多種無線ネットワーク環境における相互認証に関する研究

静岡大学 博士論文

多種無線ネットワーク環境における相互認証に関する研究

2011 年 3 月

大学院 自然科学系教育部
情報科学専攻
野村 立

目次

1. 序論:無線ネットワークシステムの動向と本研究の目的

無線ネットワークシステムは、数年前から急速に我々の生活の中に浸透してきている。第三世代移動体通信システムいわゆる3G ネットワークを利用した携帯電話は広く全世界に普及し、既に一般的なデバイスとして認知されており、一人一台の保有が進んで、生活するうえで必要欠くべからざる機器として用いられている。WLAN や WiFi と呼ばれる無線 LAN システムは、ノート PC の標準的な通信システムとして一般化し、家庭内や中小規模の企業などで簡易にネットワークを構築できる方式として着実に広がってきている。さらに、新しい無線ネットワークシステムとして、MAN(Metropolitan Area Network:中長距離エリアネットワーク)や PAN(Personal Area Network:近距離無線ネットワーク)がそれらの後を追うように現実化しつつある。

1.1. 無線ネットワーク規格

1.1.1. 3G

3G(第三世代移動通信システム)は、ITU の定める IMT-2000 規格に準拠した通信システムとして全世界に広く普及している。IMT-2000 の中には地上系無線方式として IMT-DS, IMT-MC 等の 5 種類の規格に分かれており、日本国内でも NTT docomo は IMT-DS (W-CDMA)、au は IMT-MC (CDMA2000)などのように方式が分かれている。

1.1.2. IEEE802.11

IEEE802.11[1][2]は現在では広く普及している無線 LAN 規格である。元々は伝送速度が最大2Mbps の無線ネットワークとして策定されたが、その後、通信速度や物理層・周波数帯の違いで 802.11a, 802.11b, 11g, 11n のように詳細な規格となっている。

IEEE802.11a は、伝送速度最大 54Mbps と高速であるが、周波数帯域は 5.2GHz という高い領域を利用しており減衰しやすいという欠点がある。

IEEE802.11b[3]は、周波数帯域は 2.4GHz 帯で伝送速度は 11Mbps。減衰が少なく電波が届きやすいため、最も普及している規格である。WiFi という商標のついた製品はこの規格をサポートしている。

IEEE802.11g[4]は、IEEE802.11b の利用しやすさと IEEE802.11a の高速性の双方を実現する規格であり、周波数帯は 2.4GHz、伝送速度は 54Mbps。IEE802.11b との互換性も保っており、11b と 11g 双方をサポートする無線ルータが多く製品化されている。

1.1.3. MAN

MAN とは Metropolitan Area Network の略で、中距離の無線ネットワーク規格として提案さ

れている。この領域ではIEEE802.16[5]やIEEE802.20[6]が仕様として確定されている。

IEEE802.16[5]は仕様の整理統合を踏まえてIEEE802.16-2004[7]と改定された。これは後にWiMAX(Worldwide Interoperability for Microwave Access)という規格として現実の製品化が進められている。さらに、ハンドオーバに関する仕様を追加し、IEEE802.16e[8]が策定され、それはモバイルWiMAX[9]として規格化・製品化が進められている。

IEEE802.20[6]は MBWA(モバイルブロードバンド無線アクセスネットワークシステム)とも呼ばれIPベースの無線パケット通信の仕様として策定された。

1.1.4. PAN

PANの領域ではIEEE802.15[10]が確定されている。IEEE802.15は、PANの仕様策定のために、IEEE802.11 ワーキンググループから分離独立した活動の中で策定された仕様である。その中にはBlueTooth[11]の規格も含まれている。

1.2. 今後の無線ネットワーク

既に無線ネットワークシステムの普及の時期は過ぎ、今後は、品質や利便性の向上が求められるものと考えられる。

1.2.1. 求められる要件

今後の無線ネットワークに求められる要件を、ここでは以下の2つに示している。

(1) 無線環境の有効活用

現在でも多くの携帯端末は、3GネットワークとWiFiネットワーク双方にアクセス可能な機能を搭載しており、環境やアプリケーションの種別に応じて適切なネットワークスシステムに接続して通信を行うことが可能となっている。あらゆるところに様々な種類の無線通信システムが利用可能となっており、無線を活用した新しいアプリケーションシステムが実現されるであろう。このようなネットワーク環境をユビキタス無線ネットワークと呼んでいる。ユビキタス無線ネットワークの詳細は1.2.2節に示す。ユビキタス無線ネットワークシステムにおける無線利用の第一は、無線種別を跨るアクセスを可能としている点が挙げられる。

ユビキタス無線ネットワークシステムが整い、モバイル端末がさらに普及すると、端末台数の増大に伴い、周波数の有効活用、という問題が発生してくる。無線周波数の利用頻度の低い部分を有効活用することを目的としてCognitive Radio (CR) 技術が開発されている。これにより、その場での周波数利用状況をリアルタイムに把握、柔軟で効率的でかつ信頼

性の高い帯域の活用を実現することが可能になる。CR 技術の詳細を 1.2.3 節に記載している。利用者のモバイル端末は、複数の無線システムに相互にアクセス可能となっている。今後はユビキタス無線ネットワークのさらなる普及に応じて、複数ネットワークシステムを持つモバイル端末は増加し、複数の無線種別を跨って通信を行うことが一般的になってくるであろう。

(2) 無線通信に対する QoS の向上

無線ネットワークの通信品質低下、特に通信の遅延・途絶、パケット欠落などは、今にもまして許容されなくなる。通信中の品質低下はさることながら、セッション開設から認証に要する時間の短縮が求められる。さらにモバイル端末特有の要件として、移動により無線基地局が移り変わる、ということが挙げられる。この基地局の切り替えをハンドオーバ(handover)と呼ぶ。通信実施中にハンドオーバが発生したとしても、その通信は継続せねばならず、それに起因する通信異常は最小限にしなければならない。そのためのハンドオーバの高速化の手法が提案されている[12]。また前述のユビキタス無線ネットワークにならい、今後は前述の異種無線システム間での切り替え(Vertical Handover)の機能も求められる。

1.2.2. ユビキタス無線ネットワーク

前述のように、多くの種類の無線ネットワークシステムの開発によって、様々な場所や用途で無線通信が利用される場面が増大しつつある。そのような「あらゆるところで利用可能なネットワーク」を指して「ユビキタスネットワーク」と呼ぶ。総務省では「いつでも、どこでも、何でも、誰でも」ネットワークに簡単につながる社会を目指した u-Japan 政策を立ち上げ、「ユビキタスネットワーク整備」「ICT 利活用の高度化」「利用環境整備」の 3 点からの研究開発を行っている[13]。

近年では携帯端末、スマートフォン、からノート PC にいたる多くのモバイル機器製品に 2 種以上の無線ネットワーク通信機能が組み込まれているまたは別に接続することが可能であり、機器レベルにおいては、既にユビキタス無線ネットワークへの対応が十分可能な状況になってきている(図 1-1)。

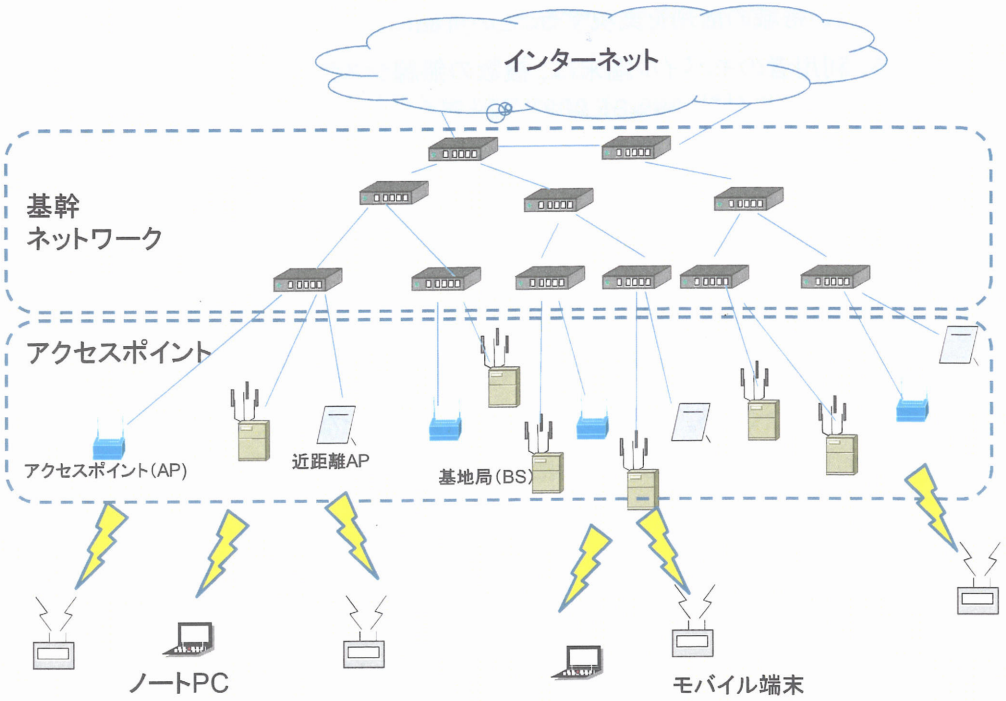

図 1-1 ユビキタス無線ネットワークシステムのイメージ

1.2.3. Cognitive Radio システム

ユビキタス無線ネットワークシステムが整い、モバイル端末がさらに普及すると、端末台数の増大に伴い、周波数の有効活用、という問題が発生してくる。

Cognitive Radio (CR) 技術は、無線周波数の利用頻度の低い部分を有効活用することを目的として開発された技術である。CR 技術により、その場での周波数利用状況をリアルタイムに把握することで、柔軟で効率的でかつ信頼性の高い帯域の活用を実現することが可能になる。既にその帯域を利用している既存のデバイスやシステムには影響を与えることなく、未使用の周波数帯域の再利用が期待されている(図 1-2)。

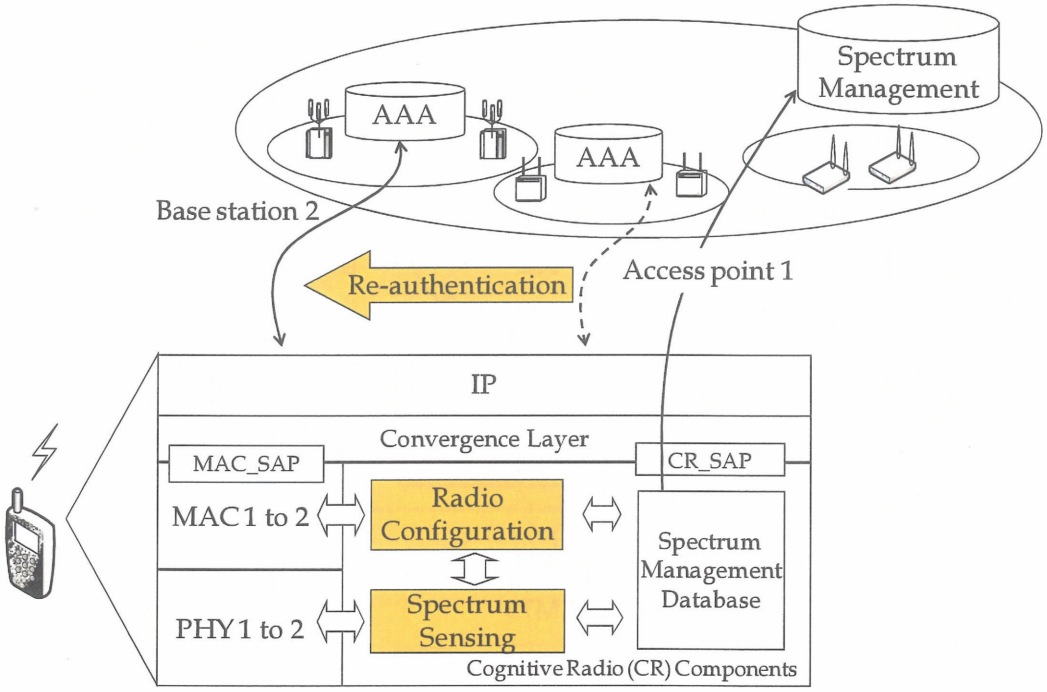

図 1-2CR ネットワークアーキテクチャ

IEEE802.22[14][15]は、Wireless Regional Area Network での仕様であり、米国にてもともと TV サービス用途として割り当てられた帯域の有効活用のために策定されたものである。TV サービス用の未使用帯域は TV 用の領域(VHF/UHF 帯)のため、包含できる範囲が広く(数十キロ)、無線ネットワーク用で活用すればその地域での新しいサービスの創出につながることが期待されている。ただ未使用帯域は使用中の帯域の「隙間」であり、干渉や既存サービスへの影響を考えると、動的に周波数を切り替えて利用する CR の方式が最適であると考えられている。

IEEE802.22 は、MT と BS および Radio Resource Database(DB)で構成される。DB にはリソースの利用状況が常に管理されており、BS は DB に問い合わせをして空きチャネルを探し、自身が利用できるチャネルの選定を行う。MT との通信はその中で利用可能なチャネルを用いる。通信が確率されたらその情報は逐次 DB にアップデートされ、最新の無線利用状況が常に DB に管理されている(図 1-3)。

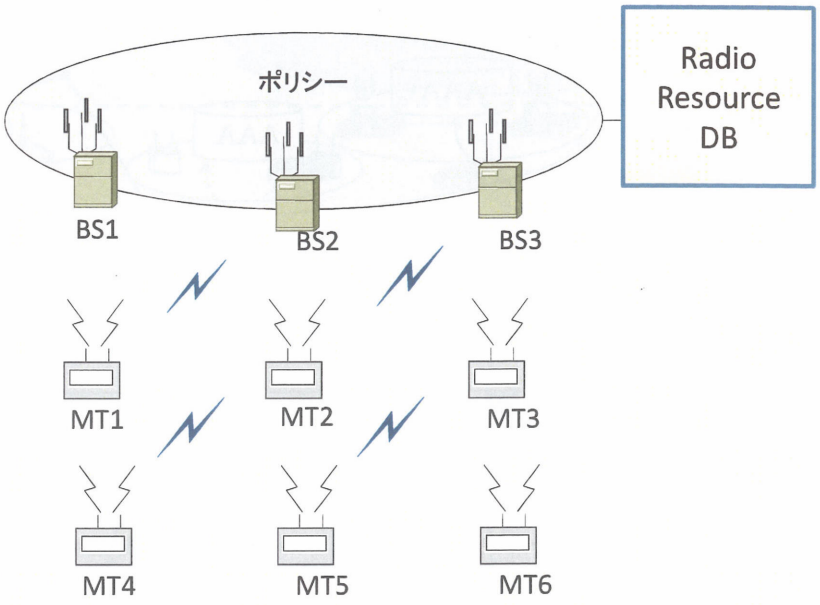

図 1-3IEEE802.22 の構成

IEEE1900.4[16]は、複数種類の無線技術によって構成されている無線ネットワークシステムでの QoS や通信の収容量を拡大するための技術である。また複数のネットワークオペレータで構成されている無線ネットワークシステムでの CR もサポートしている(図 1-4)。

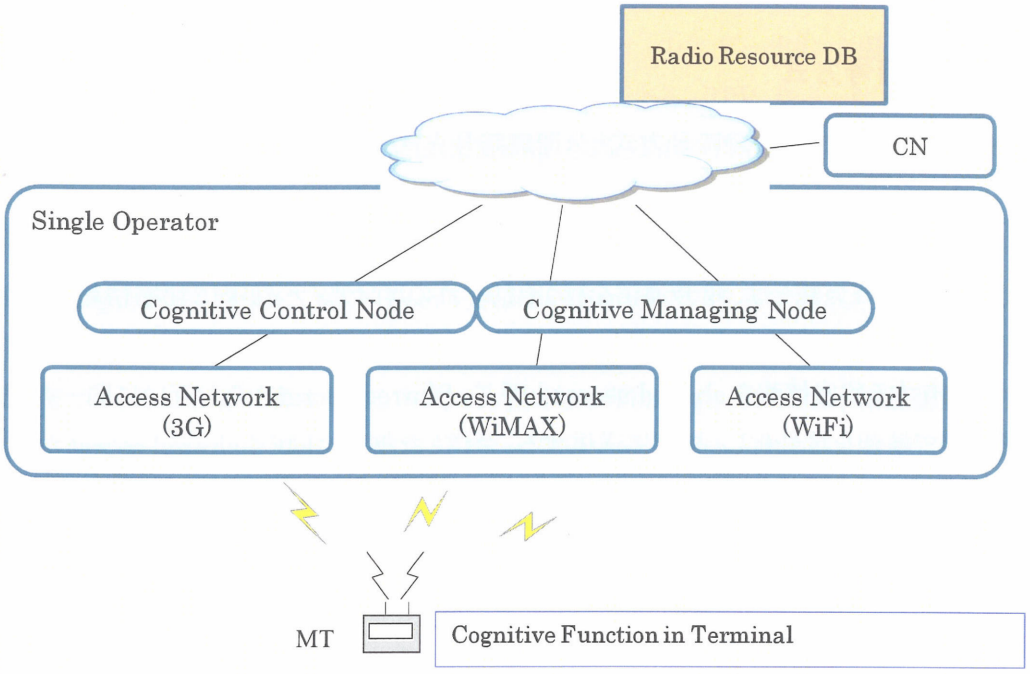

図 1-4IEEE1900.4 の構成

図 1-4 では、MT が 3G、WiFi および WiMAX の 3 つのインタフェースを実装しているシナリオを示している。MT は、そのネットワークオペレータが用意している種類の無線ネットワークの中から利用可能な一種類を選択し、その AP を用いて通信を行う。

IEEE1900.4 において、MT は最初に、その近傍の無線状況をセンシングし、利用可能な無線種別の候補を洗い出す。次に DB に Conflict の可能性等について問い合わせを行う。DB は全ての MT 及び AP の無線利用状況を管理しており、利用可能な無線システムを MT に返答する。その答えを受けて、MT は自分自身の物理層と MAC 層を再構成してその無線システムと通信可能な状態に変更し、次のステップである認証処理に移る。

1.3. 無線ネットワークのセキュリティ対策

無線ネットワークの普及につれて、情報セキュリティ対策の必要性が求められるようになり、それを実現するための検討が進められている。現在ではそれぞれの無線ネットワーク種別ごとに規格が策定されている。規格の対象は、モバイル端末とネットワークオペレータとの間の相互の認証や、暗号通信のための鍵生成などとなっている。

本節では、現在の無線ネットワークセキュリティ方式について説明する。個々のセキュリティ対策の具体論に入る前に、その前提となる暗号方式と、無線ネットワークでの標準に多く採用されている EAP(Extensible Authentication Protocol)について説明する。その内容を踏まえて、個々の

無線ネットワークセキュリティの具体的内容を説明する。

1.3.1. 暗号方式

暗号方式には、共通鍵暗号方式と公開鍵暗号方式がある[17][18]。

(1) 共通鍵暗号方式

共通鍵認証方式とは、暗号通信を行うそれぞれのエンティティが同じ秘密情報を共有しており、さらに互いがその秘密情報を利用して暗号鍵を生成し、情報を暗号化する方式である。エンティティが共有する秘密情報を shared secret と呼ぶ。Shared secret からお互いに同一の鍵を生成し、その鍵で情報を暗号化し、相手に送信する。受信した側では同じく shared secret から生成した鍵で復号する。その shared secret を持たない第三者にはその暗号文を解読することができない。

代表的な共通鍵暗号方式としては、DES[19]、AES[20]、Camellia[21]などがある。

(2) 公開鍵暗号方式

公開鍵暗号方式とは、暗号化通信と互いの認証を実現する方式である。公開鍵方式で用いる鍵は、公開鍵と秘密鍵という二つの鍵のペアで構成される。秘密鍵で暗号化した電文は対応する公開鍵でなければ復号できず、逆に公開鍵で暗号化した電文は対応する秘密鍵でなければ復号できない、という特徴を持つ。最も有名な公開鍵暗号方式としては、RSA 方式[22]がある。これは素因数分解の困難さを利用した暗号である。

公開鍵による相互認証方式は、モバイル端末側とネットワーク側がそれぞれ個別に上記の鍵ペアを作成する。それぞれ自分の秘密鍵は完全に秘匿しておき、公開鍵は互いに配布する。この公開鍵の配布方式などには、PKI(公開鍵技術基盤) 技術が用いられる[23][24]。

公開鍵方式を採用した代表的な相互認証と暗号通信のプロトコルは、SSL(Secure Socket layer)[25]である。SSL は元々 Web ブラウザと Web サーバとの間の暗号通信と相互認証のために開発されたプロトコルである。SSL において Web ブラウザが Web サーバの正当性を認証することを「サーバ認証」と呼び、Web サーバが Web ブラウザ(利用者)を認証することを「クライアント認証」と呼ぶ。プロトコルとしては双方の認証機能を備えているが、どちらか一方のみ実施しても問題ない。実際の多くの Web サイトでは、サーバ認証のみ実施し、クライアント認証はユーザ ID とパスワードを用いる「パスワード認証」を行う場合が多い。

SSL は現在では Web システムに限らずセキュアな通信にかかわる多くの場面で利用されている。SSL はほぼそのままの形で標準として策定したものが TLS(Transport Layer Security)プロトコル[26]である。

1.3.2. EAP

EAP(Extensible Authentication Protocol)[27][28]とは、主にデータリンク層上での複数の認証方式のサポートを目的として策定された認証プロトコルである。PPP やイーサネット等の上での利用を想定されている。EAP は大きく Multiplexing 方式と Pass-Through 方式に分けられる。

(1) EAP の方式

Multiplexing 方式(図 1-5)は、端末(Peer)と Authenticator との 2 者で構成される方式である。Pass-Through 方式(図 1-6)は、Peer と Pass Through Authenticator と Authentication Server(認証サーバ)の 3 者で構成される方式である。Pass-Through 方式では、相互認証の役割は Peer と Authentication Server が担う。Pass Through Authenticator は単に Peer と Authentication Server との中継を行う。その意味で Pass Through Authenticator は、端末からのネットワークアクセスの窓口の役割を持つため Network Access Server (NAS)と呼ばれることもある。

