卒業論文 1999 年度 (平成 11 年度)

Ad-hoc ネットワークにおける安全な無線データリンクの設計と実装

慶應義塾大学 総合政策学部
徳田研究会 新井 仁
学籍番号 *79600237*
arajin@ht.sfc.keio.ac.jp

卒業論文要旨　　1999年度(平成11年度)

Ad-hocネットワークにおける安全な無線データリンクの設計と実装

概　　要

近年，無線通信媒体の利用により接続機器の携帯性や可搬性を積極的に活かした移動型通信環境の構築が可能となり，今までの技術では実現できなかった領域でのネットワーク構築が現実のものとなりつつある．

無線通信媒体にはいくつか利点がある．有線通信媒体のようなケーブルなどの敷設の手間がなく，低いコストでネットワークを構築できる．また地理的な束縛を受けず，ノート型コンピュータやPDAのような小型計算機の可搬性を損なうこともない．

この無線通信媒体を用いた応用例の一つにAd-hocネットワークがある．Ad-hocネットワークは，無線通信媒体の特性を最大限に活かせる応用例として注目されている．Ad-hocネットワークの最大の特徴は，無線通信媒体によるネットワーク構成の自由度および容易な接続にある．時間的あるいは地理的に一時的なネットワークを構築する際に，ユーザは技術的な要求をされず，またネットワーク内を任意に動くことができる．

これらの利点により，Ad-hocネットワークはウェアラブルコンピューティングなど多様な分野への応用が期待されている．しかし，無線通信は空間全体を媒体として用いるため情報が漏洩しやすいという安全性の問題を持つ．また，同様の理由で，意図しない間接的な接続が容易にできてしまう．このような問題が，無線媒体の応用を制約していると言える．

本研究ではAd-hocネットワークを実現するための統合通信環境Gordiusを提案し，統合的な手法でこれらの問題を解決した．Gordiusを用いることで，Ad-hocネットワークにおける無線通信媒体の利点を損なうことなく安全なデータリンクを構築でき，また多様なデバイスで安全な無線通信を実現する．

そしてこのGordiusのうち，データリンク認証および暗号化を実現する機構ADAM (Autonomous Distributed Authentication Module)と，無線機器の違いを上位層から隠蔽しADAMを支援するプロトコルSDP (Secure Datalink Protocol)を設計，実装した．

結果として，Gordiusによりわずかなオーバーヘッドで安全なデータリンクを構築できた．また統合環境として構築したことで，他の関連研究と比較して様々な上位プロトコルやデバイスとの親和性を高めることができた．

キーワード:
1: 無線LAN　　2: Ad-hocネットワーク　　3: セキュリティ　　4: 認証

Abstract of Graduation Thesis Academic Year 1999

Design and Implementation of Secure Wireless Datalink in Ad-hoc Network Environment

Abstract

Within these years, the network communication through wireless medium has allowed us to construct of a mobile communication environment, owing to the advantages of mobility and portability in communication devices. Such improvements realized the new networking environment which has never been before.

Wireless medium have advantages in being used in network communication. Unlike wired medium, the burden of cabling construction or reconstruction can be reduced or avoided, which enables network construction at low costs.

Also wireless medium neither restrict the computing location nor spoil the portability of small, lightweight computers such as laptops and PDAs.

A new networking environment called “ad-hoc network” is drawing attention as one of the applied example which makes use of the advantages described above.

The distinguished characteristics of ad-hoc network are the flexibility of network topology and the ease of connection. It will not require a high skill from users to construct a temporary “ad-hoc” network, and he or she will be able to move freely within it. Due to these benefits, the ad-hoc network technology is expected to be applied on various fields, such as wearable computing technology.

However, we must solve some problems to realize these advantages. Having preferable features described above, the wireless medium have the security problems against eavesdropping and undesired connection. This is due to the medium transmitted throughout the room.

This paper proposes an integrated communication environment Gordius as to solve these problems in diversified way and to materialize ad-hoc network. This paper describes also design and implementation of the two entities in Gordius . One is named ADAM (Autonomous Distributed Authentication Module), which plays the role of Data-link level authentication and encryption. The other is named SDP , which supports ADAM and conceals the differences of devices from upper layers.

In this paper, we proved that the secure Data-link can be materialized with little overhead and that integrated design of Gordius achieved familiarity with upper layer protocols and lower layer devices.

Keywords: 1: Wireless-LAN 2: Ad-hoc network 3: Security 4: Authentication

目 次

図 目 次

表 目 次

第1章

序論

1.1 はじめに

近年の通信技術の革新やコンピュータの多様化などを受け，光ファイバを用いた超高速通信，電波や赤外線などを用いた無線通信など，コンピュータや周辺機器を相互接続形態の多様化が進んでいる．その中において，移動しながらにコンピュータの利用やその相互接続を維持する移動型計算機環境についても様々な研究がなされている．

そうした背景を受け，無線LAN (Local Area Network) の標準規格が IEEE (Institute of Electrical and Electronics Engineering) の分科会でIEEE 802.11[1] として定められた．ISM (Industrial,Scientific and Medical) バンドにおいて，特別な認可を必要とせず使用でき，さらなる普及が進んでいる．

移動型計算機環境では，その接続の簡易さやケーブルなどによる地理的な束縛からの解放などを目的とし，無線媒体を利用することが多い．例として，電波や赤外線を用いたコンピュータとその周辺機器の接続や，小型コンピュータへの無線通信機能の組み込みなどが挙げられる．

多様化する通信環境の一例としては，主にIETF (Internet Engineering Task Force) における分科会の一つで研究されているMANET (Mobile Ad-hoc NETwork) に代表されるAd-hoc ネットワークという分野が挙げられる．Ad-hoc ネットワークとは，時間的かつ地理的に一時的なネットワークのことである．Ad-hoc ネットワークでは，無線媒体を前提とし，ネットワークを構成するコンピュータが任意に移動しながら通信できる．また，各コンピュータの経路制御により，ユーザは隣接する相手を意識する必要がない．すなわち，移動やそれに伴う地理的な環境の変化への適応性が高い．

このように無線媒体は非常に重要視されているが，その利用に伴う問題は数多く残されている．その主なものを以下に挙げる．

情報伝達経路の変化

相互に通信し合うコンピュータの移動により接続が変化する．

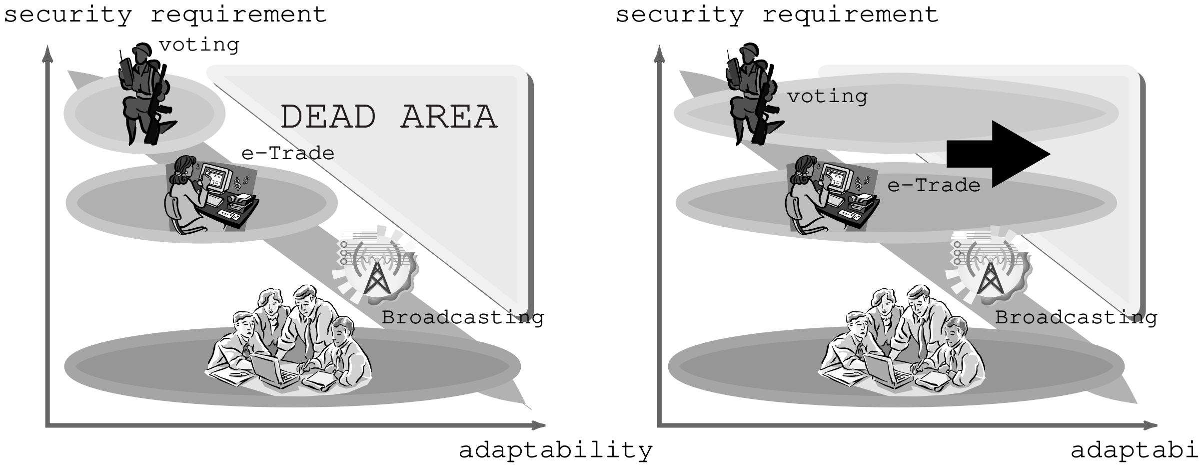
通信帯域の制約

有線媒体と比較して通信帯域が小さい．

安全性

空間を通して情報が伝わる無線媒体では，耐盗聴性や耐改竄性が低い．

こうした背景から，現在の計算機環境パラダイムは図1.1(a) に示すようになっている．すなわち，安全性と適応性は相反関係にある．



(a) current paradigm (b) paradigm shift

図 1.1: 計算機環境パラダイム

図1.1の例をとると，e-Tradeやe-Commerceと呼ばれる電子商取引をAd-hocネットワークで実現するためには，クレジットカード番号や個人情報を保護するために安全性を高める必要がある．現在のシステムでは適応性を低くせざるを得ず，そのため場所や時間などの自由度は失なわれる．

しかし図1.1(b)に示すように，安全性が高く，また適応的なネットワークが実現できると，ユーザは安全性を確保するために地理的あるいは時間的な制約を意識する必要がなくなる．

このように，適応性と安全性の両立は，次世代通信環境であるAd-hocネットワークの高度な応用の促進に必要不可欠である．この新たなパラダイムの実現には，前提技術である無線媒体の安全性向上および動的な環境変化に対応する経路制御機構が必要である．

現在，経路制御機構についてはIETF MANET分科会にて盛んに研究および議論がなされている．しかし安全性については，認証と暗号化の連携やAd-hocネットワークへの適応性などの面で解決されていない．従って，安全性の問題は経路制御の問題とは独立して解決されるべきである．

本研究ではこれらの環境を実現するため，Ad-hocネットワークでの利用を前提とした，安全かつ効率的な無線データリンク機構を提案する．

1.2 本研究の目的

本研究の目的は，Ad-hocネットワークにおいてその構築の簡易さや自由さを損なわずに安全なデータリンクを確立するシステムの提供である．

本論文では，先に述べたようなAd-hocネットワークにおける問題を解決する統合環境Gordiusを提案し，その一部としての安全なデータリンクを確立するためのシステムSDP (Secure Datalink Protocol)およびADAM (Autonomous Distributed Authentication Module)を設計，実装した．Gordiusを利用することで，有線通信に対して無線通信が必然的に受ける安全性の問題や，Ad-hocネットワークを構築する上での手続きなどのコストといった不利益をより低減することができる．

1.3 本論文の構成

本論文は，本章を含め全7章からなる．第2章において既存技術が持つ問題点を指摘・分析する．第3章では，本システムの概要について説明する．第4章でシステムの設計について，および第5章でその実装について述べる．第6章においてシステムの測定および評価を，第7章にてまとめと今後の課題について述べる．

第2章

既存技術とその問題点

現在，無線媒体を前提とした通信環境の応用例は非常に幅広く研究されている．本章では，その現状と問題点について分析する．

2.1 無線LAN

本節では，本研究の基盤技術である無線LANの概要について述べ，その問題点を指摘する．

2.1.1 無線LANの標準化

近年のコンピュータの小型化および軽量化に伴い，移動中のコンピュータの利用をユーザが望むようになってきた．そうした背景から，無線によるコンピュータネットワークが研究，開発された．

無線媒体をコンピュータネットワークに適用する利点はいくつかある．まずケーブルを敷設する手間がかからず，簡易にネットワークを構築できる．またコンピュータおよびその周辺機器を再配置する際に柔軟に対応できる．そして小型コンピュータの可搬性を損なうこともなく，ごく簡単に一時的なネットワークを構築できる．

このような利点から，無線LANは現在普及段階に入っており，1997年にIEEEが802.11として無線LANの規格標準化を行った．この規格は電波や赤外線を用いた適応的かつ自由なネットワークのための物理層およびデータリンク層について定めている．

近年ではこの規格に沿った通信装置も数多く製品化されている．しかし，まだ異種製品間での完全な互換性は保証されておらず，IEEE 802.11による標準化は完全なものとは言えない．

2.1.2 システム概要

IEEE 802.11により規定される無線LANシステムは，インフラストラクチャ型およびインディペンデント型がある．また，それぞれのシステムに適応するために，移動局は二種類の通信モードを切り替える．前者のシステムではインラストラクチャモード，後者のシステムではアドホックモードとよばれる通信形態が使用される．

