DHCP を用いたグループ鍵共有プロトコルに関する研究

増山　一光 †　　佐藤　直 ‡

情報セキュリティ大学院大学
221-0835
神奈川県横浜市神奈川区鶴屋町 2-14-1
† mgs084502@iisec.ac.jp
‡ sato@iisec.ac.jp

あらまし　グループを単位として同一の対称鍵を共有するグループ鍵共有プロトコルを用いることで，効率やセキュリティを重視した鍵管理を実現することが可能になる．本研究においては，グループ鍵共有プロトコルの先行研究を踏まえて，ネットワークにおける実装を前提として，その設計を行うものとする．具体的には，LAN を対象に DHCP を利用したグループ鍵共有プロトコルを提案する．本提案によれば，従来のグループ鍵共有プロトコルに比べ端末管理やユーザ認証がより効率的に行うことができる．

The study of the group key agreement protocol using DHCP

Kazumitsu Masuyama †　　Naoshi Sato ‡

Institute of Information Security
2-14-1 Tsuruya-Cho Kanagawa-Ku Yokohama-Shi Kanagawa 221-0835 Japan
† mgs084502@iisec.ac.jp
‡ sato@iisec.ac.jp

Abstract For secure communication among specified group members on LAN, this study proposes a protocol for sharing secret keys. The proposed protocol adds a new function for DHCP and realizes more efficient terminal management and user authentication than conventional key-sharing protocols.

1　はじめに

ネットワークにおいてグループを単位として認証やデータを秘匿する場合には，一般的にグループに参加するユーザが同一の鍵を共有することが必要となる．これを実現するものがグループ鍵共有プロトコルである．

グループ鍵共有プロトコルは Diffie-Hellman 鍵共有プロトコルに代表される 2 者鍵共有プロトコルよりも複雑である．そのため，様々な目的に応じてプロトコルの仕様も多様となっている．

たとえば，企業においてグループ鍵を用いることで，プロジェクトにおける開発に関する情報の認証や秘匿をするような場合に非常に有効である．このことから，本研究においては LAN の中における効率的なグループ鍵共有をする手法について検討するものとする．そこで，まず先行研究としてBresson らによって提唱されているグループ鍵共有プロトコル[1]を取り上げ，既存のグループ鍵共有プロトコルの問題点について指摘する．

これらを踏まえて，実装を前提として特定のグループでの認証やデータの秘匿をするために，DHCP を用いてグループのユーザの変化に柔軟

に対応することができるグループ鍵共有プロトコルを提案することを研究目的とする．

なお，本稿の構成としては，第2章では先行研究に対する考察を行い，これを踏まえて第3章では提案にあたっての検討条件を整理することにする．そして，第4章で提案方式を提示して，第5章で提案方式の課題について述べる．

2　先行研究

ユーザの参入や撤退があったときのグループ鍵の更新を速やかに行えるものとして，Bresson らによるグループ鍵共有プロトコルがあり[1]，これについて検討を行う．

このグループ鍵の配信の方法として，図1から3にあるように，Setup,Remove,Join の各オペレーションによって構成されている．ただし，紙面の都合上，3ユーザ U_1, U_2, U_3によるケースによっている．

ここでは，素数p と，この素数p を法とする原始元 g を共有している．なお，モジュロの記載「mod　p」については省略している．

2.1　Setup オペレーション

まず，Setup オペレーションについてみることにする．ここでは各ユーザ U_nがユーザ鍵 x_nを持っているものとする．このユーザ鍵 x_nは乱数によって生成される．

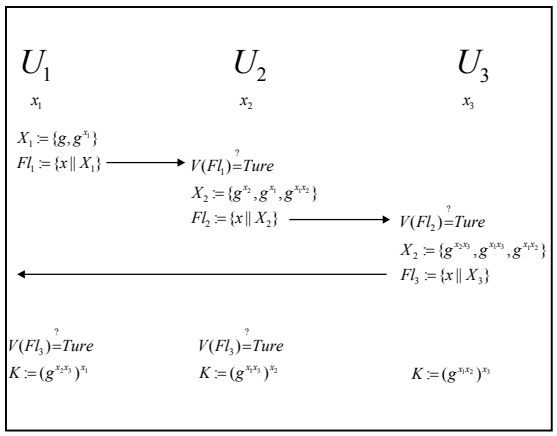

図1：Setup オペレーション

各ユーザは図1にあるように U_nから U_{n+1}に順次通信をする．U_3は Group Controller（以下GC）としての役割を持っており，ここからブロードキャスト通信を行うことで各ユーザは受け取った鍵からグループ鍵（対称鍵）を計算することになる．

