修士論文

Proximity Communication 上での情報共有アプリケーションの災害時情報伝達特性の評価

2015年2月5日

指導教員　浅見　徹　教授

東京大学 大学院情報理工学系研究科
電子情報学専攻　48-136406

小河原　健生

内容梗概

2011 年 3 月 11 日の東日本大震災では，大規模な輻輳による障害が生じていた関東甲信越地方を中心に安否確認のためのツールとして Social Networking Service (SNS) が有効であったことが報告されている．バックホール障害によってモバイルネットワークが利用できなかった地域についても，同様に SNS サービスを提供することを目指す.

第 1 に，Proximity Communication 上に Named Data Networking (NDN) を動作させることで災害時に分断された基地局配下でも，端末と基地局を使って，災害時以前と同じアプリケーションを提供することができることを示す．まず，NDN 上でのデータ同期アプリケーション ChronoSync を災害時の安否確認に利用する場合の評価を行い，全体の 10%のユーザが移動する場合，同期間隔を 1 分に設定することで，東日本大震災時の関東甲信越地方における携帯電話メールのメッセージ配信性能よりも良い性能が分断されたネットワーク内でも得られることを示す．また，消費電力は現在の携帯電話サービスの平常時におけるスマートフォンの消費電力の約 30 倍になることを示し、消費電力削減に関して大きな課題が残されていることを示す．さらに，より消費電力特性のよいシステムを提案し，被災地において本サービスを利用した場合の情報伝達性能についてシミュレーションにより示す.

第 2 に，ID-based Encryption (IBE) を Named Data Networking 上で利用することを前提に，端末とネットワークの相互認証手続き，ユーザとアプリケーションサービスプロバイダ間でのサービス利用時の ID の生成 (ID 合意)，相互認証手続きについて提案する．提案手続きは，携帯電話網のネットワーク/端末認証手続きを大幅に簡略化した分散認証を実現しており，かつ，インターネット上のサービスで現在一般的に利用されているユーザ ID とパスワードによる認証の自然な拡張になっていることを示す.

目 次

図目次

表 目 次

第1章

序論

1.1　本研究の背景

2011 年 3 月 11 日に発生した東日本大震災では，日本社会の多くが甚大な被害を受けた．携帯電話網を含む通信インフラについてもその被害の程は大きく，災害後からしばらくの間は広い地域においてサービスを利用できない状況であった．

携帯電話網にこのような耐災害性の低さをもたらした要因の一つとして，携帯電話網がコアネットワーク内のサーバ群による中央集中型の管理構成をとっていることがあげられる．サービスの認証や名前解決，アプリケーション等を提供するサーバ群のうちどれかひとつでも利用不可能になるとサービス全体が利用不可能に陥る．そのため，災害によってバックホールが切断などの被害を受けると，基地局や端末などが利用可能な状態であってもサービスは停止する．実際に東日本大震災においても，停波した基地局のうち，このようなバックホールの断線が原因であったものは停電を除くと全体の 60%にのぼる [1]．この意味では，電話網も現在のインターネットも同様であり，現行のシステムでは災害時にサービスを継続して提供することは困難である．耐災害性を高めるために，末端設備単体であっても継続してサービスを提供できるような分散的なネットワーク構成であることが望ましい．Named Data Networking (NDN) では各ルータが名前解決を行いフォワーディング先を決定する分散的なルーティングが行われる．外部のサーバへの依存度が低く，エンドノードがルータによって接続されている限り同様のネットワーク利用が可能である

現在のインターネットを刷新する技術としても注目を集めており，他の Delay Tolerant Network (DTN) やアドホックネットワークのような災害時特有のネットワークと異なり，災害前後でのシームレスな利用ができると期待される．一方，東日本大震災において，輻輳によって電話回線を使用できなかった地域では，Social Networking Service (SNS) が有効であったことが報告されている．NDN 上で動作し，ユーザ間の情報共有を可能とするアプリケーション ChronoSync を用いて SNS を構築できれば，災害時にも被災者間の安否確認などの情報共有を行うことができると考えられる．

災害時には被災地周辺で大規模なトラヒックが発生し各所で輻輳が生じた．NTT docomo によれば図 1.1 に示すように，災害時のメールサービスの状況は，被害の比較的軽かった関東甲信越地域でも 80%のメールを伝達するまでに 30 分，90%のメールを伝達するまでに 80 分の遅延が生じた [1]．この値は安否確認としては十分ではないが，とりあえず災害規模が大きくネットワークが分断された地域における安否確認システムとして，80 分を目標伝達時間として設定し，それ以下の時間で安否確認情報を共有することを目指すことにした．

