1S－2

移動透過型通信環境を実現するための セキュリティ機構の設計と実装

新井 仁[1] 永田 智大[3] 岩本 健嗣[3] 徳田 英幸[2,3]

[1]慶應義塾大学 総合政策学部
[2]慶應義塾大学 環境情報学部 [3]慶應義塾大学大学院 政策・メディア研究科

1 はじめに

近年の携帯情報端末の小型化および普及，無線LAN規格であるIEEE802.11[1]の標準化などにより，携帯情報端末によって構成される，Ad-hocネットワークなどの無線ネットワークが頻繁に利用されるようになっている．

しかし，無線を前提としたネットワークでは，その盗聴や接続の容易性などから，有線ネットワーク以上に安全性について考慮する必要がある．このため，無線データリンクをより安全に確立させる枠組みが必要となる．しかし，その安全性の実現のためにユーザへの義務を増やすことは，ユーザに対しての繁雑な作業を増やすことになり，避けねばならない．

本稿では，さまざまな無線ネットワークインタフェースに対応可能かつネットワークプロトコルを限定しない，Ad-hocネットワークを構築するための包括的な機構Gordiusを提案し，その一部であり，安全かつ容易な無線データリンク機構SDMについて述べる．

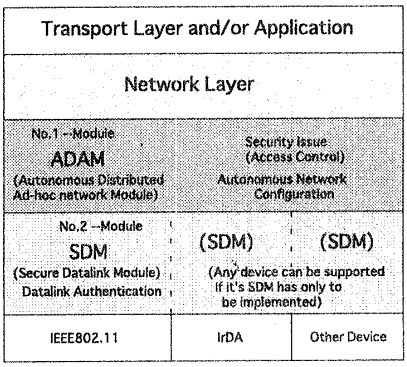

図 1: Gordius概要

2 Gordiusの概要

Ad-hocネットワークを構築するための機構であるGordiusは，ネットワークインタフェースに依存する機構を実現するSDM (Secure Datalink Module)と，ネットワークインタフェースに依存しない機構を実現するADAM (Autonomous Distributed Ad-hoc network Module)の二つのモジュールからなる．これらにより安全かつ容易な無線データリンクを実現し，SDMはデータリンク認証のためにTHAM(Two-way Handshake Authentication Model, 2.2章)を実装する．

2.1 SDMの概要と設計

SDMは，Gordiusの中においてネットワークインタフェース毎のセキュリティに関する機能の差位を吸収し，デバイスドライバの中に組み込まれる形で提供されるモジュールである．各ネットワークインタフェースに対してSDMを実装することで，多様なインタフェースを用いたAd-hocネットワークを実現できる．また，以下のような機構を実現する．

データリンク認証の実装:
無線データリンクは通常，電波や信号の可聴範囲内であれば必ず確立してしまう．これは接続が容易である反面，盗聴の危険を常に孕んでいる．この問題を解決するために，データリンクを確立させるための，パスフレーズのような鍵を元に認証を行う．

通信の暗号化:
認証後の通信をより安全に行うために，SDMを経由する通信すべてを暗号化する．データリンク認証によって得られる，WaveLAN-IEEEにおけるS-SID(Service Set ID, 3章)のようなネットワーク識別子を鍵とする暗号化を行う．

ネットワークへのアクセスコントロール支援:
ADAMの保持するアクセスコントロールリストを支援し，またこれを利用したデータリンク認証を行う．

またSDMは，その認証において以下の4つのモードを持つ．これらは，ADAMが保持するアクセスコントロールリストに基づく認証手段の種類である．

Log onモード
アクセスコントロールリストに自らの登録があるノードが，それを利用して認証を行うためのモード．

Guestモード
アクセスコントロールリストに自らの登録がないノードが認証を行うためのモード．

Sign onモード
アクセスコントロールリストに自らの登録がないノードが，自らを登録しつつ認証を行うためのモード．

Buildモード
自らを中心とした，全く新たなアクセスコントロールリストを構築し，新たなネットワークを構築するためのモード．接続する相手ノードを認証することになる．

Security Architecture for mobile ad-hoc communication environment

[1]Faculty of Policy Management, Keio University
5322, Endo, Fujisawa, Kanagawa 252, Japan
E-Mail: arajin@ht.sfc.keio.ac.jp
[2]Faculty of Environmental Information, Keio University
[3]Graduate School of Media and Governance, Keio University

