *Proc. of the IASTED Int. Conf. on CIIT*, Nov. 2004.

[12] Q. Abuein and S. Shibusawa, "New chain construction for multicast stream authentication," *Proc. of the ICENCO Int. Conf. on NTIS*, Dec. 2004.

[13] Q. Abuein and S. Shibusawa, "New hash chain for signature amortization scheme," *Proc. of the 67th IPSJ National Conf.*, 2B – 4, Tokyo, Japan, March 2005.

[14] M. Yajnik, J. Kurose, and D. Towsley, "Packet loss correlation in the mbone multicast network," *Proc. of IEEE Global Internet*, 1996.