本論文ではコアネットワークから分断されたネットワーク (分断されたネットワーク) についても平常時同様のサービスを提供することを目標としている．外部ネットワークから分断され，基地局単体とユーザの持つ端末のみからなる孤立したネットワークにおいても，インフラに依存しない Proximity Communication を利用することで局所的な端末間のコネクションを確立することができる [4–6]．

第 1 に，Proximity Communication 上に Named Data Networking(NDN) [7] を実装することにより普段と同様のサービスを展開することが可能であることを示す．さらに，災害時の分断されたネットワーク上で NDN ベースのアプリケーションである ChronoSync を模倣した安否確認システムを動作させた時の性能について評価する [8, 9]．

ChronoSync は全ユーザに対してすべてのメッセージを拡散させる Epidemic routing の形式をとるため，生じるトラヒック量は膨大である．災害時のような端末への電力供給が望めない環境下ではトラヒック量を減らし消費電力の削減に努める必要がある．しかしながら，NDN のルーティング機構を利用してトラヒック量を削減する場合，パケット単位の回線交換的制御による通信経路の制約や中継ノードのタイムアウトを受け，分断されたネットワーク間の通信では十分な性能

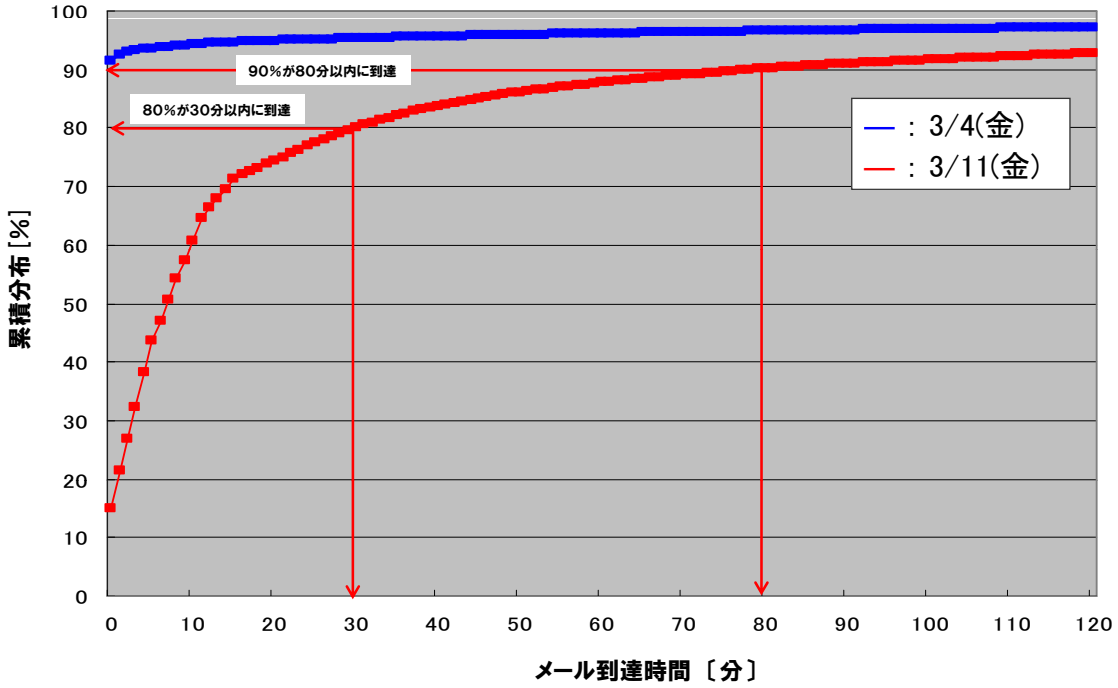


図 1.1: 東日本大震災時の関東甲信越地域におけるメール遅延 [1]

が得られない．このために提案する Name トンネリングでは，他の分断されたネットワークとのゲートウェイ機能を担うノードが各ネットワークで NDN の通信を一旦終端させ，Tunnel Object に変換して移動ノードに運ばせる [10]．Tunnel Object はゲートウェイと移動ノード間で直接やり取りされるためタイムアウトによる失敗はない．また，移動ノード間で Tunnel Object における Tunnel Interest と Tunnel Content Object はそれぞれ独立で送受されるため，経路の制限を考慮する必要がない．ChronoSync と Name トンネリングを情報伝達性能とトラヒック量の観点から比較し，Name トンネリングが ChronoSync と同程度の情報伝達性能を保ちつつトラヒック量を大幅に削減可能であることをシミュレーションにより示す．

