分散型システムにおける安全なグループ通信

2R−2

三田 浩也　中村 章人　滝沢 誠
東京電機大学

1　はじめに

現在の情報システムは、複数の計算機を *Ethernet* 等のローカルエリア網で結合した分散型の形態をとっている。また、通信衛星を利用した無線網等による、広域の通信システムも開発されている。これらの放送通信システムでは、プロトコルデータ単位(PDU)を1つ送信することにより、複数の宛先に送信できる。しかし、システム内のどのエンティティも放送されたPDUを受信できると共に、自由にPDUを放送できるので、システムを安全に保護することが問題となる。複数のエンティティ間での放送通信を安全に行うために、まず、協調動作を行う複数のエンティティ間でグループ(群)を確立する。次に、群内の各エンティティに、共通の秘密鍵を持たせることにより、放送通信の秘密性と認証性を保障する。このような群を、安全群とする。さらに、グループウェア等で要求される内証話では、群内の一部のエンティティ間で安全群を確立し、安全群内群とする。本論文では、高信頼放送通信サービスを利用し、安全群及び、安全群内群を確立するための、鍵配送手順を示し、その正しさと有効性を論じる。

2章では、システムモデルを示す。3章では、安全群の確立手順を示し、4章では、群内群について述べる。

2　システムモデル

システムは、OSI参照モデルに基づいた階層構造により構成される。最下位層からN番目の$\langle N\rangle$層は、$\langle N\rangle$エンティティから構成される。$\langle N\rangle$エンティティE_jは、$\langle N-1\rangle SAP$　NS_jで、$\langle N-1\rangle$サービスを利用する。各NS_jは、一意なアドレスNA_jを持つ。$Address(E_j)$は、NA_jを示すとする。E_jは、アドレスSA_jの$\langle N\rangle SAP$ SS_jを通して、$\langle N+1\rangle$エンティティA_jに$\langle N\rangle$サービスを提供する。ここで、$Name(E_j)$をSA_jとする。

$\langle N\rangle$群Cは、$\langle N\rangle SAP$の集合$\langle SS_1,...,SS_n\rangle$である。各$SS_i$は、$E_i$によりサポートされる。$E_i$を$C$のメンバとする。

群内の各プロトコルデータ単位(PDU)pは、以下の情報を持つものとする。

$p.SRC$ = E_jがサポートする$\langle N\rangle SAP$の$\langle N\rangle$アドレス(i.e. $Name(E_j)$)

$p.ADDR$ = E_jがサポートを受ける$\langle N-1\rangle SAP$の$\langle N-1\rangle$アドレス(i.e. $Address(E_j)$)

$p.DEST$ = 宛先エンティティの$\langle N\rangle$アドレスの集合

$p.DATA$ = データ

Secure Group Communication Protocol for Distributed Systems

Hiroya MITA, Akihito NAKAMURA and Makoto TAKIZAWA
Tokyo Denki University

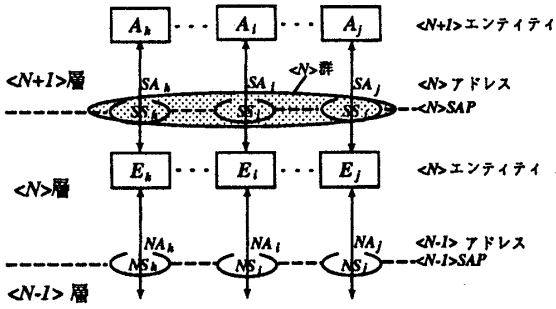

図1: システムモデル

各PDU　pに対して、$p.SRC$が、$p.DEST$内のエンティティに送信するためのデータを$p.IDATA$とする。

[定義] E_jが、PDU pを安全に受信するとは、自分宛に送信されたpを受けとり、かつ、$F(p.DATA) = p.IDATA$なる変換関数Fを持つことである。□

