グループセキュリティ通信の性能評価

豊泉　洋　　高谷　松慶　*

2001年4月5日

概要

インターネット上の各種コミュニティーにおけるグループ内の通信やマルチキャストによる有料番組の提供や企業内の重要な情報の共有サービスなど、オープンなネットワーク上で、セキュリティを確保しながら多数の人が情報を共有する必要性が高まっている。その一つの実現方法としてグループ内で共通の鍵を複数使って暗号通信を行うグループセキュリティ通信という方法が提案されている。ここでは、待ち行列の基本的な考え方を応用することにより、グループセキュリティ通信を行う場合の効率的な鍵の配置方法を導出する。

Keyword グループセキュリティ、公開鍵暗号方式、マルチキャスト、待ち行列、性能評価

1　はじめに

暗号通信の基本は、二人の人間が盗み見られることなく情報をやりとりするということである。現在、もっとも日常で使われている暗号通信のひとつとして、公開鍵暗号方式 [1] があげられるであろう。Netscape や IntenetExplorer などにも SSL(Security Socket Layer) として実装され、使われている [7]。

公開鍵暗号方式では、各ユーザーが自分で生成する公開鍵と秘密鍵を持つ。公開鍵は文字通り公開される。情報の送信者は受信者の公開鍵を使って、情報を暗号化し送信する。暗号化された情報を受信した受信者は、自分だけが知っている秘密鍵を使って、情報を復号する。公開鍵や暗号化された情報からは、秘密鍵は計算することが難しいので、公開鍵のみを使って暗号化された情報の中身を復元することはできない。このような送信者・受信者が一人ずつの形の暗号通信を one-to-one の暗号通信と呼ぼう。

インターネットの爆発的な進展により、我々はネットワーク上で誰とでも通信ができる自由を得た。ネットワーク上では、特定の目的や興味を持つ個人が集まってコミュニティーを作って、通信をすることが日常となっている。このような場合には、特定のグループ内の通信においても暗号化が必要となる。商業的にも人気番組のインターネット上での有料配信や、企業内の秘密情報のネットワーク上での共有などもグループによる暗号通信が必要となる。このようなグループ内での暗号通信をグループセキュリティ通信と呼ぼう。

グループセキュリティ通信は、送信者と受信者を特定すれば one-to-one の暗号通信で実現できる。したがって、公開鍵暗号方式だけでも解決可能である。しかし、そこには重大な性能上の問題が秘められている。スポーツリアルタイム社という架空のコンテンツ提供企業を考えよう。スポーツリアルタイム社は1万人の顧客に向かってスポーツ番組を有料でインターネット生中継しようと計画している。当然、スポーツリアルタイム社は不正な手段で放送を傍受させないために、有料で登録した1万人へ暗号化されたデータを送信する。1

* 会津大学　性能評価研究室, 〒965-8580　会津若松市一箕町鶴賀　E-mail: toyo@u-aizu.ac.jp.

万人に one-to-one 暗号通信をするためには、一つのデータパケットを 1 万回（！）も各ユーザー別の公開鍵で暗号化する必要がある。これをリアルタイムで行うことは、事実上不可能である。

スポーツリアルタイム社のエンジニアはこう考えるかもしれない。「グループで情報を共有するんだから、グループ全体が一つの暗号鍵を共有すればいいんだ。そうすれば、ひとつのパケットは一回だけ暗号化すれば良い。グループで共有する暗号鍵はあらかじめ公開鍵を使って各顧客に送っておけば完璧だ。」しかし、この方法にも性能上の大きな問題がある。スポーツ番組の生中継は、途中から見たいと言ってくる人やつまらないから見るのを止めるという人達が必ずいるのである。ちょっと気が利く人なら、最初に鍵を受け取ってから、途中から見るのを止めると言って、最初に手に入れた鍵を使って無料でスポーツ番組をみることが可能なのである。セキュリティーを確保するには、グループからの脱退があった場合には必ず共通鍵の更新が必要である。グループに参加の場合にも、その参加者が過去の秘密情報へのアクセスするのを禁止する意味で、共通鍵の更新が必要である。したがって、単純な鍵の共有では、一人の顧客が脱退すると 1 万人の顧客へ公開鍵暗号を使って共通鍵を暗号化し配信する必要がある。生中継を途切れさせないためには、参加・脱退ごとに 1 万回の暗号化をリアルタイムに行い配信する必要がある。これも事実上不可能である。