第 2 に，大規模な災害時には，家族や友人の安否確認や被害の規模など正確な情報の取得が重要である．しかしながら，中央集中型の制御を行っている通信インフラは災害直後には断線などにより利用できないことが多い．東日本大震災時には，停電を除くと約 60%の基地局がユーザ認証や名前解決，アプリケーションサービスを行う中央サーバから切断されることによって停波した [11]．そのため，ユーザによる携帯電話サービスへの需要は高かったが，基地局自体に損傷はない場合でも断線によるサービス停止で利用できなかった．そこで，設備がサーバから切断された場合にもユーザ認証や名前解決を災害前後で同等のサービスを提供できる Named Data Networking と 2 層の Hierarchical ID-based Encryption (HIDE) による自律分散システムを提案した [7, 12, 13]．本論文では，キャリアを Root Keg Generation Center (KGC) とした HIDE に基づく，ネットワークおよび端末の分散認証の手続き並びにアプリケーションへのログイン手法について具体的な提案する．

以上の提案に基づき，本論文の構成は以下のようになっている．

- 第 1 章　序論
- 第 2 章　関連研究

- 第 3 章　提案モデル
- 第 4 章　性能評価
- 第 5 章　結論

第 2 章では，本研究の基礎技術となる Proximity Communication，Named Data Networking，Hierarchical ID-based Encryption について述べる．第 3 章では，第 2 章で述べた技術を元にした，耐災害情報共有アプリケーションの構成について述べる．第 4 章では，提案モデルを災害地で用いた場合の情報伝達性能についてシミュレーションした結果について述べる．第 5 章でまとめとする．

第2章

関連研究

2.1　Proximity Communication

Proximity Communication は各デバイスの通信範囲にあるデバイスを直接接続しする通信技術である．外部のサーバやその他インフラへの依存度が低く，スマートフォンといったユーザのモバイルデバイスのみであっても，それらを接続した通信が可能である．Proximity Communication を提供するための技術としては，下記に挙げる 3GPP によって提案されている LTE Direct や Wi-Fi Alliance によって策定された Wi-Fi Direct がある [4,6]．図 2.1 は Proximity Communication でデバイスを接続するときの概略図である．

(a) LTE Direct　　(b) Wi-Fi Direct

図 2.1: Proximity Communication による接続イメージ

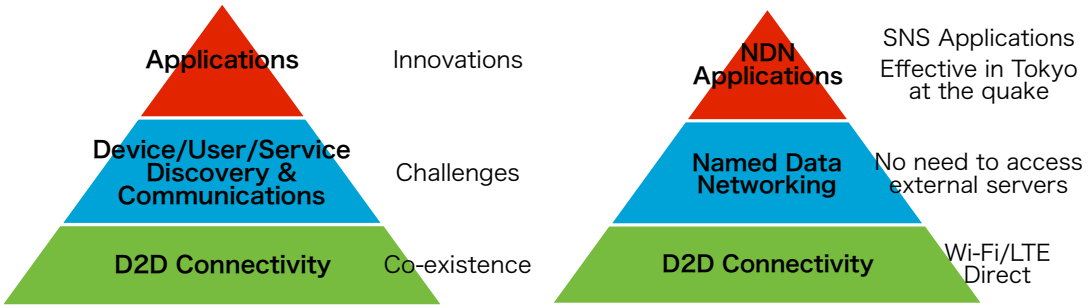
2.1.1　LTE Direct

LTE Direct では基地局とそれに接続するデバイスによってネットワークを構成する．デバイスの認証やリソースの管理は基地局で行われる．一方で，実際のデバイス間のデータ通信については，基地局を介した場合やデバイス間で直接行われる場合がある．図 2.1(a) の LTE Direct の接続イメージに対応するプロトコルスタックの概要を図 2.2(a) に示す [14]．デバイスやサービスの発見は Expression を周囲のノードへ広報することによって行われる．LTE Direct では，Time Division Duplex を利用し 20 秒毎に 64 ミリ秒の LTE Direct のための帯域を用意している．LTE Direct を利用してサービスを提供するノードは 128bit の Expression を周囲に広報し接続を待つ．

2.1.2　Wi-Fi Direct

図 2.1(b) は Wi-Fi Direct の接続イメージ図である．Wi-Fi Direct ではアクセスポイントは必要なく，デバイスが直接通信を行って接続を確立する．Wi-Fi Direct に対応したデバイスが存在すれば他の機器は必要ない．

Wi-Fi Direct では各デバイスは自身の情報を周知に放置する．接続を試みるデバイスは周知されている情報をスキャンし，自身の情報を送信することで接続要求する．