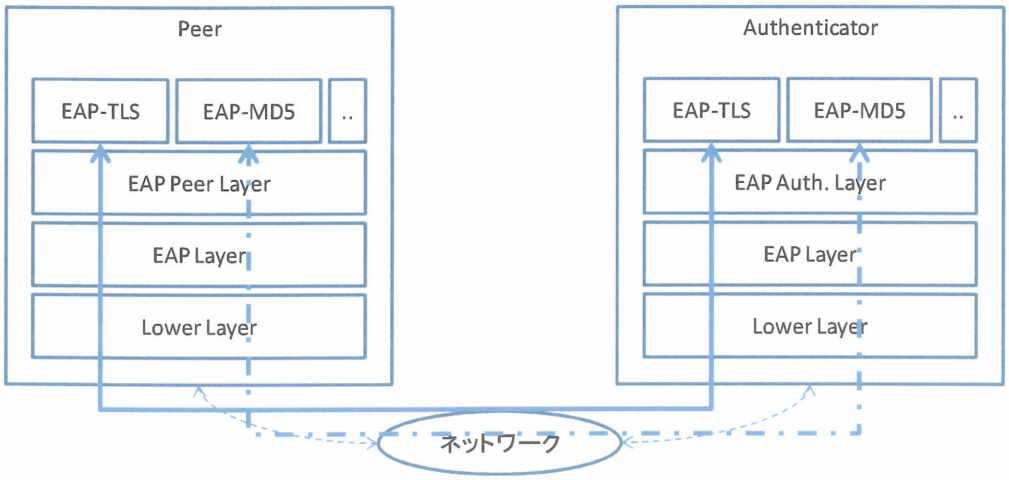

図 1-5EAP:MultiPlex 方式

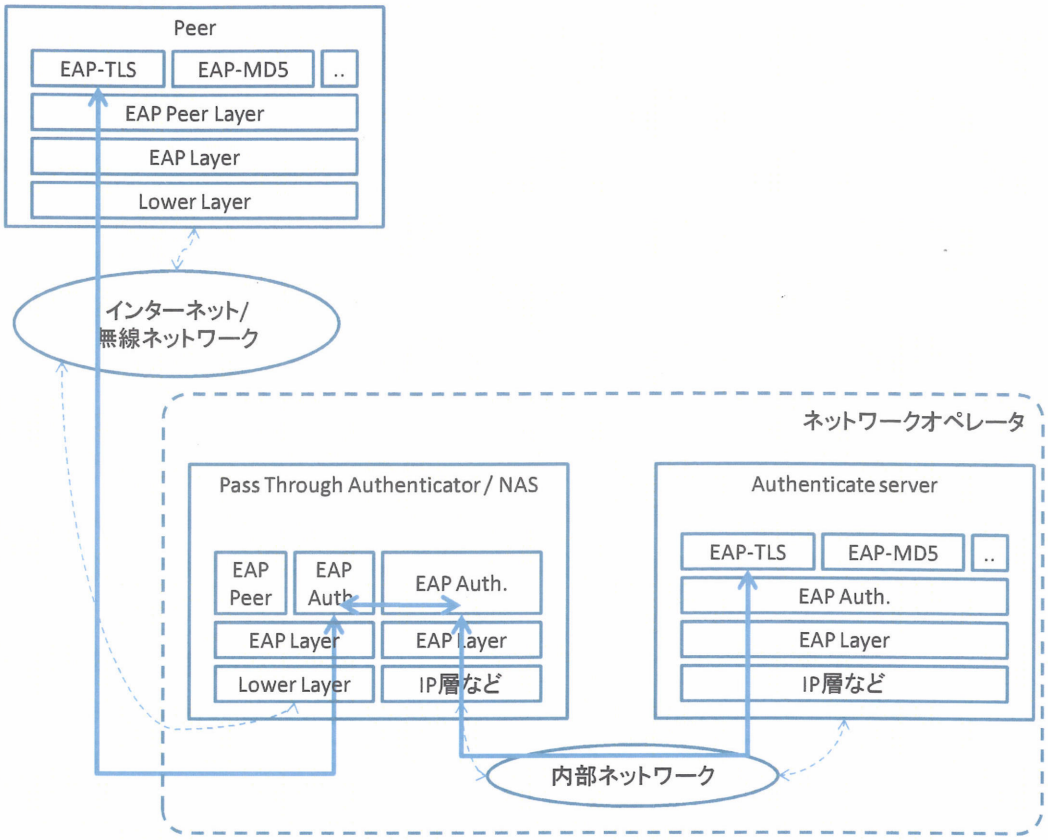

図 1-6EAP:PassThrough 方式

Multiplexer 方式では、Authenticator が Peer との相互認証処理を実施する必要がある。これは Authenticator が独自の Shared secret を持ち、Peer が固定でその Authenticator との間のみで共有すれば十分な場合には有効であるが、Peer がモバイル端末の場合等、通信実施の都度アクセスする Authenticator が変化するシステムに対しては、Authenticator がネットワークオペレータの Shared secret を常に保有するかまたは Peer が通信対象となる全ての Authenticator の Shared secret を共有するする必要があるため、現実的ではない。そのため、モバイル端末を Peer とする場合には、Shared secret を Authenticate Server で一括管理する Pass-Through 方式の採用が一般的である。

ただしこの Authenticate Server に集約する方式そのものが、Pass-Through 方式のデメリットにもなっている。第一に、認証処理の都度内部ネットワークを介して Pass through Authenticator と Authenticate server との通信が必要になる点である。Authenticate Server はその性質上中央の少数大規模サーバとして構築されるが、大規模な無線ネットワークの場合、辺境の Authenticator からのリクエスト・レスポンス時間が問題となる。第二に、Peer の認証処理を全て Authenticate Server で実施せねばならないため、その Server に掛かる負荷が大きくなる点が上げられる。

(2) EAP 鍵階層

EAP の規格においては、そのプロトコルで用いる鍵階層が定義されている。EAP 鍵階層はルートである Shared secret から、Master Session Key (MSK)と Extensible Master Session Key (EMSK)が同時に作成される。

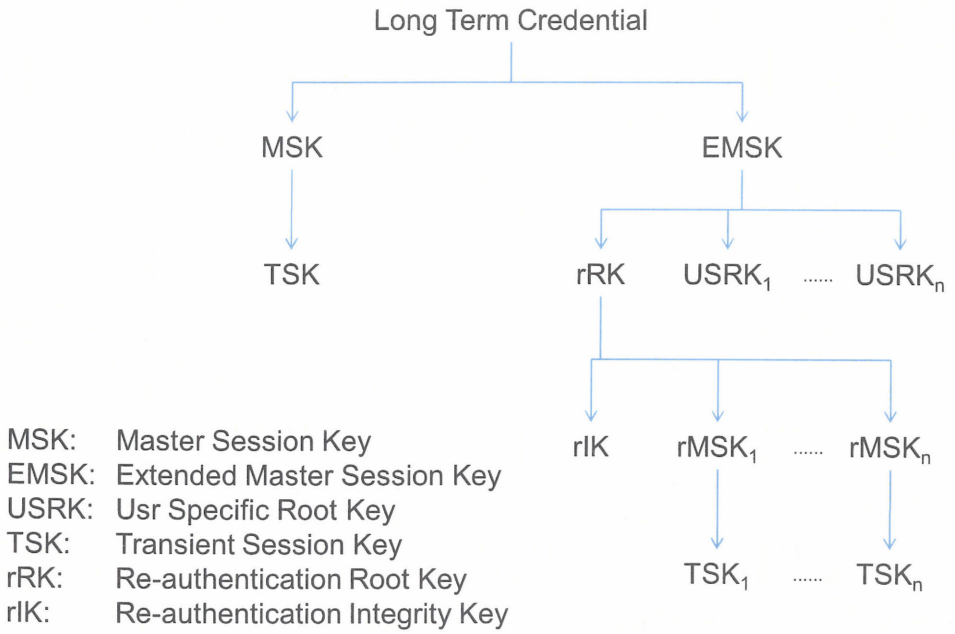

図 1-7 EAP 鍵階層

MSK は暗号通信に用いられる全ての Session Key のマスタ鍵である。この MSK を元にして、そこから Transient Session Key (TSK)が作成され、TSK により MT と Authenticator 間の通信の暗号化が実施される。

もう一つの EMSK は、そのほかの多くの用途に用いられることが想定されている。特に EMSK から作成される Re-authentication Root Key (rRK) およびそこから生成される Re-authentication Integrity Key (rIK)は MT のハンドオーバ時の再認証を実現するために用いられる。rRK からは、rIK のほかに、re-authentication 後に用いるセッションマスタ鍵として、re-authentication Mastek Session Key (rMSK)、さらにそこから Transient Session Key TSK)を生成する。

(3) EAP ベースの認証方式

EAP 層はデータリンク層の規格であり、具体的な認証プロトコルは、その上位において定義される。例えば、EAP-SIM[29]、EAP-AKA[30]、EAP-TLS[31]、EAP-TTLS[32]、PEAP[33]などがある。

EAP-SIM[29] は EAP 上に構築された共通鍵認証方式の一つである。MT 側は共通鍵を SIM(Subscriber Identity Module)の中に保持する。EAP-AKA[30]は SIM の代わりに USIM(UMTS SIM)に共通鍵を収めた認証方式である。

EAP-TLS[31]は、TLS プロトコルを EAP の上に搭載したものであり、証明書によるクライアント認証とサーバ認証の双方を行う。

EAP-TTLS[32]は、TLS のサーバ認証のみを実施する方式である。サーバ認証によって安全な通信路を確保しておき、クライアント認証は通常のチャレンジ/レスポンスによる認証を行う。

PEAP[33]は、暗号通信路として TLS のサーバ認証を用いる。サーバ認証完了後作成した安全な通信路を用いて再度 EAP 通信を行い、クライアント認証を行う。

これらの認証方式は、Multiplex 方式、Pass Through 方式の双方で実施可能であるが、多くの場合は Pass Through 方式により実現されている。このとき、ネットワークオペレータ側の Shared secret は認証サーバ(Authenticate Server)に保存される。Peer の認証処理も Pass through Authenticator を経由して認証サーバにて実施される。従って EAP による認証の実現は、認証サーバの存在を前提とした方式ということができる。

1.3.3. 現在の無線セキュリティ規格

現状では、無線ネットワーク種別ごとにそれぞれ独自のセキュリティ規格が策定されている。

(1) 3G ネットワーク

3G/GSM セルラーシステムは、携帯端末毎に異なる暗号鍵を、携帯端末とネットワーク側で共有する共通鍵暗号方式を採用している。携帯端末側は、その暗号鍵を SIM に格納しておき、ネットワーク側は一つのサーバ(Home Location Register (HLR)と呼ばれる)において管理することで、相互認証を実現している[34]。

(2) WiFi、無線 LAN

IEEE802.11[1]に基づく無線ネットワークシステムは、過去の経緯から、多くの認証方式が規格化されてきている。

Wired Equivalent Privacy(WEP)[35]は最初に考えられた IEEE802.11 ベースの共通鍵暗

号方式による認証プロトコルである。当初は無線ネットワークでの機密性確保のためのプロトコルとして期待されていたが、その後深刻な脆弱性が発見されており[36][37]、現在では利用されなくなってきている。

Wi-Fi Protected Access (WPA)[38]は上述のWEPの脆弱性対策のために考案されたプロトコルである。同じく共通鍵暗号方式であるが、より長い初期ベクタ IV(48 ビット)と、より長い鍵長(128 ビット)を採用することでWEPの弱点を克服しようとした。また、鍵更新方式としてTKIP(Temporal Key Integrity Protocol) [38]を採用した。しかしながら、この方式は近年ではストリーム攻撃に対して脆弱であることが明らかにされた[39]。そのため、WPA ベースでの近年最も堅牢な方式としては AES 暗号を採用した方式に移りつつある。WPA はパーソナルモードとエンタープライズモードの2種類の鍵管理方式が採用されている。このうちパーソナルモードは鍵共有方式である。無線ネットワークのアクセスポイント(AP)とモバイルデバイスとの間でパスフレーズを共有し、アクセス時にはそのパスフレーズを入力することにより確認を図る。

IEEE802.11i[38]はまた、認証の方式として、IEEE802.1X[40]を採用している。IEEE802.1X が採用している認証方式は EAP-TLS[31], PEAP[33], EAP-TTLS[32]などが挙げられるが、これらは全て公開鍵暗号方式である TLS に基づく認証方式を採用している。

(3) WiMaX

WiMaX[7]の認証方式は、802.1X と同様に EAP ベースの認証方式を採用している。ただし相互認証の方式は採用されておらず、サーバ認証のみ。クライアント認証は別のチャレンジ/レスポンス方式で実施する必要がある[41]。

1.3.4. CR Network のセキュリティ

周波数帯域の有効活用のために CR ネットワーク技術が現実に適用され広く展開されるためには、これまでの検討範囲とは異なる、まったく新しいセキュリティに関する検討が必要である。CR ネットワークのセキュリティソリューションは、以下に示す項目を検討していく必要がある。

1. CR ネットワークシステムで割り当てられた周波数が、適切な割り当てポリシーに従っており、不正なデバイスによるジャミングや DOS アタック等にも影響を受けずに利用可能であること。

2. MT 側の CR システムの構成モジュールが、その周波数割り当てに応じて正しく再構成されること。不正なモジュールが MT 内に入り込み、システム全体に影響を与えることのないように。

3. MT が再構成されて新しい無線システムによって通信を開始する前に、認証/再認証の処

理を確実に実施すること。

IEEE802.22 は、IEEE802.16e のセキュリティ仕様を基にしたセキュリティ層を含んでいる。そのセキュリティ層によって、メッセージ認証の導入による不正な MT からの DoS 攻撃への対処を実現している。また IEEE802.22 は完全にネットワーク主導での周波数割り当てを実施する CR システムであるため、不正な MT による周波数割り当てへの妨害を実施することができない。しかしながら MT と一つの BS の間での認証方式は存在するが、CR によるシステム再構成後の新しい BS や周波数での再認証の方式は規定されていない。IEEE802.22 の脆弱性については既に議論されており[42]、DoS 攻撃やリプレイ攻撃などの脅威が示されている。また、その脆弱性は主として、CR ネットワークを構築している BS 間のチャネルの防御が未熟であることに起因している。

CR ネットワークに対する Primary User Emulation (PUE)と呼ばれる攻撃も示されている[43]。これは攻撃者が利用許可を受けた周波数帯での通信をエミュレートすることで無線インタフェースを変更することが可能となる攻撃である。またその防御の方法および攻撃者の位置を特定する方法として、transmitter verification 法が提案されている[44]。

悪意のある MT によるジャミング攻撃から CR ネットワークを防御するために、CR の動作を保証するフレームワークが提案されている。その名称を TRIESTE と呼ぶ[45]。TRIESTE は CR システムが連携してある統一した周波数利用ポリシーを遵守するための機構である。General Purpose Cognitive Radio Layer, Distributed Spectrum Authority (DSA) layer, および Spectrum Lay Makers (SLM) layer と呼ぶ三つの層から構成されている。SLM では周波数利用のルールを策定し、DSA では MT がそのルールを遵守することを監視する役割を担う。

IEEE1900.4 は、"Network-managed and terminal helps アーキテクチャ"と呼ばれる、CR による周波数や無線システム割り当てを MT が一部サポートして実現する方式を採用している。その構成は、周波数や無線種別割り当てを決定する Network Reconfiguration Manager (NRM)と、その決定にもとづいて MT 上で CR 構成モジュールの再構築を行う Terminal Reconfiguration Manager (TRM)から構成される。CR の周波数割り当ての再構築はこれら NRM と TRM との強調によって、すなわちネットワーク側と MT 側の双方によって実施される。CR におけるセキュリティは通常の通信のセキュリティに加えて、周波数割り当て機能の堅牢性も検討の対象となる。

IEEE1900.4 は NRM の構成によって 3 つのアーキテクチャに分けられる。第一に単一または複数のネットワークオペレータが一つの NRM と複数の Radio Access Network (RAN)を持つ場合。ここで RAN とは WiFi,WiMAX、などのデバイスを指す。第二に複数のネットワークオペレータが単一の NRM を共有する場合。第一の場合は、NRM はそれぞれのネットワークオペレータのポリシーによって守られているため、NRM に対する攻撃は困難とみなしてかまわない。MT 側の TRM も、オペレータとの認証を経て通信を開始するため、攻撃者が TRM に介入する余地は無

い。

第二の場合は、NRM がオペレータの外部に設置されているため、セキュリティの検討が必要である。この場合は NRM とオペレータ間にセキュアなチャネルが用意されていることが前提となる。また TM 側の TRM は、前記と同様にオペレータの認証を必要とするためセキュアと考えてかまわない。

第三の構成としては、MT が主導で周波数割り当てを主導する構成が考えられる。この場合、もし MT 側に侵入を許した場合に、悪意のあるプログラムが周波数割り当てを故意に変更するなどの攻撃を行う可能性が想定される。この場合は MT 側の reconfiguration 時の認証を実施する必要がある。製品内部に含まれるソフトウェアモジュールの正当性を保証する仕組みとして Trusted Computing Platform[46]が提案されている。

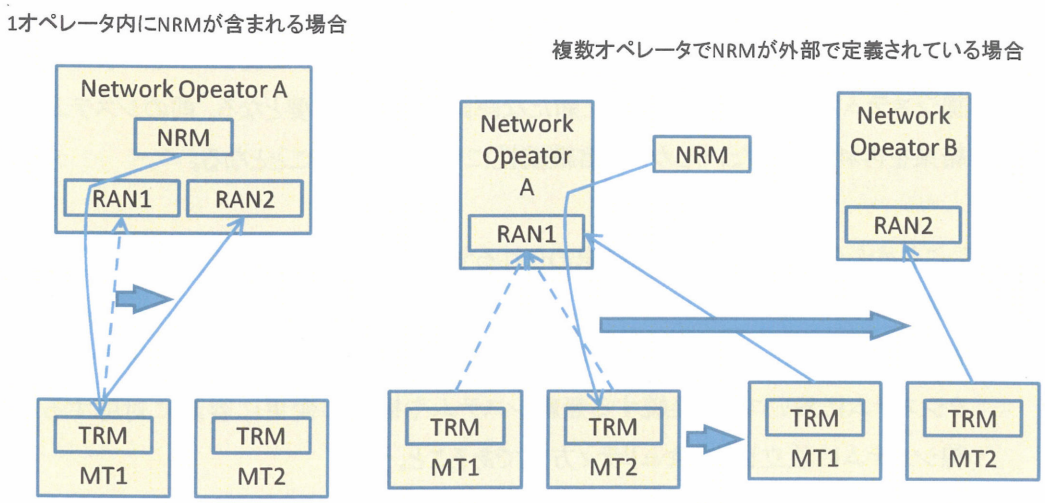

図 1-8CR ネットワークのアーキテクチャ

IEEE1900.4 には特定の認証方式は規定されていない。IEEE1900.4 の認証は、既存の無線システムにて提供されている認証アルゴリズムまたは認証方式をそのまま活用することを求めている。

CR ネットワークシステムで重要なもう一つの機能は MT と CR ネットワーク側との re-authentication(再認証)である。MT の利用者が実施している通信を途切れさせたりすることの無いように、シームレスな再認証を実現する必要がある。CR ネットワークシステムは元々 QoS を維持することを目的として開発されているため、認証・再認証フェーズにおいてもそれを維持する必要がある。この機能は複数の無線システム(WiFi、WiMAX、3G など)から構成される CR ネットワーク(IEEE1900.4 等)ではより重要になる。個々の無線システムの認証方式がそれぞれ異なるために、シームレスな認証・再認証の実現を困難にしている。

1.4. 現状の課題

現在の無線ネットワークのセキュリティ方式の一番の問題は、それぞれの無線デバイスに依存した規格が策定されており、セキュリティに関する規格もそのデバイス毎に分かれている点にある。3G は 3G の無線セキュリティの規格が、IEEE802.11 には固有の WEP や WPA という規格が、さらに IEEE802.1X という規格が存在する。WiMAX や IEEE802.16 などもそれぞれ固有のセキュリティ規格を保持している。これは、1.2 節に記載のこれからの無線ネットワークシステムにおいて、以下のような問題を引き起こすと考えられる。

- ユビキタスネットワーク環境において、複数種のセキュリティ実装をシステムに搭載する必要があり、ハンドオーバ等のネットワーク間切り替え処理などではセキュリティ実装も切り替える必要がある。これは特にモバイル端末側での処理を複雑にする。
- 無線種別ごとのセキュリティ規格においてはそれを満足する認証処理が求められ、別の無線システムに接続するたびにまた新たな認証手続きが必要となる。前のシステムで認証した結果を再利用できないため、通信継続性に支障をきたすこととなる。

従って、これからの無線ネットワークに求められるセキュリティシステムは、以下のような観点から検討する必要がある。

(1) 複数種の無線ネットワークシステムからなるユビキタスネットワークシステムや CR ネットワークシステムにおいても、接続する無線システムや構成の変更に容易に対応するために、無線システムに独立したセキュリティ方式であること。

(2) そのセキュリティ方式で実装する認証プロトコルや暗号方式そのものが、アプリケーション通信の継続性や QoS を低下させることのないこと。

1.5. 本研究の目的と進め方

本研究の目的は、前節の課題を解決するために、(1)複数種類の無線ネットワークからなるユビキタスシステムにおいて、無線システムとは独立した、(2)アプリケーションの通信品質を低下させない、まったく新しい無線ネットワークセキュリティ方式を検討し提案することである。

次の第 2 章では、新しい無線ネットワークのセキュリティのための相互認証・暗号通信方式を提案するにあたり、具体的に、どういった観点で検討・設計すべきかについて議論し、その結果を示した。

それ以降の2つの章では、その具体的な提案である、モバイル端末ーネットワークオペレータ間の相互認証プロトコル Carousel Rotating Protocol (CRP)[47][48] [49][50]について説明してい

る。

第 3 章は本研究の主要部分である CRP の説明と評価を記載している。最初に CRP の基本的考え方を示し、その後、データ構造とプロトコルの詳細、について説明した。続いてその評価として、セキュリティ面での強度に関する評価と、プロトタイプ実装によるパフォーマンスの評価、の 2 面に対して実施した結果を示している。

第 4 章では、モバイル端末による通信中の移動に伴う基地局間ハンドオーバ時の再認証(re-authentication)の実現のために、この CRP を拡張した再認証プロトコル・CRP re-authentication を示し、そのパフォーマンス面での評価結果を示している。

2. 新しい無線ネットワークセキュリティ方式の検討

本章では、これからの無線ネットワークシステムに適用すべきセキュリティモデルを検討する。

2.1. 共通鍵暗号方式か公開鍵暗号方式か

方式検討の最初のステップとして、共通鍵暗号方式を採用するか、それとも公開鍵暗号方式を採用するか、について検討する。

2.1.1. 共通鍵暗号方式の長所と短所

共通鍵暗号方式とは、1.3.1 節に記載したとおり、モバイル端末とネットワークオペレータが双方同一の情報を共有し、その情報を元に鍵を生成して、その鍵によって暗号通信と相互認証を実現する方式である。

共通鍵暗号方式の長所は、ひとえに強力で高速な暗号アルゴリズムが普及していることにある。端末側とネットワーク側である情報を共有できていれば、その共有情報(shared secret)を用いて共通鍵暗号アルゴリズムによって、相互認証や暗号化通信を行うことが可能となる。暗号アルゴリズムの評価は CRYPTOREC によって定期的に実施され報告[51]がなされている。この評価活動の中でその強度が認められた暗号アルゴリズムは、電子政府推奨暗号リスト[52]として公開されている。

逆に、共通鍵方式の短所としては、shared secret の管理とそこから生成する鍵の利用そのものにある。

第一に、shared secret から生成した一つの鍵を長時間にわたって使い続けていると、その鍵によって作成された暗号文が多量に公開されることになり、それらの暗号文から平文や暗号鍵を解読されるリスクが増大することになる。そのリスクを回避するために、暗号鍵を定期的に更新する方策が必要となる。暗号鍵を定期的に生成・更新する方式としては、ハッシュチェーンによる方式が広く用いられている(図 2-1)。これは最初の鍵を shared secret からある鍵生成関数を用いて生成し、それ以降は、その最初の鍵から同じ鍵生成関数を用いて定期的に鍵を生成し続ける方法である。最初に Shared secret を共有するとそれ以降は共有の手続きをとることなく、鍵を更新することが可能である[53]。この鍵生成関数にはハッシュ関数が多く用いられている。また、同様の方式は、セキュリティトークンによるワンタイムパスワードの生成にも用いられている。

