P2P 人狼 BBS

吉本晴洋[†] 繁富利恵[††] 副田俊介[†††]
金子知適[†] 田浦健次朗[†]

本稿では人狼 BBS というゲームを P2P 上で安全に行なうためのプロトコルを提案する。P2P での実装はサーバの管理が不要というメリットがあるが、信頼できる第三者がいないため、プレイヤーが不正を行うことができてしまう。本研究では匿名通信路やゼロ知識証明などの暗号技術を用いて不正を防止するプロトコルを提案した。

The Neighbour Wolves in Peer-to-Peer Network

Haruhiro Yoshimoto,[†] Rie Shigetomi,[††] Shunsuke Soeda,[†††]
Tomoyuki Kaneko[†] and Kenjiro Taura[†]

We propose a protocol for the neighbour wolves in peer-to-peer network. In peer-to-peer network model, we cannot assume trusted third party. Thus, player can cheet. We proposed a protocol that can prevent players from cheeting. We used cryptographic technology such as zero knowledge proof and anonymous channel.

1. はじめに

ネットワークゲームを設計する際に従来のサーバ・クライアントモデルを使用すると、サーバの設置、管理の費用および手間が膨大である。24 時間運用に耐えるサーバの設置費用や運営費は高くつき、また、たとえゲームのブームが下火になってもサーバの管理を続けなくてはならず、特に個人で開発している開発者はサーバの管理もしなければならないので、心理的負担は大変なものになる。

一方、P2P 方式を採用すると (1) サーバの管理費・手間がかからない、(2) 通信・計算の負荷を各ノードへ分散できるなどのメリットがあり、ブームが下火になればゲームも自然消滅し、またブームが再燃すれば復活するということも可能である。

しかし、このようなメリットがある一方、P2P において悪意あるプレイヤに備えて設計を行う必要がある。なぜなら P2P はサーバが存在しないために、信頼できるノードが存在しないからである。詳しく述べると、サーバ・クライアントモデルでは「サーバは信頼できる」という前提条件の元で実装を行なうため、全ての計算をサーバで行なえば悪意のある攻撃者がいたとしても、できる攻撃にはかなりの制限がある。一方、P2P モデルでは各プレイヤーがゲームを進行させる計算を分担するため、どのプレイヤーも攻撃者となりうる。つまりその計算を行っている者が悪意を持っている場合、簡単に攻撃が成功してしまう。したがって P2P を用いたシステムでは暗号技術を用いてセキュリティを保証する必要がある。

人狼 BBS は、各人の役割を秘密にした推理と説得のゲームであるため、自分以外のプレイヤーに役割を知られてしまうと、ゲームの進行に非常に不利になる。したがって悪意のあるプレイヤーは通信の監視などの手段を用いてその情報を推測し、ゲームを自分にとって有利に進めることが出来てしまう。P2P で人狼 BBS を実装する際、暗号を用いない実装ではプレイヤーにその情報が漏れてしまう危険性が存在する。また、単純に暗号を用いたとしても、「暗号を行なった通信をしていること」自体が何らかの情報となってしまう可能性があるため、慎重な実装が要求される。

本研究で想定する攻撃者のモデルは以下の通り。

・攻撃者は通信路全体の盗聴および改竄ができる
・攻撃者はゲームの進行を妨げるような攻撃はしない：計算の放棄など

† 東京大学
University of Tokyo
†† 産業技術総合研究所 情報セキュリティ研究センター
RCIS, AIST
††† 公立はこだて未来大学
Future University - Hakodate

・攻撃者の最終目的は誰がどの役割かを知ることでゲームを有利に進めることである。

2. 人狼 BBS

人狼 BBS☆ とは「汝は人狼なりや?」というゲームをインターネット上で行えるようにしたものであり、CGI 版や、MMORPG 中でできるようにしたものなど数多くのバリエーションが存在する人気ゲームである。本章ではそのルールを説明する

2.1 参加人数と期間

一回のゲームは 11〜15 人で行われる。プレイヤーは人狼と人間の二つのグループに分かれ、勝敗の決着が付くまで行なわれる。勝敗は大体数日〜10 日間で決着する。プレイヤーは BBS 上で会話しながらゲームを進行する。