(a) Proximity Communication のプロトコルスタック [14]　(b) NDN を動作させた Proximity Communication のプロトコルスタック

図 2.2: Proximity Communication と NDN のプロトコルスタック

2.2　Named Data Networking (NDN)

NDN は，以下の特徴を持つネットワークアーキテクチャである [7]．(1) データに対し ID(Name) を割り当て，データ (コンテンツ) にはその Name によってアクセスする．(2) ルータにおける経路制御も Name によって行う．(3) ルータは受信データのキャッシュを持ち，キャッシュ上に所望のデータがあれば，それを返す．Name はデータを保管しているノードの位置に依らず不変であるため，NDN では，データにアクセスするためにノードを識別する必要がない．一方，現在のインターネットアクセスでは，URL からドメイン名を取得し，Domain Name System を利用して得た IP アドレスを用いてデータを収容したホストに HTTP/TCP/IP のプロトコル・スタックで接続しデータを入手する．そのため，Domain Name Server や Dynamic Host Configuration Protocol Server などによってネットワーク内のノードが集中的に管理されている必要がある．NDN に似たアーキテクチャである P2P ネットワークも，インターネット上のオーバーレイ・ネットワークであり，インターネットのＩＰアドレスの管理，名前解決に依存している．NDN はインターネットを前提とせず，インターネットを含む種々のネットワーク上にオーバーレイできることを目指したアーキテクチャであり，アドレスの管理や名前解決を行うサーバがない．このため，災害時に中央のサーバへのアクセスが期待できない状況での利用に適していると考えられる．NDN は現在のインターネットを刷新することを目指して，VoIP 等現在のインターネット上で動作するアプリケーションを NDN に移植する検討が進められている [15]．

具体的には，NDN におけるデータへのアクセスは以下の様な流れで行われる．データを要求するノードが，Name をその中に含む Interest Packet を送信すると，受信した各ノードはそれぞれが保持している Forwarding Information Base(FIB) を参照し，Name からパケットのフォワーディング先を判断し，データを持つノードまで InterestPacket をフォワーディングする．この時，Interest Packet をフォワーディングしたノードは，Interest Packet を受け取った通信インタフェース (Face) を Pending Interest Table(PIT) に記憶し，Name に対応するデータが Data Packet として返信されてくると，PIT を参照して転送する．その際，受信データをキャッシュする．PIT には Interest Packet のたどったルートが記憶され，一種のパケット単位の回線交換的制御を行っている．FIB が正しく設定されていれば，ネットワークを中央集中管理するサーバなしで，エンドノードと中継ノード (ルータ) による分散制御によって通信できる．FIB の更新に関しては BGP に似たプロトコル等，種々の方法が提案されている [16]．

NDN では，データは配信元のみからではなく，経路のルータのキャッシュからも取得される．そのため，Secure Socket Layer のようなホストを中心としたデータの信頼性の確保は困難である．そ

こで，NDN ではデータの送信元やデータに改竄がないことを認証する仕組みがそのパケット構造内に含まれ，Data Packet はそのデータと Name の領域に電子署名を付与することが必須になっている．署名を検証することによりデータの送信元とデータの信頼性を確認することができる．これによりデータをアプリケーションサーバに集め，データの送信元やその信頼性を確保する必要がなくなる．また，ユーザ間で直接データの授受を行った場合にもその信頼性を保証することができる．今回の想定環境であるグローバル・ネットワークから分断された局所的なネットワーク内でも，署名の検証ができれば，データの信頼性を保ちつつやり取りを行うことができる．この署名の検証は，NDN のノードとアプリケーション両方によって実行できる．これは，Content Chunks 層でノード間，あるいはノードとアプリケーション間の通信していることによる．

インターネットが NDN ベースの構成になり普段から NDN が利用されるようになれば，災害によってネットワークが分断された場合にもそれぞれの孤立したネットワークで継続してサービスを提供できる．ユーザは同一のインタフェースでアプリケーションを利用できるようになり，災害前後でのシームレスなサービス提供が可能となる．