それでは、グループセキュリティ通信は不可能なのか？スポーツリアルタイム社はインターネットビジネスから撤退するべきなのか？

2 グループセキュリティ通信の方式

いくつかの実現可能なグループセキュリティ通信の方式が提案されている。これらの方式を使うことによって、スポーツリアルタイム社は、インターネットビジネスが可能になるかもしれない。

Wong [6] や RFC2627 [4] は、グループ内にサブグループの階層を作り、複数の共通鍵を使ことによって、顧客が脱退や参加した場合の共通鍵の暗号化回数を削減できるということを示した。彼らの提案する方法を再びスポーツリアルタイム社の例で説明しよう。

スポーツリアルタイム社の顧客が最初は $U_1, ..., U_{15}$ の 15 人だと仮定しよう（最初から 1 万人の顧客を集めるのは不可能？！）。

各顧客はあらかじめ、顧客ごとの秘密鍵 (S_i) と公開鍵 (O_i) を持つ。スポーツリアルタイム社には鍵サーバーがあり、初期時点で今回の生中継用の 15 人のグループ共通の鍵 $G(0)$（以下では、グループ鍵と呼ぶ）を生成する。鍵サーバーは、生中継開始前に、それぞれの公開鍵 O_i を用いてグループ鍵 $G(0)$ を暗号化する。このように、鍵 O_1 で $G(0)$ を暗号化することを $(G(0))_{O_i}$ と書く。暗号化されたグループ鍵 $(G(0))_{O_i}$ は $U_1, ..., U_{15}$ にインターネットのようなオープンなネットワークを通じて配信される。U_i は、自分の秘密鍵 S_i を用いて、$(G(0))_{O_i}$ を復号し、生中継開始前には、自分の秘密鍵とグループ鍵の組 $(S_i, G(0))$ を保持していることになる。

スポーツリアルタイム社の通信サーバーはグループ鍵によってデータを暗号化 $(Data)_{G(0)}$ する。各ユーザーに配信されたデータ $(Data)_{G(0)}$ は、ユーザーが持っているグループ鍵 $G(0)$ によって復号化する。これによってスポーツリアルタイム社の生中継が実現される。

さて、以下では、U_{15} というグループから脱退し、その後 U_{16} というユーザーがグループに新規に参加したというシナリオで、サブグループという概念がいかにユーザーの参加・脱退における鍵の暗号化回数を削減するかを見る。まずはじめにサブグループが無い場合を評価し、その後で、サブグループがある場合を考えよう。

2.1 サブグループ無しのグループセキュリティ通信

はじめに、U_{15} がグループを脱退したとする。$G(0)$ を知っているので、U_{15} を除いた新しいグループ $\{U_1,...,U_{14}\}$ のセキュリティを保つため、鍵サーバーは古いグループ鍵 $G(0)$ の変わりに新しいグループ鍵 $G(1)$ を生成する。$G(1)$ は、各ユーザーの公開鍵を用いて暗号化される。ただし、脱退した U_{15} には新しいグループ鍵は配送しないので、

$$\{(G(1))_{O_i}\}_{i=1,...,14}.$$

の暗号化必要である。したがって、U_{15} が脱退したために必要な暗号化回数 A_{15} は

$$A_{15} = 14 \tag{1}$$

となる。

さらに、別のユーザー U_{16} が新規にこのグループ $\{U_1,...,U_{14}\}$ に参加し、生中継を受信したいと申し込んできたとしよう。鍵サーバーは、古いグループ鍵 $G(1)$ の変わりに新しいグループ鍵 $G(2)$ を生成する。今度は、新しいグループ鍵 $G(2)$ の $U_1,...,U_14$ への配送に、古いグループ鍵 $G(1)$ を活用することができる。したがって、U_{16} への暗号化とあわせて、