2.2　Remove オペレーション

次にRemove オペレーションについてみることにする．ここでは U_2がグループから撤退したものとする．このことにより，グループメンバーの構成に変更が生じているので，グループ鍵を更新する必要が生じる．

その手法としては，GC である U_3の x_3を x_3'に更新をして，各ユーザに対してブロードキャスト通信を行いグループ鍵の更新を行う．

この手法では，確実にグループ鍵の更新は可能であるが，どのユーザがどの時点で撤退したのかを適切に把握した上でのグループ鍵更新が求められる．

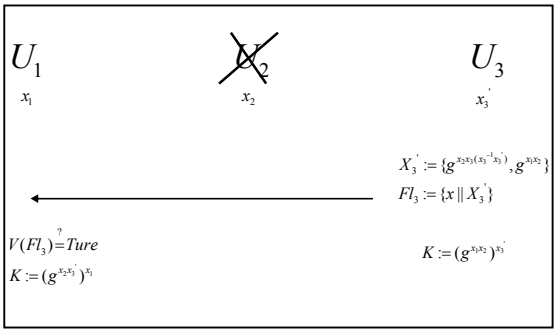

図2：Remove オペレーション

2.3　Join オペレーション

最後に，Join オペレーションについてみることにする．ここでは U_4が参入してきたものとする．新たなユーザが参入した場合にも，U_4が参入した時点以降のグループ鍵生成が求められるため，グループ鍵の更新が必要になる．

その手法としては，GC の役割をしていた U_3の x_3'をグループ構成員の変更に伴い x_3''に更新して，図3のように U_4に通信する．この時点で，GC は U_4に遷移し，グループ鍵の要素の生成後に，ブロードキャスト通信をして，各ユーザがグループ鍵を生成する．

ここでは，Remove オペレーションと同様にユーザの参入の適切な把握が必要になる．加えて，

GC が移り変わることから，新たに参入したものが GC として振る舞うことになり，管理権限をどのように移行していくかという問題が生じる．

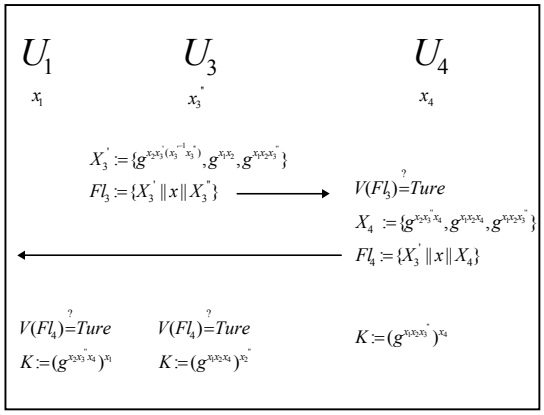

図３：Remove オペレーション

2.4 考察

Bresson らによって提唱されているグループ鍵共有プロトコルにおいては，グループの動的変化に対応したセキュアな鍵交換を実現している．しかしながら，問題点も少なくない．

具体的には，第 1 にこのプロトコルのユーザ認証方法では自分が直接認証（direct-partnering）したユーザ以外にも，そのユーザが認証した相手も“partnering”することによって起きる脆弱性である[2]．これは，時として参加者が特定の相手に「仲間はずれ」を行うことで，除外者のように扱う問題が発生する．

第 2 に参加ユーザ数が増加すると，各ユーザがグループ鍵を算出するまでの計算量が飛躍的に増加する．このことは，参加ユーザ数分だけの剰余計算が必要となると同時に,通信回数についてもブロードキャスト通信を含めて参加ユーザ数と同じ回数は必要になるので非効率であるといえる．

こうした Bresson らのプロトコルにおける課題を改善しつつ，提案に向けた諸条件について次章で検討する．

3 提案に向けた検討条件

先行研究として，Bresson らのグループ鍵共有プロトコルを考察してきた．この章では，その考察を受けてグループ鍵共有プロトコルを提案する際に必要となる検討を行うものとする．

まず，前章でも述べているがユーザ認証の問題が存在する．Bresson らのプロトコルでは基本的に P2P ネットワークを前提としたグループ鍵共有を実現している側面がある．そして，新規に参入したユーザに GC が遷移する機能を有している．このことから，正規のユーザをどのように認証するかという問題が生じるのである．確かに，第 3 者機関による証明書などを用いてグループ鍵を生成することで P2P ネットワークにおいてもかなりの安全性を確保することが可能になる．しかし，証明書を用いて P2P ネットワークを利用することは考えにくいのが現状である．そこで，グループ鍵の管理および安全性に対する新たな問題は生じるが，グライアントサーバモデルを基本形としたグループ鍵共有を実現することで認証の問題を解決する必要がある．