2.2 THAMの概要と設計

THAMとは，SDMに実装される認証モデルであり，以下の二つの認証フェーズからなる．

要求フェーズ–Request phase:
認証専用の接続を相手に要求し，その接続が確立するまでのフェーズ．認証を行う相手を特定し，その相手との一対一の接続になる．どのようなネットワークインタフェースにでも対応できるように，このフレームワークにおいて特別な方法を規定はせず，要求を成立させるための手段は任意である．

認証フェーズ–Authentication Phase:
要求フェーズが成立した後に入るフェーズ．実際に認証に必要な情報を交換する．要求フェーズにおける成立条件と同様，認証のための鍵は任意である．

2.3 ADAMの概要

ADAMは，ネットワークインタフェースに依存しない部分を実現する．具体的には，データリンクのアクセスコントロールやSDMによって提供される認証機構の設定の繁雑さの回避などである．

アクセスコントロールリストには，以下の3つが登録される．

インタフェースID
MACアドレスのような，ネットワークインタフェース固有の識別子．

ADAM ID
ADAM起動時に任意の値として生成される，論理的な識別子．

パスフレーズ
ユーザが登録時に指定する．ユーザの識別子となる．

3 IEEE802.11用SDMの実装

本稿ではSDMの一例として，IEEE802.11に準拠した無線LANインタフェースであるWaveLAN-IEEEの，FreeBSD-3.2におけるデバイスドライバを改変した．

WaveLAN-IEEEでは，ある一つのネットワークを識別するために，SSIDという30バイトの文字列からなる識別子がある．これが同一でないとデータリンクは確立しない．これをWaveLAN-IEEEにおけるTHAM認証で得て，トークンとして用いる．図2に，その動作概要を示す．なお，この図におけるNode Aはこれから認証を受けるノードであり，Node Bはその認証を行うノードである．このときNode AのSSIDは，*ANY*という，任意のSSIDとして機能するものに設定される．

要求フェーズ

要求フェーズは，認証を要求する段階であり，認証を受けるノード(Node A)からのauthconnectにより開始する．authacceptにより認証するノード(Node B)からの返事が，Node Aにより受けとられることで終了する．

authconnectは，ブロードキャストによって可聴範囲にいる相手全体に対して要求する．この要求を受けとった全てのノードはauthacceptを返信する．Node Aが実際に通信相手として選択するのは，最も早くauthacceptを受け取ったノード(Node B)だけである．

認証の間に使用される固有のSSIDを設定するため，authacceptを送信するノードは，任意のSSIDを送信する．Node Aは，これを受けとったことをNode Bに確認させるために返信を行う．この後，Node AとNode Bによる一対一の通信を確立するために両者が任意の，かつ同一のSSIDに設定される．

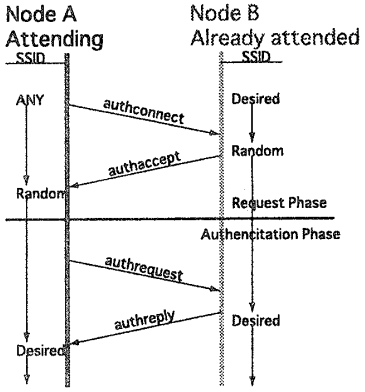

図 2: THAM動作概要

認証フェーズ

認証フェーズは，要求フェーズにより確立された一対一の通信上で行われる．

Node Aが，authrequestにより認証に必要な情報をNode Bに対して送信する．これを元にNode BはNode Aの認証を行う．それが成功すると，Node Bはauthreplyによって適正なSSIDを送信する．Node Aがそれを受けとることで認証が完了し，Node Aがネットワークに参加することが認められる．

4 関連研究

本研究と目的を同じくしたシステムとして，IEEE802.11における暗号化機構WEPがある．しかしこれは通信の暗号化レベルを「十分である必要はない」としており，またIEEE802.11規格に沿ったものにしか対応できないという点で本研究とは異なっている．

5 まとめと今後の課題

本稿では，安全かつ簡易に無線データリンクを確立させるための機構であるGordiusと，その一部として機能するSDMについて述べた．今後はADAMの実装およびシステムの実装を行い，測定，評価を行う．また，4章で述べたシステムとの比較，評価も行う．

参考文献

[1] IEEE Standards Board "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications", LAN MAN Standards committee of the IEEE Computer society, 1997

[2] Leo Monteban and WaveLAN/IEEE System Team "Software Interface Specification for Wireless Connection Interface for WaveLAN/IEEE", Lucent Technologies, 1999