$$\{(G(2))_{G(1)}, (G(2))_{O_{16}}\}$$

の暗号化が必要である。よって、U_{16} が参加したための暗号化回数 B_{16} は

$$B_{16} = 2 \tag{2}$$

となる。

2.2 サブグループ有りのグループセキュリティ通信

次に 15 人のグループを $SG_1 = \{U_1,...,U_5\}$、$SG_2 = \{U_6,...,U_{10}\}$、$SG_3 = \{U_{11},...,U_{15}\}$ の 3 つのサブグループに分けた場合を考える。生中継開始前の時点で、各ユーザーにはグループ鍵 $G(0)$ と個人の秘密鍵 S_i に加えて、自分の属するサブグループで共有するサブグループ鍵 $SG_j(0)$ が与えられる。例えば、U_6 は SG_2 に所属しているので、鍵の組として $(G(0), SG_2(0), S_6)$ を持つ。ただし、他のサブグループの鍵である $SG_1(0)$ や $SG_3(0)$ の情報は U_5 には与えられない。

ここで、U_{15} が脱退する場合を考える。この場合にも、新しいグループのセキュリティを保つために、鍵サーバーは古いグループ鍵 $G(0)$ の変わりに新しいグループ鍵 $G(1)$ を生成する。ここで、U_{15} は $G(0)$ だけではなく $SG_3(0)$ の情報も知っていることに注意しよう。さて、U_{15} は $SG_3(0)$ 以外のサブグループの鍵を知らないので、SG_1 と SG_2 のサブグループについては、それぞれ $SG_1(0)$ と $SG_2(0)$ のサブグループ鍵を使って新しいグループ鍵 $G(1)$ を配信することができる。したがって、これら 2 つのサブグループに対しては、

$$\{(G(1))_{SG_1(0)}, (G(1))_{SG_2(0)}\} \tag{3}$$

の 2 回の暗号化で済む。次は SG_3 について考える。U_{15} は $SG_3(0)$ を知っているので、$SG_3(0)$ を鍵の配送に使うことはできない。まず、新しいサブグループ鍵 $SG_3(1)$ を作成し、SG_3 の各ユーザーに個人の秘密鍵を使って配送する。したがって、

$$\{(SG_3(1))_{S_i}\}_{i=11,...,14} \tag{4}$$

方式	$A_{15}(U_{15}$ 脱退)	B_{16} (U_{16} 参加)	合計
サブグループ無し	14	2	16
サブグループ有り	7	4	11

表 1: ユーザが脱退・参加した場合のグループ全体の暗号化の回数

の 4 回の暗号化が必要になる。この新しいサブグループ鍵を使い、

$$(G(1))_{SG_3(1)} \tag{5}$$

という暗号化をすると $G(1)$ が新しいサブグループのユーザーに配送できる。したがって、U_{15} が脱退するときに必要な暗号化の回数は、(3)、(4)、(5) より

$$A_{15} = 7 \tag{6}$$

である。これは前のセクションで得られたサブグループ無しの場合 (1) の 14 回に比べて削減されているのに注意しよう。

次に U_{16} がこの 14 人のグループに新規に加わる場合も考えてみよう。また、この新しいユーザー U_{16} は SG_3 に加わるものとする。前セクションと同様に古いグループ鍵 $G(2)$ を活用することができるので、

$$\{(G(2))_{G(1)}, (G(2))_{O_{16}}\} \tag{7}$$

の 2 回の暗号化で新しい鍵 $G(2)$ が全員に対して配送できる。ただし、SG_3 のメンバーに対しては、新しいサブグループ鍵 $SG_3(2)$ の配送も必要であり、