本章では，本研究の基盤となるアドホックモードについて，用語を解説しながら説明する．また，インフラストラクチャモードについても簡単に触れる．

アドホックモード

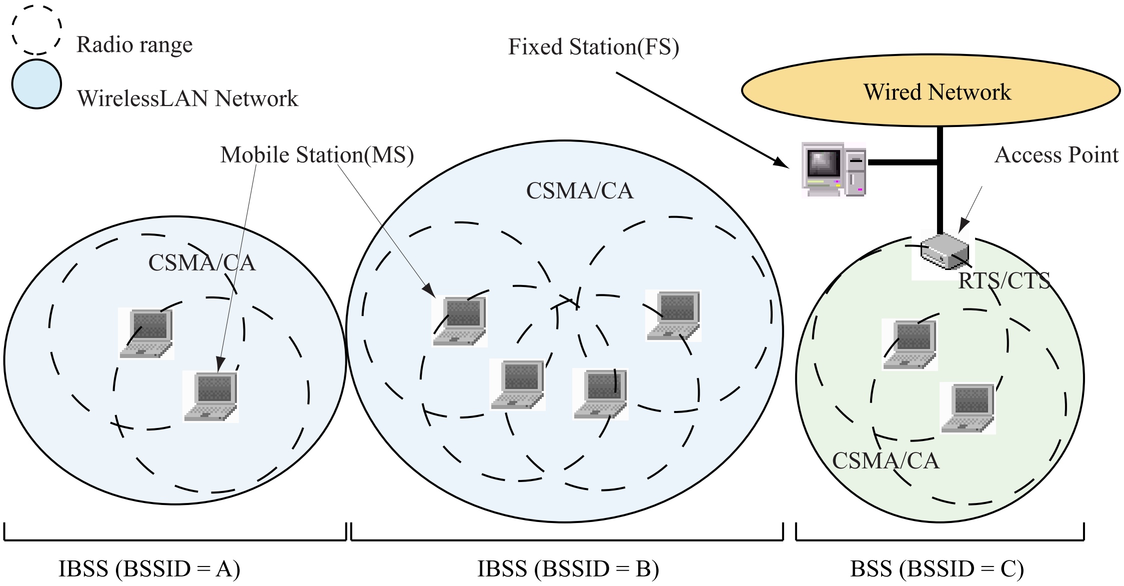


図 2.1: 無線 LAN システム概要

アドホックモードとはすべての無線端末が対等で，送信端末と受信端末が直接データを送受信する方式である．図2.1のSSID=AおよびBにその例を示す．後述するインフラストラクチャモードに比べて機器が少なくてすみ，システム構築に必要なコストを下げられるという利点がある．

以下において，図2.1中の用語について説明する．

MS(Mobile Station)

無線通信装置を備えたコンピュータあるいはその周辺機器．本論文では移動局と表す．

FS(Fixed Station)

移動局に対し，有線媒体でネットワークに接続され，移動することのないコンピュータおよびその周辺機器．本論文では固定局と表す．

AP(Access Point)

最低1つ以上の無線通信装置を備え，無線媒体間のブリッジ機構，もしくは無線媒体の可聴範囲を拡大するために用いられるリピータ機構を有する機器．有線通信装置を持ち，有線媒体と無線媒体の仲介も行なう．本論文では基地局と表す．

BSS(Basic Service Set)

ある領域において同じ無線チャネルを用いて通信する，複数の移動局および最低0個の基地局からなるネットワーク．

IBSS(Independent BSS)

基地局を含まないアドホックモードのBSS．本論文ではこれをAd-hocグループと表す．

BSSID(BSS Identifier)

個々のBSSおよびIBSSの識別子．本論文では，単にSSIDと表す．

CSMA/CA(Carrier Sense Multiple Access with Collision Avoidance)

無線LANシステムで採用される媒体アクセス制御方式．ある移動局が送信する前に他の移動局が電

波を発していないことを確認する．これをキャリアセンスという．有線媒体と異なり衝突検知が不可能なので，キャリアセンスした後，キャリアがなくても即時に送信を行なわずにランダムな時間を置いて再びキャリアセンスを行なってから発信する．しかし，複数の移動局が同時に送信を始めた場合には，電波の混信は検出できず，また回避できない．この場合，電波の混信を無視し，上位プロトコルにその処理は委ねることになる．

RTS/CTS(Ready To Send and Clear To Send)

無線LANシステムで採用される，隠れ端末問題[2]を回避するための方式．移動局がデータを送信する際，まず基地局にデータ送信要求パケットRTSを送信する．このパケットを受信した基地局はデータ送信を許可する応答パケットCTSを返信し，それを受け取った移動局だけがデータを送信できるようになる．そして端末は基地局へデータを送信し，基地局が目的の相手へ転送する．

インフラストラクチャモード

図2.1におけるSSID=Cのような接続方式をインフラストラクチャモードという．移動局のデータ送信や固定局との通信を集中制御する専用の基地局を設け，それを中心としたネットワークを構成する．このような媒体アクセス制御を行なうことで，電波の混信が起こる可能性を低くしている．しかし，基地局が移動局のデータ送信権を集中管理するため，基地局に何らかの障害が発生するとBSS全体が影響を受ける．また基地局はコストが高く，少数の移動局のみからなるネットワークでは費用対効果が低い．

2.1.3 無線LANの問題点

Ad-hocネットワークを実現する際に障害となる無線LANシステムの問題を以下にて分析する．

安全性

無線媒体は，それ自身に暗号化などの安全性を保証する機構を持たない．従って，それを利用した無線通信にも盗聴やなりすましといった安全性の問題がある．

また無線媒体の特性により，意図しないデータリンクが成立してしまう．例えば，あるコンピュータAが無線媒体で別のコンピュータBと接続されているとする．またBは同様にCと接続されている．しかし，AとCは接続されていない．この場合，BはAの情報をCに伝えることが可能であり，ここに意図しないデータリンクが起こる．この問題は，無線LANシステムが情報の転送に関して認証機構を持たないことによる．

スケーラビリティ

先述の通り，無線LANシステムではCSMA/CA方式の媒体アクセス制御で電波の混信を避ける．しかしこの方式でも多数の移動局による通信では混信を避けることが難しく，伝送速度が極端に低下する[3]．特に，基地局による媒体アクセス制御のないアドホックモードは，移動局が10台を越える規模のネットワークには向かない．

2.2 Ad-hocネットワーク

本節では，無線LANシステムの応用例であるAd-hocネットワークについて述べる．

2.2.1 Ad-hoc ネットワークの特徴

Ad-hoc ネットワークとは，無線媒体を通信手段として用いる複数の移動局からなり，時間的および空間的に制約を持つ自律ネットワークである．接続するユーザに対し技術的要求をせず，また既設の通信基盤を前提としないネットワーク構築を目的としている．

Ad-hoc ネットワークでは移動局の移動や無線媒体の状態に伴い接続形態が変化する．1 つのルータに対し複数の移動局が接続されており，ルータ自身も移動局の 1 つであることから，その接続は動的に変化する有向グラフとして表される．この概念を図2.2に示す．

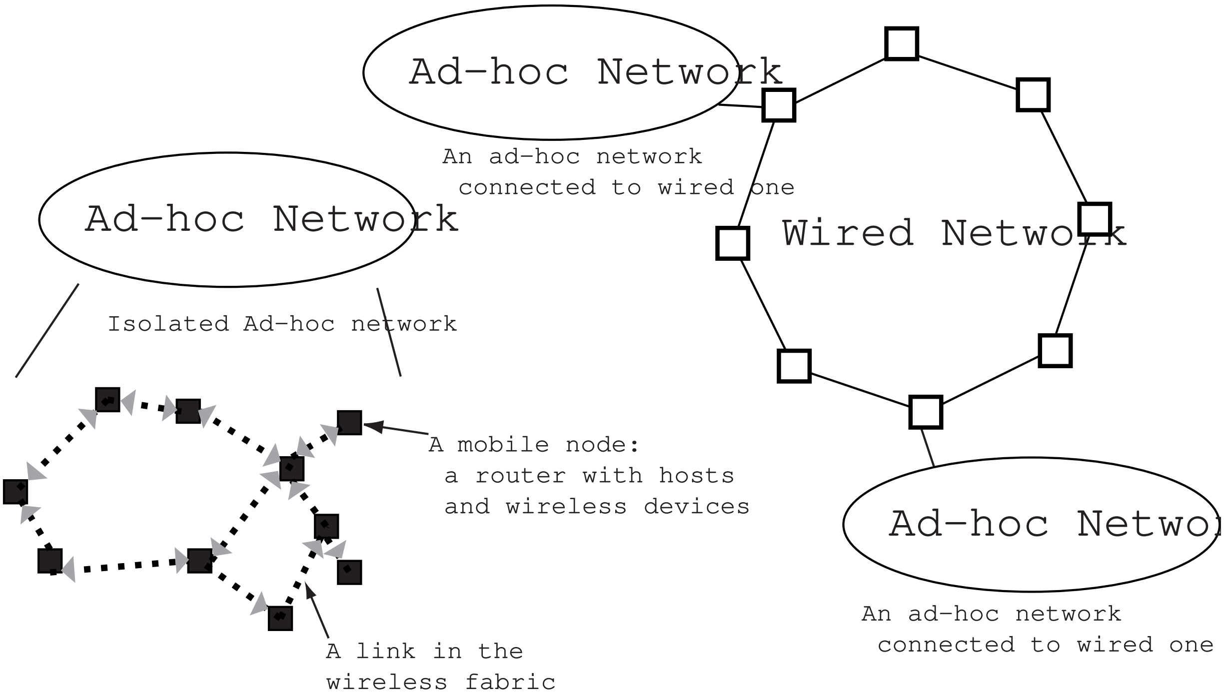


図 2.2: Ad-hoc ネットワーク概念図

これらの移動局が利用する無線媒体には，様々な特性のものがある．無線媒体には全方向性の電波も，また単方向性の衛星電波もある．赤外線のような指向性の強い光もある．そして受信機と送信機が単一の装置として機能するものや，それぞれが別々に機能するものもある．さらに，これらの装置が混在する環境においてもネットワークが確立される．

従って，移動局の接続はその位置やその受信機，送信機の可聴範囲，個々の受信レベルや無線媒体の干渉レベルなどにより，動的かつランダムに変化する．

2.2.2 Ad-hoc ネットワークの問題点

以上のような特徴を持つAd-hoc ネットワークにおいて，解決すべき問題は多数存在する．主なものについて以下で分析する．

データリンクの多様性

移動局がAd-hocネットワーク内を移動するため，データリンクの状態や相手が動的に変化する．すなわち隣接する移動局が変化する可能性がある．従って，あらゆる移動局は隣接する移動局を前提とすることなく動作しなければならない．

またAd-hocネットワークにおけるデータリンクシステムの設計では，様々なタイプの無線媒体を前提とする必要がある．具体的には，赤外線と電波，あるいは衛星からの電波とPCカードからの電波など，通信媒体の多様性を想定し，データリンク層として独立したシステムが必要である．しかし，現在ではそのようなデータリンクシステムは存在しない．

資源の制約

Ad-hocネットワークの移動局は小型かつ軽量なものが想定されている．すなわち，Ad-hocネットワークを構成する移動局は制限された資源しか持たない可能性がある．

コンピュータの小型化や軽量化が進み，処理能力の高いものが手のひらに収まる大きさになったとはいえ，固定的な利用を前提としているデスクトップ型などのコンピュータと比較すると，資源の面では不利である．

Ad-hocネットワークを構築するためには，こうした資源の制約についても考慮すべきである．

2.3 関連研究

本節では，無線LANやAd-hocネットワークおよびその安全性に関する研究について，それぞれの論旨と共に紹介する．

2.3.1 Security Architecture for Internet Protocol: IPsec

IPsec[4]は，IPv4[5]およびIPv6[6]における安全性の向上を目的として策定された．IPsecにより提供されるサービスには，アクセス制御，認証，暗号化が含まれる．これらは，以下の二つからなる．

- Authentication Header[7]
- Encapsulating Security Payload[8]

IPsecは様々なセキュリティサービスを組みあわせるための管理機構を提供し，柔軟にセキュリティシステムを構築できる．また，アルゴリズムそのものは規定していない．

IPsecでは，IPデータグラムに対する安全性保証の方針を安全性ポリシデータベース(SPD)に保持する．このSPDに基づき，通信の安全性が保証される．

これらの機能は，IPおよびその上位プロトコル全てにおいて有効である．

2.3.2 IEEE 802.11 Authentication and Privacy

IEEE 802.11では，Authentication Service および Wired Equivalent Privacy [1]という名称で認証と安全性についても規定している．

