M-069　アドホックネットワークにおけるセキュアな通信方法の提案

Research on Secure Communication in Mobile Ad Hoc Networks

山口 健輔 *　　**中山 雅哉** *

1. はじめに

近年、インフラを介さない携帯端末同士の通信形態としてアドホックネットワークが注目されている。アドホックネットワークでは、場所を選ばずにネットワークを構成できるという利点を損なわないために、認証サーバなどのインフラを仮定せずにセキュアな通信手段を確立することが望まれる。また、有線ネットワークに比べて、各ノードがネットワークの障害や物理的な障害によって他のノードと通信できなくなることが頻繁に起こりうるので、単一のノードにセキュリティ管理などの重要な役目を任せるべきではない。そこで本稿では、複数のリーダーノードが (k,n) 閾値法を用いて証明書発行用の秘密鍵のデータを分割して保持し、ネットワークに参加するノードに対して公開鍵とアドレスが組になった証明書を協力して発行することによって公開鍵暗号で用いる公開鍵の正しさを周囲のノードに証明する手段をネットワーク内のノードに提供するという手法を提案し、その有効性を示す。

2. 既存手法の問題点とその解決案

現在メッセージの暗号化および復号の手段として公開鍵暗号方式が広く用いられている。他のノードの公開鍵の正しさを確認する際には一般的にはＣＡ（Certificatioin Authority ／認証局）に公開鍵の正しさを証明する証明書を発行してもらうという手段をとることが多い。ところが、アドホックネットワークでは外部との通信が行えない場面でネットワークを構成することが考えられるため、外部のＣＡの存在に頼ると公開鍵を更新した時などに証明書を更新できなくなる可能性があるので、外部のＣＡに頼るべきではない。よって内部に認証ノードを配置することが考えられるが、アドホックネットワークではネットワークのトポロジが頻繁に変化し、リンクの切断や切り替えが頻繁に起こる事態も想定されるので、単一の認証ノードに頼ってはならない。この２点を考えると、アドホックネットワークにおいては複数の認証ノードをネットワーク内部に配置することが望ましいと考えられる。

複数の認証ノードを配置する手段として、まず同じ機能を持った複数の CA をアドホックネットワーク内に配置するという手段が考えられる。ところが、この手段では一つの CA が悪意のあるユーザに乗っ取られると、そのユーザに偽の証明書を作られてしまう。このような脆弱性を生まないために、一定数以上の CA に発行してもらった証明書だけをネットワーク内で使用できるような仕組みが望まれるが、そのためには証明書に一定数以上の CA によって発行されたという証明を付加する必要がある。

この要求を満たす手法として、(k, n) 閾値法を用いた手法 [3] が提案されている。(k, n) 閾値法とは、ある秘密データを n 個に分割した後、元の秘密データを復元するためには分割されたデータのうちの任意の k 個が必要であるという手法である。[3] で提案された手法では、まず証明書に署名するための秘密鍵を (k, n) 閾値法で分割して複数の CA(server) で保持しておく。そしてあるノードが他のノードと通信する際に、その通信相手の公開鍵の証明書に秘密鍵の分割データで署名したもの（証明書の分割データ）を server 群に発行してもらい、それが k 個以上集まったら証明書を復元し、通信相手の正しい公開鍵を入手する。この手法では (k, n) 閾値法を用いることによって、k 個以上の server が乗っ取られなければ偽の証明書を発行することができなくなっており、復元された証明書の存在自体が k 個以上の server から分割データが発行されたという証明になっている。

ところが、この手法では新たなノードと通信を始めるたびに証明書を発行してもらう必要があるため、一つのノードが多数のノードと通信することを考えると server 大量の証明書発行のリクエストが集まり、server の負荷が増大してしまうことが考えられる。また、新たなノードと通信を行おうとするたびに複数の server にリクエストを送って証明書の分割データの受信を待つ必要があるという欠点もある。

そこで本稿では、証明書を発行するための秘密鍵を (k, n) 閾値法を用いて複数のリーダーノードが分割して保持し、各ノードがネットワーク参加時に自らの証明書を発行してもらい、その証明書を他のノードとの通信時に通信相手に送ることによって自らの正しい公開鍵を入手させるという手法を提案する。

*東京大学大学院 新領域創成科学研究科

3. 提案手法

提案手法では、複数のリーダーが協力してネットワークに参加するノードの公開鍵とアドレスの組に対する証明書を発行し、各ノードがその証明書を通信相手のノードに送ることによって自らの正しい公開鍵を通信相手に入手させる。