$$\{(SG_3(2))_{SG_3(1)}, (SG_3(2))_{S_{16}}\} \tag{8}$$

の 2 回の暗号化が追加で必要となる。

したがって、ユーザー U_{16} が脱退する場合には、各ユーザーへ新しい鍵を配送するのに必要なのは、(7) と (8) より、

$$B_{16} = 4 \tag{9}$$

となる。これは前のセクションで得られたサブグループ無しの場合 (2) の 2 回に比べると増えているのに注意しよう。

2.3 サブグループと暗号化回数

以上の結果をまとめると表 1 のようになる。サブグループを導入することで、全体で暗号化の回数は減っているように見える。しかし、詳細に見ると、脱退した場合の暗号化の回数は減っているが、参加した場合の暗号化の回数は逆に増えてしまっている。したがって、どのくらいの数の参加・脱退が起こるのかの見積もりや、サブグループの数をどのようにしたときに暗号化の回数を最小にすることができるのかという問題がある。この疑問に答えるためには、待ち行列モデルの力を借りる必要がある。その力を借りることで、スポーツリアルタイム社のエンジニアは生中継の際に、安心して鍵サーバーの前に座っていることができるようになるだろう。

3 グループセキュリティ通信の待ち行列モデル

前節までで見てきたグループセキュリティ通信を待ち行列モデルとして扱うためにモデル化を行う。前のセクションで見たような形のグループセキュリティ通信のサブグループ化においては、実際に送信する通信データの暗号化は時刻 t での最新のグループ鍵 $G(t)$ のみで行い、サブグループ鍵では行わないことに注意しよう。実際には、特定の目的や属性（例えば、会社の部署）に基づいてサブグループを作り、データの暗号化もサブグループ鍵で行うことも可能であるが、以下ではこれを考えない。この仮定により、ユーザーがどのサブグループに属するということは、データの暗号通信には無関係になる。

セキュリティーグループに参加する n 番目のユーザーを U_n、U_n のグループへの参加時点を T_n、U_n がグループ内に滞在する時間を S_n とする。ユーザーがグループへ参加する時点の列 $\{T_n\}$ は到着率 λ の Poisson 過程に従うと仮定する。各ユーザーがグループ内にとどまる時間 S_n は、ユーザーごとに独立で同一な分布 $F(x) = P\{S_n \leq x\}$ に従うと仮定し、その平均値は $1/\mu = E[S_n]$ とする。また、グループ内の許容できるユーザー数に上限は無いとする。

セキュリティグループを $(SG_i)_{i=1,\ldots,N}$ の N のサブグループに分ける。以下では、セキュリティグループの数は一定であると仮定する。新しいユーザーが参加した場合には、参加するサブグループをセキュリティグループ内の全ての情報と独立に等しい確率で選択する（ベルヌーイ試行）と仮定する。すなわち、新しく参加したユーザー U_n が参加するサブグループのインデックスを I_n とすると、

$$P\{I_n = i\} = P\{U_n \in SG_i\} = \frac{1}{N} \tag{10}$$

である。

Poisson 過程をこのようにベルヌーイ試行で分離すると、各サブグループへの参加するユーザーの到着はそれぞれ独立な Poisson 過程となることが知られている ([3] P.69 を参照)。時刻 t における各サブグループ内のユーザーの数を $L_i(t)$、グループ全体のユーザーの数を $L(t)$ とする。すると、$L_i(t)$ は、到着率が λ/N、サービス時間分布が $F(x)$ に従う $M/G/\infty$ (Poisson 到着、一般サービス時間分布、無限大のサーバーを持つ待ち行列モデル) の系内客数過程となることがわかる (例えば、[2] 参照)。ここでは、待ち行列システムはセキュリティグループ全体であり、ユーザーはセキュリティグループへ参加すると同時にサービスが受けられることになる。