IEEE 802.11 Authentication service

IEEE 802.11では，以下に示す2種類の認証サービスを規定している．これらのサービスは，認証管理フレーム(Authentication Management Frame)と呼ばれるフレームを受け取ることで開始される．これらの認証は，インフラストラクチャモードでは基地局と移動局の間で，アドホックモードでは移動局同士の間で行なわれる．

Open system authentication

このサービスは，事実上認証の働きを持たない．認証を受ける側がこのサービスを要求することで，認証は成功されたとみなす．

Shared key authentication

このサービスでは，共有秘密鍵を用いて認証を行なう．認証を受ける側はこの共有秘密鍵を持っていても持っていなくても認証を受けることができる．ただし，後述するWEPを用いた通信を経由しなければならない．従って，WEPが実装されていないシステムにおいてはこのサービスは受けられない．この共有秘密鍵は，媒体アクセス制御機構を用い，書き込み専用のMIB[9]属性を持つ情報として交換されることにより，MAC管理機構の外に漏れることがない．

これらのサービスについては，認証のための方針を定め，送受信メッセージの概念的規定にとどまり，認証そのものについては規定していない．従って認証に使用するデータ，あるいはその送受信方法については実装に依存する．

Wired Equivalent Privacy: WEP

WEPは，無線媒体の本質的問題である盗聴への対策を目的とした，暗号化を元にデータの安全性を保証するアルゴリズムである．

暗号化のために，Authentication serviceを用いて得る共有秘密鍵と初期化ベクタ(Initialization Vector: IV)を用い，そのデータを交換するためのフレームフォーマットも規定されている．

この暗号化および復号化の概念図を図2.3に示す．盗聴から情報を守るため，無線媒体として情報を発信する前に，ある鍵を用いて暗号化する．そしてこの暗号化機構とは別に動く鍵管理サービスを用いて受信者に鍵を伝え，受信者はその鍵を元に復号化する．

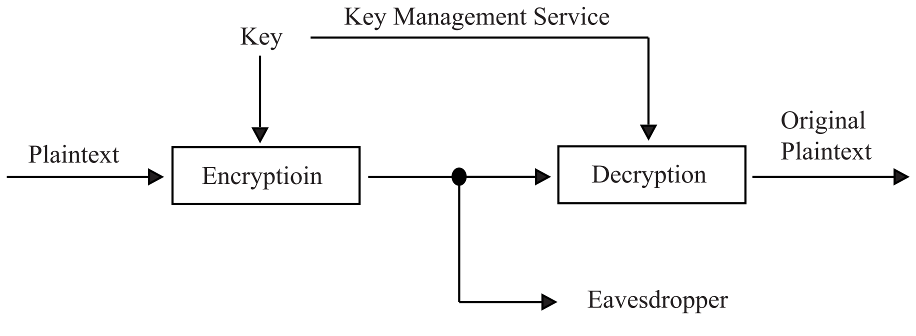


図 2.3: WEPによる暗号化/復号化概念図

なお，WEPは以下のような特徴を持つ．

堅牢性

WEPは暗号化および復号化のための鍵を任意に変更でき，また同様に初期化ベクタもある頻度で変

更することができる．これらにより，総当たり法(Brute-force technique)による暗号解読を事実上不可能にしている．

自律同期的

WEP自身が安全性に関するメッセージに同期し，自律的に状態を遷移する．すなわち，この安全性に対してユーザが受ける負荷はほとんどない．

選択可能

WEPによる暗号化は必須事項ではなく，選択可能である．

これらの特徴により無線LANシステムでの安全性は保証され，また認証によるアクセス制御も実現されている．

2.3.3 Internet MANET Encapsulation Protocol: IMEP

IMEP[10]は，2つの目的を持つネットワーク層のプロトコルである．このプロトコルは，Ad-hocネットワークを実現するための様々な経路制御アルゴリズムやネットワーク制御プロトコル，またその他の上位層プロトコルを支援するために開発されている．

このプロトコルの目的は第一に，ネットワーク全体のパフォーマンスを向上することが挙げられる．このためにIMEPでは，制御パケットや受信確認パケット，リンク状態検知のためのパケットなどといったブロードキャストされる制御パケットの数を低減するために，複数のパケットをまとめて送信する．

そして第二の目的は，様々なネットワーク層の制御アルゴリズムにおいて，共通の機能を提供することにある．Ad-hocネットワークには様々な制御アルゴリズムが存在するが，それらに共通して提供されなければならない情報はいくつかある．リンク状態検知，隣接するルータの検知とそれに対する認証，隣接する移動局の発見などがそれに当たる．これらの機能を，統一された形式で提供することで，多様な上位層プロトコルにおいて処理を簡略化できる．

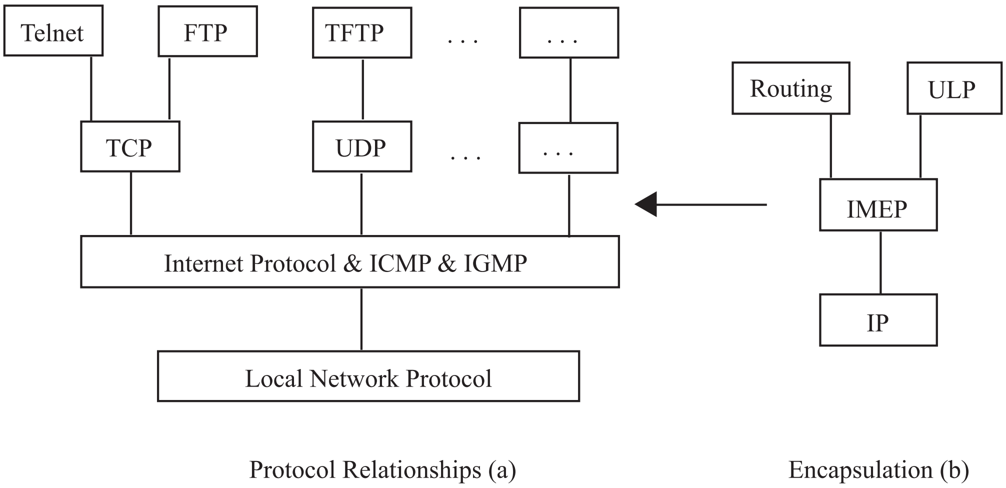


図 2.4: IMEP概念図

IMEPの概念図を図2.4に示す．IMEPはネットワーク層のプロトコルとして設計されている．既存のプロトコルスタックを図2.4(a)に示し，IMEPにより加えられるプロトコルスタックを図2.4(b)に示す．ま

た，IMEPによりカプセル化されたパケットが，図2.4(a)におけるInternet Protocolによりカプセル化されることになる．

なお，次節で述べるMAAはこのIMEPを前提としている．

2.3.4 MANET Authentication Architecture: MAA

MAA[11]は，IMEPおよびその上位層プロトコルで交換されるメッセージが認証されないことを根拠にAd-hocネットワークの脆弱性を指摘し，これを解決するために研究されている．MAAはIMEPを前提として動作する．またAd-hocネットワークを構成するルータは簡単なものから複雑なものまで様々な認証を受け入れることができる．

MAAで利用される認証のための情報を表2.1に示す．MAAはこれらの中から状況に最適なものを自由に選んで暗号化する．

表 2.1: MAA認証方式

タイプ	暗号化アルゴリズム	鍵長(bit)
001	秘密鍵およびMD5	128
002 to 009	ユーザ定義	ユーザ定義
011	RSA	512
012	RSA	768
013	RSA	1024
014	RSA	2048
021	Elliptic Curve	80
022	Elliptic Curve	120
023	Elliptic Curve	160
030	DSA	512

また，認証のために以下の情報を扱う．

Distinguished Name (DN)
情報を送る主体のRID．

CA Distinguished Name (CADN)
一人以上のユーザによって認証を受けたDN．

Public Key
情報を送る主体の持つ公開鍵．

Public Key Algorithm
表2.1に示すタイプのいずれか．

CA Digital Signature
情報を送る主体に対するCADNの署名．情報の正当性を保証するために用いる．

これらの機能により，MANETにおける認証機構が実現されている．

2.4 問題の指摘と分析

以下において，前節で挙げた関連研究の分析を行ない，その問題の指摘を指摘する．

2.4.1 暗号化

本章で挙げた関連研究では，IPsec，WEP，MAA が暗号化による安全性や堅牢性について定めている．このいずれも具体的な暗号方式については定めておらず，実装に依存する形で柔軟性を持たせている．

この設計方針は，安全性および堅牢性が実装に強く依存してしまう代わりに，将来より強力な暗号方式が開発された際にも対応できる．唯一 MAA のみが暗号方式を規定しているが，前節で述べた通りユーザが定義可能なフィールドが残されており，拡張性を持たせている．

2.4.2 Ad-hoc ネットワークへの適応性

IPsec は，Ad-hoc ネットワークに限定したものではなく，IP を用いたネットワーク全般に適用することを目的としている．一方 WEP，MAA は，Ad-hoc ネットワークにおける利用を前提として設計されている．

Ad-hoc ネットワークにおける問題点は第2.2.2項に示した通りである．以下では，各問題点について関連研究を分析する．

IPsec

IEEE 802.11 で規定されるアドホックモードでのスケーラビリティが十数台でとどまることから，IP のアドレス空間は大きすぎ，経路制御に関する制御情報およびその処理は不必要に大きい．この面から，IPsec は処理能力および記憶資源の制約に対し問題を持つ．

また，Ad-hoc ネットワークは特定のネットワークプロトコルを仮定しないため，ネットワークプロトコルである IP を前提とする IPsec は，その有効性に疑問がある．

WEP

WEP では暗号化方式および認証方式について実装に依存する形式で定められている．従って処理能力や記憶資源の制約については実装に依存する．

また WEP は一対一の認証を行なう機構を持つが，複数の移動局をグループとしてまとめ，そのグループに対する認証を行なうことができない．従って，無線 LAN システムが持つ情報の転送に関する安全性の問題を解決できない．

MAA + IMEP

MAA は，併用する IMEP が，他の層との協調性を提供する．

また MAA では認証のための情報を暗号化する機能を持つ．しかし，制御パケット以外の通信を暗号化する機能を持たないので，MAA 単体が保証する安全性は必ずしも十分とは言えない．

上記の分析をまとめたのが表2.2である．Ad-hoc ネットワーク通信の安全性保証機構として見た場合，各関連研究には多くの問題がある．その中でも特に重要な課題は，Ad-hoc ネットワークに適した認証機構への対応と，他の機構と連携した効率的な安全性の保証である．

表 2.2: Ad-hocネットワークに対する定性的比較

問題点	**IPsec**	**WEP**	**MAA**
Ad-hocネットワークへの適応性			
処理能力	△	○	○
記憶資源	×	○	○
協調性	×	×	○
汎用性	○	×	×

○ :適している，または安全　△ :中程度　× :適していない，または安全でない

2.4.3 問題点のまとめ

Ad-hocネットワークは複数の移動局からなり，その接続形態は動的に変化する．この差を吸収し，同時に無線媒体の本質的問題である安全性の問題を解決する機構が不可欠である．関連研究として紹介したIPsec，IMEP，WEP，MAAはいずれも以下の問題を解決しているとは言えない．

データリンクと他層の連携

接続形態の変化，多様な無線媒体の存在といったAd-hocネットワークの多様性に対応するための，他層との協調性が高いデータリンク機構がない．

データリンク層での安全性

現在議論されているネットワーク層のプロトコルに柔軟に対応した，安全性を保証するための機構がない．

以上のことから，安全性を保証するデータリンク機構を構築することが現在のAd-hocネットワークにおける課題である．

第3章

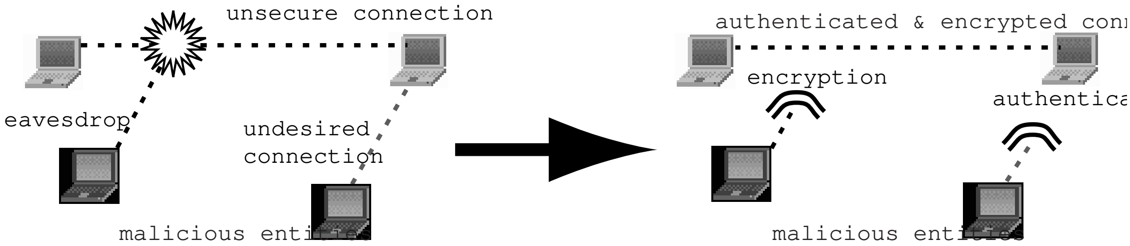
システム概要

前章では既存技術の紹介を行ない，それを元にAd-hocネットワークを実現するための問題点として協調的かつ効率的に安全性を保証するための機構が存在しないことを指摘した．また同時に，その実現のために無線媒体の利点である自由かつ柔軟な性質が失われてはならないことについても述べた．

