安全なモバイルエージェントの構築法について

北澤 繁樹, 岡本 栄司
{shigeki, okamoto}@jaist.ac.jp
北陸先端科学技術大学院大学 情報科学研究科

現在、我々を取り巻く計算機環境はますます複雑になってきている。これを解消するために、エージェント技術が注目され、応用されつつある。そのため、エージェントをいかに安全に運用するかが課題となっている。本論文では、ID-NIKS(ID-based Non-Interactive Key sharing scheme) を応用した安全なエージェントシステムの構築法を提案し、それについて考察をする。

Study on Secure Mobile Agent System

Shigeki KITAZAWA, Eiji OKAMOTO

School of Information Science,
Japan Advanced Institute of Science and Technology,
Asahidai 1-1, Tatsunokuchi, Nomi, Ishikawa, 923-1292 JAPAN

Today, since our computing environment is more complex, an agent technology has begun to attract notice. Therefore, an agent technique is used at some important places. For that reason, Agent's security problems are very serious. In this paper, we propose an agent system architecture with ID-NIKS(ID-based Non-Interactive Key sharing Scheme). Then we give some consideration and verification to it.

1　はじめに

近年、多くの人がコンピュータを使い、インターネットに接続している。コンピュータ技術の大衆化にともない、様々なサービスがネットワークを通じて提供されるようになってきた。それら各々のサービスは提供される方法も手続きも多岐に渡っている場合が多く、我々の計算機環境を複雑にする原因のひとつとなっている。

こうした計算機環境の複雑さの緩和を目的とする技術として、エージェント技術が注目され、応用されつつある [1]。エージェント技術とは、人間や他のプロセスの代理として振る舞うプログラムの総称であり、人工知能の分野で研究されてきた技術である。その様なプログラムが、人間と同じだけの知能を持つことが理想であるが、現在はそこまでは至っていない。しかしながら、ある程度の知能でも十分応用できる事例は少なくないので、エージェント技術は現在多くの分野に応用されている。例えば、情報収集やユーザインタフェース、分散コンピューティング、グループウェアなどである。

エージェント技術の中でも、特にモバイルエージェントは分散された環境を移動しながら処理を継続していくプログラムのことを言う。モバイルエージェントは移動性と自律性を兼ね備えているので、コンピュータを常にネットワークへ接続しておく必要がない。また、大量の行列データを送るよりも、それを生成するプログラムを送った方が、結果的にネットワークへの負荷を減らすことができる。よって、様々なネットワーク運営や電子マーケットに応用することができるのである。

この様に、モバイルエージェントは便利な面がある反面、次に示すような安全上の課題を解決しなければならない [2, 3, 4]。

(i) インターネットは決して安全なネットワークではない。

(ii) モバイルエージェントを送信する側が受信する側を必ずしも信用できるとは限らない。

(iii) モバイルエージェントを受信する側が送信する側を必ずしも信用できるとは限らない。

(i) に関しては、エージェントはその持ち主の代理として働くので、エージェントの内部データにその持ち主の重要な情報を持ってネットワークを移動することが多く、そういったデータを攻撃者から守る必要がある。また、エージェントはインターネット上を移動するので、攻撃者によって改ざんされる危険性がある。よってエージェントを送信する側も受信する側もエージェント内部のデータが正しいか正しくないのか考慮する必要がある。(ii) に関しては、エージェントは複数のホスト間を移動しながら送信者によって与えられた処理を遂行していくので、途中の悪意のあるホストによってその処理を妨害されたり、重要なデータを漏洩されたりする危険性がある。よって、悪意のあるホストからエージェントとそのデータを保護する必要がある。(iii) に関しては、エージェントはプログラムであるから、誰にでもそれを記述するすることができる。よって悪意のある送信者が、受信側ホストを攻撃する目的でウィルスやワームやトロイの木馬といったコードを含んだエージェントを送ってくる危険性がある。よって、その様な悪意のあるコードから受信側ホストを守る必要がある。