しかしながら、ハッシュチェーンによる方式では、もし攻撃者により任意の時点での暗号鍵が解読されてしまった場合、そこから芋づる式に次の鍵・次の鍵、という具合に鍵が再生成されてしまう。

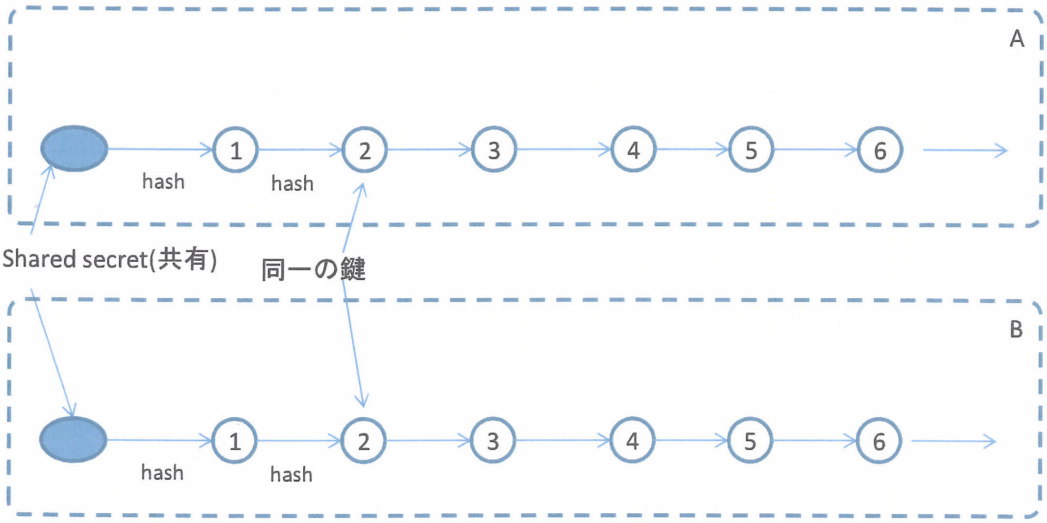

図 2-1 ハッシュチェーン

この鍵の漏洩と再生成を防止するために、鍵生成アルゴリズムの中に、鍵の予測不可能性を向上させる方式が用いられている(図 2-2)[18]。

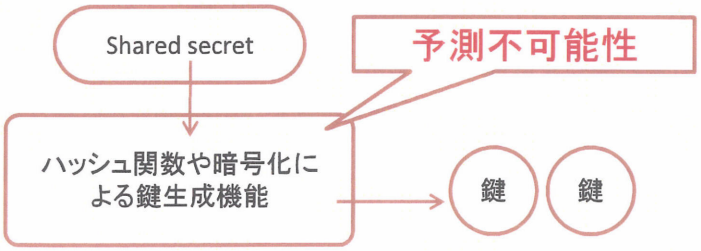

図 2-2 鍵の予測不可能性向上の方式

第二の問題点としては、shared secret の管理が挙げられる。事前に通信を行う両者の間で Shared secret を共有する必要があるが、モバイル端末のように通常遠く離れた場所にいるような機器との共有は一般に非常に困難であり、その共有手続き中に shared secret が漏洩する可能性もある。また安全に共有できたとしてもそれを門外不出とし、漏洩のリスクから回避する方策をとらなければならない。如何に鍵の予測不可能性を向上させていたとしても、Shared secret の漏洩は即、鍵の推測につながり、それが安全な通信を侵すことになる。

2.1.2. 公開鍵暗号方式の長所と短所

公開鍵暗号方式は、1.3.1 節に記載のとおり、秘密鍵と公開鍵という鍵ペアによって暗号通信と認証を行う手法である。

公開鍵暗号方式のメリットは、共通鍵暗号方式で必要となる shared secret が不要となる点にある。秘密鍵と公開鍵のペアを自身で作成して、公開鍵のみ外部に公開しておけば十分であるため、共有鍵方式にて必要となる shared secret 共有に伴う漏洩のリスクをかぶる必要が無い。

逆に、公開鍵方式のデメリットは、第一に、その暗号処理に多大な計算量を必要とするところにある。RSA 暗号[22]処理は、通常の共通鍵暗号方式に比較して 2 桁以上の計算量を必要とすることが知られている。また十分な強度の暗号処理を実施するために、鍵長も十分長くする必要があることもその傾向を加速している。

第二に、公開鍵の所有者を証明する手段が容易ではない点にある。いくら「この公開鍵は私のものです」と言ってもそれを証明する客観的な方法が無い限り意味を成さない。共通鍵方式では Shared secret 共有時になんらかの物理的手段が必要であるが逆にそのことが鍵と実際の所有者との連携を証明する最も良い方法となっている。公開鍵方式においてその所有者証明には、電子証明書[23]を用いる方式が一般的であるが、実際は下記のような複雑な運用が必要となる[55][56]。

例えば、ある Web サービスプロバイダ A が SSL 暗号化通信のサイトを構築する場合、A の公開鍵の証明のために、信頼できる第三者(Trusted Third Party:TTP)である認証局に対してその公開鍵の電子証明書の発行を依頼する。Web ブラウザ B がそのサイトにアクセスすると、SSL の認証手続きに応じて A の電子証明書が B に送信される。B はその A の電子証明書の認証を実施しなければならないが、その認証のためには、先の第三者認証局の電子証明書が必要である。B はこの第三者認証局の電子証明書も認証しなければならない。そのためにはこの第三者認証局の電子証明書を発行した認証局の電子証明書を、、という具合に、上位の認証局の電子証明書を取得・認証し続ける必要がある。これでは無限に上位まで進んでしまうため、実際には Web ブラウザに同梱されている上位認証局の電子証明書は信頼すべきもの(Trust Anchor)として、その電子証明書に達するまで認証処理を繰り返す。

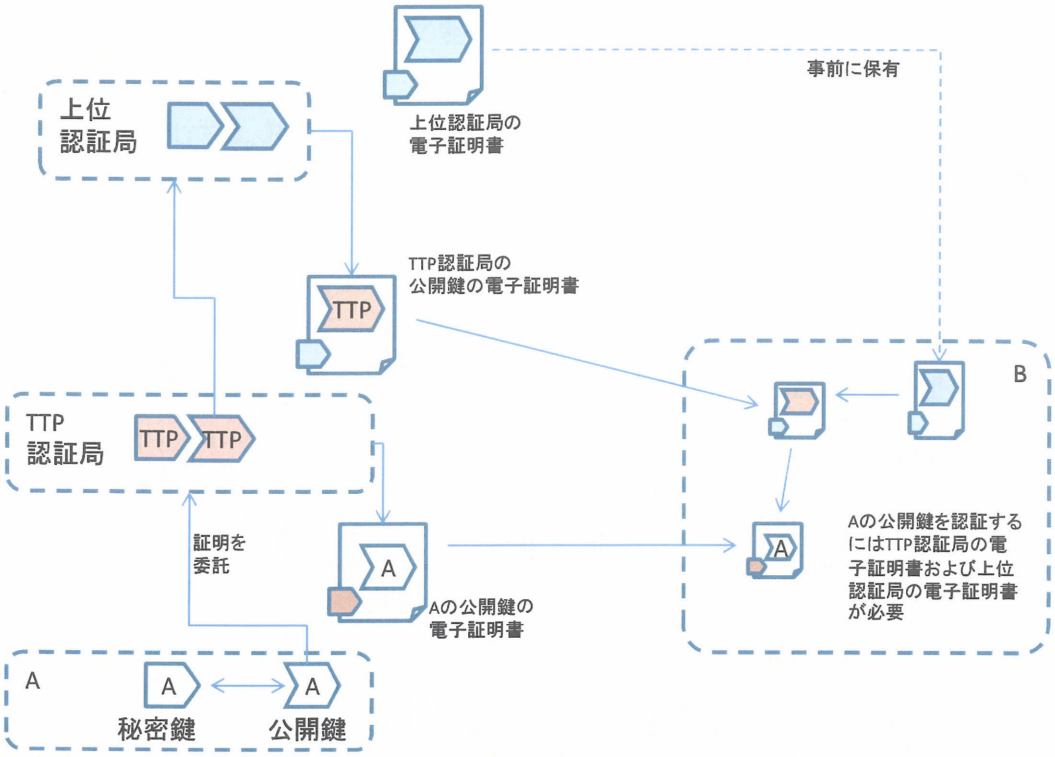

図 2-3 電子認証基盤の例

このように、公開鍵方式は、鍵を共有する手続きにおける漏洩のリスクを抑えることは可能であるが、実際にそれを実現するためには電子認証基盤のような大規模な第三者機関が必要となっている。この認証基盤のメカニズムは SSL や TLS のプロトコルに現実に組み込まれており、ブラウザがサーバを認証するにもこのような大掛かりな証明書認証の手続きが必要になる。

公開鍵方式を用いた認証方式 EAP-TLS[31], PEAP[33], EAP-TTLS[32]に共通する特徴は、全てにおいて、サーバ認証が必要となる点である。サーバ認証の処理は全てクライアント側、すなわちモバイル端末側で実施する必要がある。その具体的な手続きは以下のとおり。

(1) サーバ側からサーバ証明書を受信する。
(2) そのサーバ証明書を TTP である電子認証局の電子証明書により検証する。
(3) サーバ証明書の検証が終了した時点で、その公開鍵を用いて、鍵交換を行う。

これらの処理をモバイル端末側で実施するためには、相応の CPU 負荷とネットワーク通信量、またそれを維持するバッテリ容量が必要となる。認証の都度この処理を行う負荷は、それでなくても枯渇しそうなモバイル端末側の計算機資源を浪費することに繋がる。

なお、公開鍵方式で用いられる暗号アルゴリズムも、CRYPTOREC によって定期的な評価が実施され報告[51]がなされている。そこで認められた暗号アルゴリズムは、電子政府推奨暗号リスト[52]として公開されている。

2.1.3. 共通鍵暗号方式の採用

本節において暗号方式を比較検討してきた結論としては、共通鍵暗号方式を採用することとした。公開鍵暗号方式を採用しない理由は以下のとおり。

(1) 公開鍵暗号方式は、その暗号復号処理に多大の CPU 計算量を必要とする。
(2) 証明書認証の手続きのために、モバイル端末—ネットワークオペレータ間の通信量が増大し、応答性能の低下や処理量の増大に繋がる。

公開鍵暗号方式ではサーバ認証が必須となるため、このような負荷の増大は、特にモバイル端末側に大きな影響を及ぼすことになる。それでなくても軽量化のために限られた量の計算機資源しか搭載できないモバイル端末において、計算量や通信量の増大は無視できるものではないからである。モバイル端末に対する負荷の増大は、認証処理の応答性能に影響を与え、それが通信アプリケーション全体の QoS の低下を引き起こすことが十分予想される。

2.2. 短所の克服

新しいセキュリティ方式として、共通鍵暗号方式を採用することと決定した。しかしながら共通鍵暗号方式では前節に記載のとおりの短所が存在する。その短所を克服することが次の課題となる。

2.2.1. Shared secret の漏洩のリスク

共通鍵暗号の短所は、既に 1.3.1 節に記載のとおり、(1)鍵の再利用による解読のリスク、(2)shared secret そのものが漏洩することによるリスク、の 2 点が挙げられており、(1)については鍵生成機能において、鍵の予測不可能性を向上させることによって対処していることを示した。しかしながら、いかに鍵生成機能の能力が向上しても、(2)のリスクが顕在化してしまえば、それはその通信のセキュリティを脅かすものとなってしまう。

2.2.2. 認証サーバ

Shared secret の漏洩を防止するための最大の方策は、それを可能な限り門外不出とすることである。

そのために、モバイル端末側では、その shared secret を SIM に格納する方式を採用している

場合が多い。EAP-SIM や EAP-AKA 等はその方式を採用している。

また、ネットワークオペレータは、多くの場合、認証サーバを構築する。認証サーバにネットワーク側での shared secret や鍵の管理と、認証処理の統括の役割を持たせる。認証サーバの代表的なアーキテクチャとしては、RADIUS 方式[57][58]がある。RADIUS はクライアントサーバ型の認証モデルであり、RADIUS プロトコルの上に EAP 等の認証プロトコルが載る[59]。

認証サーバは、無線ネットワークシステムの基幹システムとして構築され、無線ネットワークシステムを構築する全てのアクセスポイント(AP)や基地局(BS)などからの認証要求に対する応答を返す機能を有している。

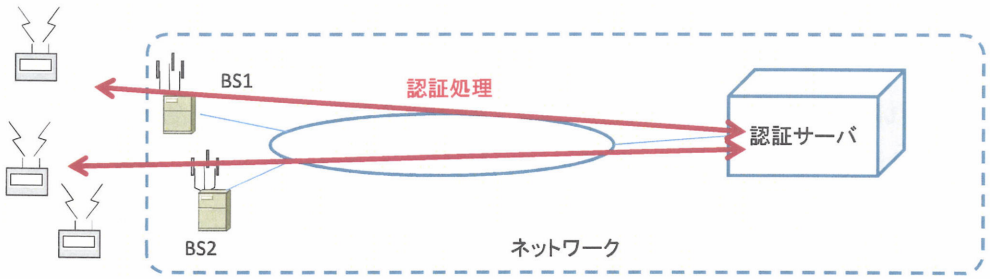

図 2-4 認証サーバの構成

認証サーバは確かに shared secret の漏洩防止には有効である。しかしながら、全てのモバイル端末からの認証要求が認証サーバにて実施されるため、以下のような課題が存在する。

(1) モバイル端末と認証サーバとの間における、認証要求の通信応答時間。これはそのモバイル端末がアクセスしている基地局とサーバとの間の物理的距離に依存するため、その増大が避けられない。
(2) 認証サーバにて実施される認証処理の負荷と処理応答性能。大量のモバイル端末から同時にアクセスが来た場合には、その処理に時間を要することとなる。

このことは、特にモバイル端末のハンドオーバ時の再認証(re-authentication)処理時間に影響を与えることとなる。モバイル端末がハンドオーバを行う時は、なんらかのアプリケーション通信を実施している場合である。そのアプリケーション通信のパケットの消失を防ぐためには再認証処理に要する時間を極力短くする必要があるが、もし再認証処理に認証サーバの介在が必要となれば、応答時間の短縮は困難となる可能性が高い。

本研究にて提案する新しいセキュリティ方式は、無線ネットワーク通信の QoS の向上を目標の一

つとしている。従って、応答の遅延の原因となる処理を極力回避するために、認証サーバを用いない shared secret の漏洩防止策を検討することとした。

2.3. 対応策:Shared secret の予測不可能性の向上

第 1 章の議論で、ユビキタス無線モバイルネットワーク環境やその後に続く Cognitive Radio ネットワーク環境などのモバイル多種無線ネットワークシステムのセキュリティに関して、以下の課題があることがわかった。

1. セキュリティ規格が無線種別に依存しているため、今後の多重無線ネットワーク環境においては認証・暗号化処理の複雑化や切り替えによる応答性能遅延などの問題が発生する。
2. 今後は無線ネットワークが当たり前の世の中になり、通信の QoS の維持・向上が求められる。それはセキュリティ機能においても変わりなく、それによって通信品質低下や途絶は回避しなければならない。

また、前節までの議論において、これらの課題を解決するための新しいセキュリティ方式について検討してきた。

1. セキュリティの認証処理の応答性能を向上させるため、共通鍵暗号方式を採用することとした。それにより、特にモバイル端末側での認証処理時間・CPU 処理量を削減し、応答性能と QoS を向上させることが可能となる。
2. しかしながら共通鍵暗号方式の課題は存在する。
3. 一つ目の課題である、暗号鍵を推測する攻撃については、従来からの鍵の予測不可能性向上策を取ることで回避可能である。
4. 共通鍵暗号方式のもう一つの課題である、shared secret が漏洩するリスクについては、認証サーバを構築する方式があるが、これでは認証処理の応答性能が低下することが避けられない。
   そのために、別の shared secret 漏洩リスクを回避する策を検討する必要がある。これが無ければ我々の求める新しいセキュリティ方式の実現は困難であるといえる。

Shared secret が唯一無二とすると、それが漏洩することによって、暗号鍵が推定され暗号文が解読されるリスクが増える。唯一無二であるにも関わらず長く利用し続けると鍵を推測されるリスクが増大する。従って通信を行う二者の間で定期的に shared secret を再共有しなければならない、というジレンマになっている。

そこで、もし shared secret が唯一無二ではなく、鍵と同様に常に定期的に更新されていくものだと仮定したらどうであろうか？

もしそれが可能であれば、最初の時点こそ shared secret 共有の手続きは必要であるが、それ以降は常に変わり続ける shared secret を用いるために、再共有する必要性をなくす事ができる。また、shared secret が変化するのであれば、もし仮にある時点での shared secret が漏洩したとしても、その時点の shared secret から生成される暗号鍵の系列は暴露される可能性が高まるが、shared secret が更新された時点で、まったく別の暗号鍵系列が生成されることになるため、元の鍵列は何の意味も無いものになり、その被害を最小限にとどめることが可能となるであろう。このような shared secret を考えることができれば、それは新しいセキュリティ方式として、有効になると思われる(図 2-5)。

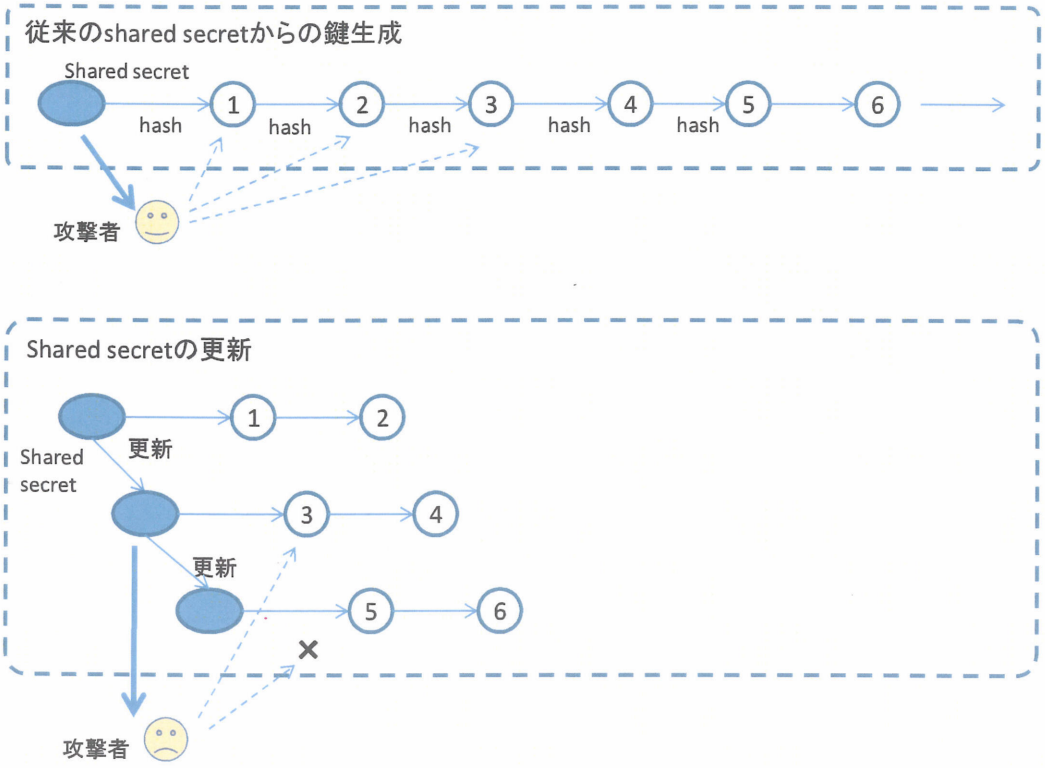

図 2-5shared secret の更新方式

当然ながら、(暗号鍵での議論と同様に) shared secret の更新が予測可能で、ある shared secret が漏洩した場合にそこから次の shared secret が推測できては何の意味もない。

従って、我々は、「**shared secret を予測不可能性を保ったまま更新する方式**」を検討し提案することとした。

本研究のターゲットとするモバイル端末とネットワークの間のセキュリティ方式を検討する上で、Shared secret を更新させるための条件は以下のものがある。

(1) Shared secret を更新していくための情報が、モバイル端末側とネットワーク側で容易に共有できるものでなければならない。
(2) 演算による更新ではなく、なんらかの外部要因に依存するものでなければならない。
さもないと、攻撃者による推測が容易となる可能性がある。
(3) Shared secret で、モバイル端末(その利用者)の識別が可能でなければならない。

これらの 3 つの条件を満足する shared secret を検討していく。
次の章では、その具体的アイディアについて議論する。

3. 新しい相互認証方式(CRP)

本章では、モバイル無線ネットワーク環境におけるモバイル端末とネットワーク側との相互認証プロトコルである Carousel Rotating Protocol (CRP)について説明する。

3.1. 基本的考え方

3.1.1. Location と Trail

モバイル端末を保有する利用者は、彼の日々の活動に応じて地域を移動し、必要に応じて、その端末を利用して通信を行う。当然、持ち主の移動に応じてモバイル端末は移動する。その利用者がいつどこで通信を開始するかは、その日の活動に基づいて決まる。通信を開始したその場所の近傍に存在する基地局やアクセスポイントのうち、モバイル端末との電波が到達するものを選定して端末と接続され、通信が実施される(図 3-1)。この「通信を開始した時点の基地局の情報」をそのモバイル端末の位置情報(以後 Location と呼ぶ)と定義する。Location は端末とネットワーク側で同時に取得できるため、両者が共有可能な情報と考えられる。この Location を通信の都度補足し続けることで、移動の履歴を記録し続けることもできる。それも両者で共有できる情報の一つである。

新しく提案するセキュリティ方式は、このモバイル端末の Location と移動の履歴(Trail)を shared secret の元として利用する方式である。

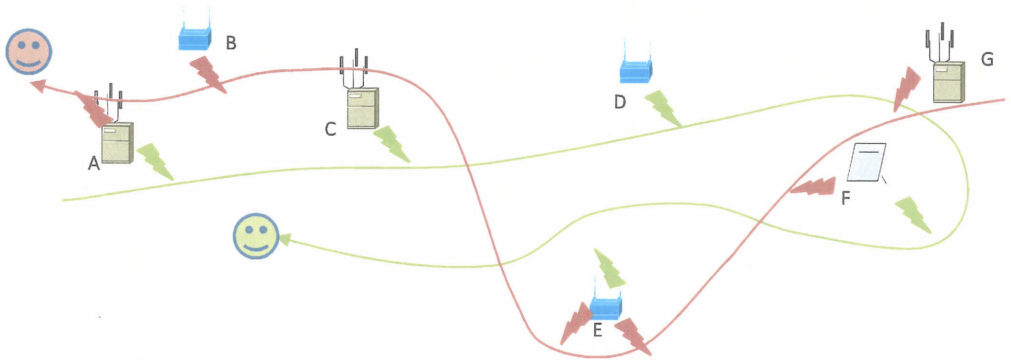

図 3-1 利用者の移動と通信のイメージ

Location と Trail が前の章で記載した 3 つの条件を満足していることを説明する。

(1) Location も Trail も、モバイル端末とネットワーク側がそれぞれ同時に取得可能であるため、互いに共有できる情報として利用可能である。通信の都度 Location を取得して Trail