本章では，以上の観点に基づきデバイス依存部とデバイス非依存部に分けたシステムGordiusを提案し，その目的と構成について述べる．

3.1 システムの目的

本研究は，効率的かつ協調的にAd-hocネットワークにおける安全性を保証するためのデータリンク機構を構築することを目的としている．Gordiusを用いることで，多様な無線媒体でAd-hocネットワークを実現でき，また通信の安全性を効率的に保証できる．



(a) vulnerable ad-hoc network　(b) robust ad-hoc netwo

図3.1: Gordiusが実現する機構

既存のシステムでは，図3.1(a)に示すように悪意を持つホストに対し盗聴の危険性や意図されない接続を許してしまう．こうした問題を解決するために，Gordiusは認証および暗号化を行うことで情報の安全性を高め，図3.1(b)のように堅牢な通信を実現する．

3.2　要求仕様

Ad-hocネットワークは，無線媒体の持つ利点を最大限に活かしている．従って，これらの問題の解決に際し以下のような点が失われると，Ad-hocネットワーク自体の有用性が低下することになり，これは避けなければならない．

- ネットワークに接続するために電波や光などの媒体に制約を受けないこと
- 接続のための手順が有線に比べて簡易であること
- ケーブルなどによる地理的制約を受けないこと

3.3　本システムの構成

本節ではGordius の構成について概観し，それぞれの役割と連携について述べる．

3.3.1　Gordius システム

Gordius は多様な無線デバイスでAd-hocネットワークを実現する柔軟性を持つプロトコルを実装した2つのモジュールからなる．これらはAd-hocネットワークにおけるデバイス非依存の管理を行ない，他の層との協調連携機能を持つモジュールADAM と，デバイス依存部の管理と暗号化処理を行なうモジュールSDM である．図3.2に本システムの概念図を示す．

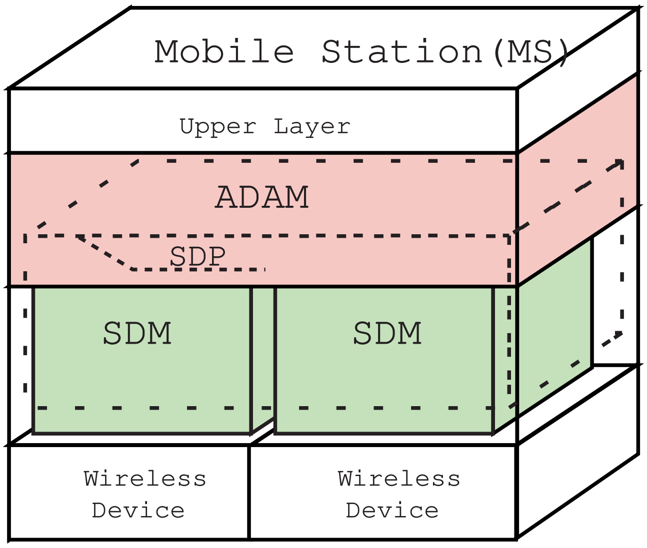


図 3.2: Gordius 概念図

3.3.2　Secure Datalink Module

Gordius システムのデバイス依存部はSDM (Secure Datalink Module) と呼ばれ，個々のデバイス毎に用意される．SDM はデバイスドライバの一部として実装されることを想定している．任意のデバイスに対してSDM が提供されることで，そのデバイスを用いた安全なAd-hocネットワークの構築が保証される．

SDM は，後述するADAM に対して認証のための通信インタフェースを持ち，またADAM からの指示により通信を暗号化するための機能を持つ．

様々な無線デバイスを用い，それらの間で統一された認証および暗号化を行なうためには柔軟性を持つ管理機構が必要である．SDM は，この管理機構を支援するためのSDP を実装したデバイスドライバである．

3.3.3 Secure Datalink Protocol

SDP (Secure Datalink Protocol) は，認証のためのメッセージを定めたプロトコルである．このメッセージ交換は，ユーザデータの交換と同様に安全性が必要で，SDP ではこれらの暗号化についても定めている．

暗号化方式は将来に高性能化および高速化が見込まれており，様々な方式を選択できるべきである．従ってSDM およびSDP では暗号化方式については特定せず，拡張性を持たせている．

3.3.4 Autonomous Distributed Authentication Module

図3.2における非デバイス依存部の機能を実現するのがADAM (Autonomous Distributed Authentication Module) である．SDM が提供するインタフェースを用い，認証を行なう．

既に認証を受けた関係によりAd-hoc ネットワークを構築しているホストの集まりをAd-hoc グループと定義する．各ホストは，ADAM を用いることでAd-hoc グループに対するアクセス権を認証を経て得ることができる．ADAM は多様なデバイスのSDM を統轄する機構として働く．またAd-hoc グループのアクセス制御リストを保持し，このリストに基づき認証が行なわれる．このアクセス制御リストは各移動局が持つADAM の間で自律的に交換され，Ad-hoc グループ内で共有される．

第4章

設計

本章では，Gordius システムの設計について述べる．はじめに本システムにおけるデータリンク構築のためのプロトコルSDP について述べる．次にデバイス非依存部を担うADAM について述べる．なお，SDM はSDP のデバイス依存部の処理を担うモジュールとして定義されているため本章では直接言及せず，第5.1節にてモジュールの実装例として述べる．

4.1 Secure Datalink Protocol

本節では，認証のためのプロトコルであるSDP について説明する．

4.1.1 プロトコル概要

SDP は，認証および暗号化のためのメッセージを交換するプロトコルである．メッセージ交換の手順を図4.1に示す．

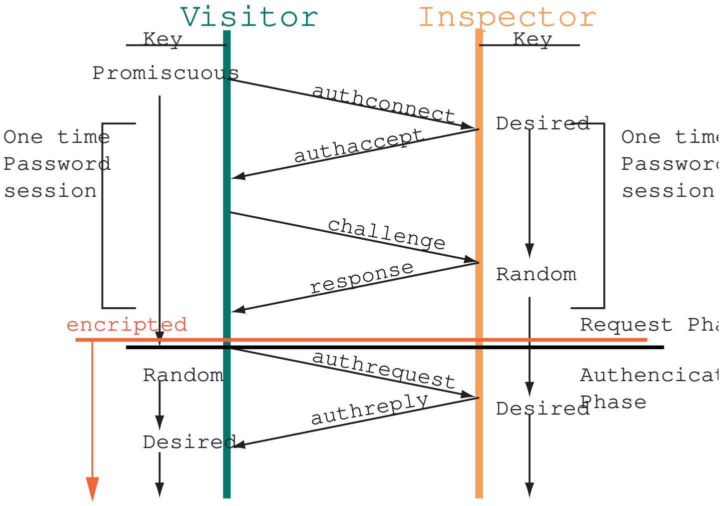


図 4.1: SDP メッセージ

SDP を用いた通信主体には2種類ある．それぞれについて以下で説明する．

inspector

後述する各認証フェーズにおいて，認証を行なう側のホストをinspectorとする．具体的にinspectorになり得るホストは，通常既にAd-hocグループに属している．ただし，後述するADAMにおける認証モードがBuildモードである場合には，認証を要求するホストがinspectorとなる．

visitor

同様に，認証を受ける側のホストをvisitorとする．visitorとなり得るホストは，いずれのAd-hocグループにも属していないか，これから接続を要求するAd-hocグループ以外のグループに属しているホストである．またinspectorと同様，ADAMの持つ認証モードがBuildモードの場合は，認証を要求されたホストがvisitorとなる．

4.1.2 認証フェーズ

SDPには，2つの認証フェーズがある．以下でそれぞれについて説明する．

Request phase

認証データを交換するためには，その認証データが漏曳することを防ぐために暗号化する必要がある．その暗号化のための鍵を取得するための認証がRequest phaseで行なわれる．また，Request phaseで行なわれる暗号化および認証はワンタイムパスワード[12]を用いて実現される．なお，この認証はinspectorとvisitorの一対一のものであり，Ad-hocグループとは関係ない．

この認証は，まずはじめに認証を行なう側であるinspectorが，予めある鍵を用意する．この鍵をseedとする．visitorからの認証要求があり，inspectorがその認証を行なうと判断すると，inspectorはこのseedをvisitorへ送信する．この後，inspectorはseedを，一方向性ハッシュ関数を用いて認証鍵に変換する．

visitorはseedを受信すると，同じく一方向性ハッシュ関数を用いてseedを認証鍵に変換する．その後，この認証鍵をさらにもう一度ハッシュ関数を用いて変換し，これをinspectorに対し返信する．

inspectorは，用意しておいた認証鍵をもう一度ハッシュ関数にかけ，visitorから返信された認証鍵と比較する．一致していれば認証が成功したと見なす．一致していなければ，認証が失敗したものと見なす．

この手順を，図4.2に示す．

Authentication phase

Authentication Phaseでは，Ad-hocグループに参加するための認証が行なわれる．このフェーズでは，Request phaseで取得した鍵を元に情報は全て暗号化される．

Request phaseでの認証と異なり，このフェーズでの認証はAd-hocグループに対するものである．なお，ここで行なわれる認証は第4.2節にて詳細に説明する．

4.1.3 フレームフォーマット

SDPが交換するメッセージは6つのタイプを持つ．全てのメッセージは，図4.3に示すフォーマットに従って送信される．以下で各フィールドについて説明する．

`SDP_mtype`

各メッセージを識別するためのID．

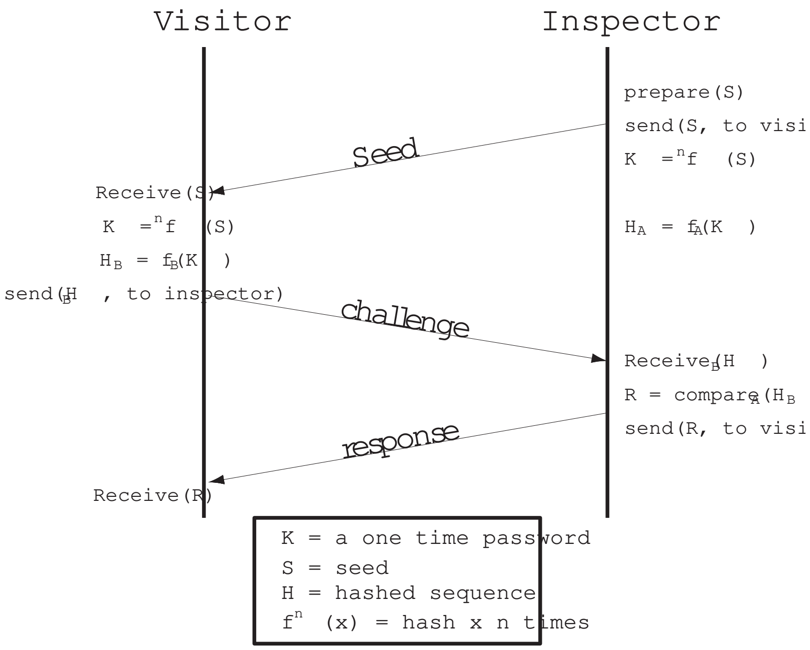


図 4.2: ワンタイムパスワード

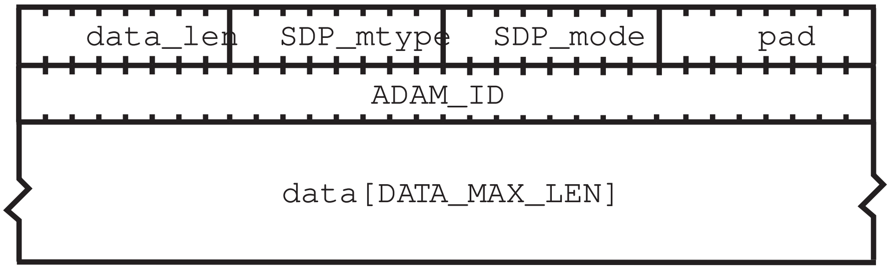


図 4.3: SDP フレームフォーマット

`SDP_mode`
認証を行なう際のモード．第4.2.3 項参照．

`ADAM_ID`
各ホスト上のADAM を一意に識別するID．第4.2.4項参照．

`datalen` 次に示すデータフィールドの長さ．

`data` データフィールド．各メッセージで処理される個有のデータ．

`SDP_data`フィールドは，伝達すべき鍵やワンタイムパスワードにおけるチャレンジメッセージなどを格納するためのフィールドである．これらの情報はメッセージごと，あるいはデバイスごとに変化し，実装に依存するために可変である．詳細は第4.1.4項にて述べる．