2.3 ChronoSync

図 2.3 に示す ChronoSync ベースのアプリケーションを導入したノードは主に 2 つのモジュールから成る．データ同期を行う ChronoSync 本体と ChronoSync からのデータ変更を受けて動作するアプリケーションである．アプリケーションは ChronoSync からのデータ変更通知を受け取り，アプリケーションに必要な動作を実行する．ChronoSync では，アプリケーションにデータ更新通知を行うことのみを行い，アプリケーションがどのような動作をするかは関知しない．ChronoSync は，自ノードの持つデータをデータの Name からハッシュ関数により生成される Digest として管理する．その変遷は Digest Log として保存されている．この Digest を Name に含む sync interest と呼ばれるパケットを各ノードが送信することでノードの状況を広報する．Sync Interest を受け取ったノードは Digest Log から Digest の表すデータセットを取り出し，自身の持つデータと差分があればアプリケーションに知らせる．ChronoSync はネットワークの分断からの復帰にも対応しており，それには Recovery Interest と呼ばれるパケットが利用される．分断から復帰したノードは他のノードとは異なるログを記録しているため，Digest Log によって Digest を解決できない可能性がある．この場合に，Recovery Interest を送信する．Recovery Interest を受け取ったノードは差分ではなくすべてのデータの情報を返信する．このプロセスにより，切断から復帰したノードについてもデータセットの同期が可能である．ChronoSync をインストールしたノードが分断されたネットワーク間を移動することにより DTN を構成し，災害時にも広範囲で情報共有を行うことができる．しかしながら，ChronoSync ではノード間の Round Trip Time 程度の間隔で同期が行われるが，災害時には消費電力を抑えるために通常よりも長い同期間隔をとる必要がある．本論文でのシミュレーションでは，ユーザ間でのメッセージ同期はユーザがメッセージを生成した時とネットワークを移動した時のみに行われるものとした．

2.4 3GPP ネットワーク/ユーザ認証

現在の LTE ネットワークでは，無線区間においてキャリアとユーザが相互に認証し，鍵合意をするプロトコルとして，Authentication and Key Agreement(AKA) を使用している [17,18].

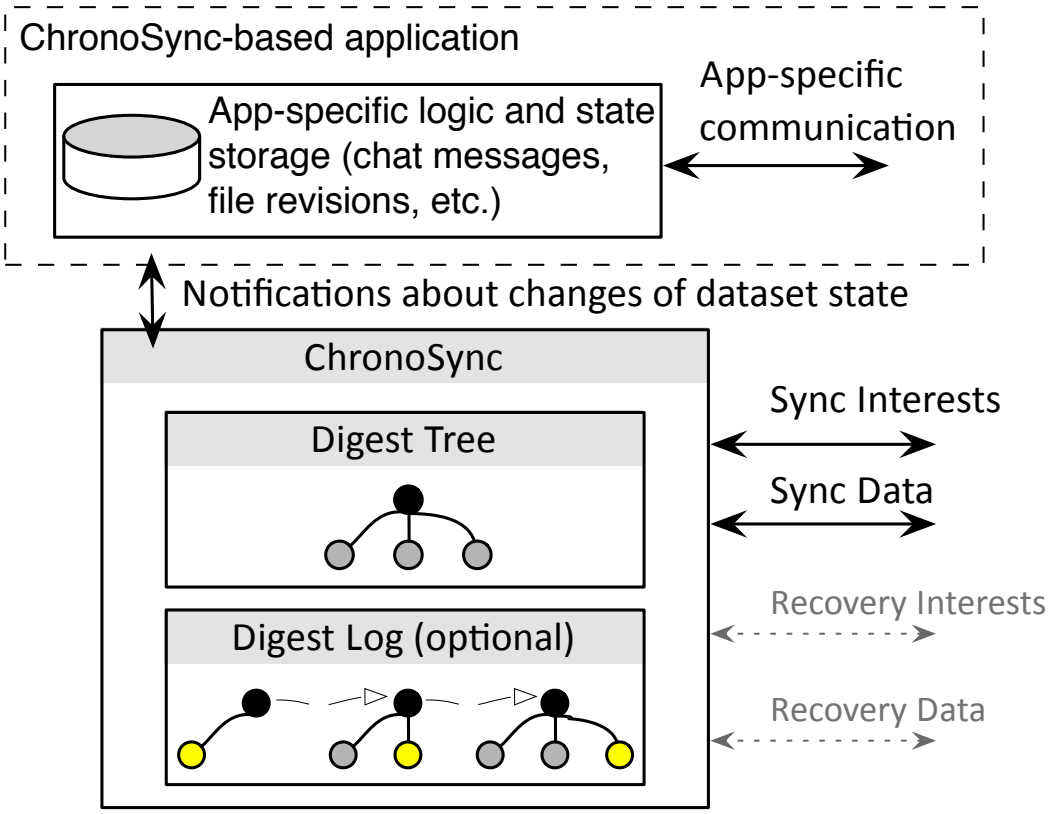


図 2.3: ChronoSync 概要図

AKA では図 2.4 に示す USIM カードに保存されている秘密情報を利用して認証を行う．USIM のアーキテクチャは物理層，トランスポート層，アプリケーション層の 3 層に分かれてそれぞれ規格化されている．アプリケーション層には PKI 機能も実装されており，秘密鍵を保存することができる [19]．PKI 機能専用のコマンドとして鍵生成，ユーザ証明書のダウンロード，署名生成を実行できる．署名生成の実行には PIN (Personal Identity Number) 2 コードが必要であり，第三者による不正使用を防いでいる．