を常に更新することが可能であるため、shared secret として利用できる。

(2) Location およびそれから派生する Trail1 は、モバイル端末と利用者の移動という物理的活動によって発生する情報である。

(3) モバイル端末の移動と通信の開始は、その利用者の移動によって決定される。その移動と、それに伴う通信が利用者によってそれぞれ異なるとすれば、一般的には Trail 情報を用いて個々の端末の識別が可能であると思われる。
ただし、ある場所に設置されまったく移動しない固定端末が存在する可能性もある。Location がまったく変更しないため、近傍に複数の固定端末がある場合にはそれらの Trail は同一となる可能性が高いが、これについては Location 情報を変換する Convert 関数(詳細は後述)によって各端末の識別が可能である。

ただし、モバイル端末の移動が進むにつれて、都度新しい Location が追加されていくため、Trail は無限に長くなっていく。その Trail を計算可能なレベルで管理するために、本プロトコルでは、Carousel というデータ構造により取り扱う。

この Carousel が本方式の shared secret となる。

3.1.2. システム構成

CRP で想定しているシステム構成の概要を図 3-2 に示す。CRP では、認証処理のための認証サーバを利用しない方式を目指しているため、EAP での Multiplex 方式を採用する。そのために CRP は EAP 上に搭載することも可能である。[50]では実際に EAP 上に搭載した EAP-CRP の提案をしている。本章で説明するプロトコルの詳細は[50]に沿ったものである。

認証処理は全てモバイル端末と基地局との間にて実施される。Shared secret はそのために基地局にて保持されるが、端末の移動に伴って shared secret は先に認証処理を完了した基地局から次にモバイル端末が接続される基地局に受け渡される。Shared secret は都度更新されるために、厳重に管理する必要は無いが、その通信経路であるネットワークはセキュアなチャネルが確保していることを仮定している。

Location Registory は、モバイル端末の shared secret をバックアップするためのサーバとして利用する。モバイル端末の shared secret は基本的に各基地局で保存しているが、メモリ許容量等の制約により保存できなくなった場合に、その shared secret を Location registory に渡すことにより、その損失を防止する。認証サーバではないため、各基地局から Location Registry へのアクセスは必要最小限にとどめられる。

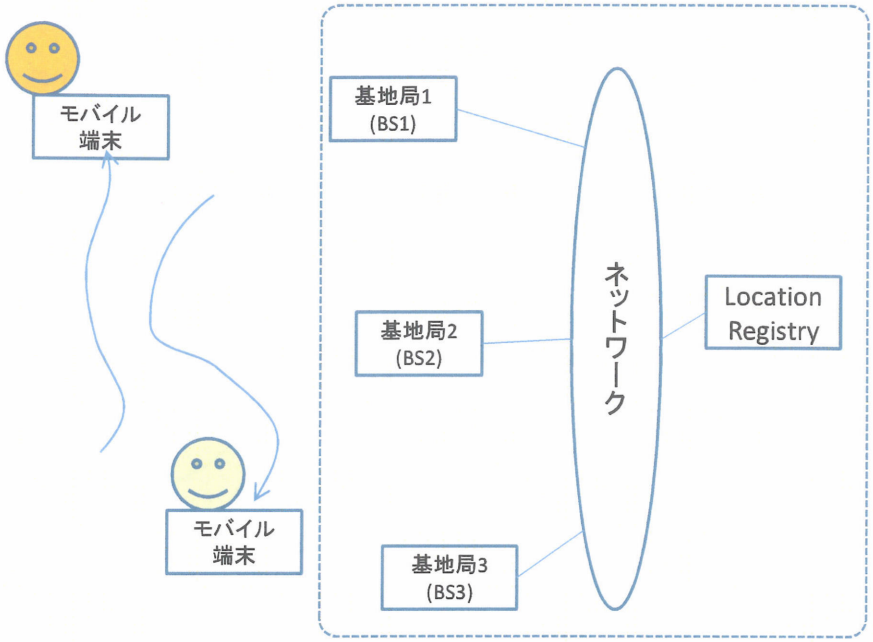

図 3-2 システム構成の概要

3.2. Carousel とは

3.2.1. Carousel の構造

Carouselとは、遊園地のメリーゴーランドのことであるが、空港のBaggage Claimに設置されているベルトコンベア状に回転する装置とするほうが連想しやすいかもしれない。到着した旅客機から降ろされた荷物はCarousel上に載せられ、持ち主に引き取られるまでBaggage Claim内をぐるぐる回り続ける。新しい荷物が降ろされるたびに、Carousel の空いた位置にランダムに配置され、ぐるぐる回り続けることになる。我々の提案するプロトコルでは、この Carousel の構造を、Trail 情報の管理に用いる。

本プロトコルでの Carousel は、複数の有限個の Cell で構成される Circular List である。それぞれの Cell の中には Location 情報が格納される。Carousel には、Circular List 上の任意の Cell を指す Entry Point を持つ。Entry Point は Circular List 上を自由に移動することができる。この Entry Point の移動を、Carousel の Rotation と呼ぶ。Carousel に対する Location 情報の代入は、その Entry Point が指している Cell に代入されることになるが、もし Entry Point が指した Cell に古い Location 情報が代入されている場合は、新しい Location 情報で書き換えられる。

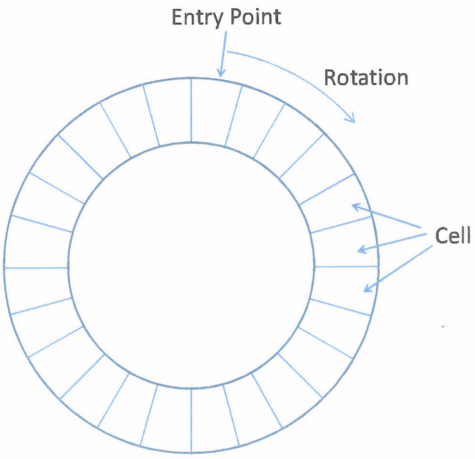

図 3-3 Carousel の構造

Location 情報を Carousel に代入する前に Carousel を Random に Rotation させる。この Random Rotation 処理によって、Carousel 内の Location 情報はランダムに配置されることになる、この Random Rogation 処理が、Carousel の予測不可能性の向上に貢献している。詳細は後述。

3.2.2. Carousel の同期

あるモバイル端末の Trail 情報を取り扱うために、Carousel のペアを利用する。ペアのうち一方の Carousel はそのモバイル端末が、他方はネットワーク側が持つ。互いの Carousel に格納されている Trail 情報が互いに同一であれば、その Trail 情報を Shared Secret として、それから共通鍵を生成することが可能であり、その鍵を用いて相互認証を行うことが可能となる。この状態のことを「Carousel は同期している」と呼ぶ。

モバイル端末（およびその利用者）が移動して、あたらしい位置で通信を行うと、新しい Location 情報が生成されて Trail 情報が更新される。その Location 情報により一方の Carousel の内部も更新されるが、その瞬間は互いの Carousel が同期していない状態となる。そのため、Carousel から共通鍵を生成するには、互いの Carousel を再同期させる必要がある。

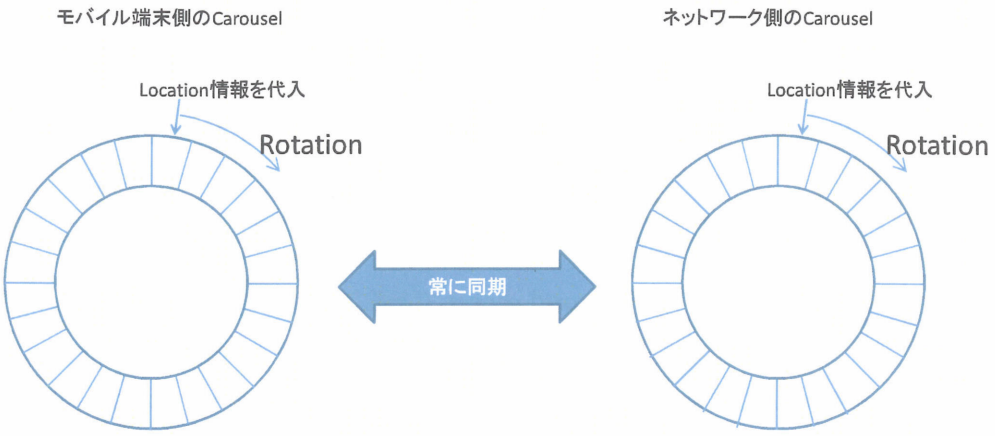

図 3-4Carousel の同期処理

モバイル端末の利用者の移動によって、新しい Location 情報が作成されると、そのモバイル端末の Trail 情報を管理する Carousel のペアのうち一方に(Random Rotation を介して)その Location 情報が代入され、その内容が更新される。この状態ではその Carousel のペアは同期していないことになる。再び同期状態に戻すには、もう一方の Carousel が同じ Location 情報を同じ Cell に代入し同一の Trail 情報の配置となればよい。

再同期処理は、最初の Carousel を持つエンティティがその Carousel から鍵を生成する処理から始まる。その鍵で認証コードを暗号化し他のエンティティに送信する。それを受け取ったエンティティでは、Carousel を Rotation した後に Location 情報を代入し、そこから鍵を生成する。生成した鍵で受信したメッセージを復号し、認証コードを取り出す。もし正しく認証コードが取り出せていなければ、Rotation と代入の処理を、正しい認証コードを取り出せるまで繰り返す。最後の Rotation が終了しても正しい認証コードが復号できない場合は認証失敗である。

正しい認証コードが生成できた時点で、このエンティティは「Carousel の同期が成功した」ことを認識し、そのメッセージ再び暗号化して元のエンティティに返す。

この処理により、双方のエンティティは互いに Carousel が再同期したことを認識する。これにより相互認証を実現したことになる。

3.3. プロトコルの説明

本章では、前節に記載の Caorusel と Trail 情報を用いたモバイル端末とネットワーク側の相互認証を実現するためのプロトコルについて説明する。プロトコル自体の名称は Carousel Rotating Protocol (CRP)と呼ぶが、EAP をベースに設計されているため EAP-CRP と記載している。

3.3.1. Carousel の初期設定

Carousel は本プロトコルでの shared secret であるため、その情報の初期共有の手続きが必要である。

Carousel の最初の同期は、レガシーなセキュリティ技術を用いた安全なネットワーク環境下にて行われなければならない。具体的には端末側およびネットワーク側の Carousel の各セルにランダムなビット列が代入される。

3.3.2. Location 変換関数

2.3 節で記載した、「位置を固定した端末」に対しても Trail による識別を可能とするために、本関数を導入する。この関数は、現在の端末の Location と任意の文字列とを用いて、ある決められた計算式で変換する機能を持つ。具体的には任意のハッシュ関数を用いることを想定している。このハッシュ関数の種別は、予めモバイル端末およびネットワーク側で予め使用するハッシュ関数を決めておかなければならない。

以後の解説の中では、この変換関数を、

$$L = \mathrm{Convert}(\mathrm{Loc}, R)$$

と記載する。ここで Loc は Location を、R はプロトコルの処理中に受け渡しされたランダムな文字列を示す。

3.3.3. CRP の鍵階層

図 3-5 に CRP で用いる鍵階層を示す。この階層は図 1-7 に示した EAP の鍵階層に基づく。

モバイル端末の Carousel が、この鍵のルート要素となる。通常の EAP 鍵階層モデルではここに Long-Term Shared secret が置かれ、それは厳重に管理されなければならないが、Carousel を用いた本プロトコルでは、Shared secret が常に更新されるため、厳重に管理する必要がない。

MSK や EMSK は、その MT とネットワーク側との Carousel ペアの同期が完了した後に生成される。TSK は(通常の EAP と同様に)MSK から生成されてセッション鍵となる。

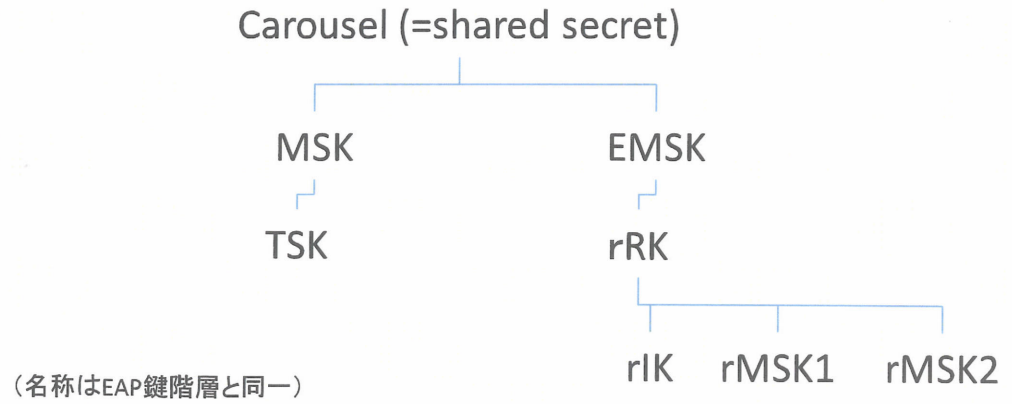

図 3-5 CRP の鍵階層

3.3.4. CRP プロトコル

本節は、CRP のプロトコル詳細を説明する。フロー図を図 3-6 に示す。以後の説明のため、モバイル端末を MT、基地局を BS と呼ぶ。

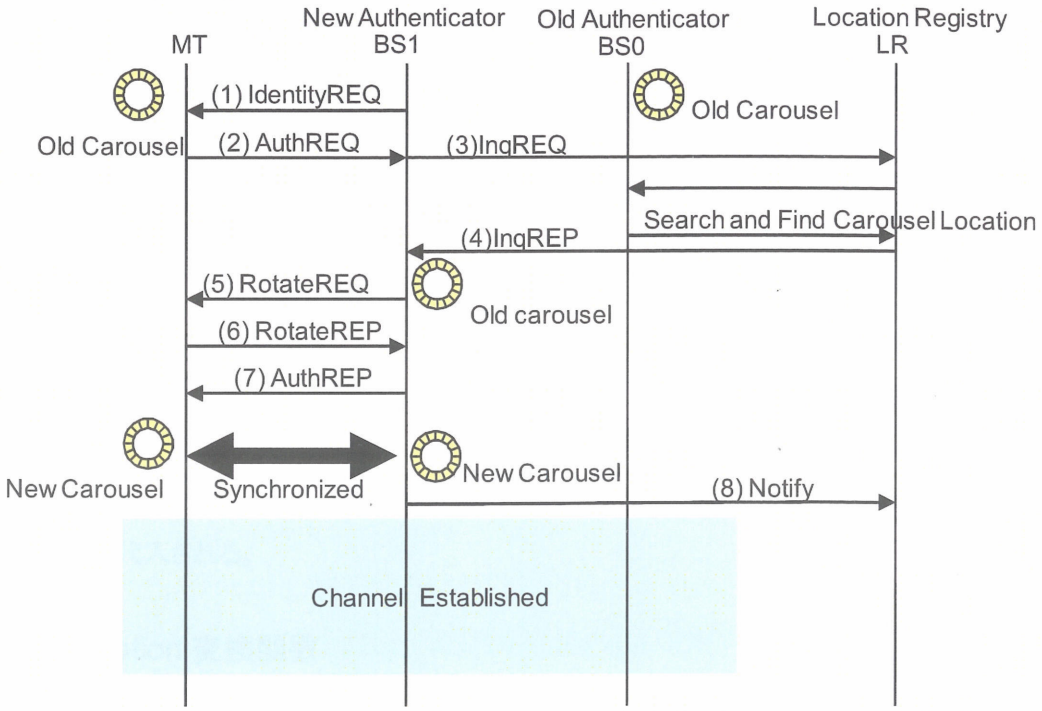

図 3-6 CRP のフロー図

CRP では BS が Authenticator の役割を担う(図 3-6 の BS0, BS1)。そのため、ネットワーク側の Carousel はこの BSn が保持することになる。個々のモバイル端末の Carousel と連携するネットワーク側の Carousel の管理情報は、Location Registry (LR)が担っている。LR には、個々のモバイル端末の Carousel を保持している BS の識別子、またはそのモバイル端末の Carousel 自身を持つ。ネットワーク側の通信は、全てセキュアなチャネルを介して行われることとする。

以後の記法は以下のとおり。

- $\{MSG\}_K$ は、データ列 MSG を鍵 K で暗号化した結果を示す。
- A||B は、データ列 A とデータ列 B の連接を示す。

以前は BS0 と認証して通信していたモバイル端末 MT が、今度は BS1 を用いて通信を開始する場合の CRP の流れは以下のとおりとなる。

1. BS1 → MT : IdentityREQ()
   MT を検出した BS1 は、IdentityREQ メッセージをその MT に対して送信する。

2. MT → BS1 : AuthREQ(ID_{MT} ,{ID_{BS0}}K_g)
IdentityREQ メッセージを受信した MT は、自分自身の識別子とをパラメータにしたAuthREQメッセージを送信する。本メッセージに、MTが直前に認証した基地局(BS0)の ID である ID_{BS0} を Kg で暗号化したデータを追加することも可能である。このメッセージが、CRP を用いた相互認証の開始となる。

3. BS1 → LR : InqREQ(ID_{MT})
BS1 は、自分自身がその MT の Carousel を保持していない場合は、LR に InqREQ メッセージを送り、その MT の Carousel を問い合わせる。
もし{ID_{BS0}}K_gが含まれていれば、それを復号して BS0 の ID を知りそこに MT の Carousel を問いあわせる。

4. LR → BS1 : InqREP(ID_{MT} ,CR_{MT})
LR はその MT の Carousel (CR_{MT})を、InqREP メッセージに載せて BS1 に返送する。

5. BS1 → MT : RotateREQ({R_1||MAC_1}K_N)
BS1 は受信した Carousel(CR_{MT})から認証用の鍵 K_Nを生成する。K_Nを生成する前に、予め CR_{MT}の random rotation を実施しておく。
BS1 はその K_Nでメッセージ R_1||MAC_1を暗号化する。ここで R_1は BS1 で作成したランダムな文字列であり、MAC_1はその R_1から導出される認証コードである。
BS1 は生成した暗号メッセージ{R_1||MAC_1}K_Nを、RotateREQ メッセージに載せて MT に送付する。

6. MT → BS1 : RotateREP({R_1||R_2||MAC_2}K_M)
RotateREQ メッセージを受信した MT は、その暗号メッセージの復号を試みる。具体的には以下の処理を行う。

   A) Carousel を 1 ステップだけ Rotation する。

   B) Rotation した結果の Carousel から復号鍵 K_N'を生成し、その鍵で暗号メッセージの復号を試みる。復号後のメッセージを仮に R'||MAC'とすると、R'から導出した認証コードが MAC'と合致しなければ、鍵生成に失敗したとみなして、再度ステップ(A)に戻り、次の Rotation の確認を行う。
   もし合致していれば、正常に復号できた、すなわち、R'=R_1、かつ、MAC'=MAC_1、従って、K_N'=K_N と判断できる。従って、その時点の MT の Carousel は先のステップで BS1 が Rotation した後の Carousel と同一であると判断してかまわない。ここで処理を停止する。

C) もしCarouselのRotationが1周したにもかかわらず合致するMAC'が生成できなかったならば、認証は失敗とみなされる。

この時点で、MTはBS1の認証に成功したことになる。
次に、MTは、現在のCarouselにその場のLocation情報をConvert()で変換した値Lを代入し、そのCarouselから認証鍵K_Mを生成する。ConvertのRにはR'を与える。
MTは、上のステップで算出したR'(すなわちR_1)と、新たに生成したランダムデータR_2と、$R_1||R_2$から導出した認証コードMAC_2の連接($R_1||R_2||MAC_2$)をK_Mで暗号化して、そのデータをRotateREPメッセージに載せてBS1に送信する。

7. BS1 → MT : AuthREP($\{R_2||MAC_2\}K_M'||\{ID_{BS1}\}K_g$)
BS1はRotateREPメッセージを受信すると、まず復号用の鍵を以下の手順で生成する。

A) BS1はCR_{MT}にLocation情報をConvertした値Lを代入する。Convertの第二引数にはR_1を与える。

B) CR_{MT}から復号用の鍵K_M'を生成する。

RotateREPメッセージに載せて渡されたデータを上記のKM'で復号化する。その結果を$R_1'||R_2'||MAC_2'$とすると、($R_1'||R_2'$)から導出された認証コードがMAC_2'と同一であれば、復号に成功したとみなすことができる。このとき、$R_1=R_1'$かつ、$R_2=R_2'$かつ、$K_M=K_M'$といえる。この段階でMTとBS1のCarouselは互いに同期したとみなすことができる。すなわち、MTとBS1の相互認証は完了したといえる。

BS1は$\{R_2||MAC_2\}$を鍵K_M'で暗号化したものと、BS1自身のIDをネットワーク側の各BS共通の鍵であるK_gで暗号化したものを、AuthREPメッセージに載せてMTに送信する。

AuthREPメッセージを受信したMTはそれをK_Mで復号化する。それに成功し、かつR_2とMAC_2が正しいならば、MTは相互認証が完了したことを知る。

8. BS1 → LR : Notify(ID_{MT})
最後にBS1は自分自身がMTのCarouselを持っていることをLRに送信する。

MTとBS1は共に、相互認証が完了した後で、CarouselからMaster Session Key (MSK)

を作成し、それにより暗号通信を実施する。

3.4. セキュリティの観点からの評価

本節では、この EAP-CRP がセキュリティの観点からみて満足すべきものかどうかを評価していく。

第一に、新しいセキュリティ方式の基本的要件として提示した、shared secret の予測不可能性に関して、本方式が十分な強度を持っているか否かについて検証する。

次に、攻撃者が Carousel を予測するうえで前提となる、Trail 情報の取得について、その手法を含めた実施可能性について検討する。

最後に、一般的なセキュリティの要件として、NIST-SP 800-48[61]で提唱している以下の 3 つの観点について簡単に考察する。

- Confidentiality(機密性)
  その情報が認証されていない第三者から参照かつ利用されないことを示す指標。
- Integrity(完全性)
  MT とネットワーク側での通信時に、送受信される情報が破壊されたり改ざんされることがないことを示す指標。
- Availability(可用性)
  MT とネットワーク間の通信が妨害されることのないことを示す指標。

3.4.1. 用語の定義

最初に、以後の議論に用いる用語の定義を行う。

(1) Carousel の長さ
Carousel を構成する Cell の個数。以後は n で表す。

(2) Trail の長さ
そのモバイル端末の Trail に含まれる Location 情報の個数。以後の議論では m で表す。

(3) Bounded Carousel
全ての Cell に Location 情報が代入されている Carousel を Bounded Carousel と呼ぶ。

(4) Unbounded Carousel
少なくとも一つの Cell に Location 情報が代入されていない状態で、初期設定値の Cell が残っている Carousel を Unbounded Carousel と呼ぶ。

Carousel の初期共有直後、すなわち各 Cell にランダムなビット列が代入されている状態の Carousel は、Unbounded Carousel である。利用者が移動し、Location が生成される(Trail が延びる)につれて、Carousel に Location が代入され、Bounded 状態に近づいていくことになる。

3.4.2. Carousel の予測不可能性の評価

(1) 前提条件

Unbounded Carousel は初期設定時のランダムビット列をその内部に保持し続けている。そのランダムビット列の再生成は困難であるため、Unbounded Carousel の予測は不可能であると考えて問題ない。

(2) Carousel 予測不可能性の定義

定義.1.