2.2 役 割 決 め

プレイヤーには開始時に人狼、占い師などの役割がランダムに与えられる。誰がどの役割であるかは他プレイヤーには知らされない。以下はその一部。

・人狼: 人狼は互いに誰が人狼かを知ることがきる。また、一晩に一人だけ人間 (人狼以外の役割のプレイヤー) を襲撃して殺すことができる。ただし、人狼が複数いても一晩に殺せるのは一人だけ。人狼達は専用の秘密の BBS を持っていて、その BBS 上で誰を襲撃するかなどの相談を行うことができる。

・占い師: 一晩に一人だけ、参加者の正体を占って人狼／人間の区別を知ることができる

・狩人: 一晩に一人だけ、人狼の襲撃から守ることができる

2.3 投票による処刑

生きている全てのプレイヤーは一晩に一人、プレイヤーを処刑することができる。誰を処刑するかは多数決の投票によって決定する。これによって人狼を全て処刑することが人間の目的となる。ただし、その投票には人狼も参加するため、人狼たちは自分たちが処刑されないように議論を誘導する。

2.4 勝敗の決定

最終的に全ての人狼を排除すれば人間側の勝ちであり、人狼の方が人数が多くなったら人狼側の勝ちである。

3. 問題点と解決の方針

P2P で人狼 BBS を実現するためには多くの解決すべき問題点が存在する。その問題点および本研究で提案する解決策を以下に列挙する。

・各プレイヤーへの役割の公平な割り当て

どのプレイヤーがどの役割に割り当てられるかはランダムに決定しなければならない。サーバを利用した人狼 BBS では、サーバがランダムに役割を割り当てればいいのだが、P2P ではこの操作をある特定のページのプレイヤーが行い、そのプレイヤーが攻撃者だった場合、その割り当てを作為的に行うことによって、どのプレイヤーにどの役割を割り当てるか操作することができる。解決策は 5.1 章で説明する。

・人狼同士の会話

人狼同士は互いに誰が人狼であるかを知っていて秘密の BBS を用いて会話をする。しかし、ゲーム開始時には誰がどの役割かを知ることはできない。そのため、人狼になったプレイヤーは全員に対して “あなたは人狼ですか？” と尋ねる必要があるのだが、暗号を用いないと、その時点で自分は人狼であることがバレてしまう。したがって、自分がどのプレイヤーであるかを悟られないようにしながら、自分は人狼であることを証明する必要がある。解決策は 5.2 章で説明する

・占い師

占い師は毎晩一人占いに指定したプレイヤーが人狼か人間かが分かる。ただし、誰が占われたかは他のプレイヤーには分からない。これを実現するには 占い師はプレイヤーを一人指定し、指定されたプレイヤーは自分が人狼か返答する。というプロセスを行う必要があるのだが、そのためには自分が占い師であるという証明をしながら、誰が占い師および誰が占われたかは他のプレイヤーには分からないようにする必要がある。解決策は 5.3 章で説明する。

・時刻の問題

人狼 BBS は数日間に渡って行われるゲームであり、1 日単位でゲームを区切る。したがって、時計という概念が重要である。攻撃者は自分のコンピュータの時計を進めることでゲームがあたかも進行したように見せかけることができる。これを防ぐには、P2P に参加している全てのプレイヤーからランダムに数人選択し、その時刻の中央値を取ると良い。

4. 利用する暗号技術

本章では提案プロトコルで用いる暗号技術の説明を行う

4.1 離散対数問題

N を十分に大きな任意の素数とし、g を N を法とする原始元とし、x を任意の整数としたとき、$y = g^x \bmod N$ という式を計算する。g, x, N が与えられ

☆ http://wolfbbs.jp/

た状態でこの y を求めることは容易いが、g, y, N が与えられた状態でこの式を満たす x を求めることは難しいとされている。これを離散対数問題[4] と呼ぶ。本研究ではこの離散対数問題を解くことは困難であるという仮定のもとでプロトコルを構成する。

4.2 電 子 署 名

公開鍵暗号の秘密鍵、公開鍵のペアを (sk, pk) としたとき、あるデータ x および sk を入力とする署名用関数の出力 $s = Sign(sk, x)$ を sk を用いた x に対する署名と呼ぶ。Sign は一方向性関数であり、その出力 s から sk および x を知ることはできない。また、この x および pk を入力とする署名検証用関数の出力 $v = Verify(pk, x)$ は 正当な pk, x を用いない限り、s と一致しないので、pk に対する正当な sk を知らない限り $v = s$ を満す s を生成することはできない。これを電子署名と呼ぶ。代表的なものとして ElGamal 署名[2] や RSA 署名[5] などが存在する。