AKA プロトコルは，図 2.5 に示すような流れで認証と鍵合意が行われる．図 2.5 において，K とは，ユーザ USIM (Universal Subscriber Identity Module) と HSS(Home Subscriber Server) のみが互いに知る非公開共通鍵で，それぞれの USIM の中に固有で製造時から内蔵されている 128bit の値である．

AKA は，以下のように実行される [3]．ユーザ端末 UE (User Equipment) が MME (Mobility Management Entity) に，HSS の公開鍵 PK_H で暗号化した $IMSI$ (International Mobile Subscriber Identity)(=A) と HSS の IDID_{HSS} を送信し認証を要求する．A を受け取った MME は PK_H で暗号化した SNID(Service Network Identity)(=B) を A とともに認証要求として HSS へ送る．MME から認証要求を受けた HSS は自身の秘密鍵 SK_H を用いて復号し，IMSI および SNID を得る，IMSI および SNID を登録者リストから照合し確認する．その後，HSS は乱数配列 RAND(1,⋯,n) と Authentication vector である AV(1,⋯,n) を下記に式によって生成する．|| を連結，$\oplus$ を排他的論理和，f_K は鍵 K による暗号化とする．$AV = SNID||XRES||K_{ASME}||RAND$,

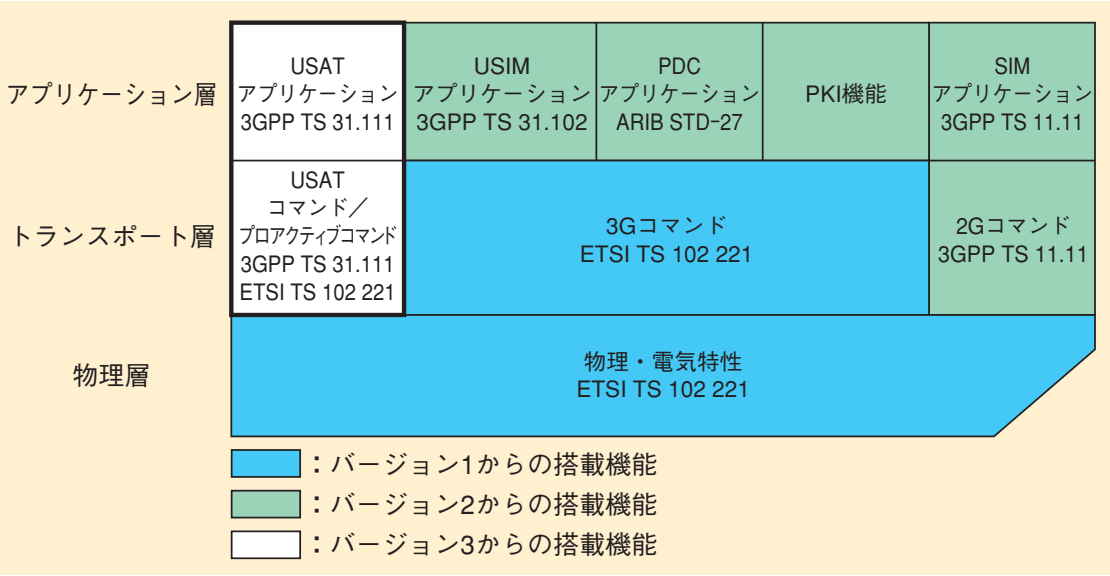


図 2.4: UIM バージョン 3 のアーキテクチャ[2]