$M/G/\infty$ では、システムが定常状態であると仮定すると任意時点 t での系内客数 $L_i(t)$ は、以下のように平均 $\lambda/(\mu N)$ の Poisson 分布であらわされる。

$$P\{L_i(t) = n\} = \frac{1}{n}\left(\frac{\lambda}{\mu N}\right)^n e^{-\lambda/(\mu N)} \tag{11}$$

さらに、各サブグループへ参加するユーザーの到着過程が独立なので、$\{L_i(t)\}_{i=1,\ldots,N}$ は独立で、同一な Poisson 分布を持つことがわかる。

Poisson 分布の性質より、各サブグループに参加している人数の平均値は

$$E[L_i(t)] = \frac{\lambda}{N\mu} \tag{12}$$

となり、全ユーザーの数の期待値は、

$$E[L(t)] = \sum_{i=1}^{N} E[L_i(t)] = \frac{\lambda}{\mu} \tag{13}$$

であらわされる。また、時刻 t でのグループ鍵を $G(t)$、サブグループ鍵を $(SG_1(t),...,SG_N(t))$ とする。以下では、$G(t)$ や $SG_i(t)$ は右連続な関数とする。$G(t)$ は、各ユーザの到着時点 $\{T_n\}$ および退去時点 $\{D_n = T_n + S_n\}$ でジャンプを持つ。また、$SG_i(t)$ も同様にそのサブグループへの到着・退去が起こった時点にジャンプを持つ。

4 待ち行列モデルを使った暗号化回数の評価

前節で作ったモデルを使って、暗号化の回数を評価する。

4.1 ユーザーの参加

まず、新しいユーザー U_n がセキュリティグループに参加した場合を考えよう。U_n は SG_{J_n} に参加しているので、U_n の参加時点 T_n で再発行の必要な鍵は、グループ鍵 $G(T_n-)$ と $SG_{J_n}(T_n-)$ の二つである。これらの鍵の再発行は、U_n がグループ鍵 $G(T_n-)$ と $SG_{J_n}(T_n-)$ の二つを知らないということを前提に、以下の手順によって行われる。

1. 鍵サーバーが新しいグループ鍵 $G(T_n)$ と新しいサブグループ鍵 $SG_{J_n}(T_n)$ を生成する。
2. 鍵サーバーが古いグループ鍵を使って、新しいグループ鍵を
$$(G(T_n))_{G(T_n-)}$$
のように暗号化し、U_n の参加直前にすでに参加していた $L(T_n-)$ 人の ユー ザーに配送する。
3. 鍵サーバーが古いサブグループ鍵を使って、新しいサブグループ鍵を
$$(SG_{J_n}(T_n))_{SG_{J_n}(T_n-)}$$
のように暗号化し、U_n の参加直前にすでに参加していた $L_{J_n}(T_n-)$ 人 のユーザーに配送する。
4. 最後に、鍵サーバーは、ユーザー U_n の公開鍵を使って、
$$\{(G(T_n))_{O_n},(SG_{J_n}(T_n))_{O_n}\}$$
のように暗号化を行い、これを U_n に配送する。

したがって、U_n が参加したことで必要となる暗号化の回数を B_n とすると、

$$B_n = 4 \tag{14}$$

であり、これはサブグループの数や参加人数によらず一定である。一般にサブグループの中にさらにサブグループを作って、階層構造を作っていくと、M 階層の場合には、

$$B_n = 2M \tag{15}$$

となることがわかる。

4.2 ユーザーの脱退

次にユーザー U_n が脱退したときを考えよう。U_n は SG_{J_n} に参加しているので、U_n の脱退時点 D_n で再発行の必要な鍵は、グループ鍵 $G(D_n-)$ と $SG_{J_n}(D_n-)$ の二つである。ただし、参加の時と違い、U_n は $G(T_n-)$ と $SG_{J_n}(T_n-)$ の二つを知っているということに注意すると、以下の手順で、鍵の再発行ができる。