> Carousel の予測不可能性 とは、
> 「攻撃者がモバイル端末の全ての Trail 情報を入手した場合に、その Trail 情報からそのモバイル端末の Carousel を再構成することの困難さの度合い」である。

定義.1.は前提条件より、以下のように言い換えることができる。

定義.1A.

> Carousel の予測不可能性は、
> 「そのモバイル端末の Trail 情報に含まれる Location 情報から生成可能な Bounded Carousel の場合の数」で示される。

同様に以下の系を得られる。

系(1)

> Carousel の長さを n とすると、その Carousel が Bounded Carousel である必要条件は、$m \geq n$ (ここで m は Trail の長さ)である。

Carousel の Random Rotation により、一度 Location が代入された Cell に再び Location が代入される場合もあるため、$m \geq n$は十分条件ではないことに注意が必要である。

Carousel の予測不可能性を、CC_n^mと表記する。CCとは Carousel Complexity の略称である。

(3) Carousel 予測不可能性(CC)の算出

ここではCC_n^mを算出する計算式を導出する。

長さ m の Trail から構成される長さ n の Carousel の集合C_n^mをとし、同じく Bounded Carousel の集合をBC_n^m、Unbounded Carousel の集合をUC_n^mとすると、定義より明らかに、

$$BC_n^m \cap UC_n^m = \emptyset$$

および

$$BC_n^m \cup UC_n^m = C_n^m$$

である。これにより、Bounded Carousel の集合BC_n^mは、

$$BC_n^m = C_n^m - UC_n^m$$

で表される。ここで、明らかに、

$$C_n^m = n^m$$

である。また、UC_n^mであるが、長さ n の Unbounded Carousel は、長さ$(n-i)$の Bounded Carousel に、i個の Unbounded な Cell を追加したもの、と考えられる。この Bounded Carousel の個数は、CC_{n-i}^mと表せるため、これに Unbounded Cell を追加した組み合わせの個数が求める値となる。すなわち、

$$UC_n^m = \sum_{i=1}^{n-1} \binom{n}{i} CC_{n-i}^m$$

で表すことができる。従って、

$$CC_n^m = n^m - \sum_{i=1}^{n-1} \binom{n}{i} CC_{n-i}^m$$

となる。

(4)　予測不可能性の具体的評価

前節の検討に基づき、Carousel の予測不可能性を具体的に評価する。

明らかに、

$$CC_2^m = 2^m - 2$$

であることから、CC_n^mは再帰的に計算可能である。その結果をグラフ化したものを、図 3-7 に示す。横軸に m を、縦軸にCC_n^mをとっている。複数あるグラフの直線はそれぞれ Carousel の長さ n を示している。CCは Bounded Carousel のみ対象とするため、Bounded Carousel の必要条件に基づき($m \geq n$)の場合のみプロットしていることに注意。

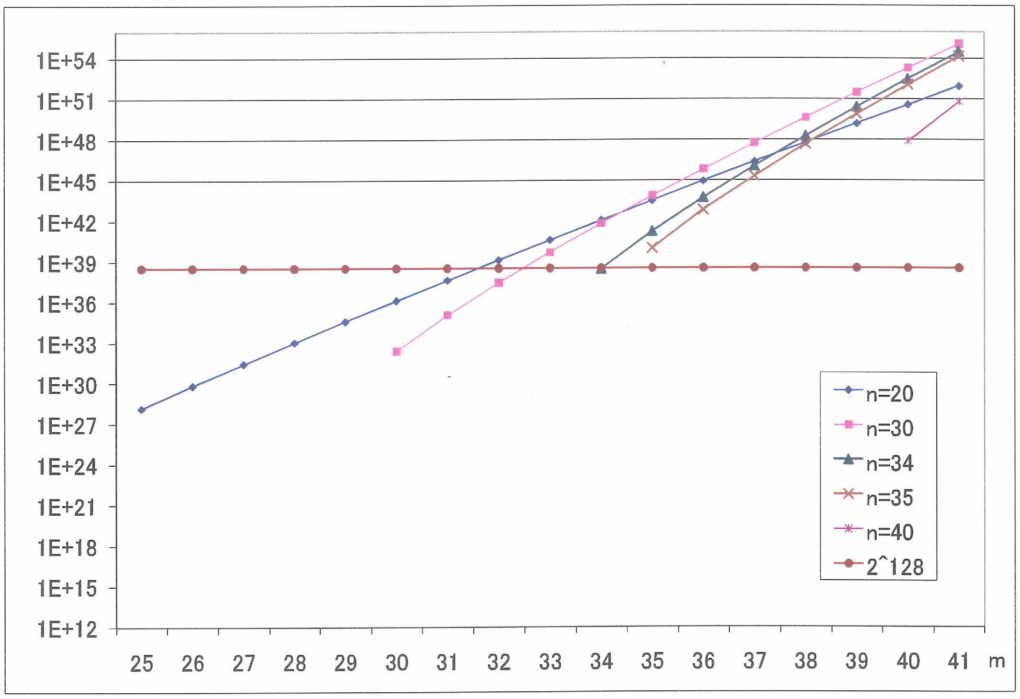

図 3-7 Carousel の予測不可能性の算出

(5)　Carousel 予測不可能性の考察

ここまでの結果を踏まえて、Carousel の予測不可能性に関して考察する。

予測不可能性の一つの尺度として、2^{128}という値を挙げる。この数値は、128ビットの鍵長の暗号システムを総当り攻撃する場合に必要となる場合の数である。十分強力な暗号システムの鍵長の指標として用いられている。(図 3-7 に、参考のために、2^{128}の値もプロットした。)。shared secret

の予測不可能性に関しても、この尺度を用いて考えることとする。すなわち、

ある Carousel の CC の値がこの尺度より大きい場合には、その Carousel は攻撃者からの Carousel 再生成の攻撃に対して、十分強力と判断して問題ないと考えてよい。すなわちそのような Carousel は十分な予測不可能性を持つと判断してよいものとする。

図 3-7 によれば、$n = 35$の点が、この尺度を越える境界となると考えてよい。Carousel の長さを 35 以上とすることによって、$(m \geq n \geq 35)$となる全ての条件において、CC_n^mは 2^{128} を超えることを保証できていること、すなわちその Carousel の予測不可能性は十分高いといって良いことがわかる。

では、Bounded Carousel を作成できない$(m < n)$となる条件下ではどうか？この場合は、(1)の前提条件の通り、その Carousel は予測不可能であるため、再生成することはできない。

従って、本評価の結論としては、Carousel の長さを 35 以上とすれば、全ての場合において、Carousel(=shared secret)の予測不可能性は十分高いといえる。長さ 35 の Carousel は本章に記載した実際の相互認証プロトコルにおいて、現実的に処理可能な長さである。現実的に処理可能なデータ量で十分高い予測不可能性を満足している点において、本方式の有効性を示しているものと考えてよい。

3.4.3. 攻撃者による Trail 取得の可能性

Carousel の予測不可能性の検討では、攻撃者はモバイル端末の全ての Trail を取得していることが前提であった。それにもかかわらず Carousel の予測不可能性は十分高いという結論を得た。

それでは、そもそも攻撃者はモバイル端末の Trail を完全に取得することが可能なのであろうか？本節ではその可能性について検討していく。

攻撃者が何もないところから Trail を取得(推測)する場合は、ターゲットであるモバイル端末とその利用者が移動する地域のアクセスポイントや基地局の位置を把握し、どの位置のどの基地局で通信を行うかを推測し、その基地局のリストから Trail 情報を生成する必要がある。

この評価のために、Trail の複雑性(Trail Complexity。以後 TC)を次のように定義する。

定義.2.

> Trailの複雑性とは、
> 「定められた領域内に存在する基地局の一覧から、そのモバイル端末の Trail 情報を再生成することの困難さの度合い」である。

本節では、基地局等の配置とモバイル端末の移動に関してあるモデルを定義し、そのモデルに基づき TC を定式化して評価する。

(1) 基地局とモバイル端末の位置モデル

地上に存在する物体の位置を把握する方法は様々ある。GPS[62]、電波強度や電波到達方向または電波到達時刻で推測する方法[63]、あるいは地図をメッシュで区切り、そのメッシュ毎に把握する方法[64][65][66]。

EAP-CRP の Location 情報の前提として、モバイル端末(MT)とネットワーク側でその情報を共有する必要がある。GPS モデルは、端末のみ位置検出が可能、電波強度方式も同様である。従って、本モデルは基地局(BS)の ID を Location 情報として採用した。

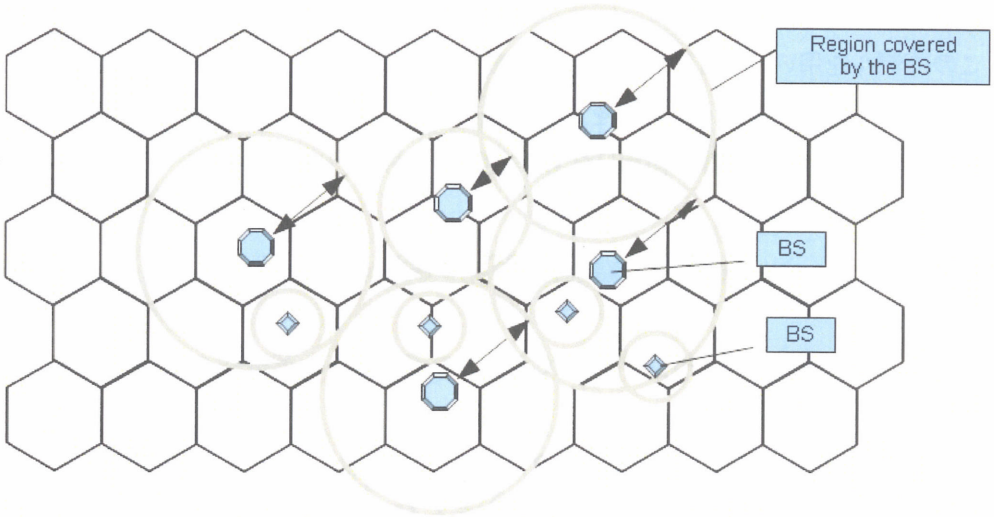

図 3-8BS と MT の移動モデルの模式図

図 3-8 に想定している BS と MT のモデルの模式図を示す。地表面は仮想的に6角形のメッシュ(以後 HEX と呼ぶ)で区切られている。その地表面に、様々な無線システム(3G、WLAN、または PAN 等)の BS が設置されている。これらの BS により無線ネットワークシステムが構成されている。個々の BS はそれぞれの無線種別に応じてその電波到達領域(図 3-8 の円で描いた部分)が異なる。BS の配置状況でその領域は重なり合っている。MT は、自分自身の現在位置で到達可能な BS を探しだし、もし複数の BS が抽出された場合はそこから1種類を選択して、その BS を通じて通信を行うことになる。

モデル化された地表面の HEX のそれぞれに対して、この電波到達領域が重なり合っているため、その HEX ごとに、その内部から通信が可能な BS の集合 *RS(H)*、およびその HEX の中での電波到達領域の密度 *Density(H)*を定義することができる(ここで H は HEX を示す)。例えば図 3-8 中の HEX H_1は、二つの BS(それぞれ BS1 と BS2)の電波到達領域が重なっているため、

$$RS(H_1) = \{BS1, BS2\}$$

である。また、BS1、BS2 それぞれの電波到達領域と H_1との重なりの面積の割合を1と 0.5 とすると、

$$Density(H_1) = 1.5$$

となる。

*Density(H)*は、その H の中で通信を実施する場合に採用する BS の選択肢の場合の数を定量

化するための指標として用いる。

このモデルを用いて、利用者とMTの移動をモデル化する。利用者の移動の際にそのMTによって通信を開始した場所の6角形を、H_1, H_2, H_3, ..., H_m とすると、その MT の Trail 情報 $Trail_{MT}$は、その中で通信に利用したBSのリストであるため、

$$Trail_{MT} \equiv BS_m \parallel BS_{m-1} \parallel \cdots \parallel BS_1$$

である。ここで$BS_i \in RS(H_i)$とする。TCは、この $Trail_{MT}$の再構成の困難度と同じである。

上記の $Trail_{MT}$の定義から、TCは、ターゲットが通信を行った時のHEXである H_{i-1}から、ターゲットが移動して次に通信を開始するHEXであるH_iを推測する場合の数と、そのH_iの中でのBS_iの選択($BS_i \in RS(H_i)$)の場合の数によって決まる。

(2) HEXの選択肢について

MTの移動と、通信を行うBSの選択肢の間の関係性についての検討が既になされている [13]。個々のHEXの大きさは固定であり、領域を一様に満たしていると仮定する。その領域でMTの利用者が移動している状況下において、そのMTによる通信実施時の位置であるHEXの選択肢は、そのMTを持っている利用者の移動速度と、通信間のインターバル(ある通信から次の通信までにかかる時間)によって決まる。この関係を *call-to-mobility ratio* と呼び、ρで定義する:

$$\rho = \frac{\lambda_c}{\lambda_m}$$

ここで、λ_cは2通信間のインターバルを示し、λ_mは最初の通信からその利用者がそのHEXから抜けるまでに要する時間を示している。この時、MTが次に通信を行うまでにK個のHEXを通り過ぎる場合の確率密度関数は、以下のように示される[66]:

$$\propto (K) = \begin{cases} 1 - \dfrac{1 - f_m^*(\lambda_c)}{\rho} & K = 0 \\ \dfrac{1}{\rho}[1 - f_m^*(\lambda_c)]^2[f_m^*(\lambda_c)]^{K-1} & K > 0 \end{cases}$$

ここで、f_m^*はMTがあるHEXに滞在している時間の密度関数である。

従って、2つの通信の間に、そのMT(および利用者)が通り過ぎるHEXの個数の期待値 K_{exp}

は、以下の式となる。この値はλ_cとλ_mによって決まる。

$$K_{exp} = \left\lceil \sum_{k=0}^{K} \alpha(k)k \right\rceil$$

最後に、このK_{exp}をもとに、次の通信が行われるHEXの個数の期待値$N(K_{exp})$は、以下の式で求められる。

$$N(K_{exp}) = \sum_{i=1}^{K_{exp}} 6i + 1$$

(3) 基地局の密度

前述の通り、そのHEXの中での電波到達領域の密度*Density(H)*を定義することができる(ここでHはHEXの領域を示す)。

あるHEXの中に複数のBSが配置され、それらの電波到達領域が全てそのHEX内に含まれているような状況では、個々のBSiの電波到達領域の面積をS_iとすると、

$$S_i = \pi r_i^2$$

となる。ここでr_iは電波到達領域の半径を示す。

HEXの面積を一様にSとすると、そのHEXの密度は、

$$Density(H) = \frac{1}{S}\sum_{1=1}^{n} S_i = \frac{1}{S}\sum_{1=1}^{n} \pi r_i^2$$

となる。ここで、$n = |RS(H)|$である。

実際の*RS(H)*や*Density(H)*は、その領域での物理的なBSの配置に依存することは明らかである。しかしながらこの論文では、TC の検証を目的としているため、密度の指標としてその地域の平均値を参考にすればよい。すなわち、

$$E(H) = \frac{1}{n}\sum_{i=1}^{n} Density(H_i)$$

を評価の尺度として用いれば十分である。

(4) Trail Complexity の定量化

上記までの検討により、Trail Complexity(TC)は、以下のように定義できる。

$$TC = \left(N(K_{exp}) \cdot E(H)\right)^{m}$$

ここで m は Trail の長さである。

(5) Trail Complexity による Trail 情報の堅牢性の評価

(2)節に記載のとおり、$N(K_{exp})$はρと利用者(およびその MT)の移動速度の分散 V によって決まる。計算を簡易にするために、その移動速度はガンマ分布に従うと想定すると、そのときの$N(K_{exp})$はρと V から表 3-1 のように決まる。

この数値を元に、Case1、Case2、Case3 毎に TC を計算したグラフを図 3-9 に示す。縦軸が TC を示し、横軸は Trail の長さを示している。Case1、Case2 共に、常に隣接する HEX にて次の通信を行う、と想定した簡単なモデルであるが、それに対しても TC の値は高くなっていると考えられる。

表 3-1 ρ、分散、およびその時の HEX の選択肢

	ρ	V	$N(K_{exp})$
Case 1	1	$10/\lambda_m^2$	7
Case 2	1	$1/\lambda_m^2$	7
Case 3	5	$10/\lambda_m^2$	19

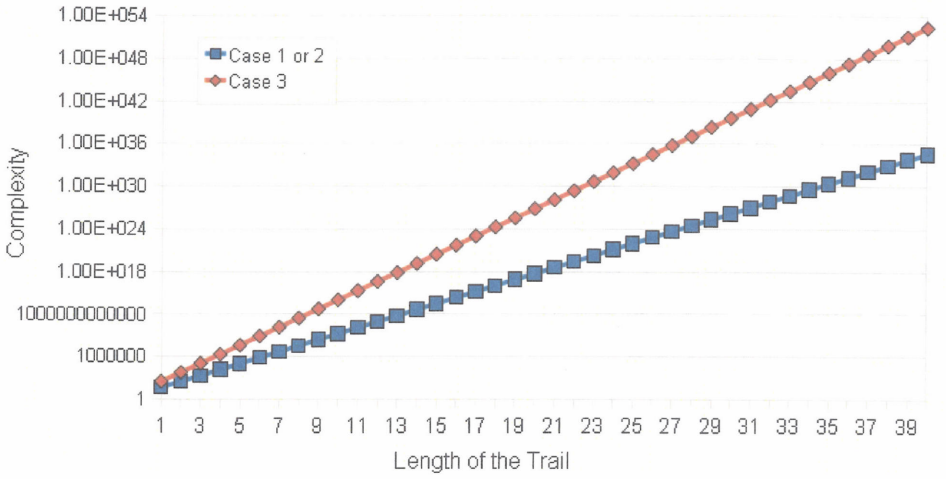

図 3-9 Trail Complexity

前節において、Carouselの長さnを35以上とすれば、全ての場合においてその予測不可能性は十分高い、という結論を得た。この前提条件として、$(m \geq n)$である場合のみCarouselの再生成が可能であるため、必然的に、十分な予測不可能性を持つCarouselにおいては$(m \geq n \geq 35)$という条件が成立する。この条件のもとでのTCは10^{30}を超えており、Trailを推測することは非常に困難であるという結論が導かれる。

3.4.4. ストーキング攻撃への対応

攻撃者がターゲットの Trail を取得することを目的として、ストーカー行為を行うことも考えられる。この場合には、通信を行う基地局を全て取得されてしまう。これを用いて Trail を生成するのは十分に可能である。本節では、ストーキングによる Trail の取得においても Carousel の予測不可能性によりそれを再生成することは困難であることを示す。

3.4.2 節の議論において、Carousel が再生成される必要条件は、それが Bounded Carousel であることがわかった。またその逆に、Unbounded Carousel であるならばそれは再生成されないことになる。Location の代入時に Carousel は Random Rotation が行われるが、その処理の結果として、Carousel が Bounded Carousel になる確率はどの程度になるのであろうか？

長さ n の Carousel に対して、長さ m の Trail 情報が与えられたときに、その情報を用いて Bounded Carousel が成立する可能性を、PB_n^mとすると、3.4.2 節の結果より、PB_n^mは

$$PB_n^m = \frac{CC_n^m}{n^m}$$

であらわされる。

図 3-10 に、このPB_n^mをグラフにしたものを示す。それぞれのグラフは長さ n の Carousel において、長さ m の Trail 情報を代入したときの値を示したものである($m \geq n$)。

図 3-10 が示すように、Carousel の長さがある程度の長さを超えると、十分長い Trail 情報があったとしても、Carousel が Bounded とならない状態が発生し得ることが判る。何度 Rotation を実施したとしても、初期設定値が Carousel に残る状態がある程度高い確率で発生しうることが示されている。

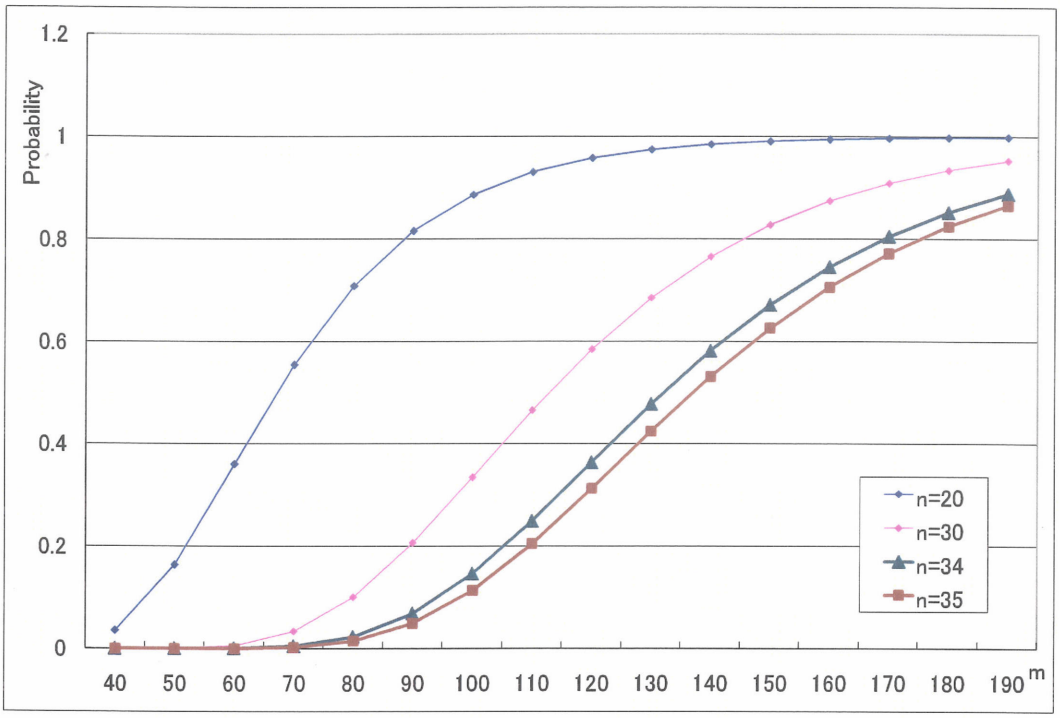

図 3-10 Bounded Carousel が作成される確率

これは、攻撃者がストーキング行為により十分な長さ($m \gg n$)の Trail 情報を入手できたとしても、その Carousel の中には、攻撃者がストーキング行為を開始した以前の Location 情報が残っている状況がある程度高い確率で想定できるため、如何に長い Trail を取得したとしても、Carousel を再生成することが困難であることを示している(図 3-11)。