次に，グループ鍵の生成にあたって，いかに高速かつ効率的に実現するかという検討すべき事項がある．これについては，Diffie-Hellman 鍵共有プロトコルを基本としたグループ鍵生成のプロセスにおいては，一般的には公開鍵暗号方式を用いるよりは高速処理が可能であるが，各ユーザに対して複雑な演算や演算量の増大という問題が生じることになる．これに関しては単に数論的アプローチにだけでなく，演算プロセスの分割といったプロトコルの運用に基づいたアプローチによって負担を軽減する手法についても検討するものとする．

4 提案方式

4.1 前提条件

前章の検討を踏まえて，グループ鍵共有プロトコルを実現するために，Dynamic Host Configuration Protocol（以下 DHCP）[4]を用いることにする．その主な理由としては DHCP がネットワークでの動的かつ自動的にホストの設定を行うので，ネットワークの動的変化に対応できるからであり，この機能をグループ鍵共有で活用することで，効率的な運用を目指すものとする．

今回，グループ鍵共有を行う際に利用するものとして，以下，広く利用されている DHCP（RFC2131）を例に検討する．

なお，本章におけるグループ鍵演算における定義は，次の通りである．

U_n ：ユーザ

n：ユーザ番号

x_n ：ユーザ鍵

（ハッシュ値 $h(ID_n \| PW_n)$ によって生成）

ID ：ユーザ ID

PW：パスワード

x_0 ：サーバ鍵（乱数によって生成）

$\{g^{\prod_{(x_k \mid k\in[0,i]\wedge k\neq n)}} \mid n \in [1,i]\}$ ：グループ鍵の要素（自分以外のユーザの鍵の要素）

k：サーバとユーザを含むユーザの集合

4.2 DHCP を用いたグループ鍵共有プロトコルの手法について

まず，DHCP はクライアントサーバの形態を前提にしており，クライアントとサーバにそれぞれ専用のプログラムがある．そのやり取りによって，IP アドレスをはじめとしてホストの設定情報を提供するものである．この過程を利用して，前章で検討したユーザ認証の問題を解決しつつ，グループ鍵共有を実現しようとするものである．そこで，DHCP のメッセージ交換の順を追って，その手法について示すことにする．

提案システムにおいては，DHCP におけるユーザ認証機能を付加させた認証 DHCP で，グループ鍵共有を行うことを検討する．まず，通常の DHCP のメッセージ交換を用いてクライアントに仮 IP アドレスを付与する．最初にクライアントから Discover メッセージをブロードキャストして，サーバを探すという作業を行うことになる．DHCP においてはメッセージ交換においてイーサネットフレームの Mac アドレスで通信していることから，Discover の段階で Mac アドレスに対する認証を実施する．しかし，Mac アドレス認証だけではこれ自体が詐称されている可能性があるので，認証には不十分である．

Discover メッセージを受けてクライアントに対して Offer メッセージを返送する．これは候補となる IP アドレスを通知するものであるが，ここでは仮 IP アドレスの候補を通知する．クライアントはこの候補である IP アドレスに問題なければ，サーバへの取得依頼の Request メッセージを送信する．これを受けて，サーバが Ack メッセージを返送することで仮 IP アドレスを発給する．

仮 IP アドレスの発給を受けたクライアントは，認証用 Web にアクセスしてユーザ ID および PW による認証を行う．この際，ユーザの ID および PW を用いて，ハッシュ値を用いてユーザ鍵を生成する．具体的には $h(ID \| PW)$ となる．このユーザ ID および PW はサーバからあらかじめ発給されるものとし，したがってサーバは各ユーザのユーザ鍵を保有している．

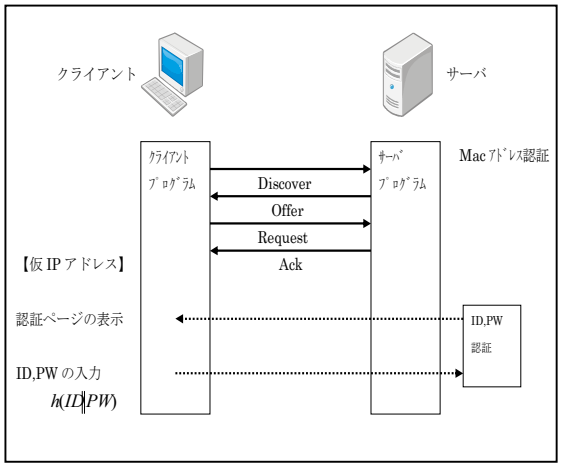

図４：DHCP メッセージ交換（1）

認証ができたことで，クライアントに対して正規の IP アドレスを発給する．その流れとしては，通常の Discover，Offer，Request，Ack というメッセージ交換で行うが，すでに Mac アドレスの認証や仮 IP アドレスの発給がされているのでユニキャスト通信でメッセージ交換が行われることになる．ここでの処理は Rebinding 期間が過ぎた場合の Rebind と同様である．

