グループ指向型鍵管理方式の遠隔会議システムへの応用

5T−5　関　一則　高木　和幸　武藤　康史　紙田　剛　岡田　謙一　松下　温
慶応義塾大学

1　はじめに

近年、ネットワークの発達にともない、グループ間での通信が活発となってきたが、その一方、情報を不当に得ようとするハッカーが急増している。このようなハッカーから情報を守るため暗号化の技術は不可欠であり、この分野の研究も活発である。しかしながら、現在の段階では、グループ通信に適した暗号化、及びその際に必要な鍵の管理方法も確立されていないため、我々は、グループ指向のMCK(modified copy key)という独自の鍵管理方式を提案してきた。

今回、我々はこのMCK鍵管理方式を適用して、グループ通信の具体的な応用例である遠隔会議システムの初期モデルを、UNIXにおいて実装することに成功した。そこで、本稿ではこのシステムの概要その評価をを述べる。

2　グループウェア[1]

2．1　グループウェアの現状

近年複数の利用者間で情報を共有、交換し、互いに協力しながら、各種の問題解決や業務遂行を図る、グループウェアの実現への要求が高まっている。グループウェアの対象となる協同作業のアプリケーションとしては、全ての共通基盤となる会議システムと、グループ意志決定(GDSS)、共通文書作成、ソフトウェア分散共同開発、遠隔教育など、その上位に位置ずけられる個別アプリケーションとに分類できる。

このように、全ての基盤となる遠隔会議システムの実現は、地理的制約を解消し、オフィス業務の効率化を実現するという意味で、非常に有益である。

2．2　会議システムの必要条件

会議システムは、特定のグループ間での情報交換をベースとしたオフィス機能の1つと考えられ、必要な条件としてつぎのものが考えられる。

（1）会議の多様性

会議システムの対象となる会議の形態そのものは、目的、メンバー、期間、ロケーション及び使用するOA機器などによって様々であり、多様化している。そのため、目的別にシステム内のウィンドウを分けるなど、会議の多様性への配慮が必要となる。

（2）　セキュリティ機能

会議が正常に運営されるためには、議事内容の不正な改ざんや、部外者の会議への不当な参加を防止しなけらばならない。

このために、会議に参加する権利を持つ当事者であるかどうかの認証を行うことや、当事者にしか復号化できないような鍵で、議事内容を暗号化する必要がある。

（3）　高速性

会議の円滑な進行を実現するためには、頻繁に行われる意見交換や、議決を取る場合などの動作を迅速に行う必要があり、リアルタイムに近い通信が要求される。

（4）　操作性

会議システムでは、通常の会議で参加者が、目や耳や口、手で行っている動作を端末を通して行うことになる。そのため、マウスを多用することや、そのほかの新たなマンマシンインターフェイスの導入が必要となる。

（5）　公平性

発言内容が、完成された知識に含まれる場合などには、著作権にあたるものが、発言者の権利保護という意味で重要な問題となる。

3　MCK鍵管理方式[2]

この方式では、以下のようにして、ピースPを鍵を生成するための情報、関数fは一方向関数として、ある鍵Kから新しい鍵K'を生成する。

$$K'=f(f(\cdots f(f(K,P1),P2),\cdots,Pn-1),Pn)$$

ここで、n個のpによって新たに生成できる鍵の数は、

$$\sum_{r=1}^{n} {}_nC_r = 2^n - 1$$

となり、1人のユーザは1個の鍵とn個のPを管理することにより、2^n個の鍵を管理することになる。よって、n個のPと1つの鍵を管理することにより、n人のユーザとあらゆる組み合わせで、暗号化を用いた通信が可能になる。

具体的にユーザが5人の場合を考えれば、図1のように、まずユーザUiはPiを持たないようにする。例えば、U1とU4が通信する場合には、共通鍵K0とP2,P3,P5により、先の方法に従って鍵を生成する。

$$K=f(f(f(K0,P2),P3),P5)$$

ここで、U2はP2,U3はP3,U4はP4を持っていないので、彼らに同じ鍵は生成できない。同様にU1,U2,U5でグループ通信を行いたい場合には、U3の持っていないP3と、U4の持っていないP4,さらにK0で鍵を生成し、通信すればよい。なお、全員に同報を