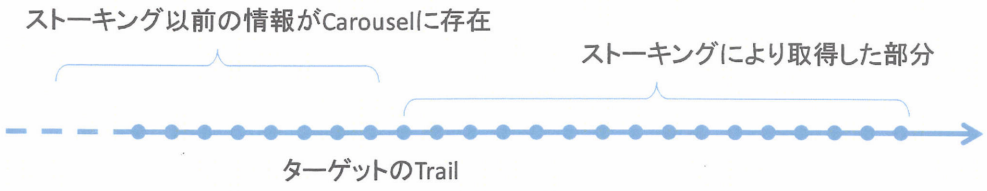

図 3-11 ストーキング行為により取得した Trail 情報と Carousel 内の情報

この問題を解決するために、攻撃者は、十分長い時間ストーキング行為を繰り返し、非常に長い Trail を取得するかもしれない。しかし次には Carousel Complexity(CC)による複雑度が壁となり、結局 Carousel の再生成は非常に困難である。

3.4.5. その他のセキュリティ評価

ここでは、一般的なセキュリティの要件として、NIST-SP 800-48[61]で提唱している以下の 3 つの観点について簡単に考察する。

(1) Confidentiality

EAP-CRP における Confidentiality とは、 あるモバイル端末とネットワーク側との CRP のプロトコルのやり取りの中で、通信データが解読され盗聴されたりしないことを示す。

CRP を実施中のパケットは暗号化されて送受信されている。その暗号方式は、十分な評価を受けた堅牢な暗号アルゴリズムを用いることによって、防御可能である。CRP の仕様では暗号アルゴリズム等は特に指定する必要がないため、その時点での十分な強度を持つアルゴリズムを採用すれば良い。暗号アルゴリズムの堅牢性の評価は CRYPTOREC によって定期的に実施され報告[51]がなされている。堅牢性が認められた暗号アルゴリズムは、電子政府推奨暗号リスト[52]として公開されている。

(2) Integrity

ここでは CRP の Integrity について検討する。ここで言う Integrity とは、 あるモバイル端末とネットワーク側との CRP プロトコルのやり取りの中で、通信データが改ざんされたり、破壊されたりしないことを示す。

CRP は無線ネットワークでの相互認証のためのプロトコルであるので、モバイル端末とネットワークの基地局の間での直接通信が前提となっている。従ってその間に第三者が入る余地が無いため、中継によるパケットの改ざんや破壊を実施する man-in-the-middle アタックは困難である。

もし仮になんらかの方法で攻撃者が不正なパケットを作成して送信したと仮定する。前節の議論で、十分な長さの Carousel を保持していれば、攻撃者がその Carousel を再生成するのは非常に困難であることを示した。CRP のプロトコルはパケットの内容を Carousel から生成した鍵を用いて暗号化して送受信を行う。さらに、データ中にメッセージ認証コード(MAC)を追加しており、それによって常に受信データの正当性(送信元が正しく認証されている。正しい鍵を持っている)を確認している。もしここで不正なパケットを受信した場合には、それを、排除することは可能である。

さらに、攻撃者がなんらかの方法でパケットを削除することが考えられる。もしくは、無線状況の不備により、メッセージが正しく届かない状況も考えられる。この場合でも以下の理由により CRP による同期の維持は可能である。

1. もし仮に攻撃者が AuthREQ()や RotateREQ()や RotateREP()メッセージを削除した場

合、モバイル端末も基地局も認証プロセスを停止することができる。古い Carousel が互いに維持できているため、Carousel の同期の維持は可能。

2. AuthREP()メッセージが削除されたとしても、モバイル端末も基地局も共に同期が完了したとみなして、暗号化されたメッセージを送受信することによってそれを確認できる。

(3) Availability

CRP の Availability を低下させる行為とは、モバイル端末とネットワーク間の通信を妨害する行為である。

攻撃者が偽のモバイル端末を配置して、偽の AuthREQ メッセージを送信する可能性がある。逆に攻撃者が偽の基地局を設置して、モバイル端末からの AuthREQ メッセージに対して偽の RotateREQ メッセージを返す場合がある。どちらの場合に対しても、偽の機器が正しい Carousel を保持していない限り正しい暗号文を作成できないため、その攻撃は失敗する。正しい Carousel の生成が困難であることは 3.4.2 節に記載のとおりである。

また、偽の基地局がリプレイアタックをかけることが考えられる。例えば偽の基地局が、正しい基地局の RotateREQ メッセージを盗聴しておき、次のモバイル端末からの AuthREQ メッセージに対してその盗聴したメッセージを送信する可能性が考えられる。しかしながら RotateREQ 送信前の Random Rotation によって鍵が変更されているため、モバイル端末はそれを認識してそのメッセージを削除できる。従ってリプレイアタックに対しても問題ない。

完全に CRP の通信を妨害するためには、jamming などの手法で通信そのものを妨害することが考えられるが、その手法および対策については本論文の検討範囲外である。

3.4.6. セキュリティ評価のまとめ

本節では、Trail および Carousel というデータ構造を用いた本プロトコルのセキュリティ面からの評価を行った結果を示した。

その結果として、以下のような知見を得ることができた。

(1) Carousel というデータ構造は、shared secret の予測不可能性向上のために大きな役割を担っている。その長さ n が 35 以上であれば、十分安全な shared secret として利用することが可能である。
(2) Carousel 生成の前提条件である Trail 情報の取得については、推測による方式は非常に困難であることが示された。攻撃者がストーキング行為により Trail の収集は可能ではあるが、それに拠ったとしてもそこから実際の Carousel を生成することが困難であることも示した。

評価の結果として、本方式における Carousel の shared secret としての利用は、無線ネットワークシステムのセキュリティを向上する上で非常に高い評価を与えることができると結論付けてよい。

また、Carousel の長さが n が 35 以上という条件は、実際の認証システムを構築する場合に十分計算可能なデータ量であり、その面からも本方式の有効性が示されていると考えられる。

この Carousel の長さ 35 は、以降の節での、CRP の性能評価におけるパラメータとして用いられている。

3.5. パフォーマンス評価

第2章において、本方式の目的は、認証などによる演算処理が、モバイル端末の CPU 負荷や応答性能をできる限り軽減することを目的としている。ここでは、CRP を実際に実装し、そのパフォーマンスを評価することで、それが実現できているか否かを確認する。

3.5.1. パフォーマンス評価の考え方

パフォーマンス評価では、以下の 2 点について確認した。

(1) 負荷の集中が想定されるモバイル端末の CPU 負荷の評価

(2) 認証処理全体の応答性能の評価

比較対象とした既存の方式は、共通鍵暗号方式では、

- ハッシュチェーン方式
- EAP-AKA による認証方式

を対象とし、公開鍵暗号方式では、

- EAP-TLS

を採用した。

3.5.2. プロトタイプ環境

プロトタイプを作成した環境を表 3-2 に示す。

表 3-2 プロトタイプ構築環境

MT 側	CPU	Intel Centrino 1.7GHz
	OS	Ubuntu Linux 9.01
BS 側	CPU	Intel Core2 DUo
	OS	Ubuntu Linux 9.01

また、プロトタイプ作成に使用した暗号アルゴリズムを表 3-3 に示す。

表 3-3 選定した暗号アルゴリズム

暗号化アルゴリズム	AES-CBC128
メッセージダイジェスト関数	SHA-1

プロトタイプ実装に当たっては、多くのシステムで活用されている OpenSSL[67]の暗号実装を採用した。

また、3.4.2 節の記載に従い、Carousel の長さを 35 として設計をしている。

3.5.3. モバイル端末の CPU 負荷に関する評価

本節では、モバイル端末側での CPU 負荷に関する評価した結果を示す。

CRP におけるモバイル端末側での CPU 負荷は、3.3.4 節の(6)ステップにて、Carousel を 1 ステップずつ Rotation して同期の検証を行うステップである。Carousel の同期が確認されるまで鍵生成→パケットの復号を繰り返し実施する。この繰り返しの回数によって、CPU 負荷と応答性能が変わる。

(1) 公開鍵暗号方式との比較

最初に、EAP-TLS との比較結果を図 3-12 に示す。ハッシュチェーン方式、EAP-AKA 方式、それから CRP の CPU 負荷と、公開鍵方式としての EAP-TLS でのサーバ認証を実施した場合の CPU 負荷をプロットしたものである。CRP で示している数値はそれぞれの Random Rotation 実施時の最大ステップ数を示している。例えば 2 は、Random Rotation 時の entry point の移動が最大 Cell 二つ分まで、ということとお示している。複数回試行した上での平均値、最小値、最大値をそれぞれ'MEAN'、'MIN'、'MAX'で示している。また、'WORST'は、常に最大回数だけ Rotation した場合の CPU 負荷を示している。

この結果をみると、当然ながら、共通鍵暗号方式を採用したメリットが明らかに示されている。EAP-TLS は無線ネットワーク環境の相互認証として多く用いられている方式であるが、公開鍵暗号方式に基づく処理の負荷が高いために、電力消費量の制約により小パフォーマンスの CPU しか採用できないモバイル端末上では、その応答性能や電力消費量の面で課題となるであろう。それに比較して共通鍵暗号方式を採用した相互認証方式では、CPU 負荷が圧倒的に低く、小パフォーマンス CPU を用いても十分な応答性能と低電力消費を実現することが可能と考えてよい。CRP もその仲間に含まれるわけであるが、他の共通鍵暗号方式と同様に EAP-TLS と比較して非

常に低い負荷を示しており、十分優位性があると見て問題ない。本方式を採用したことは間違いではなかったことがわかる。

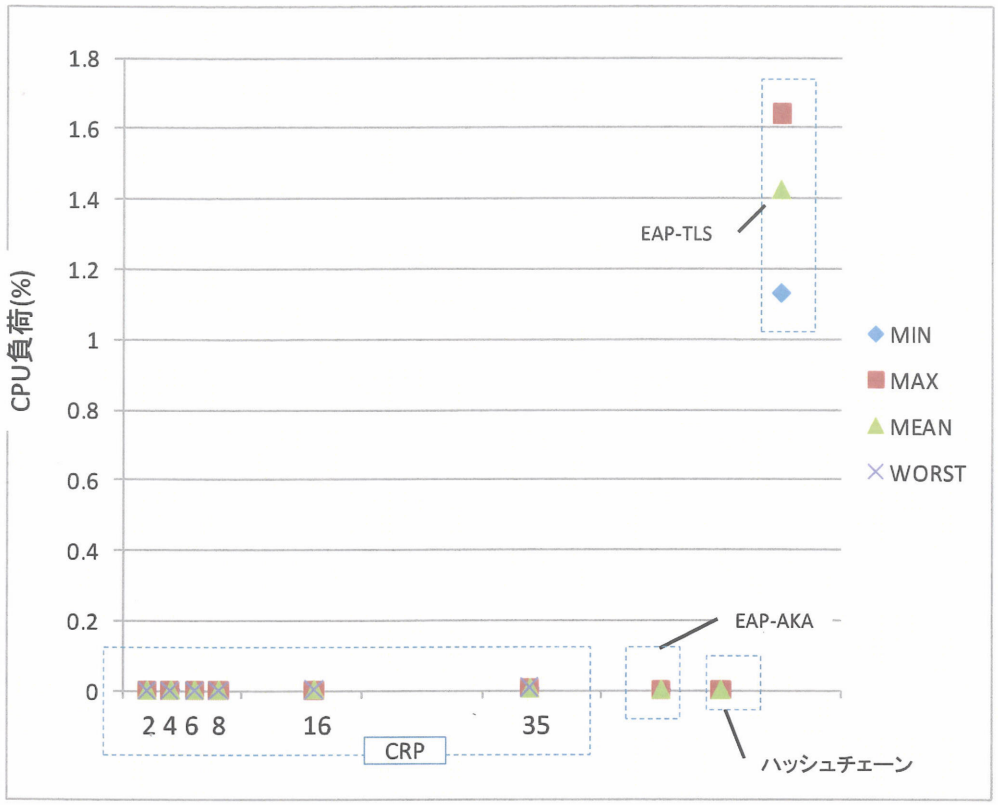

図 3-12 モバイル端末側での CPU 負荷(EAP-TLS を含む)

(2) 共通鍵暗号方式との比較

図 3-13 は、今度は共通鍵暗号方式の間での検証結果を示している。図中のシンボル等の意味は、前記と同様である。

実際に性能検証の結果からわかることは、従来の共通鍵方式が明らかに負荷は低いということである。EAP-AKA 方式では固定の Shared secret を元にした暗号計算を実施しているため、またハッシュチェーン方式では最低限の演算で鍵の更新が可能となっている。

それに比較して、CRP 方式では、Carousel と Trail により、shared secret の予測不可能性向上を目指したため、従来方式に比較して若干処理量が増大していることがわかる。これはモバイル端末上において、Rotation を 1 ステップ実施しながら、ダイジェスト値計算→鍵生成→メッセージ復号→メッセージ認証、という Carousel 同期の手続きを繰り返しているためである。

しかしながら、その増大量は、他方式に比較して軽微であり、このグラフ結果からどう判断するか、

という点については、その差は共通鍵方式のメリットである軽量性を覆すことはないと考えてよいと思われる。想定している十分な強度を持つ長さ 35 の Carousel の場合においても。このようなモバイル端末側での複雑な処理を実施しているにもかかわらず、そのために必要な CPU 負荷は大きくはないと見てよい。

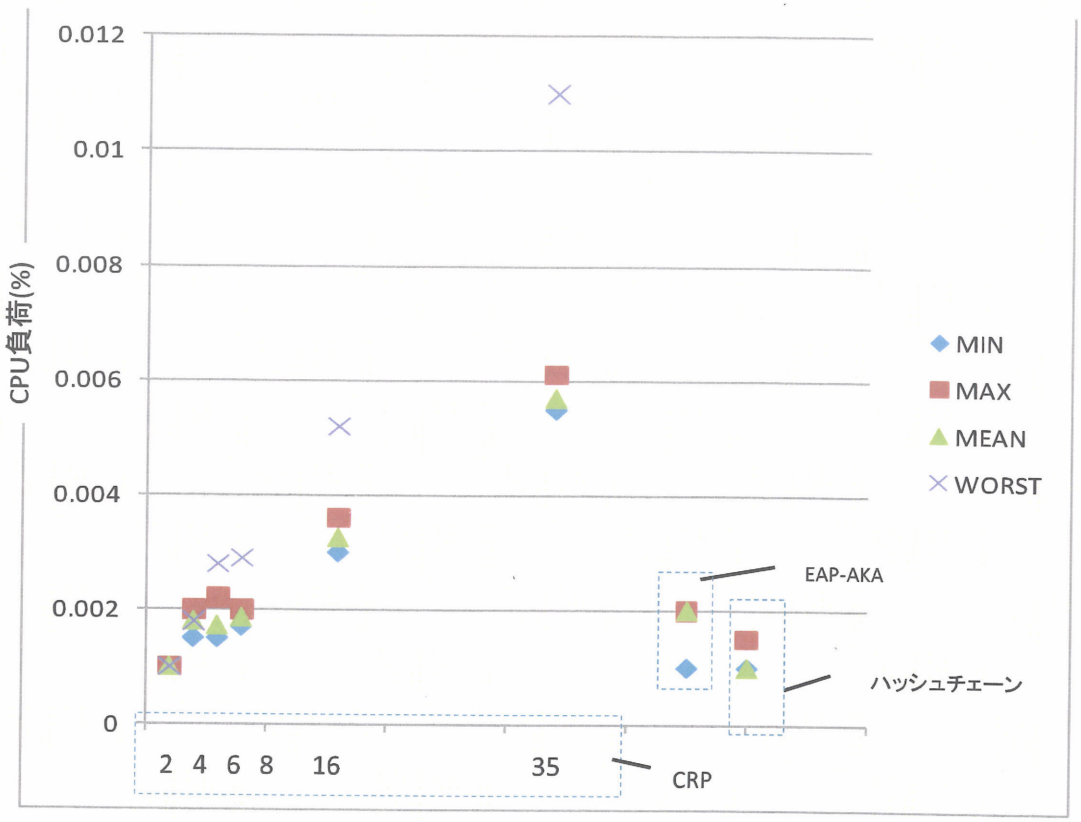

図 3-13 モバイル端末側での CPU 負荷(Rotation 回数別)

3.5.4. 相互認証処理の応答性能

本節では、実際の相互認証処理にかかる時間(応答性能)を評価する。CRP、EAP-AKA および EAP-TLS の比較を実施した。それぞれの方式に対して複数回の試行をし、処理時間を計測したものである。EAP-TLS は相互認証実現のために、サーバ認証・クライアント認証の双方を実施する設定とし、必要なプライベート証明書を作成し活用した。

表 3-4 に、応答性能をモバイル端末側で計測した結果を示した。また、図 3-14、図 3-15 およ

び図 3-16 にそれぞれの性能結果をグラフで表した。それぞれ、3 種類の数値を測定した。'REAL'はそれぞれのプロトコルで相互認証が完了するまでに要した実応答時間を示している。'USER'はそのプロトコルがユーザプログラム上で動作している時間を示している。'SYS'はそのプロトコルが OS 内部で動作している時間を示している。相互認証の処理においては、'USER'は暗号化/復号処理やプロトコル本体の処理に掛かる時間を示しており、'SYS'は通信等の I/O 処理に掛かる時間(ただし I/O 待ちは除く)を示している。I/O 待ちに掛かる時間('Blocked')は、CPU 時間としては算出されないため、'REAL'の値から'SYS'と'USER'を差し引いたものとして算出した。

表 3-4 各認証方式の相互認証処理にかかる時間

	Real(秒)	Sys(秒)	User(秒)	blocked(秒)
CRP	0.018	0.012	0.002	0.004
EAP-AKA	0.012	0.010	0.002	0.001
EAP-TLS	0.190	0.018	0.090	0.083

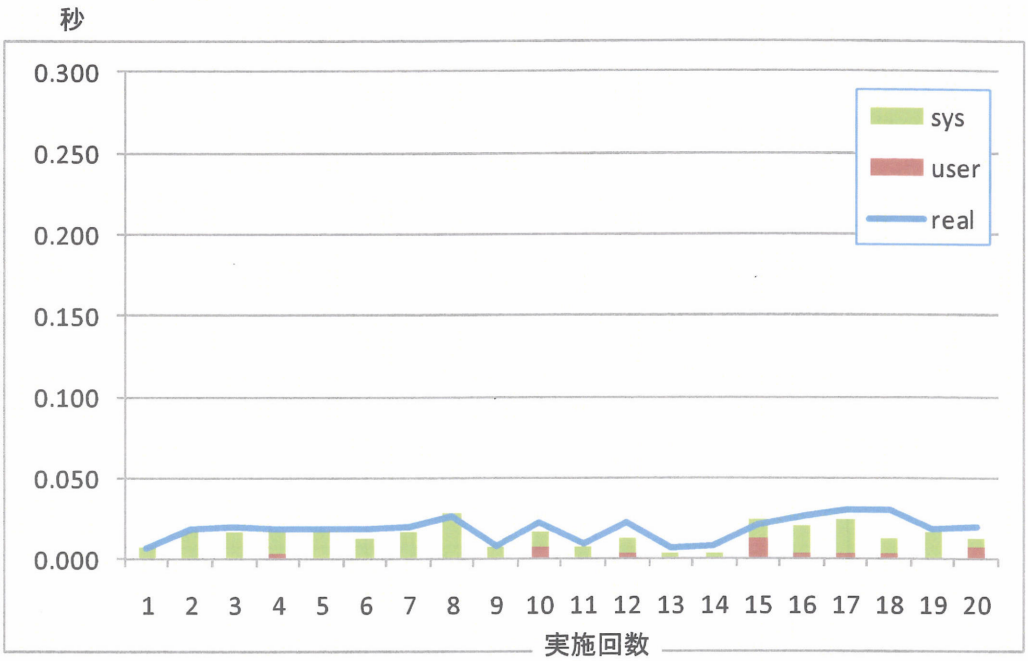

図 3-14CRP の応答性能(秒)

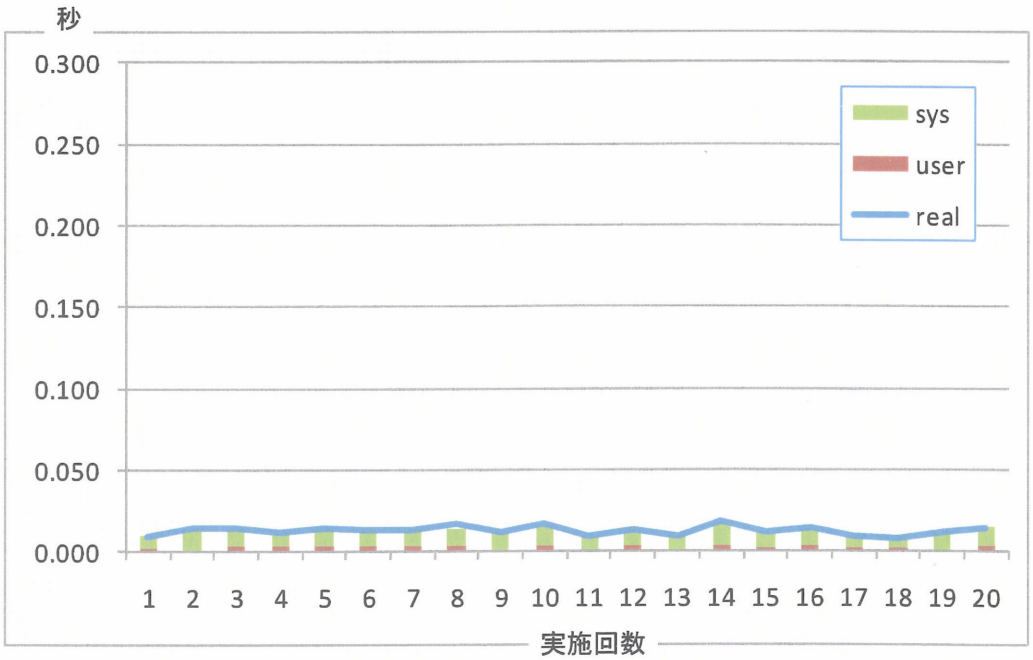

図 3-15EAP-AKA の応答性能(秒)