これらの課題は暗号技術とディジタル署名技術を応用することにより、解決されると考えられる。しかしながら、暗号技術やディジタル署名技術を応用する場合、新たに鍵管理の問題が生じてくる。なぜなら、エージェントは複数のホストをインターネットを通じて移動して行くのでエージェント固有の鍵を持つことができないからである。よってユーザやホストが何らかの形で暗号技術やディジタル署名技術の秘密情報を保持しなければならない。

エージェントシステムの安全性を保持するために、現在最も多く用い入られているのがRSA 暗号に代表される公開鍵暗号技術である。しかし、公開鍵暗号技術を実際のシステムに応用する場合には、CA(Certification Authority) などの導入により公開鍵の正当性を証明しなければならない。したがって処理やそれに伴うデータが増すので、エージェントにとって必ずしも適した暗号技術とは言えない。

そこで、本論文では現在一般に用いられている公開鍵暗号技術の代わりとして ID-NIKS (ID-based Non-Interactive Key sharing Scheme) 技術の応用を提案し、ID-NIKS を用いたエージェントシステムの構築法とその安全性について考察する。

2 ID-NIKS

2.1 ID-NIKS の特長

ここでは、ID-NIKS の概要について簡単に述べる。ID-NIKS の重要な特長は以下の 2 点である [5, 6]。

- 互いの鍵共有の際、予備通信を伴わない。
- ユーザ A がユーザ B との共有鍵 K_{AB} でメッセージを暗号化した場合、それを復号できるのはユーザ A を除けば、ユーザ B のみである。したがって、ユーザ B はメッセージを正しく復号できたならば、そのメッセージは確かにユーザ A によって生成されたものであることがわかる。

これらの特長は、エージェントシステムを構築する際には都合が良い。なぜなら、モバイルエージェントはプログラムであるため、一般にテキストデータよりも容量が大きくなりがちである。よって、頻繁に通信する必要があれば、かえって通信コストは大きくなってしまうので、鍵共有の際、予備通信を伴わなければ通信コストを抑えることができる。また、共有鍵で認証するため、エージェントの認証に必要なデータも減らすことができる。

2.2 ID-NIKS の一般的なプロトコル

ID-NIKS の一般的なプロトコルを図 1に示す。

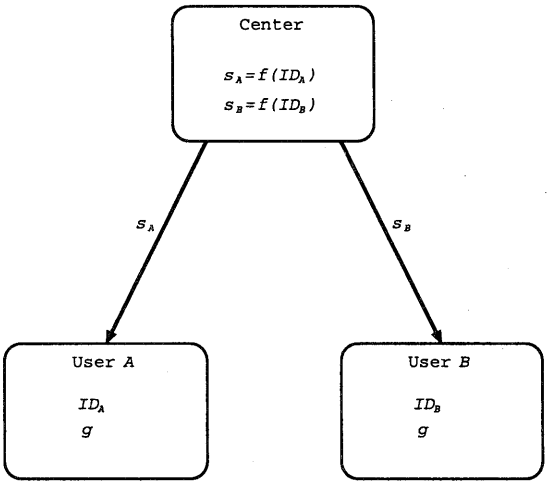

図 1: Overview of ID-NIKS

仮定

1. センタはユーザ i の ID 情報 ID_iを入力するとユーザ i の秘密情報 s_iを出力する秘密情報生成関数 $f, f(ID_i) = s_i$を秘密に持つ。

2. ユーザ i は (i は全てのユーザ) 自分の秘密情報 s_iと鍵を共有する相手 j(jは全てのユーザ) の ID 情報 ID_jを入力すると共有鍵 K_{ij}を出力する共有鍵生成関数 $g, g(s_i, ID_j) = K_{ij}$を持つ。(全てのユーザ共通の関数)

3. ユーザ i とユーザ jが鍵共有の際互いに生成する共有鍵 K_{ij}と K_{ji}の間には、$K_{ij} = K_{ji}$という関係が必ず成り立つ。したがって鍵共有関数 Fは、

$$\begin{aligned} g(s_i, ID_j) &= g(f(ID_i), ID_j) = F(ID_i, ID_j) \\ g(s_j, ID_i) &= g(f(ID_j), ID_i) = F(ID_j, ID_i) \\ \therefore F(ID_i, ID_j) &= F(ID_j, ID_i) \end{aligned}$$