4.1.4 メッセージタイプ

SDP で交換されるそれぞれのメッセージについて，以下で説明する．

authconnect メッセージ

ユーザからの指示や上位層からの通知により，Ad-hoc グループに対する認証を要求する必要が生じると，visitor はauthconnect メッセージをブロードキャストする．このメッセージにおけるフィールドを表4.1に示す．

表 4.1: authconnect メッセージ

フィールド名	内容
`SDP_mtype`	Authconnect
`SDP_mode`	visitor が望むモード
`ADAM_ID`	自ホストが持つADAM の識別子
`SDP_datalen`	`SDP_data` フィールド長
`SDP_data`	Ad-hoc グループ識別子

authconnect を送信したvisitor は，ある一定時間authaccept メッセージを待つ．その時間内にauthaccept メッセージが受信されない場合にはタイムアウトと見なし，自らの認証状態を authconnect メッセージ送信前の状態に戻す．

また authconnect メッセージはブロードキャストされるため，visitor が接続を望む Ad-hoc グループを識別する必要がある．このため，`SDP_data` フィールドに Ad-hoc グループを特定する識別子を置く．なおこの識別子はSSID とは異なるものであり，Gordius システムにより設定されるものである．

authaccept メッセージ

authconnect メッセージを受信したホストは，同メッセージ内の`SDP_data` フィールドにある Ad-hoc グループ識別子から，visitor に対する認証を行なうか否かを判断する．もし認証を行なわないと判断した場合には行動を起こさず，状態も遷移しない．

認証を行なうと判断した場合には，表4.2に示される形式でauthacceptメッセージを返信する．ただしこの際，何ら状態の遷移は起こらない．これは，authacceptメッセージがvisitorに無視される可能性があるためである．

authacceptがvisitorによって無視されず，authrequestが送信される時点で，authacceptを送信したホスト群からinspectorが決定される．

表 4.2: authacceptメッセージ

フィールド名	内容
`SDP_mtype`	Authaccept
`SDP_mode`	authconnectメッセージからコピー
`ADAM_ID`	自ホストが持つADAMの識別子
`SDP_datalen`	`SDP_data`フィールド長
`SDP_data`	challenge-response seed(本文および図4.2参照)

Authentication phaseでは通信を暗号化する必要があり，この暗号化に共通の鍵を得るための認証をauthaccept，challengeおよびresponseメッセージにて行なう．authacceptメッセージではこの認証で用いるワンタイムパスワードのためのseed Sを送信する．このSは`SDP_mtype`フィールドに格納される．

authconnectメッセージを受信した全てのホストがauthacceptメッセージを送信するため，visitorは複数のauthacceptメッセージを受信することになる．しかしvisitorは，それらのauthacceptメッセージのうち時間的に最も早く受信したもののみを有効とする．従い，authacceptメッセージを送信したinspectorは，後述するvisitorからのchallengeメッセージを受信しない限りauthconnectメッセージを受信しなかったのと同等の状態となる．

challengeメッセージ

authconnectを送信した後のvisitorは，authacceptメッセージを受信するとauthentication phaseに移る．

このフェーズでは，visitorはauthacceptメッセージに含まれるSを元に認証鍵Kを作成する．その後，この鍵をハッシュ関数にかけてH_Bを作成し，ワンタイムパスワードとして送信する．

challengeメッセージのフィールドを表4.3に示す．

表 4.3: challengeメッセージ

フィールド名	内容
`SDP_mtype`	Challenge
`SDP_mode`	authacceptメッセージからコピー
`ADAM_ID`	自ホストが持つADAMの識別子
`SDP_datalen`	`SDP_data`フィールド長
`SDP_data`	One time password

responseメッセージ

visitorが送信したchallengeメッセージに対し，その認証結果を返すのがresponseメッセージである．図4.2に示すとおり，visitorが送信した，ハッシュされた鍵H_Bを受信したinspectorは，自らが作成したハッシュされた鍵H_Aとそれを比較する．

このH_AとH_Bが一致していれば正しく認証されたと判断し，Authentication phaseへと移る．一致していなければ，認証が失敗したと判断する．

responseメッセージのフィールドを表4.4に示す．

表 4.4: responseメッセージ

フィールド名	内容
`SDP_mtype`	Response
`SDP_mode`	challengeメッセージからコピー
`ADAM_ID`	自ホストが持つADAMの識別子
`SDP_datalen`	`SDP_data`フィールド長
`SDP_data`	認証結果(Success / Failure)

authrequestメッセージ

responseメッセージを受信したvisitorは，その結果が失敗であれば自らの認証状態を，authconnect以前へ戻す．成功であればinspectorへauthrequestメッセージを送信し，Authentication phaseへと移る．

このフェーズでの認証はAd-hocグループ内での暗号鍵を取得することを目的とする．なお，このフェーズにおける暗号化はRequest phaseで取得した鍵Kを用いて行なう．

responseメッセージを受信したvisitorは，認証を要求するために認証データを送信する．送信する認証データは第4.2.4項にて説明する．

表4.5にauthrequestメッセージのフィールドを示す．

表 4.5: authrequestメッセージ

フィールド名	内容
`SDP_mtype`	Authrequest
`SDP_mode`	responseメッセージからコピー
`ADAM_ID`	自ホストが持つADAMの識別子
`SDP_datalen`	`SDP_data`フィールド長
`SDP_data`	認証データ(第4.2.4項参照)

authreplyメッセージ

inspectorはauthrequestメッセージを受信した後，その中に含まれる認証データを元に暗号鍵のための認証を行なう．この認証には4種類あり，それらについては第4.2.3項にて説明する．

authreplyメッセージのフィールドを表4.6に示す．

表 4.6: authreply メッセージ

フィールド名	内容
`SDP_mtype`	Authreply
`SDP_mode`	authrequest メッセージからコピー
`ADAM_ID`	自ホストが持つ ADAM の識別子
`SDP_datalen`	`SDP_data` フィールド長
`SDP_data`	認証結果 (Success/Failure)

4.2 Autonomous Distributed Authetication Module

本節では，Gordius のデバイス非依存部を管理する ADAM について説明する．

4.2.1 モジュール概要

ADAM は，SDM が提供するインタフェースに従ってデータリンクを確立するための認証を行なう独立したモジュールである．上位層からの Ad-hoc ネットワークへの接続要求を受け取り，SDP により提供される手段で認証を行ない，その結果を上位層へ伝える．

このデータリンク認証のために，各ホスト上の ADAM がアクセス制御リストを保持する．またこのリストは，自律的に各ホスト間で協調し，データの整合性を保つ．

また，ADAM は SDP が持つ機能の一部を担う．具体的には，認証データを受け取った後，そのデータを分析して次の動作を決定する．この動作は，SDP におけるメッセージの送信あるいは認証結果の通知のいずれかである．図4.4に，ADAM の概念を表す状態遷移図を示す．

4.2.2 安全性要求レベル

ADAM が提供する認証機構は安全性レベルを持つ．このレベルは，Ad-hoc グループが visitor に対し要求するレベルである GSL(Group Security Level) と，visitor が Ad-hoc グループに要求するレベルである ASL(Access Security Level) とに分かれる．

これを用いることで Ad-hoc グループを多様な形態で実現でき，また目的に応じた安全性のレベルを定めることができる．このレベルは数字で表わされ，数字が小さいほど安全性が高い．以下で，安全性要求レベルについて説明する．

GSL

Ad-hoc グループを構築する際に設定する安全性レベル．GSL 0 から 2 のレベルで安全性を設定され，数字が小さいほど安全性のレベルは高い．

GSL 0

このレベルにあるネットワークでは，アクセス制御リストに登録がないホストは認証を受けることができず，Ad-hoc グループに参加できない．

GSL 1

アクセス制御リストに登録がないホストは，登録することで接続が許可される．登録がある場合には GSL 0 と同様である．

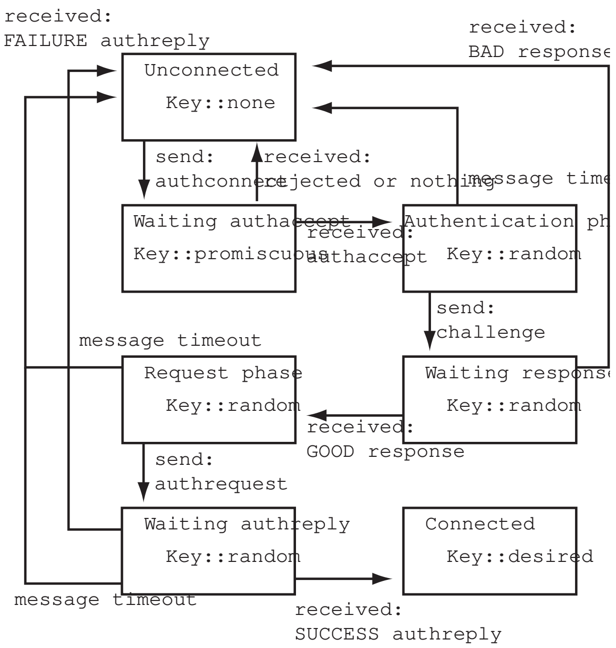


図 4.4: ADAM 状態遷移図

GSL 2

最低の安全性レベルであるGSL 2では認証は行なわれず，接続を要求すれば無条件に認められる．

ASL

ASLは，visitorがAd-hocグループに要求する安全性のレベルである．ASLは，visitorがauthconnectを送信する際に`SDP_mode`フィールドの値として送信される．visitorが要求するASLよりAd-hocグループのGSLが高い場合，visitorは認証を受けられない．

なお，visitorの要求するASLとそれに対し接続が許可されるGSLの関係を表4.7に示す．

表 4.7: GSLとASLの対応

GSL	ASL
0	0
1	0および1
2	2

GSL 2であるAd-hocグループに対しASL 2のみが許可されるのは，GSL 2のAd-hocグループにアクセス制御リストが存在しないためである．

4.2.3　認証モード

ADAMが行なう認証には4つのモードがある．それぞれGSLの0から3に対応しており，認証のための手順が異なる．以下では，それぞれについて説明する．

Log on モード

アクセス制御リストに自らの登録があるホストが，それを利用して認証を行なうためのモード．GSLが0のAd-hocグループに対する接続を要求する際に用いる．

Sign on モード

アクセス制御リストに自らの登録がないホストが，自らを登録しつつ認証を行なうためのモード．GSLが0もしくは1のAd-hocグループに対する接続はこのモードを用いて行なわれる．

Guest モード

アクセス制御リストに自らの登録がないホストが認証を行なうためのモード．リストに自らを登録することなくデータリンクを構築する．GSL 2を用いてAd-hocグループを構成する．

Build モード

自らを中心とした，全く新たなアクセス制御リストを構築し，新たなネットワークを構築するためのモード．接続する相手ホストを認証する．すなわちこのモードに限り，認証要求を発行するホストが認証を行なうことになる．

これらのモードを用いることで，目的に応じて柔軟なAd-hocグループを構築できる．

4.2.4　認証データ

アクセス制御リストに登録する認証データを以下に示す．

IFID

ネットワークインタフェースの識別子．主にMACアドレスが使用される．

ADAM_ID

各ホスト上のADAM を一意に定める識別子．

PassPhrase

各ホスト上のユーザが指定するパスフレーズ．

ADAM はこれらのデータを認証に用いる．物理的な識別子，論理的な識別子，ユーザ個有の鍵を全て一致させることでAd-hocグループへの認証を行なう．

暗号化のためのインタフェース

第2.4.1項で述べた通り，安全性に関してはプロトコルで規定せずに，インタフェースを提供する形で実装に依存する柔軟性を持たせるべきである．従ってSDP では規定しておらず，ADAM が制御する必要がある．