4.3 匿名通信路

匿名通信路とはあるメッセージを Alice から Bob に送る際に、受信者 Bob には送信者が誰か特定できないようにするプロトコルである。匿名通信路には様々な方式が存在するが、今回使用するものは (1)P2P で使用可能かつ (2) 返信可能なものでなくてはならない。返信可能というのは送信者は誰か特定不能であるが、その送信者に返信はできるというものである。このような条件を満たすものに Onion Routing[7] が存在する。本研究ではこのプロトコルを使用する。

4.4 メンタルポーカープロトコル

メンタルポーカープロトコルは信頼できる第三者がいない状態でポーカーを行うというプロトコルである。これは、トランプを配布する際に、誰がどのトランプを選んだかを知られることなしに、かつ、トランプが完全にランダムに配布されるようにするためのプロトコルである[6]。本研究ではトランプを配布する代わりに役割を配分するのに使用する。トランプは 53 枚だが、役割は参加人数であり約十数人なので、計算にかかる時間はかなり減ることが予想される。

4.5 離散対数問題の答えを知っていることをゼロ知識で証明するプロトコル

ゼロ知識証明とはある知識 x を知っているということを “ 他人に x を知られることなしに” 証明するためのプロトコルである。このプロトコルを使えば、Alice が Bob に x を知っていることを証明した後でも、Bob は他の Charlie や David に自分が x を知っているということを証明することはできない。本研究で必要なのは離散対数問題の答えを知っていることをゼロ知識証明するためのプロトコルであり、Chaum ら[1] が提案しているものを使用する。

4.6 鍵交換プロトコル

鍵交換プロトコルは公開されたネットワーク上で同じ秘密鍵を共有するプロトコルであり、例え盗聴されても共有した秘密鍵は盗聴者には分からない。本研究では IKE (Internet Key Exchange) というプロトコル[3] を利用する。

5. 提案プロトコル詳細

本章では提案プロトコルの詳細を説明する。概要としては参加者に役割が公平に割り当てられるようにメンタルポーカープロトコルを使用する。また、人狼同士が互いに自分が人狼であることを相手に証明するため自分の役割を証明できるようなデータをブロードキャストしておき、その証明を匿名通信路上で行う。

以下、$a|b$ は a と b を連結したものである。例えば、a が 100 ビットで b が 200 ビットなら $a|b$ は 300 ビットで、その上位 100 ビットは a で下位 200 ビットは b である。また、$g^x \bmod N$ と表記した時の N は十分に大きな任意の素数を示し、g は N を法とする原始元とする。

5.1 役 割 決 め

(0) ゲームに参加する各プレイヤーはそれぞれ公開鍵と秘密鍵の対 (pk_i, sk_i) を生成し、その公開鍵 pk_i を匿名通信路 (4.3 章参照) を用いて他のプレイヤーにブロードキャストする

(1) ゲームに参加するプレイヤーの一人 Alice は各役割を示す一意なラベル $yakuwari$ を設定する。例えば、以下の通り

人狼 A: $yakuwari_0 = 1$
村人 A: $yakuwari_1 = 2$
占い師: $yakuwari_2 = 3$

(2) Alice はゲームに参加する他のプレイヤーに対してメンタルポーカープロトコル (4.4 章参照) を利用して $yakuwari_i$ を配布する

(3) 各プレイヤーはそれぞれ乱数 r_i および $z_i = g^{(r_i|yakuwari_i)} \bmod N$ を生成する。
$message_i = yakuwari_i|z_i$ を生成し、$message_i$ に自分の秘密鍵で署名を行ったもの $Sign(sk_i, message_i)$ を付加したものを他のプレイヤーに対して匿名通信路を用いてブロードキャストする

(4) $message_i$ およびその署名を受け取ったプレイヤーは署名が有効なものであることと、各署名がそれぞれ別の秘密鍵によって署名されていることを確認する。もし同じ秘密鍵で署名されたものが見つかった場