ここで，最後の Ack メッセージにおいてオプションを利用する．これは，本来的にはネットワーク情報などを通信するために使用するものである．ここでは，DHCP の未定義のオプションを使用し

たり，ISC 社の DHCP に見られるようなユーザ定義のオプションを利用する．このオプションは可変長となっているので，グループ鍵の要素になる計算結果を文字列として送信させるデータ容量を確保することができる．そして，Ack メッセージを受けとったクライアントは正規の IP アドレスを受け取ると同時に，自分以外のユーザの鍵情報であるグループ鍵の要素を受け取り，自らのユーザ鍵を用いてグループ鍵を生成する．

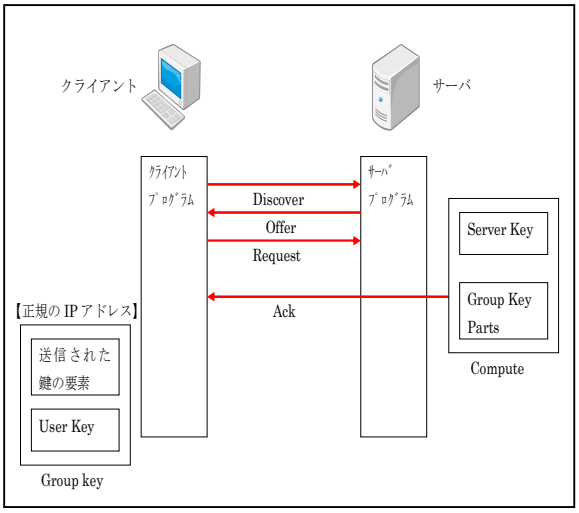

図５：DHCP メッセージ交換（２）

なお，クライアントがネットワークから離脱するときには，Release メッセージによって IP アドレスは返却することになるが，その際にグループ鍵は適切に廃棄されるものとする．

4.3　グループ鍵の演算方法

次にグループ鍵の生成に関して，その詳細を述べることにする．ここでは，前章での検討を踏まえて，ユーザの演算負荷を減少させ，効率的なグループ鍵の演算を目指すものである．

具体的には，Ack メッセージによるグループ鍵生成の詳細な流れは図６のようになる．この図について，まず，前提となる部分を解説する．クライアント側にある User Key は ID,PW 認証を行った際に，ハッシュ値 $h(ID\|PW)$ を用いて生成したものである．前述のように，ID,PW はあらかじめサーバから提供され，これらをサーバが保持することで，サーバは全ユーザの User Key の算出が可能である．

Group Key Parts は，サーバが ID,PW を発給した段階で User Key を算出できることから，グループ鍵を共有するユーザのグループ鍵の要素を事前に計算して準備したものである．

たとえば，ユーザ U_1 U_2 U_3 の間でグループ鍵を共有する場合，U_1 のグループ鍵の要素は自らのユーザ鍵を除いた x_2x_3 となる．そこで，Group Key Parts で $g^{x_2x_3}$ を事前に算出する．

Server Key はサーバが独自に保有している鍵であり，乱数を発生させることで生成させる．これを User Key に加えて，グループ鍵を生成する．従来の方法ではグループ鍵は User Key によって構成されるため，鍵の更新には参加者の鍵を更新しなければならないので難しい側面がある．これに対して，提案方式では，Server Key を更新させることでグループ鍵の更新を容易に実現しようとするものである．具体的には，$(g^{x_1x_2x_3})^{x_0}$ というグループ鍵があった場合には，Server Key を更新することで $(g^{x_1x_2x_3})^{x_0'}$ のようにグループ鍵自体を更新することができる．