通信の暗号化はADAM が行なう．だが，SDP のヘッダ内をも暗号化するため，最終的な暗号化はSDMの中で行なわれる必要がある．従って，ADAM はSDM に対し暗号化ルーチンへのインタフェースを提供する必要がある．

4.2.5　認証アルゴリズム

ADAM の認証アルゴリズムを図4.5に示し，その動作を以下で説明する．

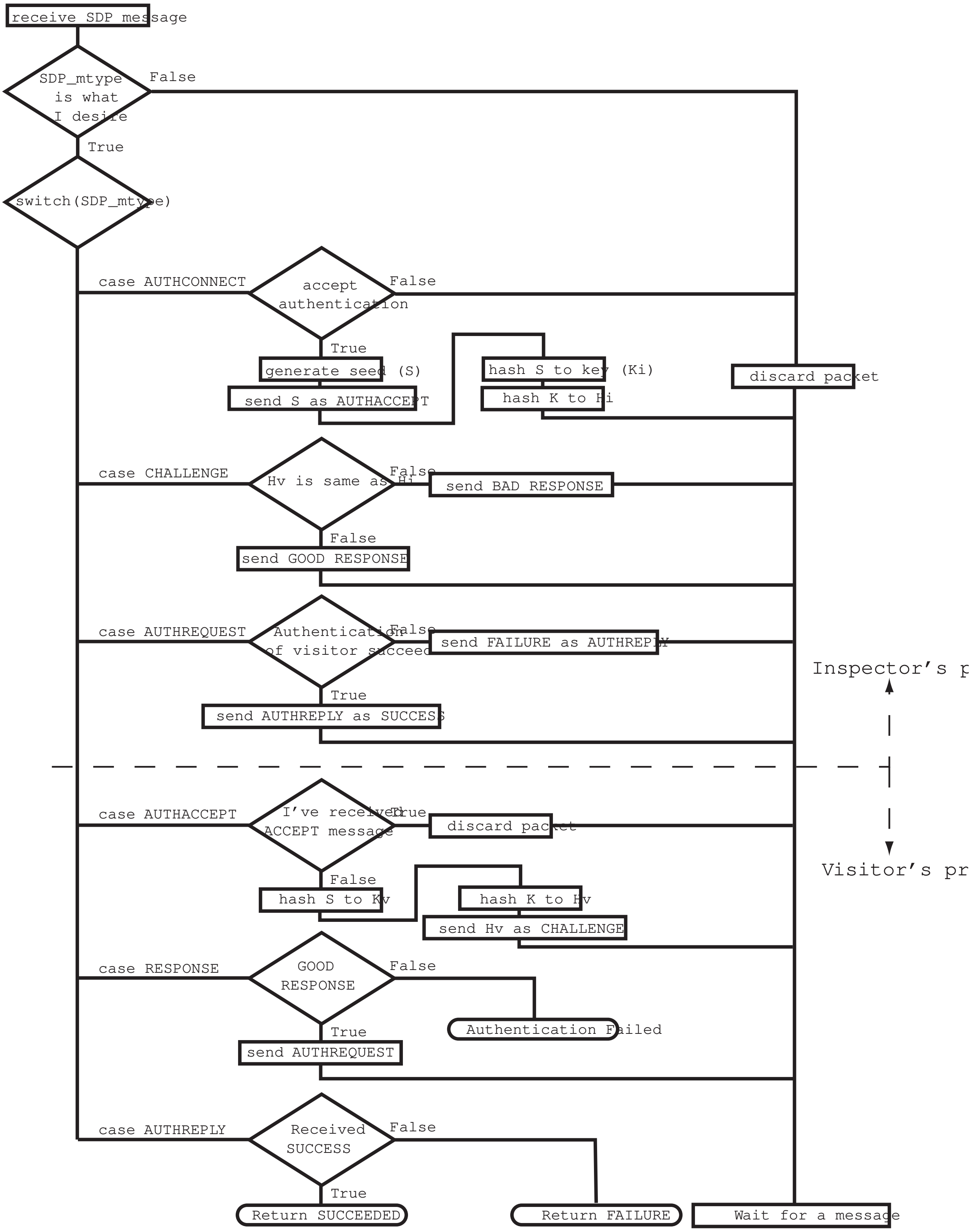


図 4.5: ADAM 動作アルゴリズム

メッセージの受信と識別

SDP メッセージを受信することから ADAM の動作は始まる．SDP メッセージを受信すると，そのメッセージを受信するべき状態であるかを判断する．その状態にない場合はメッセージを破棄する．受信すべき状態であればそのメッセージタイプを識別し，値に応じた適切な処理を行なう．

authconnect メッセージの処理

authconnect メッセージを受信した場合，authaccept メッセージを返信するか否かを判断する．返信する場合，ワンタイムパスワードによる認証のための変数を設定し，authaccept メッセージを送信する．

authaccept メッセージの処理

authaccept メッセージを受信した場合，既に authaccept メッセージを受信しているか否かを判断する．受信していなければ，ワンタイムパスワードによる認証のための変数を設定し，challenge メッセージを送信する．

challenge メッセージの処理

challenge メッセージを受信した場合，Request phase の認証を行なう．この認証結果を，response メッセージとして送信する．

response メッセージの処理

response メッセージを受信した場合，Request phase の認証結果を識別する．この認証が成功した場合，Authentication phase の認証を行なうために認証データを authrequest メッセージとして送信する．Request phase の認証が失敗した場合，状態を初期のものに戻す．

authrequest メッセージの処理

authrequest メッセージを受信した場合，Request phase の認証を行なう．この認証結果を，authreply メッセージとして返信する．

authreply メッセージの処理

authreply メッセージを受信した場合，Authentication phase の認証結果を識別する．この認証が成功した場合，取得したネットワークへの接続権を元に設定を行なう．失敗した場合には，初期状態に戻る．

4.2.6 認証機構のスケーラビリティ

安全性を高める目的と処理を簡略化する目的から ADAM では，一つの Ad-hoc グループに対する認証機構のみ提供する．すなわち，たとえ二つの無線通信機器を持っていたとしても，複数の Ad-hoc グループへ同時に接続できない．

仮にある移動局 A が，G_A および G_B という二つの Ad-hoc グループに接続しているとする．G_A に属する移動局 B は A との認証関係を持っているが，G_B に属する移動局 C とは認証関係がない．ここで A は B から情報を受け取ることができ，そしてその情報を C へ伝えることができてしまう．すなわち，認証関係にない移動局同士が通信できてしまうことになる．

これを回避するためには認証機構を拡大する必要があるが，その分処理が複雑になり，また送受信するべき情報量も増す．これは本研究の目的からはずれるため，設計方針には採らない．

第5章

実装

本章では，第4章にて述べた設計に基づいた実装例を示す．無線機器は，IEEE 802.11規格準拠のLucent Technology社製WaveLAN/IEEE PCカードを用い，開発マシンはIBM社製のThinkPad 570を用いた．また開発はオペレーティングシステムにFreeBSD 3.2-Releaseを用い，SDMおよびADAMは同オペレーティングシステムのカーネルの中に実装した．

なお暗号化にはDES[13]ライブラリを同カーネルに組み込んで使用し，一方向性ハッシュ関数はMD5[14]ライブラリを用いた．

5.1 Secure Datalink Protocolの実装

SDPの実装は，FreeBSDにおけるPCカードサポートモジュールであるPAO3により提供される同PCカードドライバ`if_wi.c`を元に行なった．また本システムのために，ヘッダファイル`if_wi-gordius.h`を新たに定義した．

5.1.1 ether_sdp構造体

SDPにおける6種類のメッセージを交換するために，新たに`ether_sdp`構造体を宣言する．この構造体はSDPメッセージを格納し，送受信のバッファとして使用する．図5.1にその宣言を示す．

`/usr/src/sys/i386/isa/if_wi-gordius.h`

```
struct ether_sdp {
        u_char  data_len;           /* length of data field, 1octet */
        u_char  SDP_mtype;          /* Message type, refer to above, 1octet */
        u_char  SDP_mode;           /* Mode flag, 1octet */
        u_char  pad;                /* A pad, of cource, not used, 1octet */
        u_int   ADAM_ID;            /* sender's ADAM-ID, 4octets */
        u_char  data[DATA_MAX_LEN];/* Data */
};
```

図 5.1: `ether_sdp`構造体

また，このメッセージがSDPのものであることを示すため，`ETHERTYPE_SDP_NCRPT`および`ETHERTYPE_SDP_CRYPT`という定数を定義する．これを図5.2に示す．これらのメッセージタイプを持つフレームを受信すると，SDMはそれぞれに対応する処理を行なう．

/usr/src/sys/net/ethernet.h

```
#define ETHERTYPE_IP            0x0800  /* IP protocol */
#define ETHERTYPE_ARP           0x0806  /* Addr. resolution protocol */
      ... ... ...
/* XXX - add more useful types here */
#define ETHERTYPE_SDP_NCRPT     0x1122  /* SDP noncrypt data */
#define ETHERTYPE_SDP_CRYPT     0x1222  /* SDP crypt data */
     ... ... ...
```

図 5.2: フレームタイプ宣言

5.1.2 グローバル変数

Gordius システムにおける状態を保持するために，表5.1に示すグローバル変数を宣言する．

表 5.1: SDM におけるグローバル変数

変数の型	変数名	解説
`u_char`	`gd_flag`	認証モードを保持するフラグ
`u_char`	`gd_state`	SDM の状態を保持するフラグ

これらはGordius の状態を表すために大域的に参照される必要があるため，グローバル変数とした．

5.1.3 SDM 関数群

`wi`デバイスドライバをSDM 化するために，新たに関数を定義した．それらの関数について表5.2で説明する．

表 5.2: `wi`デバイスドライバにおけるSDM 関数群

関数名	解説
`adam_input()`	SDP メッセージを受信し，ADAM へ渡す．
`wi_gordius_output()`	SDP メッセージをデバイスへ送る．
`wi_gordius_authconnect()`	authconnect メッセージを送信する．
`wi_gordius_authaccept()`	authaccept メッセージを送信する．
`wi_gordius_challenge()`	challenge メッセージを送信する．
`wi_gordius_response()`	response メッセージを送信する．
`wi_gordius_authrequest()`	authconnect メッセージを送信する．
`wi_gordius_authreply()`	authconnect メッセージを送信する．
`wi_gordius_enable_promisc()`	promiscuous モードを設定する
`wi_gordius_setssid()`	SSID を，引数に示される文字列に設定する．

5.1.4 タイムアウト

各メッセージ送信後に一定時間が経つと，認証相手との接続が失なわれたと判断しタイムアウトする．同時に，これまでのメッセージにより遷移した状態を全て初期状態に戻す．

このタイムアウトの機能は，FreeBSDの持つ`watchdog`機能を用いて実装した．これは，`ifnet`構造体の持つメンバである`if_timer`に，秒単位の粒度で間隔を設定することで実現される．

5.1.5 authacceptメッセージに対する割り込み禁止

authconnectメッセージがブロードキャストされ，複数のauthacceptメッセージが返信される可能性があることを第4.1.4項で述べた．

従って，既にauthacceptメッセージを受信しその処理を行なっている間に別のauthacceptメッセージを受信し割り込みがかかると，状態の不整合が起こる可能性がある．これを回避するために，authacceptメッセージを受信したと判断した直後に，状態が完全に遷移するまでネットワークからの割り込みを禁止する．

この実装を，図5.3に示す．

/usr/src/sys/i386/isa/if_wi.c

```
static void wi_rxeof(sc)
        struct wi_softc         *sc;
{
     ... ... ...
        /* Receive packet. */
        m_adj(m, sizeof(struct ether_header));

        /* pass SDM data packets if it fits */
        if (ntohs(eh->ether_type) == ETHERTYPE_SDP_NCRPT) {
                if (es->SDP_mtype == SDP_MTYPE_AUTHACPT) {
                        s = splimp();
                        flag = 1;
                }
                wi_gordius_input(ifp, m, eh->ether_shost, SDP_NONCRYPT);
                if (flag) splx(s);
     ... ... ...
        } else {
                ether_input(ifp, eh, m);
        }
        return;
}
```