$K_{ASME} = s10_K(f3_K(RAND), f4_K(RAND), SNID)$, $XRES = RAND \oplus SNID$ である．AV(1,⋯,n) と IMSI を MME の公開鍵 PK_M で暗号化したもの (=C) を MME へ送る．MME は C を復号して AV から要素を 1 つ選択し，その中の $RAND(i)$，$SNID$，$K_{ASME}(i)$ に対応する Key Set Identifier の KSI_{ASME} および IMSI から算出する $S-TMSI$(S Temporary Mobile Subscriber Identity) を UE の公開鍵 PK_U で暗号化したもの (=D) を UE へ送る．$S-TMSI$ は再アクセスの時に用いられる．すでに KSI_{ASME} と K_{ASME} の 1 対 1 の対応がとれているため，KSI_{ASME} から K_{ASME} を検証でき，初期処理なしでセキュア通信が可能である．UE は D を復号し，$S-TMSI$ を検証することで HSS を認証する．認証後，$RES(i) = RAND(i) \oplus SNID$ と K_{ASME} を算出し，$RES(i)$ を MME へ返信する．MME は $RES(i)$ と $XRES(i)$ を比較し UE を認証する．以降は K_{ASME} を MME と UE 間の暗号鍵となり，暗号鍵 $CK(i)$ とインテグリティ鍵 $IK(i)$ を生成しセキュア通信に用いる．また，UE は自身の秘密鍵 SK_U も同様に暗号鍵として利用できる．例えば，課金情報に署名を付加し，PK_H 暗号化して HSS へ送信することが可能である．

2.5　Hierarchical ID-based Encryption

ID ベース暗号とは，メールアドレス，名前などの文字情報 (ID) を公開鍵として用いる暗号技術であり，その代表的なものに Boneh, Franklin による Weil ペアリングを用いた Identity-based Encryption (IBE) がある [20]．公開鍵が識別子から生成されるため，公開鍵証明書を必要としない点が特徴である．秘密鍵は，秘密鍵生成局 Key Generation Center (KGC) が各 ID のユーザに対して計算し配布する．IBE では，すべてのユーザの秘密鍵は単独の KGC によって生成されるため，KGC への負荷が大きい．

Hierarchical ID-based Encryption (HIBE あるいは HIDE と略記される）は，ID ベース暗号の秘密鍵生成局 KGC を階層化させた方式であり，大元の KGC を Root KGC と呼ぶ [12]．すなわち，HIDE は，ユーザ ID を木構造の各ノードに対応させ，ユーザ ID に対応する秘密鍵はそのユーザ

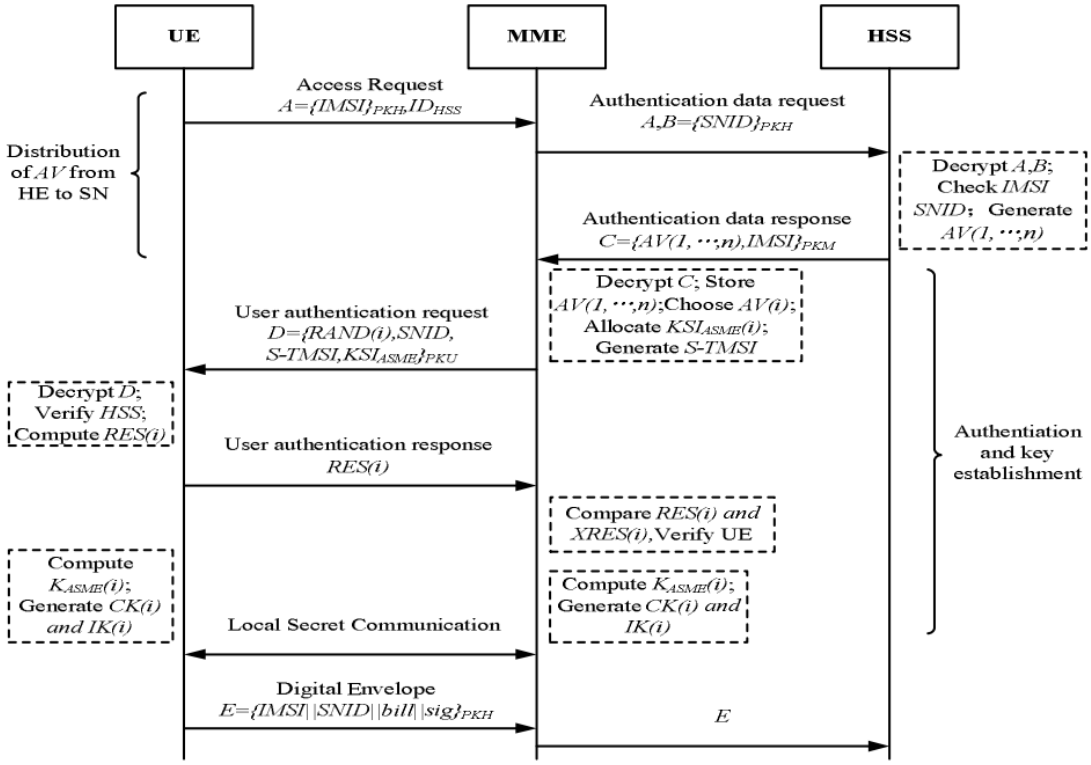


図 2.5: SE-EPS AKA の処理の流れ [3]