Application of The Key Management Method to A Remote Conference System
Kazunori Seki, Kazuyuki Takagi, Yasushi Mutoh, Takeshi Kamita,
Kenichi Okada, Yutaka Matsushita
Keio University

行う場合には、K0をそのまま用いる。

	P1	P2	P3	P4	P5	K0
U1	×	○	○	○	○	○
U2	○	×	○	○	○	○
U3	○	○	×	○	○	○
U4	○	○	○	×	○	○
U5	○	○	○	○	×	○

図1．各ユーザが持つピース

4　MCK方式に基づく会議システムの実装

4．1　環境

我々は、グループ通信に適したMCK方式に基づくセキュリティ機能付き遠隔会議システムをUNIX上で実現した。開発言語はC言語で、ツールとしてはX-Window上でX-Viewを使用した。通信を行うプロトコルはRPCに基づいたもので、通信は全て同報により行っている。

4．2　暗号方式

暗号アルゴリズムとしては、会議に必要な高速性を考慮し、DES(Data Encryption Standard)[3]を使用した。

4．3　実行形態

システムは、MCK方式に基づく鍵の生成から、その暗号化、ウィンドウ管理までを司るメインプロセスと、通信を管理する子プロセスから成る。ピースの配送は既になされているものとし、ユーザがそれぞれファイルに管理しているものとする。

システムを立ちあげると、まずウィンドウ上に、登録されているユーザの名前が表示される。通信を行う前に、通信を行うユーザーをこのウィンドウ上で選択する。するとシステムは、あらかじめファイルから配列に読み込んだピースから適するものを選び、このグループ用の鍵を生成する。鍵が生成されたのち、用いる機能の選択が要求される。

子プロセスは常に、送られてくる情報を管理しており、パケットを受け取ると、ヘッダについている情報からパケットの種類を判断し、メインプログラムにシグナルを送る。メインプログラムがこのシグナルを受け取ると、パケットの種類に適した機能を持つウィンドウを自動的に開き、情報を伝える。

4．4　機能

システムの持つ機能としては、メッセージをそう受信するためのウィンドウと、無記名投票を行うためのウィンドウを準備した。

（1）　メッセージウィンドウ

メッセージを入力すると、既に生成されている鍵によって暗号化され、同報される。受信に際しては、自動的に復号化され、表示されるが、正しい鍵でなければ、暗号化された状態のメッセージが表示されることになる。

メッセージのやりとりは、自分自身も含めて、ユーザの名前とともにテキスト上に残る。なお、会議録として、これを保管することもできる。

（2）　無記名投票ウィンドウ

このウィンドウを開くと、まず選挙名の入力が要求される。入力が終わり選挙を開始すると、新たなウィンドウが開き、新任不信任などの投票内容を入力する。発起人が選挙終了の通達をすると、重複投票などの不当な投票を削除した後、投票結果がウィンドウ上に表示される。

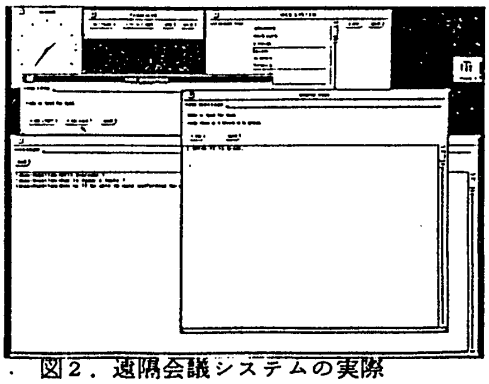

図2．遠隔会議システムの実際

5　おわりに

我々の会議システムにおいて実際に通信を行った結果、会議としての情報交換は十分に成り立ったが、システムの反応の高速性という点にやや問題が残った。今後の課題としては、

1．高速性をさらに増すための暗号方式の工夫
2．グループウェアとしての完成度を高めるための機能の拡張や、より良いマンマシンインターフェイスの導入

などが挙げられる。

6　参考文献

[1]阪田史朗他、”グループ通信アーキテクチャーマルチメディア分散会議システム構築のための基本概念−”、信学技法 Vol.89, No.190, OS89-26, pp13-18, 1989.

[2]武藤康史他、”グループに適した暗号化鍵の管理と配送システム”、情報処理学会第42回全国大会、1991

[3]"Data Encryption Standard", FIP Pub. 46, National Bereau of Standard, Washington, D. C., 1977