Fを知っているエンティティだけが、送られてきた$p.DATA$を受け取れる。暗号化及び復号化は、Fの一例である。

[定義] 群C内にあるE_jにより送信された全PDUを、C内のエンティティだけが安全に受信できるとき、Cは秘密性を満足する。このとき、Cを秘密群とする。□

[定義] 群C内のE_jは、受信したPDUが、C内のエンティティにより送信されたものである場合に限り、これを安全に受信する。このとき、Cを認証群とする。□

秘密群で、群外のエンティティは、群内で送信されたPDUを受信できない(秘密性)。認証群は、群外のエンティティは、群内にPDUを送信できない(認証性)。

[定義] 秘密性と認証性を満足する群Cを安全群とする。□

つまり、安全群C内で送信されたPDUは、C内でのみ受信でき、かつC内で送信されたPDUだけが、C内で受信される。つまり、群外のエンティティは、C内のメンバを偽装できない。

群C内の全エンティティだけに、共通の秘密鍵Kを配送することにより、安全群Cを確立できる。

[仮定] 次の仮定を設ける。

(1) $\langle N-1\rangle SAP$で送信されたPDUは、全$\langle N-1\rangle SAP$で受信可能である。
(2) 各$\langle N\rangle$エンティティE_jは、$p.ADDR$を改変できない。
(3) E_jは、$p.SRC$と$p.DEST$を改変できる。□

$\langle N\rangle$エンティティE_jは、$\langle N-1\rangle$サービスを利用して、送信された各PDUを送受信できる。pを受信したとき、E_jは、$p.DEST$が、$SA_j(=Name(E_j))$を含むなら受け

とり、そうでなければ、無視する。$p.SRC$ を $Name(E_j)$ 以外の $\langle N \rangle$ アドレスを用いる E_j を偽エンティティとする。$p.SRC = Name(E_j)$ たる E_j を真エンティティとする。

群 C 内の全 $\langle N \rangle$ エンティティ $E_1, ..., E_n$ だけが、共通の秘密鍵 K を持ち、K を利用してPDUを暗号化するなら、C は安全である。本論文では、公開鍵方式及び $\langle N-1 \rangle$ 放送サービスを利用して、$E_1, ..., E_n$ だけに K を配送する方式について論じる。

3 安全群

$\langle N-1 \rangle$ 放送通信サービス上において、安全な群を確立するための安全群確立手順について述べる。先ず、各 $\langle N \rangle$ エンティティ E_j に対して、以下の仮定を設ける。

[仮定]
(1) 公開鍵 PK_i、秘密鍵 SK_i を持つ。
(2) 全 $\langle N+1 \rangle$ エンティティの公開鍵を知っている。
(3) 他の $\langle N+1 \rangle$ エンティティの $\langle N-1 \rangle$ アドレスを知らない。
(4) 他の $\langle N+1 \rangle$ エンティティの $\langle N \rangle$ アドレスを知っている。
(5) いつも動作中である。 □

暗号化又は復号化 Y に対して、$Y(\langle v_1, ..., v_n \rangle) = \langle Y(v_1), ..., Y(v_n) \rangle$ とする。さらに、各 E_j は、値の組 $t = \langle v_1, ..., v_n \rangle$ に対して、秘密鍵 K を得ることができる一方向性関数 $F(t)$ を持つ。

群に参加しようとする $\langle N \rangle$ エンティティの集合を $Dom(C)$ とする。群確立要求を出す能動的と、その要求を待つ受動的との2種類の $\langle N \rangle$ エンティティがある。

