2003年日本オペレーションズ・リサーチ学会
春季研究発表会

グループセキュリティサービスにおける暗号鍵管理サーバの性能評価

会津大学 ＊高谷 松慶 TAKAYA Matsuyoshi
01307082 会津大学 豊泉 洋 TOYOIZUMI Hiroshi

1 はじめに

暗号鍵を配送する為に複数の暗号鍵を使うグループセキュリティ通信において暗号鍵管理サーバの性能評価を行う。「グループセキュリティ」とはグループに所属する正規のユーザが共有する情報を機密性、完全性を保ちながら通信を行うサービスモデルである。

グループセキュリティ通信を実現する方法としてグループに所属するユーザが暗号鍵を共有し、情報を暗号化し、複号化を行う方法がある。しかし共有する暗号鍵はグループに参加、脱退が起きた場合にグループセキュリティを維持する為に更新をする必要がある。暗号鍵を配送するとき、複数の暗号鍵を使うことにより、グループのユーザが新しい暗号鍵を手に入れるまでに掛かる時間を短縮する方法が提案されている [1][2]。[4] はこのセキュリティモデルを M/G/∞ 待ち行列に当てはめグループセキュリティを維持する為に必要な暗号化の回数を最小化することができることを示した。本論文では暗号鍵管理サーバに M/G/1 待ち行列を当てはめ、新しい暗号鍵を手に入れるまでの時間を算出し暗号鍵の数の最適値を求める。

2 グループセキュリティモデル

暗号鍵の配置を n 階層としたグループセキュリティサービスを考える（図 1 を参照)。各階層の暗号鍵は対称鍵で鍵の長さは全て同じとし、第 1 階層はグループ鍵で第 2 階層から第 n 階層まではサブグループ鍵とする。各階層に所属するサブグループの数を d とする。必ず第 n 階層のサブグループでユーザの参加、脱退が起こる。参加、脱退が起こる第 n 階層の i 番目のサブグループに所属するユーザの数を $N_n(i)$ とする ($1 \leq i \leq d^{n-1}$)。([1][2] 参照) 以下では暗号処理の待ち時間を最小にする d を求める。

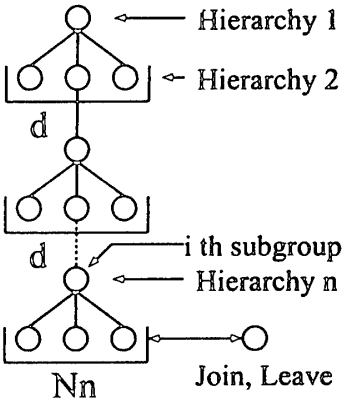

図 1: グループへの参加、脱退

3 サーバの仕事

サーバの行う仕事には 3 つのステップが存在する。参加、脱退を受けられるかどうかの審査、新しい暗号鍵の作成、その配送の為の暗号化である。

3.1 審査

最初に参加、脱退の要求を受け入れるかを審査する。ここでは一定の時間で審査し、全ての要求を受け入れるものとする。その時間を Ju とする。

3.2 暗号鍵の作成

次に対称鍵の作成である。一つの暗号鍵の作成に掛かる時間を M とする。参加の場合はグループ鍵、サブグループ鍵、サーバとユーザ間の対称鍵（個人鍵）を作成する。よって作成する対称鍵の数は $n+1$ となり、暗号鍵を作成するのに掛かる時間は (n + 1)M となる。また脱退の場合は個人鍵は必要ないので作成する暗号鍵の数は n となり、暗号鍵を作成するのに掛かる時間は n· M となる。