   という関係を満たすので、Fは対称関数である。

4. 全てのユーザはある決まった暗号化関数 Eとその復号関数 Dを持っている。

以上の仮定に基づき、ユーザ A とユーザ Bが、鍵共有と暗号通信をする際の手続きを示す。

センタ (準備)

1. センタはユーザ A とユーザ B の秘密情報 s_A, s_B をそれぞれの ID 情報 ID_A, ID_B と秘密情報生成関数 f を用いて生成する。
2. 生成した秘密情報 s_A, s_B を安全な通信路を用いて A, B に送る。

鍵共有とメッセージの送信 (ユーザ A)

1. ユーザ A は秘密情報 s_A とユーザ B の ID 情報 ID_B から、共有鍵 $K_{AB} = g(s_A, ID_B)$ を生成する。
2. 生成した共有鍵 K_{AB} と暗号化関数 E を用いてメッセージ M を暗号化する。
3. 暗号化したメッセージ $E(M)$ をユーザ B へ送信する。

鍵共有とメッセージの受信 (ユーザ B)

1. ユーザ B は暗号化されたメッセージ $E(M)$ をユーザ A から受け取る。
2. 秘密情報 s_B とユーザ A の ID 情報 ID_A から $K_{BA} = g(s_B, ID_A)$ を生成する。
3. 生成した共有鍵 K_{BA} と復号関数 D を用いてメッセージ $M = D(E(M))$ を復号する。

3 ID-NIKS を用いた安全なモバイルエージェント

3.1 プロトコル

ID-NIKS を用いた安全なモバイルエージェントシステムの応用例として、商品購入エージェントシステムを図 2に示す。

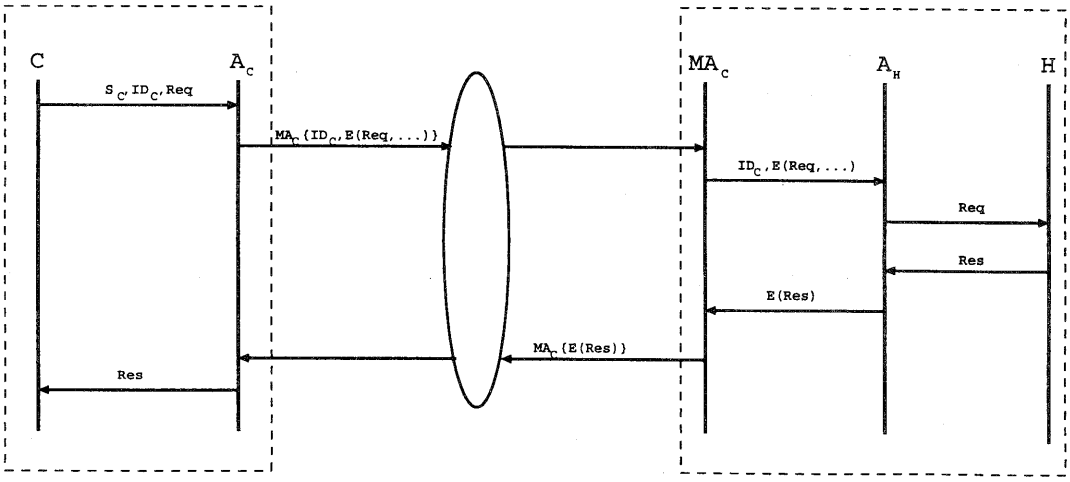

図 2: Secure Agent System with ID-NIKS

仮定

- ユーザ (C) は、買いたい物が何か決まっている。
- ホスト (H) は、商品購入の受け付けサービスを行っている。
- ユーザとホスト (H) は、ある ID-NIKS のメンバである。よって、
  - ユーザは ID-NIKS の秘密情報 s_C を既に持っている。
  - ホストは ID-NIKS の秘密情報 s_H を既に持っている。
  - ユーザおよびホストは共有鍵生成関数 g を持っている。
  - ユーザおよびホストのエージェント A_C, MA_C, A_H は正しく動作する。