図 5.3: authacceptの受信による割り込みの禁止

5.1.6 Promiscuousモード

SDPが動作するためには，データリンク層におけるpromiscuousモードを実現する必要がある．

仮に，既にAd-hocグループGが存在しているとする．Gでは既に独自の鍵K_Gを用いて通信を暗号化している．

この場合，あるホストBがG内の任意のホストAに対して認証を要求する場合，BはAへ情報を送信する手段を持たない．そのため，既知の鍵K_Pを用いることでAがBの要求を受け取ることができるという

機構を実現する必要がある．この K_P を用い，あらゆるホストに対して要求を伝達する機構がpromiscuousモードである．

WaveLAN/IEEEでは，PromiscuousモードとしてSSIDにANYという文字列を設定している．送信側がSSIDにANYを設定していると，それだけでデータリンクが成立し，情報をブロードキャストできる．

本実装では，Promiscuousモードにはこの機能を用いた．なお，表5.2における`wi_gordius_enable_promisc`関数はこのPromiscuousモードを設定するための関数である．

5.2 Autonomous Distributed Authencitacion Module の実装

ファイル名`kern_adam.c`としてソースファイルを作成し，カーネル内に独立した1つのオブジェクトとしてADAMの実装を行なった．

5.2.1 ADAM コントロールブロック

SDMとのインタフェースを管理するために，ADAMコントロールブロックを定義する．これは，SDMの持つ関数へのポインタをメンバに持つ構造体として宣言される．

図5.4に，ADAMコントロールブロックの宣言を示す．

/usr/src/sys/i386/adam/kern_adam.h

```
struct adam_cb {
        int (*send_authconnect)
        __P((struct ifnet *, int));
        int (*send_authaccept)
        __P((struct ifnet *, u_char *, u_char));
      ... ... ...
        int (*enable_promisc)
        __P((struct ifnet *, u_char *));
      ... ... ...
};
```

図 5.4: adam_cb構造体

この構造体のメンバは全て関数へのポインタであり，これらのメンバにSDMへのインタフェースを全て格納する．また，Promiscuousモードの設定関数のポインタもここに示される．

5.2.2 adam_main関数

ADAMの主たる処理は，全て`adam_main`関数の中で行なわれる．表5.2で説明した`adam_input`関数も，最終的に`adam_main`関数を呼び出し，次に送信するべきメッセージを送る．

この関数の主な処理は，図4.5に示すアルゴリズムに従っている．

5.2.3 認証データ

Authentication phaseにおける認証には，図5.5に示す認証データが使われる．

/usr/src/sys/i386/adam/kern_adam.h

```
struct authkey {
        u_char  shaddr[6]; /* WaveLAN/IEEE MAC address */
        u_int   ADAM_ID;        /* ADAM ID that I have */
        u_char  passphrase[20]; /* pass phrase specified by User */
};
```

図 5.5: adam_authkey 構造体

5.2.4 暗号化ルーチンのインタフェース

本実装では，暗号化にDESを用いた．DESモジュールとSDM とのインタフェースを設定するために，crypt_info構造体を定義する．図5.6に，この構造体の定義を示す．また，そのメンバの解説を表5.3に示す．

/usr/src/sys/i386/adam/kern_adam.h

```
struct crypt_info {
        int (*encrypt)(...)
     ... ... ...
        int (*decrypt)(...)
     ... ... ...
        int (*keygenerate)(...)
     ... ... ...
        void *extention;
}
```

図 5.6: crypt_info 構造体

表 5.3: crypt_info 構造体のメンバ

メンバ名	解説
*encrypt	暗号化のためのルーチン．
*decrypt	復号化のためのルーチン．
*keygenerate	鍵を作成するためのルーチン．
*extention	拡張性を実現するポインタ(本文参照)

図5.6以外のルーチンが必要な場合，*extentionメンバに構造体を格納できるvoid型のポインタを利用する．関数へのポインタをメンバに持つ構造体を新たに定義し，*extentionにそのポインタを代入することで各種ルーチンを利用できる．

第6章

測定と評価

この章では，前章で説明した実装例を用い，本論文が提案するGordiusシステムの実験測定および評価を行なった．これを通して本システムの優位性を示す．

本実験では，通信の暗号化によるオーバーヘッドを測定することで，Gordiusの提供する安全性および協調性への対価を示す．また認証開始から完了までの時間を測定し，接続のためのコストおよび簡易さを示す．

また，本システムと目的を同じくした関連研究と比較し，本システムの優位性を示す．

6.1 評価方針

Gordiusシステムの目的は，安全かつ効率的にAd-hocネットワークを構築するためのデータリンク機構の提供にある．本章ではこの点に基づき，Gordiusシステムの評価を行なう．

いかなるコストでGordiusの提供する安全性を得られるかを，定量的評価にて考察する．またシステムのボトルネックを探すために，各部での処理時間を計測し，評価を行なう．

また，Gordiusの関連研究と比較した優位性を，安全性および処理効率の面から定性的に評価する．

6.2 定量的評価

本節では，定量的分析手法によりGordiusの優位性を示す．

6.2.1 実験環境

Gordiusの評価として，第5章で示した実装例を用いて3つの実験測定を行なった．第一に，Gordiusが提供する安全性を利用する際に支払わなければならない対価を分析するため，Gordiusを用いた通信と用いない通信でのスループットの変化を測定した．第二に，Gordius認証のためのオーバーヘッドを分析するために，認証開始から認証完了までの時間を測定し，計測した．第三に，実装を評価するために，認証ステップの処理時間を計測した．

実験には，表6.1に示すような機器を用いた．なお，無線機器にはLucent Technology社製無線LANカードであるWaveLAN/IEEEを使用した．

6.2.2 実験測定

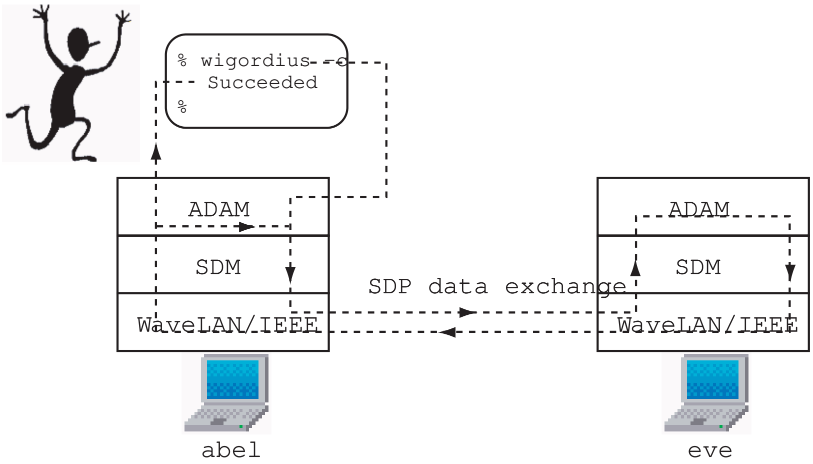
本節では，Gordiusを定量的に評価するための実験について説明する．

表 6.1: 測定機器

ホスト名	機器名	CPU	メモリ
abel	IBM ThinkPad 570	Mobile Celeron 366MHz	64MB
eve	日立 PriusNote 210	MMX Pentium 133MHz	72BM

実験A:認証に必要なオーバーヘッドの測定

Gordius は要求仕様の一つに，いくつかある無線媒体を用いたネットワークの利点である接続簡易性の維持を持つ．またinspectorが認証のために拘束される時間がAd-hocグループにおける通信を阻害する危険性もある．この点を評価するために，ユーザが認証を望むイベントを起こしてから認証が完了するまでの時間を測定した．また，認証レベルは全て最低のものを用い，認証モードはGuestモードを用いた．実験環境を，図6.1に示す．



```
% wigordius -c
 Succeeded
%
```

図 6.1: 実験Aの環境

認証の要求にはユーザレベルでのプログラム`wigordius`を作成した．この中で`ioctl`システムコールを用いて`wi`デバイスドライバへジャンプし，`authconnect`関数を呼び出している．今回試行回数は100とし，ユーザ空間における時間の測定はCライブラリである`gettimeofday`関数を用いた．またカーネル内の時間はFreeBSDカーネルの機能である`microtime`関数を用いて測定した．

また同実験環境を客観的に示すために，pingメッセージの往復時間を測定した．メッセージサイズをICMPヘッダを含めて1500バイトとし，試行回数は100とした．

実験B:暗号化によるスループット低下の測定

Gordius では，認証を受けた通信環境での情報全てを暗号化するため，暗号化しない通信よりもCPUにかかる負荷が高い．その結果として，実効スループットは低下するはずである．この程度を実験Bで測定した．実験環境を，図6.2に示す．

スループットの測定方法には`ttcp`プログラムを用い，暗号化を行なわないケースAと，Gordius を用いて暗号化を行なったケースBで比較した．`ttcp`の送信をabelで，受信をeveで行ない，計測のためのパケッ

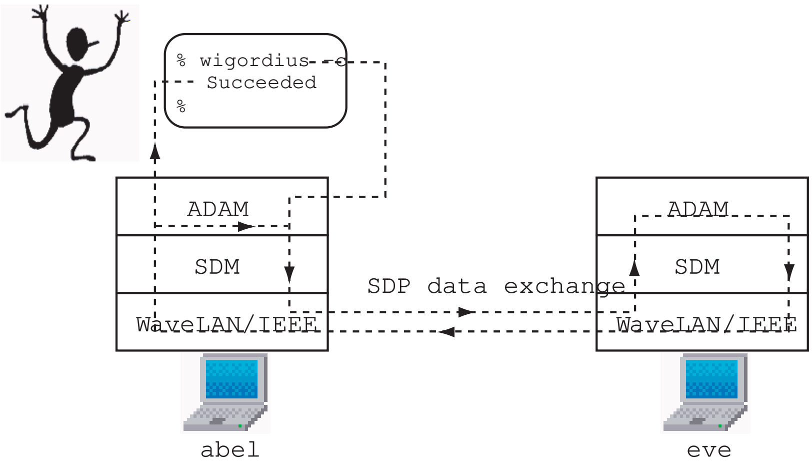


図 6.2: 実験Bの環境

トは，サイズを8192バイト，総数を2048に設定した．なお，実際に利用される場合を想定し，kainを含め3台のAd-hocグループの中で測定した．また，試行回数は100とした．

実験C:ボトルネックの分析

実験Cでは，実験Aで判明したinspectorの拘束時間のうち，Gordiusにおける認証部分のボトルネックを調べた．SDMの持つ主要関数が開始する時点と終了する時点でマイクロ秒単位の時間を100回計測した．表6.2に，測定した関数群およびその処理内容を示す．

表 6.2: 測定した関数群

関数名	解説
authconnect	認証要求パケット送信
authaccept	認証要求を受け入れるか否かの判断およびハッシュの作成，送信
challenge	ハッシュの作成，送信
response	ハッシュの比較，結果返信
authrequest	暗号化
authreply	暗号化，認証

6.2.3 実験結果の分析

実験A:認証に必要なコスト

実験Aでは，認証に必要なコストを測定した．その測定結果を表6.3に示す．なお，`gettimeofday`関数はマイクロ秒の粒度で時間を得るが，関数呼出しのオーバーヘッドを鑑みて有効数字を4桁とした．

ユーザはコマンドひとつを入力するだけでAd-hocネットワークへの認証が済み，その所要時間は約69ミリ秒である．Gordiusシステムを用いずにユーザ自らが認証を受け，ネットワークへの接続のための設定をする時間は69ミリ秒以下であるとは考えにくい．従って，本システムは十分に簡易かつ高速と言える．

表 6.3: 測定結果A:認証コストの測定

分析項目	平均値	標準偏差	最大値	最小値
認証完了まで	68.95	0.37	70.37	68.44
ping メッセージ	21.71	0.28	22.70	21.25

(試行回数:100，単位:ミリ秒)

実験B:暗号化によるスループット低下

実験Bでは，暗号化によるスループットの低下を測定した．図6.4に測定結果の表を示す．

表 6.4: 測定結果B:スループットの平均値と変化

ケース	平均値	標準偏差	最大値	最小値
A	1.22	0.01	1.23	1.16
B	1.12	0.02	1.14	1.06
スループットの変化			92%	

(試行回数:100，単位:メガビット毎秒)