1. 鍵サーバーが新しいグループ鍵 $G(T_n)$ と新しいサブグループ鍵 $SG_{J_n}(T_n)$ を生成する。
2. 鍵サーバーが新しいサブグループ鍵を U_n の退去直後時点で SG_{J_n} に参加しているユーザーの公開鍵を使って

$$\{(SG_{J_n}(D_n))_{O_k}\}_{k=1,\ldots,L_{J_n}(D_n+)}$$

のように暗号化し、$L_{J_n}(D_n+)$ 人の のユーザーに配送する。ここで、 k は D_n+ 時点で、SG_{J_n} に参加しているユーザーへの番号付けとす る。

3. 鍵サーバーが新しいグループ鍵 $G(T_n)$ を D_n 時点での各サブグルー プ鍵（SG_{J_n} については、上の手順で更新されている鍵）を使って、

$$\{(G(D_n))_{SG_i(D_n)}\}_{i=1,\ldots,N}$$

のように暗号化し、全ユーザーに配信する。

したがって、U_n が脱退したことで必要となる暗号化の回数を A_n とすると、

$$A_n = L_{J_n}(D_n+) + N \tag{16}$$

であることがわかる。一般にサブグループの中にさらにサブグループを作り、階層構造を作っていくと、階層数が M、各階層でのサブグループの数を N_m とした場合には、

$$A_n = L_{J_n}(D_n-) + \sum_{m=1}^{M} N_m \tag{17}$$

となることがわかる。

4.3 最適なサブグループ数

暗号化の回数は、(14) と (16) よりサブグループの数とサブグループに参加している人数の数によって決まることがわかった。とくに (14) より、参加時点での暗号化の回数は一定であるので、退去時点の暗号化回数のみについて考えれば十分である。以下では、最適化問題として、退去時点の暗号化回数 A_n の期待値を最小にするサブグループ数 $N^{\min}$ を求めるという問題を考える。A_n は、鍵サーバーにとっては、処理リクエストのバーストになる重要な指標であることに注意しよう。(16) より、A_n の期待値は

$$E[A_n] = N + E[L_{J_n}(D_n+)] \tag{18}$$

となる。ここで、到着・退去時点に ± 1 ステップの遷移だけを許すような系内客数プロセスについては、到着時点に見る系内客数と退去時点に後に残す系内客数の分布は等しいことが知られている（[2] の P176 参照）。よって、

$$P[L_{J_n}(D_n+) = k] = P[L_{J_n}(T_n-) = k] \tag{19}$$

さらに、Poisson Arrival See Time Average(PASTA)([5] p.294) により Poisson 到着しているユーザーが見る系内客数分布は、任意の時点での系内客数分布に等しい。すなわち

$$P[L(t) = k] = P[L_{J_n}(T_n-) = k] \tag{20}$$

である。したがって、(11) より $P[L_{J_n}(D_n+) = k]$ も Poisson 分布であり、その期待値は $E[L_{J_n}(D_n+)] = \lambda/(N\mu)$ である。したがって、

$$E[A_n] = N + \frac{\lambda}{N\mu} \tag{21}$$

となる。簡単な計算により、$E[A_n]$ は $N=(\lambda/\mu)^{1/2}$ で最小になることがわかる。よって、

$$N^{min}=\left(\frac{\lambda}{\mu}\right)^{1/2} \quad =(E[L(t)])^{1/2} \tag{22}$$

が最適なサブグループ数である。すなわち、セキュリティグループに参加する人数の期待値の平方根が最適なサブグループ数である。

さらに暗号化回数の分布も (16) と $P[L_{J_n}(D_n+)=k]$ も Poisson 分布であることから求めることができて、

$$P[A_n^{min}=k]=\frac{1}{k-(\lambda/\mu)^{1/2}}\left(\frac{\lambda}{\mu}\right)^{\{k-(\lambda/\mu)^{1/2}\}/2} e^{-(\lambda/\mu)^{1/2}} \tag{23}$$