3.2 プロトコル

1. ユーザ C は、ホスト H の ID 情報 ID_H、および商品購入リクエスト Req をエージェント A_C に渡す。
2. A_C は秘密情報 s_C、ID 情報 ID_H および共有鍵生成関数 g を用いて共有鍵 $K_{CH} = g(s_C, ID_H)$ を生成しそれを用いて Req を暗号化する。
3. エージェントは自身のコード部分のハッシュ値 h を共有鍵 K_{CH} を用いて暗号化する。
4. モバイルエージェント MA_C は $E(Req), E(h), ID_C$ を内部データとして持って H へ移動する
5. ホストエージェント A_H は MA_C から $E(Req), E(h), ID_C$ を受け取る。
6. A_H は ID_C、秘密情報 s_H および g を用いて共有鍵 $K_{HC} = g(s_H, ID_C)$ を生成し $E(h)$ を復号し、h が正しい値であることを確認した後、$E(Req)$ を復号して Req を取り出す。
7. Req に記述されている内容を H が受領するかしないかを判断し、その旨 Res を A_H を通して K_{HC} で暗号化して A_C に伝える。
8. MA_C は $E(Res)$ を受け取った後、ユーザの元へ移動する。
9. A_C は MA_C から $E(Res)$ を受け取り、復号してユーザに Res を渡す。

4 システムにおける安全性の評価

変数

先に示した応用例で用いている変数は以下のように分類できる。

公開情報 : $ID_C, ID_H, E(Req), E(Res), h, g$

センタの秘密情報 : f

ユーザの秘密情報 : s_C

ホストの秘密情報 : s_H

ユーザ, ホスト間の共有情報 : $K_{CH} = K_{HC}, Req, Res$

これらに関する安全性は、ID-NIKS の変数と同様なので、使用する ID-NIKS と暗号システムの強度に依存する。

ノード間認証

本システムでは共通鍵を用いた認証を行う。よって、共通鍵 $K_{CH} = K_{HC}$ が外部に洩れないようにしなければならない。

記述言語の安全性

モバイルエージェントのコードに関して、本システムではコードのハッシュ値を共有鍵で暗号化することにより、署名を施している。よって、ホスト側はコードの所有者の特定をできるようになっている。しかし、たとえ所有者が特定できたとしても重大な被害が出てからでは遅いので、モバイルエージェントの記述言語として実行コードの解析と危険なコードの排除をする言語を用いる必要がある。

5 まとめ

本論文では、ID-NIKS の特長がエージェント技術の安全面における課題を解決するのに適していることに着目し、ID-NIKS を用いた安全なモバイルエージェントの構築法の提案と安全性の検証をした。本論文の例では、1 対 1 の基本的なモデルについて考察したが、今後、複数ノードを移動するようなモバイルエージェントへの応用について考察する。

謝辞

本論文の作成にあたり、数々の有意義な意見を頂いた多田 充先生, 双紙 正和先生および研究室の皆さんに心から感謝致します。

参考文献

[1] K. Nagao, “最新エージェント技術”, bit Vol.31 No.2, pp.3-6, 共立出版, Feb 1999.

[2] T. Sander, C. F. Tschudin, “Towards Mobile Cryptography”, IEEE Symposium on Security and Privacy, pp.215-224, IEEE Computer Society Press, 1998.

[3] R. S. Gray, “Agent Tcl: A flexible and secure mobile-agent system”, Proceedings of Fourth Annual Usenix Tcl/Tk Workshop, pp.9-23, 1996.

[4] T. Nakajima, T. Watanabe, “Distributed Object Technologies and Mobile Agents”, The Journal of The Institute of Electronics, Information and Communication Engineers(IEICE) Vol.80 No.4 pp.357-363, 1997-4.

[5] Y. Murakami, M. Kasahara, “New ID-Based Non-Interactive Key Sharing Schemes”, Technical Report of The Institute of Electronics, Information and Communication Engineers(IEICE), ISEC98-31, 1998-9.

[6] T. Matsumoto, H. Imai, “On the KEY PREDISTRIBUTION SYSTEM: A Practical Solution to the Key Distribution Problem”, Advances in Cryptology: Proc. of CRYPTO’87, LNCS 293, pp.185-193, Springer-Verlag, 1987.