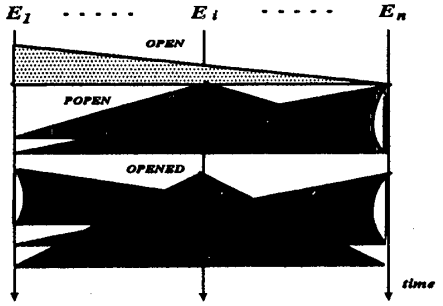

図 2: 基本的な手順

[安全群確立手順] [図2]
(1) ある能動的エンティティ E_i が、$\langle N-1 \rangle$ サービスを利用して、$p.DATA = SK_i(\langle PK_1(t_i), ..., PK_n(t_i) \rangle)$、$p.SRC = E_i$ 及び $p.DEST = \langle E_1, ..., E_n \rangle$ を $OPEN$ p として送信する。ここで、t_i は乱数である。
(2) E_k が、E_i から $OPEN$ 又は $POPEN$ p を受信した後で、$Name(E_k)$ が、$p.DEST$ に含まれているなら、E_k は、t_i を得る。乱数 t_k を引き、t_k を同じ手順で暗号化したもの、つまり、$q.DATA = SK_k(\langle PK_1(t_k), ..., PK_n(t_k) \rangle)$ を $POPEN$ p として送信する。
(3) 全エンティティから $OPEN$ 又は $POPEN$ を受信した上で、E_k は一定時間待ち、$q.DATA = SK_k(\langle PK_1(\langle t_1, ..., t_n \rangle), ..., PK_n(\langle t_1, ..., t_n \rangle) \rangle)$、を $OPENED$ q として送信する。
(4) 全 $\langle N \rangle$ エンティティから、$OPENED$ を受信した上で、E_k は秘密の群鍵 $K = F(\langle t_1, ..., t_n \rangle)$ を得る。これで、安全群は確立された。 □

4 群内群

安全群内の一部の $\langle N \rangle$ エンティティ間での秘密群通信を考え、これを群内群とし、その確立方式について述べる。群内群は、内証話等の特殊な通信型態をとる時、安全群内でメンバが抜ける時に、共通の秘密鍵 K を利用しての群の再確立を行なう場合等に必要となる。

[群内群の確立手順] 群内群確立手順とは、安全群確立手順と同様に、安全群内での各 $\langle N \rangle$ エンティティが、新たな乱数 t'_m を公開鍵方式を利用して送信しあい、一致した乱数の組 $\langle t'_1, ..., t'_m \rangle$ により、群内群での共通の秘密鍵 K' を持つことである。群内群確立における全送受信データもまた、K により暗復号化されている。 □

群内群 C' が確立されるとは、C' 内の $\langle N \rangle$ エンティティだけが、かつ全 $\langle N \rangle$ エンティティが、共通の秘密鍵 K' を知る事である。

群内群の有効性を、偽 $\langle N \rangle$ エンティティが存在する状況下で、安全群を確立するために送信されるPDU数より評価する。群内群の確立を行なうには、新たに群を確立する方式と、今述べた群内に部分群を確立する方式とがある。システム内の全 $\langle N \rangle$ エンティティ数を U とし、真と偽の $\langle N \rangle$ エンティティ数をそれぞれ T と F とする。新たに安全群を確立する場合の全PDU数は、$2(T+F)$ である。これに対して、安全群内群確立において、安全群内の真と偽の $\langle N \rangle$ エンティティ数をそれぞれ t と f とすると、安全群内群確立における全PDU数は、$2(t+f)$ である。つまり、安全群内において、新しく安全群を確立するよりも、群内群を確立することは、コストの軽減に有効である。又、安全群内の共通の秘密鍵 K を利用するので、群外の $\langle N \rangle$ エンティティに対して、二重の安全保護が確保できる。

5 おわりに

グループウエア等の分散型応用では、放送通信サービスが、重要な通信サービスとなる。本論文では、放送通信網上に安全群を確立する手順を示した。電子会議システム等における内証話といったような通信を提供するために、安全群内群を示した。この方式は、新たに安全群を確立するよりも効率的で、より安全な群通信を提供することが可能である。今後の課題として、移動体通信での、安全群の確立方式を考察中である(例えば、SAP が、不定、又は、変化する時)。

参考文献

[DENN83] Denning, D.E., "Cryptography and Data Security", Addison-Wesley, 1983.

[NAKA91] Nakamura, A. and Takizawa, M., "Reliable Broadcast Protocol for Selectively Ordering PDUs," *Proc. of the 11th IEEE ICDCS*, 1991, pp.239-246.

[TAKI87] Takizawa, M., "Cluster Control Protocol for Highly Reliable Broadcast Protocol," *Proc. of the IFIP Conf. on Distributed Processing*, 1987.