合、その $message_i$ は偽造されているとみなす。

この $message_i$ は各プレイヤーが自分に割り当てられた役割が $yakuwari_i$ であることを約束する (コミット) ものであり、後述のプロトコルで自分が真に $yakuwari_i$ を担っていることを証明するのに使用する。ただし、匿名通信路を用いているために、各プレイヤーは誰がどの役割であることを知ることはできない。また $message_i$ に付加された署名は他人がこのメッセージを偽造するのを防止するために必要である。

5.2 人狼同士の自己紹介

(5) 人狼プレイヤー (Jinro1) は他のプレイヤー (Jinro2,Murabito1,...) に対して 4.1 の (3) で配布した $z_0 = g^{x_0} \bmod N$ を満たす x_0 を知っているということをゼロ知識証明 (4.5 章参照) を用いて証明する。ただし、この証明の際には匿名通信路を用いる。
また、この時に、鍵交換プロトコル (4.6 章参照) を用いて同じ秘密鍵 key_j を共有しておく

(6) メッセージを受け取ったプレイヤーは z_0 に対応する $yakuwari_0$ が人狼であることを確認して、
自分が人狼であるならば $z_1 = g^{x_1} \bmod N$ を満たす x_1 を知っていることの証明書および自分の IP アドレスを key_j を用いて暗号化し、返信する

以上で人狼同士はお互いの IP アドレスを知ることができたので、今後は key_j を用いて秘密の相談をすることができる。このプロトコルの安全性は離散対数問題の困難性、匿名通信路の匿名性のどちらか弱い方となる。

5.3 占 い 師

(7) 占い師は一晩に一人、指定したプレイヤーに対して $z_2 = g^{x_2} \bmod N$ を満たす x_2 を知っているということをゼロ知識証明を用いて証明する。ただし、この証明の際には匿名通信路を用いる。

(8) 指定されたプレイヤーは受け取った z_2 に対する $yakuwari_2$ が占い師であることを確認して、$z_3 = g^{x_3} \bmod N$ を満たす x_3 を知っていることの証明書を返信する

(9) 占い師は z_3 に対する $yakuwari_3$ を確認することで指定したプレイヤーが人狼かどうかを知ることができる

6. まとめと今後の課題

本研究では人狼 BBS においてメンタルポーカープロトコルを使用することによって各プレイヤーの役割が公平に配分され、また、匿名通信路およびゼロ知識証明を使い、正体を明かすことなく自分の役割を証明することができるようにしたプロトコルを提案した。このプロトコルによって、プレイヤーが役割の割り当てを故意に操作したり、通信路を盗聴することで誰がどの役割かを知るということを防ぐことができる。

本稿で提案したプロトコルには問題点がいくつか残っている。以下に列挙する。

(1) 占い師は人狼か人間かどうかだけでなく、狩人など、役割も分かってしまう

(2) 占い師が不正して一晩に 2 人以上の役割を聞き出すことが出来てしまう

(3) 占い対象は自分が占われたことが分かってしまう

(1) はプロトコル開始時に自分の役割をコミットする際に「人狼か人間か」のデータを追加してコミットすることで解決できる。(2) はあらかじめ占い師が誰を占うかをコミットしておくか、占いの対象となったプレイヤーは占われた後に自分が占われたという証拠をブロードキャストすることで解決できる。

参 考 文 献

1) D. Chaum, J.-H. Evertse, J. Graaf, and R. Peralta. Demonstrating possession of a discrete logarithm without revealing it. In A. M. Odlyzko, editor, Advances in Cryptology—CRYPTO '86, pages 200– 212. Springer-Verlag, 1987.
2) T. El-Gamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE TIT, vol. IT-31:4, pp 469–472, 1985.
3) Harkins, D. and Carrel, D., "The Internet Key Exchange (IKE)", RFC2409, November 1998
4) A. Menezes, P. Oorschot, and S. Vanstone, "Handbook of Applied Cryptography," CRC Press, 1997.
5) Ron L. Rivest, Adi Shamir, and Leonard M. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2):120–126, February 1978.
6) A. Shamir, R. L. Rivest, and L. M. Adleman. Mental poker. In D. Klarner, editor, The Mathematical Gardner, pages 37–43. Wadsworth, Belmont, California, 1981.
7) Syverson, P., Reed, M. G., Goldschlag, D. M.: Anonymous Connections and Onion Routing. IEEE Journal on Selected Areas in Communication, 1998, 16(4):482-494