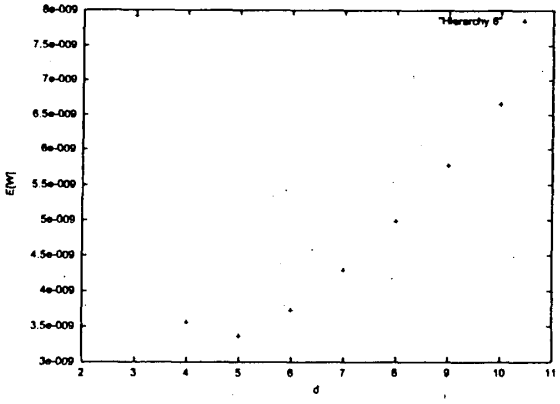

図 2: d と平均待ち時間

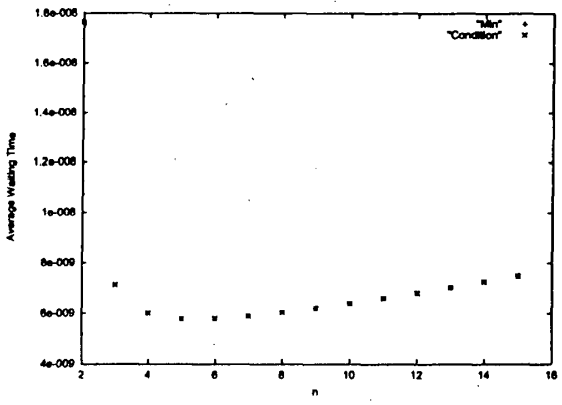

図 3: Min → 平均待ち時間を最小にする d Condition → $d = (\frac{\lambda}{\mu})^{\frac{1}{n}}$

3.3 暗号化

一つの対称鍵を対称鍵で暗号化を行うのに掛かる時間を c、一つの対称鍵を非対称鍵で暗号化を行うのに掛かる時間を p とする。

グループに参加するユーザには個人鍵をユーザの非対称鍵で暗号化し、個人鍵で各階層の対称鍵を暗号化を行う。また新しい各階層の対称鍵を各階層の古い対称鍵で暗号化を行う。よって参加においての暗号化に掛かる時間は $2n \cdot c + p$ となる。

脱退の場合は、脱退するユーザが持つ暗号鍵で暗号化しないように注意しなくてはならない。各階層の新しい暗号鍵をその下の階層の暗号鍵で暗号化する。暗号化に掛かる時間は $c(d(n-1)+N_n(i))$ となる。

4 M/G/1

参加、脱退のリクエストの到着間隔がポアソン過程に従い、サービス時間 S は

$$S = \begin{cases} ju + (n+1) \cdot M + 2n \cdot c + p & \text{参加のとき} \\ ju + n \cdot M + c(d(n-1) + N_n(i)) & \text{脱退のとき} \end{cases} \quad (1)$$

に従うとして M/G/1 待ち行列でモデル化する。$N_n(i)$ はポアソン分布に従い、第 n 階層の各サブグループに所属するユーザの平均人数は

$$E[N_n(i)] = \frac{\lambda}{\mu \cdot d^{n-1}} \quad (2)$$

となることがわかっている [4]。これらを利用し、Pollaczek-Khinchin の式 [3] から暗号鍵管理サーバでの処理の平均待ち時間を求める。

5 数値例

各ユーザがグループに滞在する平均時間を 60 分 (E[T] = 60 分)、グループ内の平均のユーザの人数を 10,000 人 (λE[T] = 10,000)、階層を 6、Ju = 10^{-5} 分、M = 10^{-7} 分、c = 10^{-7} 分、p = 10^{-6} 分とする。結果を図 2 に示す。d = 5 が待ち時間を最小にすることがわかる。図 3 は上記の条件を元に階層数 n を変化させ、平均待ち時間を最小にする d と近似値 $d = (\frac{\lambda}{\mu})^{\frac{1}{n}}$ との比較を表す。

6 まとめ

平均待ち時間を最小にする d を求めることができた。$d = (\frac{\lambda}{\mu})^{\frac{1}{n}}$ を目安に平均待ち時間を最小にする d を近似することができる。また平均待ち時間を最小にする階層数 n を求めることができることを示した。

参考文献

[1] C.K. Womg, M. Gouda, and S.S. lam. Secure group communications using key graphs. IEEE/ACM Trans. on Networking, Vol. 8, No.1m pp.16-30, 2000.

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

[3] L.Kleinrock. Queueing Systems Vol. 1. John Wiley and Sons, 1975 pp. 190

[4] 豊泉 洋, 高谷 松慶. グループセキュリティ通信の性能評価, 日本 OR 学会第 45 回シンポジウム, 2001