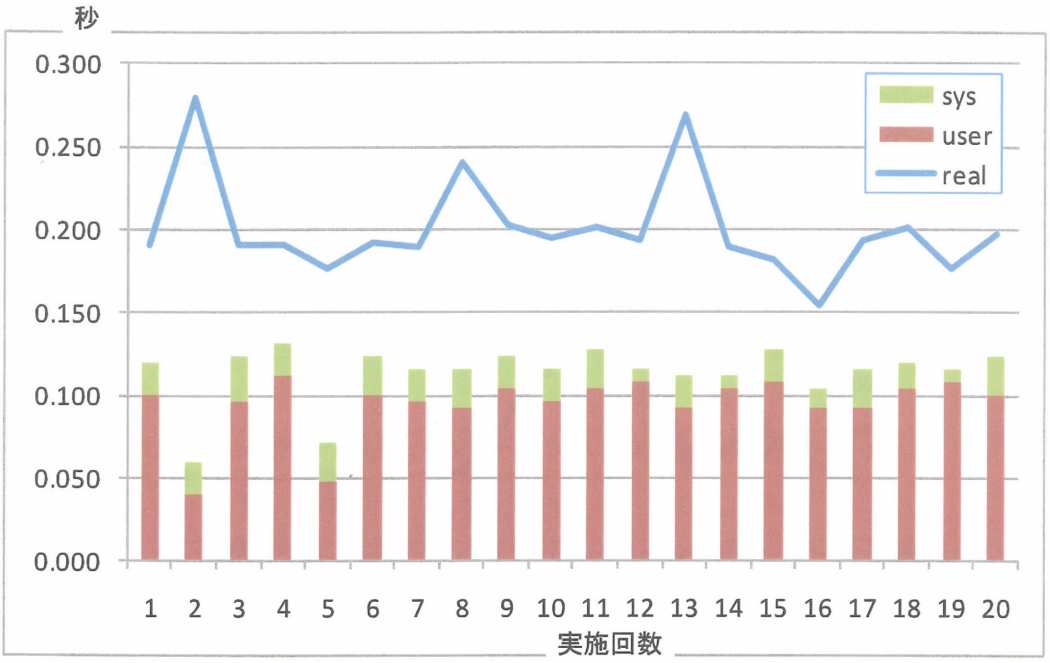

図 3-16EAP-TLS の応答性能(秒)

表 3-4、図 3-14、図 3-15 及び図 3-16 について議論する。

EAP-AKA と CRP との差はほとんど無い。この点からも CRP は共通鍵方式としての優位性を保持していると考えてよい。

'SYS'時間は 3 方式共に処理時間はほぼ同じである。I/O 処理に掛かる時間は全体に対して無視できると考えてよい。

'USER'時間は、EAP-TLS に比較して EAP-AKA、CRP が非常に低い。CRP については、グラフに現れない程低い場合もある。これは 3.5.3 節に記載したとおり、暗号化処理の計算量が、CRP が相対的に少ないことに起因している。

'REAL'時間は、'USER'時間の差以上に、CRP と EAP-TLS との差が拡大している。この差は、'Blocked'時間の差として現れている。本検証における'Blocked'時間は、主として通信時の I/O 待ちの時間を示している。通信時の I/O 待ちは、ネットワーク側、BS 側での処理時間に起因する遅れを示している。EAP-TLS では、ネットワーク側でクライアント認証を行うために、認証サーバへの問い合わせや認証処理に掛かる時間が必要となる。それが全体の応答性能の低下の原因となっている。

'Blocked'時間の増加を示すもう一つの指標は、相互認証に必要なデータ通信量である。図 3-17 に CRP と EAP-TLS での相互認証実施時のモバイル端末とネットワークとの間のデータ通信

量をバイト数で示している。EAP-TLS のデータ通信量が多くなっているのは明らかであり、このことも'Blocked'時間の増加の容易である。

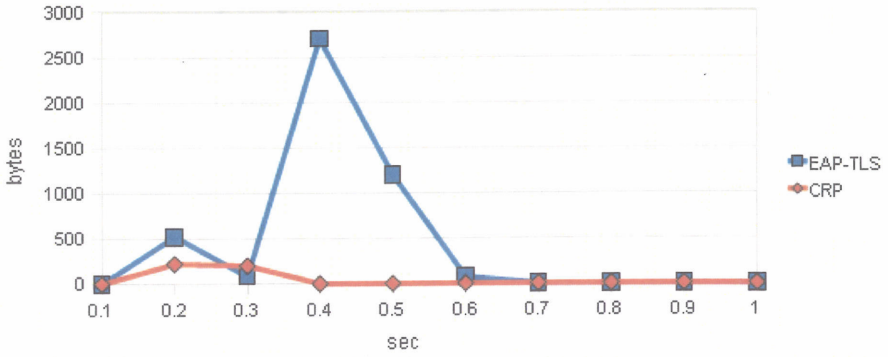

図 3-17CRP および EAP-TLS 実施時の通信量

前述のとおり、暗号化処理による'USER'時間の差と、データ通信量に因る'Blocked'時間の差が、'REAL'時間の差として現れており、CRP の応答性能が高いことを示していると考えてよい。

3.6. まとめ

第 3 章では、shared secret の予測不可能性を向上させるために、都度更新される shared secret を利用した新しいセキュリティ方式として、モバイル端末とネットワークオペレータ間の相互認証と暗号通信の方式"CRP"を提案した。CRP は、モバイル端末の位置情報(Location)とその履歴(Trail)を端末とネットワーク側で共有する情報として用い、それを Carousel と呼ぶデータ構造に格納して管理するプロトコルである。モバイル端末が移動し、通信を行うたびに、その位置の情報によって Carousel が更新される。この Carousel をモバイル端末とネットワーク側双方の shared secretとして用いることによって、「都度更新され予測不可能なshared secret」を実現している。

本方式に対して、セキュリティの観点とパフォーマンスの観点からの評価を行った。

(1) セキュリティの観点からは、今回の方式で採用した Carousel の予測不可能性について評価を実施した。結果として、現実的なデータサイズ(Carousel の長さ)で、その予測不可能性を十分満足できることを確認することができた。
また、ストーキング行為に対しても、それによってCarouselの再構築は非常に困難であることを示すことができた。

(2) パフォーマンスの観点からは、Carousel の予測不可能性を満足した上で、他の方式に比較して遜色ない CPU 負荷と応答性能を実現していることを確認できた。もちろん、公開鍵暗号方式と比較して十分高速な処理が可能であることも確認できた。

4. ハンドオーバ時の CRP による再認証に関する考察

4.1. 目的

第 3 章までの研究で、モバイル端末の位置情報を用いて shared secret の予測不可能性を向上させた新しい相互認証プロトコル“CRP”を提案した。本方式により、モバイル端末と基地局を利用した高速で安全な相互認証が可能となった。しかしながら、実際のモバイル無線ネットワーク環境では、モバイル端末が通信をしながら移動する場合もあり、その移動につれて接続する基地局が変化する(ハンドオーバ)機能が必要である。ハンドオーバ時においてもモバイル端末とネットワーク側の相互認証により得たセキュアなチャネルは確保する必要があるため、新しい基地局とモバイル端末間で新たに認証を行う必要がある。ただし、その間もアプリケーション通信は継続しているため、その通信の品質に与える影響を最小限にしなければならない。

そこでハンドオーバ時の再認証方式が必要となる。本研究では、CRP をベースとして、モバイル端末のハンドオーバが発生した時の再認証方式を検討し、その評価を行う。

4.2. ハンドオーバ

ハンドオーバとは、モバイル無線ネットワーク環境において、アプリケーションの通信を維持しつつ、モバイル端末の移動に応じて接続する基地局を移動させる技術のことである。基地局が変わるにつれて、通信に必要となるコンテキストを現在の基地局から次の基地局へと転送する必要がある。このコンテキストの中にはセキュアな通信の維持に必要な認証情報や鍵に関する情報も含まれる。

1.2 節に、今後のモバイル無線ネットワークシステムの想定を説明した。この環境下でのハンドオーバとしては、以下の条件について検討する必要がある。

1. 基地局を跨る、通常のハンドオーバ
2. ユビキタス無線ネットワーク環境や CR ネットワーク環境の実現を想定し、異なる物理ネットワークシステム間でのハンドオーバ(図 4-1)

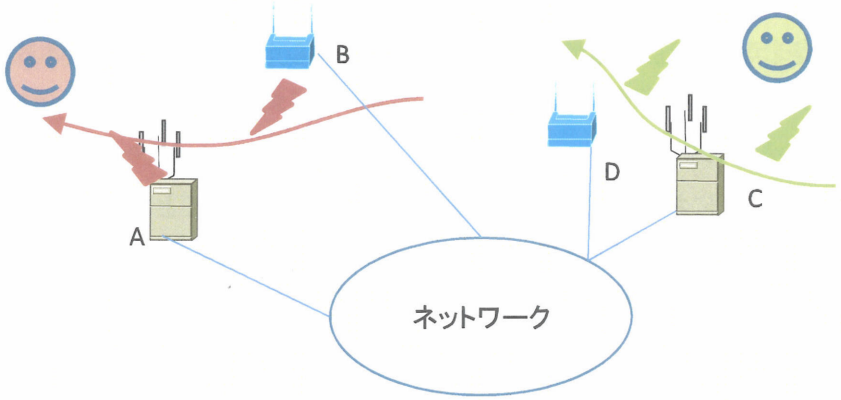

図 4-1 モバイル端末の移動とハンドオーバ

4.3. 関連研究

4.3.1. ハンドオーバ時のセキュリティに関する研究

モバイル端末での通信において Mobile IP が提案されている[70][71]。Mobile IP は基地局のハンドオーバを DataLink 層で実施させ、その上の IP 層は仮想的に維持することによって、アプリケーションレベルの互換性とセッションの維持を実現しているものである。パケットの喪失については TCP 層およびアプリケーション層によってリカバリするものと想定している。Mobile IP での基地局のスイッチングの方式として、必要に応じてハンドオーバを行う Lazy Cell Switching(LCS)、モバイル端末の移動状況を把握して次の基地局に対してヒントとなる情報を送付する Hinted Cell Switching(HCS)などの方法がある。それぞれの方式について、ハンドオーバ時のパケットの消失の度合いも研究されている[72]。

また、IEEE802.11 のハンドオーバについては、モバイル端末が近隣アクセスポイントのチャネルをスキャンする処理を最短にするアルゴリズム[73]や、アクセスポイントのネットワーク構成に応じた位置情報とその近隣アクセスポイントの情報をデータベース化した LocationServer を構築することによってモバイル端末の移動に応じてハンドオーバ時間を短縮する方法[74]などが提案されている。

CR ネットワークシステムにおいて、異なる物理ネットワーク環境や異なるプロバイダ間でのハンドオーバを行う場合については、物理ネットワークシステム間でのセキュリティコンテキストを転送する方式として、ハンドオーバ前と後のネットワークシステムで共有するセキュリティネットワークを構築し、そこに共通の認証サーバ等を設置する方法[75]や、ドメイン間でのハンドオーバ(ROAMING)の場合の認証や鍵交換の方式として、ドメインの異なるアクセスルータ間でのセキュリティコンテキストの交換プロトコル[76]などが提案されている。

4.3.2. EAP による re-authentication プロトコル

EAP をベースとした再認証プロトコルとしては、EAP-ER[60]が標準として提案されている。

(1) 再認証のための鍵階層

EAP-ER では、EAP において定義された鍵階層を用いて、EMSK と rIK という再認証用の鍵を生成している(図 4-2)。Long Term Shared secret から生成された EMSK をベースとして作成したrRK を元として、rIK と rMSK を生成する。

rIK は、Peer と Authenticate Server との間での認証に用いる鍵で、モバイル端末およびネットワークが再認証プロトコルで相互にやりとりする認証用の nonce を暗号化して互いを認証するために用いる。

rMSK は、認証終了後のセキュアなチャネルの確保のための鍵である。

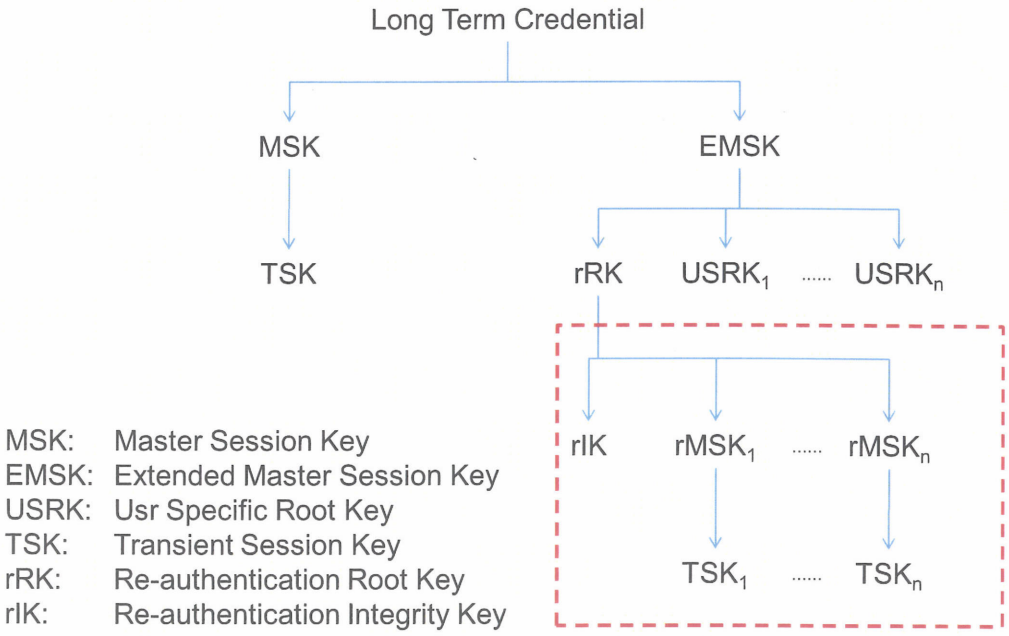

図 4-2 再認証のための EAP 鍵階層

(2) EAP-ER の詳細

EAP-ER は、事前に認証が完了した時点で生成した EMSK からさらに生成した鍵を用いることにより、Authenticate Server 及び Peer 上での認証処理を簡略化し、その負荷を軽減することを目的としている(図 4-3)。

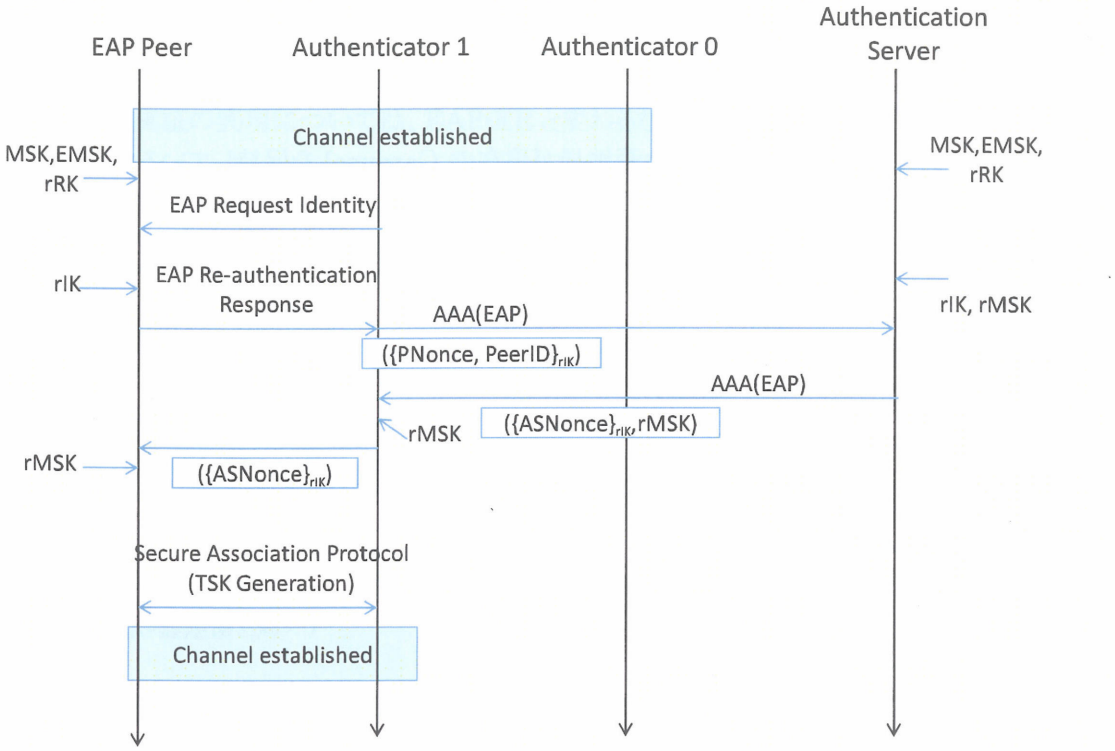

図 4-3 EAP-ER のフロー図

Authenticator が shared secret や認証のための rIK を知る必要はなく、メッセージの暗号・復号は Peer と Authenticate Server にて実施される。Authenticator は Peer から送付されたをそのまま Authenticate Server に送信して検証を行う。Authenticate Server の結果をみて認証が成功したことがわかれば、その結果を Peer に送信する。

4.3.3. 再認証プロトコルにおける課題と解決策

再認証のためのプロトコルである、EAP-ER の課題は以下のものがある。

(1) Shared secret が Authenticate Server で管理されている。
Authenticate Server(認証サーバ)の利用は、認証にかかる応答時間の増大に繋がるため、本研究の目標としては、認証サーバを用いない相互認証方式を検討してきた。従って、EAP-ER をそのまま採用することは困難である。

CRP では、前回認証を実施した基地局が現在の Carousel を保持しているため、ハンドオーバ時の再認証時には、新しく接続する基地局が前回の基地局に対して問い合わせを実施することになる。rIK は前回の基地局が生成し保持する。ハンドオーバを行う2つの基地局は物理的に近傍にあることが想定されるため、従来の方式である認証サーバと基地局間の通信と比較してより短い応答時間での再認証処理が期待できる。

以後は、CRP を用いた再認証プロトコルの詳細について説明し、続いてそのパフォーマンス面での評価を行った。

4.4. CRP Re-authentication プロトコル

4.4.1. CRP RE-authentication での鍵階層

CRP で用いる鍵階層を図 4-4 に示した(図 3-5 の再掲)。この階層は図 1-7 及び図 4-2 に示した EAP の鍵階層に基づく。

MSK や EMSK は、そのモバイル端末とネットワーク側との Carousel ペアの同期が完了した後に生成される。TSK は(通常の EAP と同様に)MSK から生成されてセッション鍵となる。EMSK は、CRP re-authentication による再認証を実施するときに用いる rIK の生成元として用いられる。rIK を用いた再認証の実現については、EAP-ER と変わるものではない。

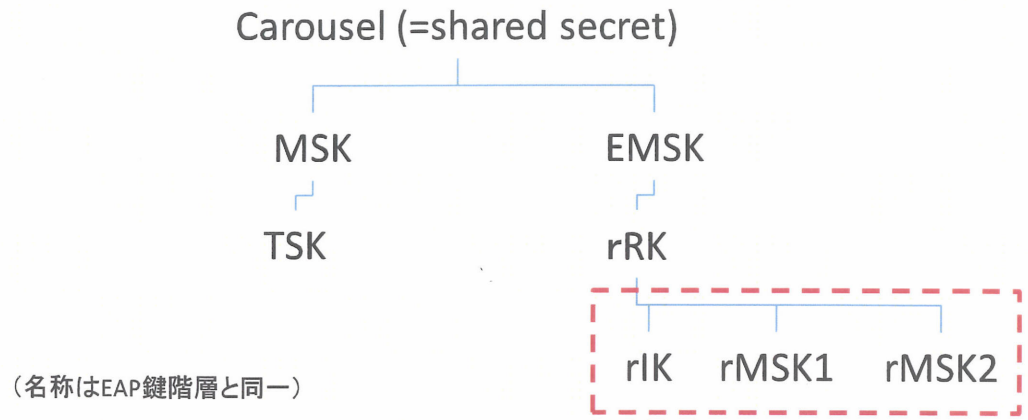

図 4-4 CRP の鍵階層

4.4.2. プロトコルの説明

本節では、CRP プロトコルをベースにした再認証のためのプロトコルである、CRP Re-authentication プロトコルの詳細を示す。

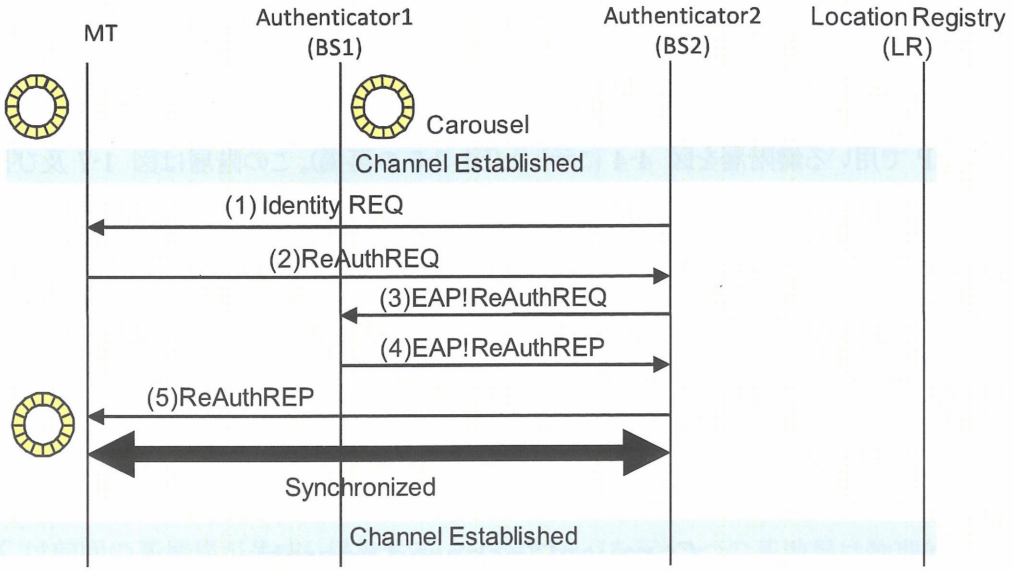

図 4-5CRP re-authentication プロトコルのフロー図

CRP re-authentication プロトコルの詳細は以下のとおり。以下では、モバイル端末(MT)がBS1 から BS2 へのハンドオーバを実施することを想定して示している。

1. BS2 → MT : IdentityREQ()
   BS2 は IdentityREQ()を MT に送信する。

2. MT → BS2 : ReAuthREQ({R_3||ID_{BS1}} rIK,{ ID_{BS1}}K_g)
   MT は BS1 との相互認証が完了した後で、EMSK から rIK を生成しておく。
   MT はランダムな文字列 R_3 と、MT 自身が今現在認証を受けて通信している BS の識別子である ID_{BS1} との連接、すなわち{R_3||ID_{BS1}}を先ほどの rIK で暗号化して、さらに認証時に受信した{ ID_{BS1}}K_g を ReAuthREQ メッセージに搭載して BS2 に送信する。

3. BS2 → BS1 : EAP!ReAuthREQ({R_3||ID_{BS1}}rIK, ID_{MT})
   BS2 は、受信したメッセージから K_g を利用して ID_{BS1} を取り、BS1 に{R_3||ID_{BS1}}rIK と ID_{MT} を送信する。

4. BS1 → BS2 : EAP!ReAuthREP({R_3||R_4}rIK, rMSK)
   BS1 は受信した EAP!ReAuthREQ メッセージのデータ部を BS1 自身の生成した rIK で復号する。正しく復号できれば再認証は成功である。BS1 は新たなランダム文字列 R_4 を生成し、{R_3||R_4}を同じ rIK で暗号化して、EAP!ReAuthREP()メッ