この実験結果から，暗号化によるパフォーマンスの低下が8%であることがわかった．

実験C:ボトルネックの分析

実験Cでは，本実装の評価を行なうためにボトルネックを分析した．図6.3にその結果を示す．

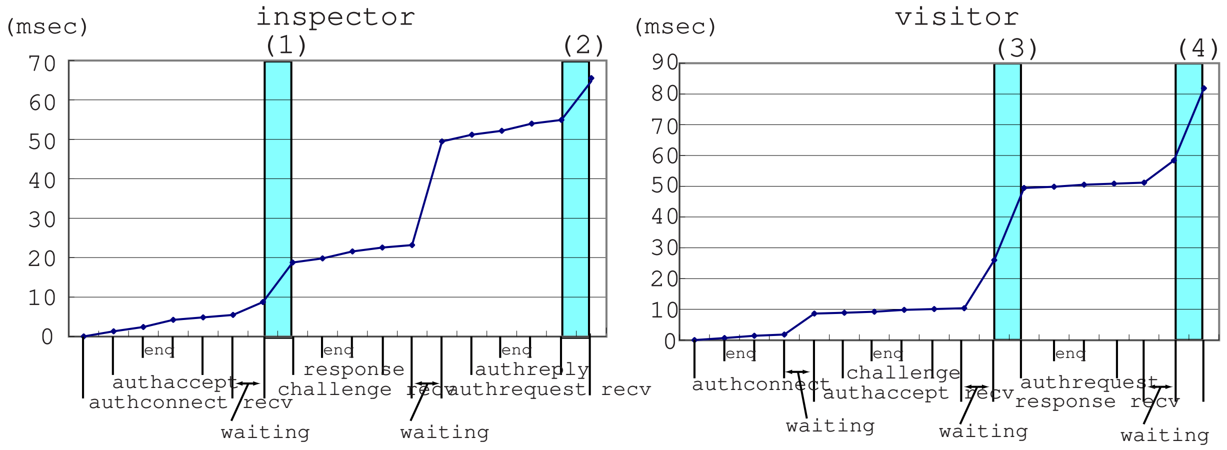


図 6.3: 測定結果C:ボトルネックの分析

図6.3中で，網掛けで示す部分が特に重要なボトルネックである．これらはそれぞれ以下の処理を行なっている部分である．

(1) challengeメッセージ受信後のハッシュ作成

(2) authrequest メッセージ受信後の復号化

(3) response メッセージ受信後のハッシュ作成

(4) authreply メッセージ受信後の復号化

このことから，DESおよびMD5モジュールが本実装のボトルネックになっていることがわかる．従って，これらのルーチンの高速化が本実装の有用性を高めるための懸案となる．

6.3 定性的評価

本節では，Gordius システムを関連研究と比較することで評価する．比較項目は第2.4.2項に挙げた項目を用いる．なお，Gordius 以外の項目については第2.4.2項にて説明している．

表 6.5: Ad-hoc ネットワークに対する定性的比較

	IPsec	WEP	MAA	Gordius
Ad-hoc ネットワークへの適応性				
処理能力	△	○	○	○
記憶資源	×	○	○	○
協調性	×	×	○	○
汎用性	○	×	×	○

○ :適している　△ :中程度　× :適していない

関連研究のいずれも，第2.4.1項で述べたように具体的な暗号方式を定めていない．これは，将来のよりよい暗号方式にも対応するための拡張性と取れる．本システムにおいてもこの方針を採用している．従って，これらの研究に対し暗号化の面から安全性の評価はできず，また意味がない．

表6.5に適応性評価について示し，以下で説明する．

処理能力
: Gordius の持つボトルネックがDESおよびMD5の処理部にあることから，Gordius が要求するコンピュータの処理能力は実装に依存する．

記憶資源
: 現在ADAM の保持するアクセス制御リストは主記憶上に保持されており，またその縮小については考えられていない．これはGordius が前提とするスケーラビリティが十数台のAd-hoc ネットワークであることによる．

協調性
: Gordius は，様々な無線通信機器に対応できること，あらゆるネットワーク層プロトコルと協調できることを目的としている．これが実現されたことで，無線LAN システムをはじめ赤外線などでAd-hoc ネットワークを構築できる自由度を得ることができた．

汎用性
: デバイス依存部と非依存部を分離したことにより，多様なデバイスや上位層を支援することができた．

6.4 考察

実験Aの結果から，Gordius が提供する認証機構は無線通信媒体の持つ簡易さを損なわずに実現されたことがわかる．実験Bの結果から暗号化によるオーバーヘッドを示し，安全性のための対価を示した．また実験Cの結果に実装例の持つボトルネックを示し，今後解決すべき問題について分析した．そして関連研究と本研究の比較を行ない，既存のシステムより優れた協調性および認証機構を提供したことを示した．

無線LANシステムではCSMA/CA方式にてアクセス制御を行ない，電波の混信を防ぐ方式を採っている．また指向性が高い赤外線を利用したシステムでは，空間に情報が伝播することがなく安全性が高い分，広範囲な通信ができない．Ad-hocネットワークはこうした特徴を持つ媒体を前提としているため，ネットワークのスケーラビリティは小規模なものに限られる．

本システムはこのようなスケールを前提とし，協調性が高く柔軟に安全性を提供する無線データリンク機構を実現する目的で開発され，その目的は達成されている．

第7章

結論

前章では，本研究の定性的評価と定量的評価を行ない，その考察を行なった．その結果Gordius が目的とした安全性，効率性を十分に実現できたことを示し，またその機能を得るためのコストを示した．

本章では，結論および今後の課題について述べる．

7.1　まとめ

本研究はAd-hoc ネットワークにおける安全な無線データリンク構築機構を実現するため，以下に挙げる事項について研究した．

- Ad-hoc ネットワークにおける安全性
- 多様な状況に対応できる柔軟な認証機構
- 協調性の高い暗号化機構
- 様々なデバイスでAd-hoc ネットワークを実現するための指針

現在の分散計算機環境のパラダイムは，安全性を求めれば適応性が低くなり，適応性を求めると安全性は低くなるというジレンマを持つ．このような計算機環境では，電子商取引や投票など機密性の高い情報は，適応的なネットワーク環境を通じて伝達できない．これは時間的あるいは地理的な自由度という，移動型計算機環境の利点を損なうことを意味する．

本研究ではこの移動型計算機環境のパラダイムをシフトさせることを目的とした．すなわち，移動型計算機環境および無線媒体を用いた応用例の一つであるAd-hoc ネットワークを基盤とした．安全かつ適応的な通信環境の構築である．

高い安全性を必要とする通信環境をより適応的なものにするため，本研究では無線データリンクにおける認証機構および暗号化機構を持つGordius を提案し，設計および実装を行なった．Gordius はデバイス非依存部ADAM とデバイス依存部SDM に分かれ，それらの通信方式を規定するSDP を持つ．

Gordius により，高い安全性と高い適応性を両立できる計算機環境が実現でき，安全なAd-hoc ネットワークという新たな計算機環境のパラダイムを提供できた．

7.2　今後の課題

第6章定量的評価および定性的評価から，以下に示す項目がGordius システムの今後の課題として挙げられる．

アクセス制御リストの高機能化

現在のGordiusシステムが持つアクセス制御リストは，Ad-hocグループへの接続が可能か不可能かの情報しか保持していない．しかし，認証レベルに応じてアクセスの種類を設定できれば，より利便性の高いAd-hocネットワークを実現できる．例えば，情報の受信のみを許可する認証関係を実現できれば電波の衝突を低減することができ，無線LANシステムでより効率的な通信が可能になる．

ADAMの自律性向上

現在のADAMにはAd-hocグループ内のアクセス制御リストの変化を，自律的に検出する機構がない．より柔軟で簡易なAd-hocネットワークを実現するためには，ADAM自らが自律的にAd-hocグループ内のアクセス制御リストを管理することが望ましい．

効率的な再送機構の実現

現在のGordiusシステムは効率的な再送機構を持たない．電波の混信などにより情報が正しく伝達されず，認証に失敗する．本来はADAMが情報の正しさを検証し，効率的にメッセージを再送することが望ましい．

システムのパフォーマンス

第6.3節で示した通り，inspectorが認証のために拘束される時間は決して小さなものではない．Ad-hocグループ全体のパフォーマンス向上のために，暗号化を含めたシステム全体の速度向上が望まれる．

経路制御機構との協調

Ad-hocネットワークにおける問題は経路制御にもある．経路制御との効率的な協調がなされてはじめて，適応的かつ安全な移動計算機環境が実現される．

謝辞

本研究の機会を与えて下さり，懇切丁寧な御指導を賜りました慶應義塾大学環境情報学部教授の徳田英幸博士ならびに村井純博士に深く感謝致します．また，絶えず御助言と御指導を頂きました，同学部の中村修博士と楠本博之博士に深い感謝の意を表します．本論文作成にあたり適切な御指摘および御指導を頂きましたSFC研究所所員西尾信彦氏に感謝致します．

本研究を進めていく上で，様々な議論をし助言してくださった慶應義塾大学徳田・村井・中村・楠本研究室のメンバー諸氏に感謝の念を表します．特に，常に共に研究を励ましあい，貴重な助言および議論をする機会を頂いた岩井将行氏，楠本晶彦氏，中村勇樹氏，西野秀明氏，原嶋章介氏，由良淳一氏に深く感謝します．

そしてMCng研究グループおよびKMSF研究グループのメンバー諸氏には実作業において多大なる手助けを頂き，ここに深く感謝の念を表します．

また政策・メディア研究科修士課程の岩本健嗣氏，永田智大氏，楠根雄志氏，古坂大地氏には執筆の最後まで協力して頂きました．ここに限りない敬意を表し，深く感謝致します．

最後に，数々の`panic`にもクラッシュすることなく，また兄弟喧嘩もせず設計および実装を耐え抜いた神々しき愛機kain，abelおよびeveに，そして荒んだ心を暖かく癒して頂いたCaster oneおよび家族にも尽きない感謝の意を表します．

以上をもって謝辞と致します．

平成12年2月28日
慶應義塾大学 総合政策学部
新井　仁

参考文献

[1] IEEE 802.11 Working Group for Wireless Local Area Networks, “IEEE Std 802.11, 1999 edition”, 1999

[2] Tobagi, F.A., Kleinrock, L., “Packet switching in radio channels: Part II - The hidden terminal problem in carrier sense multiple-access and the busy-tone solution”, IEEE Trans. Commun. Vol.COM-23, No.12, pp.1417-1433

[3] 松野浩嗣, 『パケット無線ネットワークにおけるメディアアクセス制御プロトコルの効率について』, 情報処理学会研究報告, p.25-32, 1999

[4] Stephen Kent, Randall Atkinson, “Security Architecture for the Internet Protocol”, RFC 2401, 1998

[5] Postel, J., “Internet Protocol”, RFC 791, 1981

[6] Stephen E. Deering, Robert M. Hinden “IPv6 Specification”, RFC 2406, 1998

[7] Atkinson, R., “IP Authentication Header”, RFC 2402, 1998

[8] Atkinson, R., “IP Encapsulating Security Payload”, RFC 2406, 1998

[9] Philip Miller 著, 苅田幸雄 監訳 『マスタリングTCP/IP 応用編』, オーム社, p21-23, 1998,

[10] M. Scott Corson, S. Papademetriou, Philip Padapopoulos, Vincent Park, “Internet MANET Encapsulation Protocol”, Internet-Draft, 1999

[11] Stuart Jacobs, M. Scott Corson “MANET Authentication Architecture”, Internet-Draft, 1999

[12] Neil Haller, “One-Time Password”, RFC1760, 1995

[13] “DATA ENCRYPTION STANDARD(DES)”, Federal Information Processing Standards Publication 46-2, 1993

[14] Rivest R., “The MD5 Message-Digest Algorithm”, RFC 1321, 1993

[15] Gary R. Wright, W. Richard Stevensm, “TCP/IP Illustrated, Volume 2”, Addison Wesley, 1995

[16] 松下 温, 『分散協調メディアシリーズ 7 ワイヤレスLAN アーキテクチャ』, 共立出版, 1996