となる。また、暗号回数の期待値は、

$$E[A_n^{min}]=2(E[L(t)])^{1/2} \tag{24}$$

となる。

単位時間内に起こる平均の暗号化回数 C は、

$$C=\lambda(E[A_n]+E[B_n])=\lambda(E[A_n]+4) \tag{25}$$

で与えられる。したがって、最適なサブグループ数の場合の単位時間内の平均の暗号化回数 C^{min} は

$$\begin{aligned} C^{min} &= \lambda(E[A_n^{min}]+4) \\ &= \lambda(2E[L(t)]^{1/2}+4) \end{aligned} \tag{26}$$

で与えられる。

また、一般に階層数が M の場合には、各階層ごとのサブグループの数の最適値を N_i^{min} とすると、

$$N_1^{min}=\ldots=N_M^{min}=\left(\frac{\lambda}{\mu}\right)^{1/M}=(E[L(t)])^{1/M} \tag{27}$$

となることも容易に証明できる。

5 数値例：スポーツリアルタイム社のマルチキャスト

ユーザーの数の期待値が 10,000 人を想定しているスポーツリアルタイム社を再び考えよう。各ユーザーがセキュリティグループ内に滞在する時間の期待値を 30 分とする。すなわち $\mu=1/30$、$\lambda=\mu E[L]=1000/3$ である。(22) より、最適なサブグループ数は

$$N^{min}=10000^{1/2}=100 \tag{28}$$

であることがわかる。鍵サーバーへの処理負荷のバーストに相当する退去時点の暗号化回数の期待値は、

$$E[A_n^{min}]=200 \tag{29}$$

であり、単位時間（1 分間）当たりの平均暗号化回数 C^{min} は、(26) より

$$\begin{aligned} C^{min} &= \frac{1000}{3}(2\cdot 100+4) \\ &= 68000 \end{aligned} \tag{30}$$

となる。比較のため、この結果とサブグループ数を変えた場合の結果を表 2 にまとめる。

10,000 人のような大規模なマルチキャストをセキュリティに注意を払って行う場合には、サブグループの数の最適値が重要な意味を持つことがわかる。スポーツリアルタイム社のエンジニアは、サブグループを 100 作って運用することにより、有料スポーツ番組の生中継が可能になるであろう。

サブグループ数	$E[A_n]$ (退去時点での暗号化回数)	C(平均暗号化回数/min)
サブグループ無し	10000	3334×10^3
10	1010	338×10^3
100	200	68×10^3
1000	1010	338×10^3

表 2: ユーザが脱退した場合の暗号化の回数

6 まとめ

暗号化されたマルチキャストサービスにサブグループとサブグループ鍵というコンセプトを導入することにより、セキュリティグループ通信が可能になり、さらに、想定されるグループに参加するユーザー数の平方根程度の数のサブグループを作ることが、暗号化回数を最小化する意味で、最適であることを示した。

今後は、さらに参加人数の時間的な変化に合わせたダイナミックなサブグルーピングやネットワーク構造なども考慮したグルーピングを考え、さらに効率的なセキュリティグループ通信を実現する方法を検討する必要があるであろう。

参考文献

[1] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. on Inform. Theory*, Vol. 22, No. 6, pp. 644–654, 1976.

[2] L. Kleinrock. *Queueing Systems Vol. 1.* John Wiley and Sons, 1975.

[3] S. M. Ross. *Stochastic Processes.* John Wiley and Sons, 1996.

[4] D. Wallner, E. Harder, and R. Agee. Key management for multicast: Issues and architectures. *Request for Comments: 2627*, 1999.

[5] R.W. Wolff. *Stochastic modeling and the theory of queues.* Princeton-Hall, 1989.

[6] C.K. Wong, M. Gouda, and S.S. Lam. Secure group communications using key graphs. *IEEE/ACM Trans. on Networking*, Vol. 8, No. 1, pp. 16–30, 2000.

[7] 岡本栄司. 総論-社会を変革する暗号技術. オペレーションズ・リサーチ, Vol. 45, No. 10, pp. 497–591, 2000.