まずネットワークの準備段階において、証明書を発行するリーダーノードを複数決めておく。そして、その中の一人が証明書を発行するための秘密鍵 Kcr と、それに対応する公開鍵 Kcu を生成する。Kcu はあらかじめすべてのノードに配布しておく。リーダーノードはこの Kcr を (k, n) 閾値法で分割して、その分割データを保持する。なお、どの分割データも他の分割データと異なるものとする。(k, n) 閾値法とは、ある秘密データを n 個に分割し、そのうちの任意の k 個から元のデータを復元できるが、どの k-1 個からも元のデータは復元できないという手法である。ネットワークに参加するノードは最初に参加要求をブロードキャストし、それを受け取ったリーダーノードは閾値法によって分割された形の証明書をそのノードに発行する。そのノードは分割された証明書を K 個以上集めたら、完全な形の証明書を復元することができる。なお、(k, n) 閾値法による分割及び結合については、[2] に詳しく示されている。そして各ノードは、Route Discovery の際に Route Request パケットに証明書を付加して相手ノードに送り、相手ノードは Route Reply に証明書を付加して Route Request の送信元ノードに送る。

3.0.1 有効性の検証

本手法は公開鍵の証明書をネットワーク内部の複数のリーダーノードが発行するという点で、場所や環境を選ばずにいつでもネットワークを構成できるというアドホックネットワークの利点を損なわずに公開鍵の証明機構を実現していると言える。

また、アドホックネットワークではネットワークのトポロジが頻繁に変化し、リンクの切断や切り替えが頻繁に起こる事態も想定されるので単一の認証ノードに頼ることは望ましくないが、本手法では (k, n) 閾値法を用いて複数のリーダーノードに認証機能を分散することで、最大 k-1 個のリーダーノードが悪意のあるユーザに乗っ取られても偽の証明書を発行することはできず、またいくつかのリーダーノードがネットワークの障害やノードの故障などによって通信できない状態に陥っても、k 個のリーダーノードと通信できさえすれば証明書を発行してもらうことができる。

さらに、[3] の手法では 1 台の server が発行する証明書の数は (ネットワーク内のノード数＊各ノードの平均通信相手ノード数) であるが、本手法では証明書の公開鍵の所有ノードがリーダーノードに証明書を一度だけ発行してもらって自ら他のノードに証明書を送るため、1 つのリーダーノードが発行する証明書の数は (ネットワーク内のノード数) だけである。現実には各ノードの平均通信相手ノード数が 1 以下であるような状況は稀であると考えられるので、一般的な状況下では本手法のリーダーノードの負荷は [3] の手法の server の負荷に比べて低いと言える。

また、[3] の手法では各ノードが他のノードと新たに通信を始めるたびに閾値以上の証明書の分割データを受信するのを待つ必要があるが、本手法ではネットワークの参加時に一回だけ待つだけでよい。つまり、相手ノードへの経路が分かっているとすると、ネットワークへの参加要求送信から最初のノードとの通信開始までの時間は両者で同じだが、２つ目以降のノードとの通信開始前には [3] の手法では相手の証明書の発行待ち時間が発生するが、本手法では待ち時間は発生しない。よって、各ノードの平均通信相手ノード数が 1 を超える場合、すなわち一般的な状況下においては、本手法に比べて [3] の手法では余分な待ち時間が発生すると言うことができる。

これらの点を考慮すると、本手法はアドホックネットワークにおいて有効であり、[3] の手法よりも優れていると言える。

4. おわりに

本稿では、複数のリーダーノードが (k,n) 閾値法を用いて証明書発行用の秘密鍵データを分割して保持し、ネットワークに参加するノードに対して公開鍵とアドレスが組になった証明書を協力して発行するという手法を提案し、その有効性を示した。

参考文献

[1] Haiyun Luo, Petros Zerfos, Jiejun Kong, Songwu Lu, Lixia Zhang. ”Self-securing Ad Hoc Wireless Networks”. (2002)

[2] Jiejun Kong, Petros Zerfos, Haiyun Luo, Songwu Lu, Lixia Zhang. ”Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks”. International Conference on Network Protocols (ICNP). (2001)

[3] Lidong Zhou, Zygmunt J. Haas. ”Securing Ad Hoc Networks”.(1999)