セージに載せて BS2 に送付する。その時同時に、最認証時のセッション鍵である rMSK を送信する。

5. BS2 → MT : ReAuthREP({R_3| |R_4}rIK)
BS2 は BS1 からわたされた{R_3| |R_4}rIK をそのまま ReAuthREP()メッセージに載せて MT にわたす。
MT はそれを受けて、rIK で復号し、R_3 が正しく復号されたことを確認し、再認証が成功したことを知る。

4.4.3. BS1 が Carousel を保有していない場合

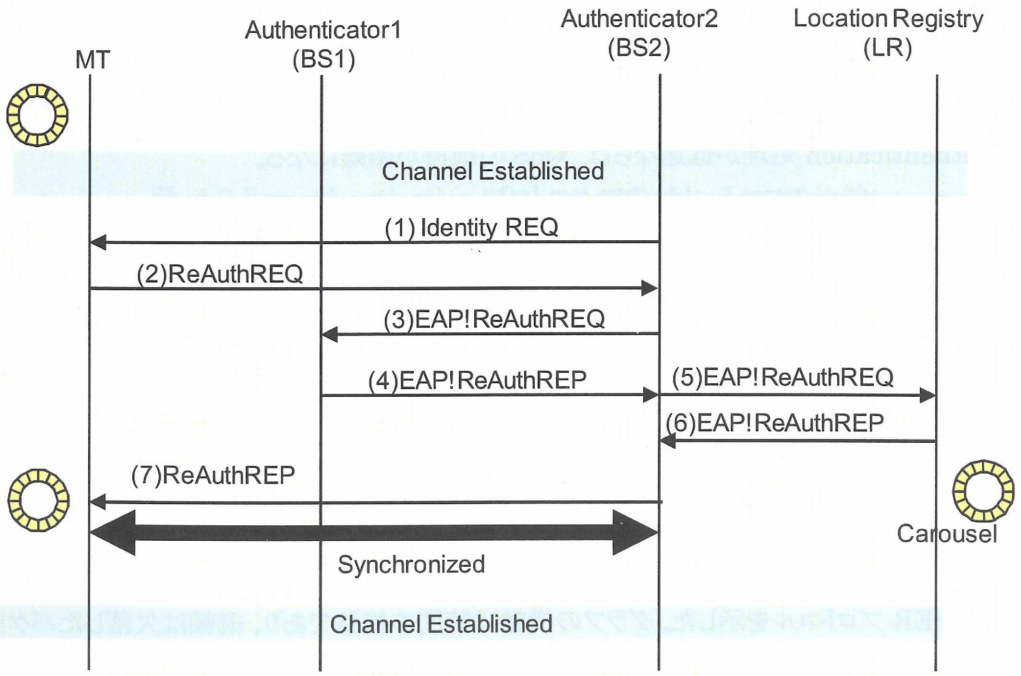

図 4-6BS1 が保有していない場合

BS1 は自分自身のメモリ容量等の都合で、Carousel をそれ以上保有できない状況に置かれることがある。その場合、Carousel は Location Registry に保存される。

ステップ 11 において、BS2 から BS1 に対して EAP!ReAuthREQ()メッセージを出してもエラーとなる。この場合 BS2 は Location Registry に対して同じ問い合わせを行う。Location Registry は BS1 から渡された正しい Carousel を保持しているため、CRP re-authentication の処理は継続され、同期は継続されてセキュアなチャネルは MT と BS2 との間で設立される。

4.5. CRP Re-authentication の評価

本節では、CRP Re-authentication の評価を行う。以前の論文では、CRP re-authentication の評価として、無線ネットワークシステム間のハンドオーバ時の性能について評価を行った。

ここではさらに、re-authentication プロトコルがアプリケーション層のプロトコルに与える影響について議論していく。

4.5.1. 評価の考え方

MT が CR ネットワーク上の BS1 を介して通信を実施していたと想定する。例えば MT が移動したことにより BS1 との電波強度が低下し、逆に BS2 の強度が上昇したなどの理由により、ある時点で MT が BS1 から BS2 に通信を切り替える判断をすることが考えられる。この場合、MT は自分自身とネットワークとの通信の QoS を維持しつつ、BS1 から BS2 へのハンドオーバを実現する必要がある。BS2 へのハンドオーバを実現するためには BS2 での再認証が必要となり、もし re-authentication 処理が低速ならば、QoS の維持が困難になる。

そこで、本節での評価は、MT が無線ネットワークを介して VoIP アプリケーションプログラムを利用している場合を想定し、re-authentication プロトコルの違いで QoS がどの程度低下するかを検証した。VoIP アプリケーションプログラムは、音声を G.711[68]や G.729[69]といったコーデックで変換したパケットを RTP で送信することで音声通信の品質を維持するものである。

4.5.2. 評価結果

図 4-7 は、上記の VoIP アプリケーションプログラムによる通信中にそのパケットがどの程度欠落するかをシミュレーションした結果を示したものである。比較対照として、CRP re-authentication と EAP-ER プロトコルを示した。グラフの横軸は時間の推移であり、縦軸は欠落したパケットを示している。図の直線で示したグラフは CRP re-authentication の検証結果で、点線で示したものは EAP-ER の検証結果である。直線上に三角形やひし形のシンボルが存在するが、それはその時に re-authentication プロセスが動作したことを示しており、その時点でパケットが欠落したことを示している。個々の直線の名称、例えば CRP(x,y)や ER(x,y)等の、x は BS1 と BS2 間の想定転送時間を、y は認証サーバと BS 間の想定転送時間を示している。

図 4-7 に示したとおり、CRP re-authentication は EAP-ER と比較して若干パケットの欠落が少ない結果となっている。これは遠隔にあるサーバ等への通信量が影響している。EAP-ER に限らず、AAA サーバ等の認証サーバを設置するアーキテクチャの場合は、そのサーバへのリクエストとレスポンスの受領が必要となるため、どうしても応答速度の遅延が生じてしまう。CRP はそれに比較して必ずしも遠隔のサーバに問い合わせを出す必要がなく BS1 と BS2 間での通信のみで処理

可能であるため、その分だけ re-authenticaion の応答時間が短縮できている。本検証の想定は認証サーバとの通信応答時間は 5 ミリ秒および 10 ミリ秒を想定しているが、これが長くなればなるほどパケットの欠落、ひいては QoS の低下につながると考えられる。

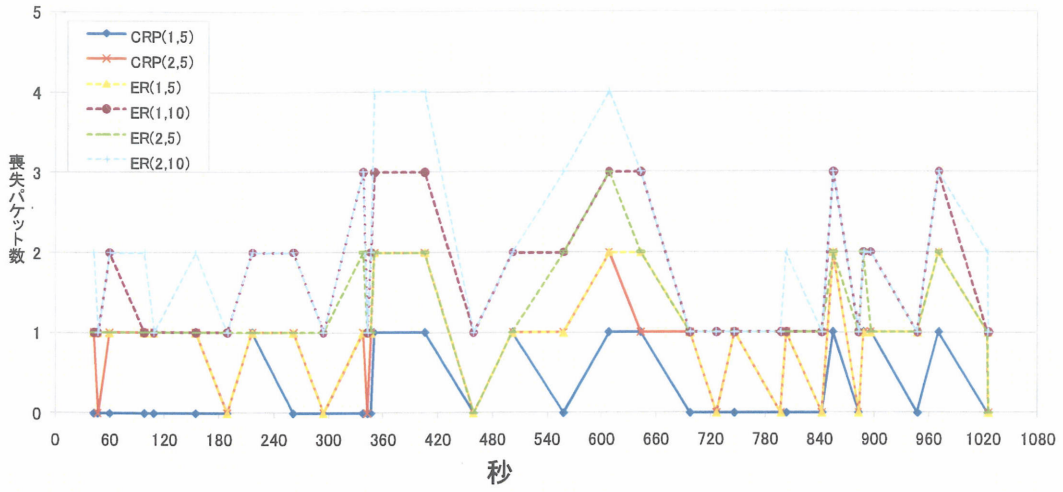

図 4-7 Re-authentication プロトコルでのパケットロスの比較

4.6. まとめ

本章では、モバイル端末のハンドオーバ時の応答時間短縮を目的として、CRP をベースとする再認証プロトコルを検討した。結果として、EAP の標準的な再認証プロトコルである EAP-ER と CRP の Carousel を用いた shared secret の特徴を組み合わせて、再認証時の認証情報の引継ぎを基地局間で実施する方式を取り入れた、CRP re-authentication プロトコルを提案した。その特徴は以下のとおり。

(1) 認証サーバを用いず基地局間のみでの通信により再認証を実施するため、応答時間の短縮を実現。

また、実際に、アプリケーション通信の品質への影響に関する検証を行い、EAP-ER 方式と比較して、CRP re-authentication プロトコルが、再認証実施時のパケット消失の割合が、改善していることを確認した。

5. おわりに

本研究では、これから広がるであろう多重無線システムから構成されるユビキタス無線ネットワーク環境やCognitive Radioネットワーク環境において、情報セキュリティ方式に対して求められるであろう:

(1)複数の無線システムから共通で利用可能なセキュリティ方式であること

(2)アプリケーション通信サービスの品質を低下させないこと

という二つの要件を満足することのできる新しい方式を検討した。

これらを実現する新しいセキュリティ方式の考え方として、「shared secretの予測不可能性を向上させた、共通鍵暗号方式を元にした認証・暗号通信方式」が最適である、との知見を得、その結果として、以下のような結論を得られた。

(1) モバイル端末の位置情報(Location)とその履歴(Trail)を、「利用者の移動に応じて更新され、かつモバイル端末とネットワーク側で共有できる情報」として考え、その Trail を Carousel と呼ぶデータ構造で管理することで shared secret として利用するプロトコル"CRP"を考案した。

(2) この Carouselというデータ構造を用いることで、逐次更新されるshared secretを実現し、またそれが現実的に計算可能なデータ量で十分な予測不可能性を持っていることを確認した。

その拡張として、Carousel を用いた、ハンドオーバ時の再認証プロトコルである CRP re-authenticationを提案し、以下のような結論を得られた。

(3) EAP-ERの鍵管理方式とプロトコルをベースとし、CarouselとCRPを用いた拡張を施すことで認証サーバを利用しない方式に変更することができた。それにより再認証処理時のアプリケーション通信への影響(アプリケーションパケットの消失)をEAP-ERと比較して低下させることに成功した。

無線ネットワークシステムは普及が進み、セキュリティの規格も確定している分が多いが、CR ネットワーク環境などのように今後さらに進歩していく無線ネットワークシステムにおける、セキュリティ方式の候補の一つとして提案できるものと考えている。

謝辞

本研究は、筆者が 2004 年からの独立行政法人 情報通信研究機構の「次世代無線ネットワークアーキテクチャ研究開発」プロジェクトに参加した中で進めたものを基礎とし、静岡大学創造科学技術大学院博士課程入学後に、それをまとめたものである。静岡大学創造科学技術大学院 情報学部の水野 忠則先生には、指導教官として、研究の遂行に関してご指導ご助言いただいた。また、情報通信研究機構の黒田 正博氏には、このようなプロジェクトに参加する機会を与えて頂き、時には重要な助言を頂いた。お二人には特に深い感謝の意を表する。また、同大学院 情報学部の西垣 正勝先生、峰の博史先生、ならびに同大学院 環境・エネルギーシステム専攻の佐古猛先生には、学位論文の事前審査等において的確なコメントやご助言を頂いた。特に西垣先生には何度もレビュー頂く機会を頂戴し、満足な論文としてまとめることができた。感謝の意を表する。

最後に、三菱電機株式会社神戸製作所の皆様については、筆者の勝手な活動について快く了承してくださったおかげで、最後まで遂行することができた。感謝の意を表する。

参考文献

[1] IEEE 802.11: (online) available from (http://www.ieee802.org/11/)

[2] 松江 英明、守倉 正博: "802.11 高速無線 LAN 教科書", IDG ジャパン, 2003

[3] IEEE 802.11b working group: "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band", IEEE, 2003

[4] IEEE 802.11g working group: "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band", IEEE, 2003

[5] IEEE 802.16: (online) available from (http://www.ieee802.org/16/)

[6] IEEE 802.20: (online) available from (http://www.ieee802.org/20/)

[7] IEEE 802.16 working group: "Part 16, Air Interface for Fixed Broadband Wireless Access Systems", IEEE, 2004

[8] IEEE802.16e working group: "IEEE: Amendment to IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems – Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation Licensed Bands", IEEE, 2005

[9] WiMAX Forum: (online) available from (http://www.wimaxforum.com/)

[10] IEEE 802.15: (online) available from (http://www.ieee802.org/15/)

[11] The Official Bluetooth® Technology Info Site: (online) available from (http://www.bluetooth.com/)

[12] Rajeev Koodli and Charles Perkins, "Mobile IP Fast Handovers", RFC-4988, IETF, Oct. 2007

[13] 総務省, u-Japan 政策 (online) available from (http://www.soumu.go.jp/menu_seisaku/ict/u-japan/)

[14] IEEE 802.22: (online) available from (http://www.ieee802.org/22/)

[15] Carlos Cordeiro, Kiran Challapali, Dagnachew Birru, and Sai Shankar N: "IEEE 802.22: The first worldwide wireless standard based on cognitive radios", in Proc. IEEE International Symposium, New Frontiers Dynamic Spectrum Access Networks, 2005

[16] IEEE1900.4: (online) available from
(http://grouper.ieee.org/groups/scc41/4/index.htm)

[17] J.A.ブーフマン, "暗号理論入門", シュプリンガージャパン(株), May. 2007.

[18] 結城 浩: "暗号技術入門ー秘密の国のアリス", ソフトバンククリエイティブ(株), Dec. 2008.

[19] NIST: "FIPS PUB 46-3: DATA ENCRYPTION STANDARD (DES)", Oct. 1999

[20] NIST: "FIPS PUB 197: ADVANCED ENCRYPTION STANDARD (AES)", Nov. 2001

[21] Mitsuru Matsui, Junko Nakajima and Shiho Moriai, "A Description of the Camellia Encryption Algorithm", RFC-3713, Apr. 2004

[22] RSA Rabolatories: "PKCS #1 v2.1: RSA Cryptography Standard", (online), available from (http://www.rsa.com/rsalabs/node.asp?id=2125)

[23] David Cooper, Stefan Santesson, Stephen Farrell, Sharon Boeyen, Russell Housley and Tim Polk: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC-5280, May 2008

[24] 小松 文子, "PKI ハンドブック", 株式会社ソフトリサーチセンター, Nov, 2000

[25] Alan O. Freier, Philip Karlton and Paul C. Kocher: "The SSL Protocol Version 3.0" , (online)
available from (http://www-ailab.elcom.nitech.c.jp/security/ssl/draft302-j.html), Nov. 1996

[26] Tim Dierks and Eric Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC-5246, Aug. 2008

[27] Larry J. Blunk and John R. Vollbrecht: "PPP Extensible Authentication Protocol (EAP)", RFC-2284, IETF, Mar. 1998

[28] Bernard Aboba, Larry J. Blunk, John R. Vollbrecht, James Carlson and Henrik

Levkowetz: " Extensible Authentication Protocol (EAP)", RFC-3748, IETF, June. 2004.

[29] Henry Heverinen and Joseph Salowey: "RFC-4186: Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)", RFC-4186, IETF,Jan. 2006

[30] Jari Arkko and Henry Haverinen: "RFC-4187: Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", RFC-4187,IETF,Jan. 2006

[31] Bernald Aboba and Dan Simon: "PPP EAP TLS Authentication Protocol", RFC-2716, IETF, Oct. 1999

[32] Paul Funk and Simon Blake-Wilson: "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)", RFC-5281, IETF, Aug. 2008

[33] Ashwin Palekar, Dan Simon, Glen Zorn, Simon Josefsson, Hao Zhou and Joseph Salowey: "Protected EAP Protocol (PEAP) Version 2", (online) available from (http://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-10), Oct 2004

[34] "3G Security, Security Architecture (Releases 5)", 3GPP TS33.102 V5.5, Sep, 2004

[35] IEEE 802.11 working group: "Wireless Lan Medium Access Control (MAC) And Physical Layer (PHY) Specifications", Information Technology-telecommunications And Information exchange Between Systems-Local And Metropolitan Area Networks-specific Requirements, part 11,1997

[36] Jesse Walker: "Unsafe at any key size; An analysis of the WEP encapsulation", IEEE 802.11 doc 00-362, Oct, 2000

[37] Nikita Borisov and Ian Goldberg and David Wagner: "Intercepting mobile communications: the insecurity of 802.11", MobiCom '01: Proceedings of the 7th annual international conference on Mobile computing and networking, page 180 – 189, 2001

[38] IEEE 802.11i working group: "Amendment 6: Medium Access Control (MAC) Security Enhancements", IEEE, 2004

[39] Martin Beck and Erik Tews: "Practical attacks against WEP and WPA", Proceedings of the second ACM conference on Wireless network security, 2009

[40] IEEE802.11 working group: "IEEE 802.1X Port-Based Network Access Control", IEEE, 2001

[41] David Johnston and Jesse Walker, "Overview of IEEE 802.16 Security", IEEE Security and Privacy, pp. 40-48, May-June, 2004

[42] Kaigui Bian and Jung-Min Park: "Security Vulnerabilities in IEEE 802.22", ICST WICON, 2008

[43] Przemyslaw Pawelczak: "Protocol Requirements for Cognitive Radio Networks", (online) available from (https://doc.freeband.nl/dscgi/ds.py/Get/File-60831) ,2005

[44] Ruiliang Chen, Jung-Min Park and Jeffery H. Reed: "Defense against Primary User Emulation Attacks in Cognitive Radio Networks", IEEE journal on Selected Araas in Communications Special Issue on Cognitive Radio Theory and Applications,2008

[45] Wenyan Xu., Pandurang Kamat and Wade Trappe: "TRIESTE: A Trusted Radio Infrastructure for Enforcing Spectrum Etiquettes", First IEEE Workshop on Networking Technologies for Software Defined Radio Networks, 2006

[46] Trusted Computing Group: (online) available from (http://www.trustedcomputinggroup.org)

[47] Ritsu Nomura, Masahiro Kuroda, and Daisuke Inoue, "Location-based Key Management for Ubiquitous Wireless Network," In proceedings of WPMC 2005, Vol.1, pp.51-55, Sep. 2005.

[48] Masahiro Kuroda and Ritsu Nomura, "Radio-independent Mobile Authentication Protocol for Ubiquitous Network," In proceedings of WPMC 2005, Vol.3, pp.1703-1707, Sep. 2005.

[49] Ritsu Nomura, Masahiro Kuroda, and Tadanori Mizuno, "Evaluation of EAP based Re-authentication Protocol for High-speed Vehicular Handover in Cognitive Radio Networks," In proceedings of CrownCom 2007, Vol. 1, Aug. 2007.

[50] Masahiro Kuroda, Ritsu Nomura and Wade Trappe: "A Radio-independent

Authentication Protocol (EAP-CRP) for Networks of Cognitive Radios", The Proceedings of IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks, Vol 1, pp 70 -79, Jun. 2007.

[51] 情報通信研究機構, 情報処理推進機構, Cryptrec report, 2009

[52] 総務省、経済産業省, 電子政府推奨暗号リスト, 2005

[53] Leslie Lamport: "Password authentication with insecure communication", Vol 24, pp 770 – 772, Communications of the ACM, Nov. 1981

[54] RSA Rabolatories: "PKCS #1 v2.1: RSA Cryptography Standard", (online), available from (http://www.rsa.com/rsalabs/node.asp?id=2125)

[55] 青木 隆一、稲田 龍、村井 純: "PKI と電子社会のセキュリティ", 共立出版, 2001

[56] 塚田 孝則: "企業システムのための PKI", 日経 BP 社, 2001

[57] Carl Rigney, Allan C. Rubens, William Allen Simpson and Steve Willens: "Remote Authentication Dial In User Service (RADIUS)",RFC-2865, IETF, June 2000

[58] Paul Congdon, Bernard Aboba, Andrew Smith, John Roese and Glen Zorn: "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines", RTF-3580, IETF, Sep. 2003

[59] Bernard Aboba and Pat R. Calhoun: "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)" ,RFC-3579, 2003

[60] Vidya Narayanan and Lakshminath Dondeti, "EAP Extention for Efficient Re-authenticaton"(online), available from
(http://tools.ietf.org/html/draft-vidya-eap-er-02)

[61] Tom Karygiannis and Les Owens: "Wireless Network Security 802.11, BlueToothand Handheld Devices", NIST, Nov. 2002

[62] P. Enge and P. Misra: "Special Issue on Global Positioning System", Proc. of the IEEE, page 3-15, Jan. 1999

[63] James J. Caffery, Jr. and Gordon L. Stüber, "Overview of Radiolocation in CDMA Cellular systems", IEEE Cummunication Magazine, Apr. 1998

[64] Ian F. Akyildiz, Joseph S. M. Ho, and Yi-Bing Lin, "Movement-based location update and selective paging for PCS networks", IEEE Personal Communication Magazine, vol. 5, no. 18, pp. 13-23, Oct. 2001

[65] Jie Li, Yi Pan and Xiaohua Jia, "Analysis of Dynamic Location management for PCS networks," IEEE Trans. on Vehicular Technology, vol. 51, no. 5, pp. 1109-1119, Sep. 2002.

[66] Yi-Bing Lin, "Reducing Location Update Cost in a PCS Network," IEEE/ACM Transactions Networking, vol. 5, pp. 25-33, Feb. 1997

[67] OpenSSL: (online) available from (http://www.openssl.org/)

[68] ITU: "Pulse Code Modulation (PCM) of Voice Frequencies", ITU-T Recommendation G.711

[69] ITU: "Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)". ITU-T Recommendation G.729

[70] Charles Perkins: "IP Mobility Support", IETF, RFC-2002, Oct 1996

[71] Charles Perkins: "Mobile IP, Design Principles and Practices", Wireless Communication Series, Addison-Wesley, 1997

[72] Nikolaus A. Fikouras and Carmelita Gorg: "A complete Comparison of Algorithms for Mobile IP Hand-offs with Complex Movement Patterns and Internet Audio", In Proceedings of the Fourth International Symposium on Wireless Personal Multimedia Communications (WPMC), Aalborg, Denmark, Sep. 2001

[73] Kyoungnam Kwon and Chaewoo Lee: "A Fast Handoff Algorithm using Intelligent Channel Scan for IEEE 802.11 WLANs", Advanced Communication Technology, 2004, The 6th International Conferences on, page 46-50, Sep. 2004

[74] Chien-Chao Tseng, Kuang-Hui Chi, Ming-Deng Hsieh and Hung-Hsing Chang: "Location-based Fast Handoff for 802.11 Networks" IEEE Communications Leters, Vol.9, No.4 Page 304-306, Apr. 2005

[75] H Wang and A. R. Prasad: "Security Context Transfer in Vertical Handover", Personal, Indoor and Mobile Radio Communications, 2003, PIMRC 2003, 14th

IEEE Proceedings on, Vol.3, Page 2775-2779, Sep. 2003

[76] Rene Soltwisch, Xiaoming Fu and Dieter Hogrefe: "A Method for Authentication and Key Exchange for Seamless Inter-domain Handovers", In proceedings of 12th IEEE International Conference on Networks 2004, Page 463-469, Nov. 2004