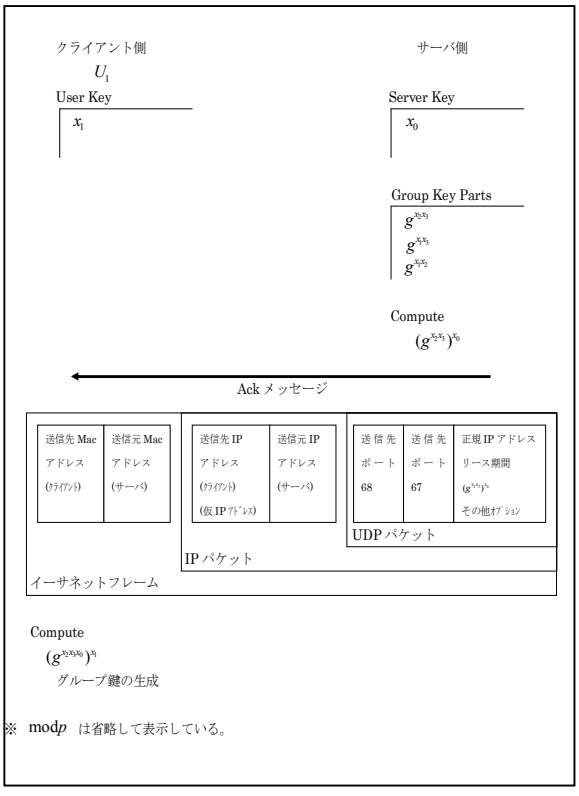

図６：Ack メッセージを用いたグループ鍵の生成

実際のグループ鍵生成の流れとしては，次のと

おりである.

①サーバ側で Server Key と Group Key Parts から送信するためのグループ鍵の要素を演算

②その要素を Ack メッセージのオプションに組み込んで送信

③クライアント側で受信したグループ鍵の要素とユーザ鍵を用いてグループ鍵を演算

このようなプロセスから，演算プロセスを分割してグループ鍵を生成することで効率化を図るものである.

4.4 提案方式の特質

本提案方式においては，認証 DHCP の方式を参考にして，グループ鍵共有を実現した．認証 DHCP においては，Web を用いた認証を行うために IP アドレスは必要不可欠である. そのため，仮 IP アドレスを発給したうえで，認証を行うことになる．この認証の際に利用される ID，PW からハッシュ値を用いてユーザ鍵を生成する．このユーザ鍵は ID, PW がサーバから発給されるため，サーバは事前にユーザ鍵を算出しておくことが可能となっている.

本提案方式の独自性としては，第１にグループを構成するユーザ鍵から，各ユーザのグループ鍵の要素あらかじめ計算しておくことで，グループ鍵生成時の計算負荷をあらかじめ低減させておこうとする点にある．このことは，図 6 にあるようにグループ鍵の生成までにどのユーザでも，Group Key Parts に対して Server Key と User Key の演算の２回で生成することができる.

第2に Ack メッセージのオプションにグループ鍵の要素を組み込んで，送信する点にある．これは，グループ鍵の要素の計算結果を 16 進数表示して文字列として送信する．これを受け取ったユーザ側は，この文字列を数値として認識して，ユーザ鍵を用いてグループ鍵を演算する.

これらのことから，従来の手法である各ユーザによるバケツリレー方式とブロードキャスト通信によるグループ鍵の生成よりも効率的であることがいえる．さらに，セキュリティ面はサーバの盗難という問題があるが，サーバのバックアップならびに Server Key の更新により確保することが可能である.

５　課題

本提案方式における課題としては，次のようなものがある.

- 既存の DHCP と提案システムのトラフィックの比較
- DHCP のパケットサイズへの問題の有無
- 本提案方式を採用した際の DHCP リレーエージェントの動作確認
- IPv6 への対応

６　おわりに

本稿では, DHCP の機能を用いてグループ鍵共有プロトコルの設計を展開してきた.

今後の研究予定としては，このような提案方式を実装して，前章で取り上げた課題の検証を行なっていくものとする.

参考文献

[1] Emmanuel Bresson,Oliver Chevassut,David Pointcheval,Jean-jacques Quisquater:“provably authenticated group diffie hellman key exchange“, In Proc. of 8th ACM Conference on Computer and Communications Security ,pp.255 - 264,Nov,2001

[2] 伊藤忠彦, 櫟肅之:“動的グループ鍵交換プロトコルのUC安全性について“, SCIS2008,pp23,Jan, 2008

[3] Y. Kim, A. Perrig, G. Tsudik: “Simple and Fault-Tolerant Key Agreement for Dynamic Collaborative Groups“ , In Proc. of 7th ACM Conference on Computer and Communications Security,pp.235-244, 2000.

[4]RFC2131
http://www.ietf.org/rfc/rfc2131.txt