の親が生成する．

図 2.6 は本システムで用いる HIDE の階層構造である．Root KGC としてはネットワークインフラを提供するキャリアを想定している．キャリア (Root KGC) は，ユーザの ID に基いてユーザの秘密鍵を生成する．各ユーザはキャリアからシステムパラメータと自身の秘密鍵を受け取る．システムパラメータは同一のキャリアに所属しているユーザであれば共通であるため，ユーザは暗号化および復号を KGC へアクセスすることなく自律的に行うことができる．異なるキャリアに所属するユーザについても，そのキャリアのシステムパラメータを取得することで，データを暗号化してやり取りを行うことが可能である．

2.6　インターネットアプリケーションのアカウント作成手続き

インターネットでのアプリケーションにおいてアカウントを発行する際は，ユーザを一意に特定できるように，他のユーザと重複しない固有の文字列を ID として各ユーザに発行する必要がある．このため，例えば，現在の Twitter でのアカウント発行手続きでは，図 2.7 のように，ユーザが「Choose your username」の欄に任意の文字列を入力することで ID を決定する [21]．入力された文字列が既に発行されている ID と一致する場合は，図 2.6 に示すように，Suggestions に表示されるような他の文字列に変更するよう促される．図 2.6 のように，他のユーザの ID と重複しなければアカウントを発行できる仕組みになっている．

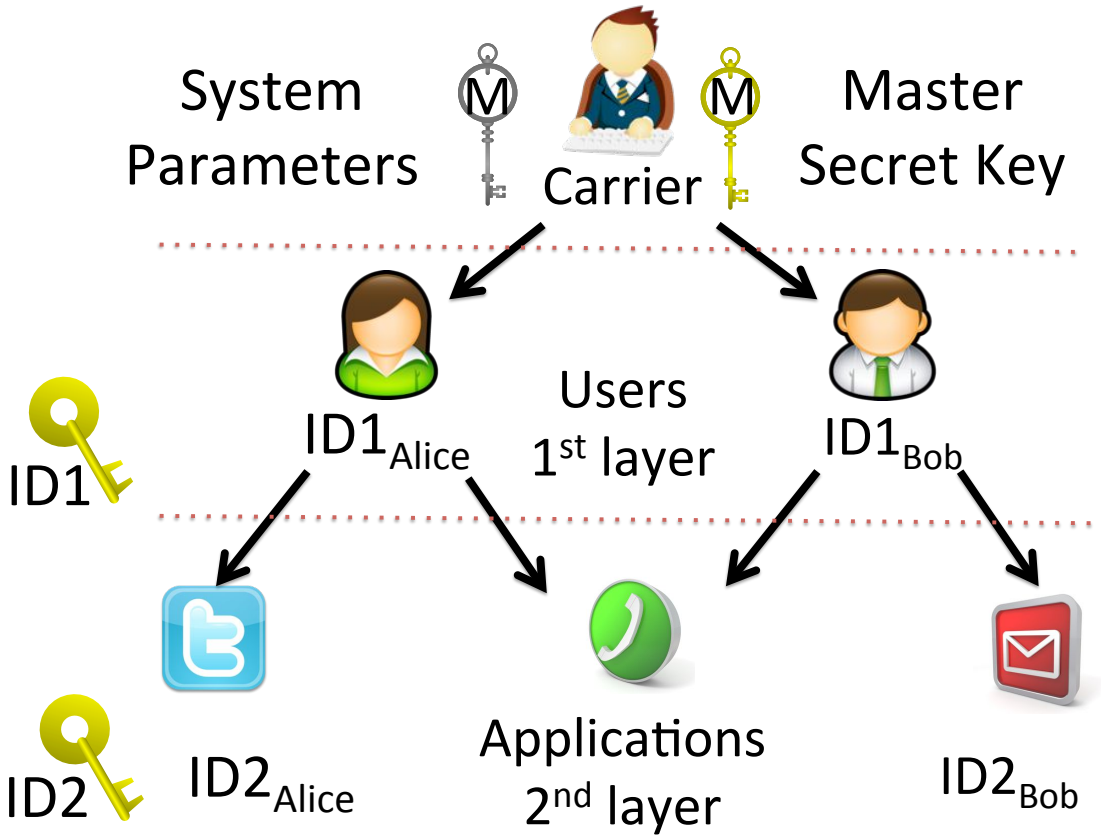


図 2.6: HIDE の階層構造

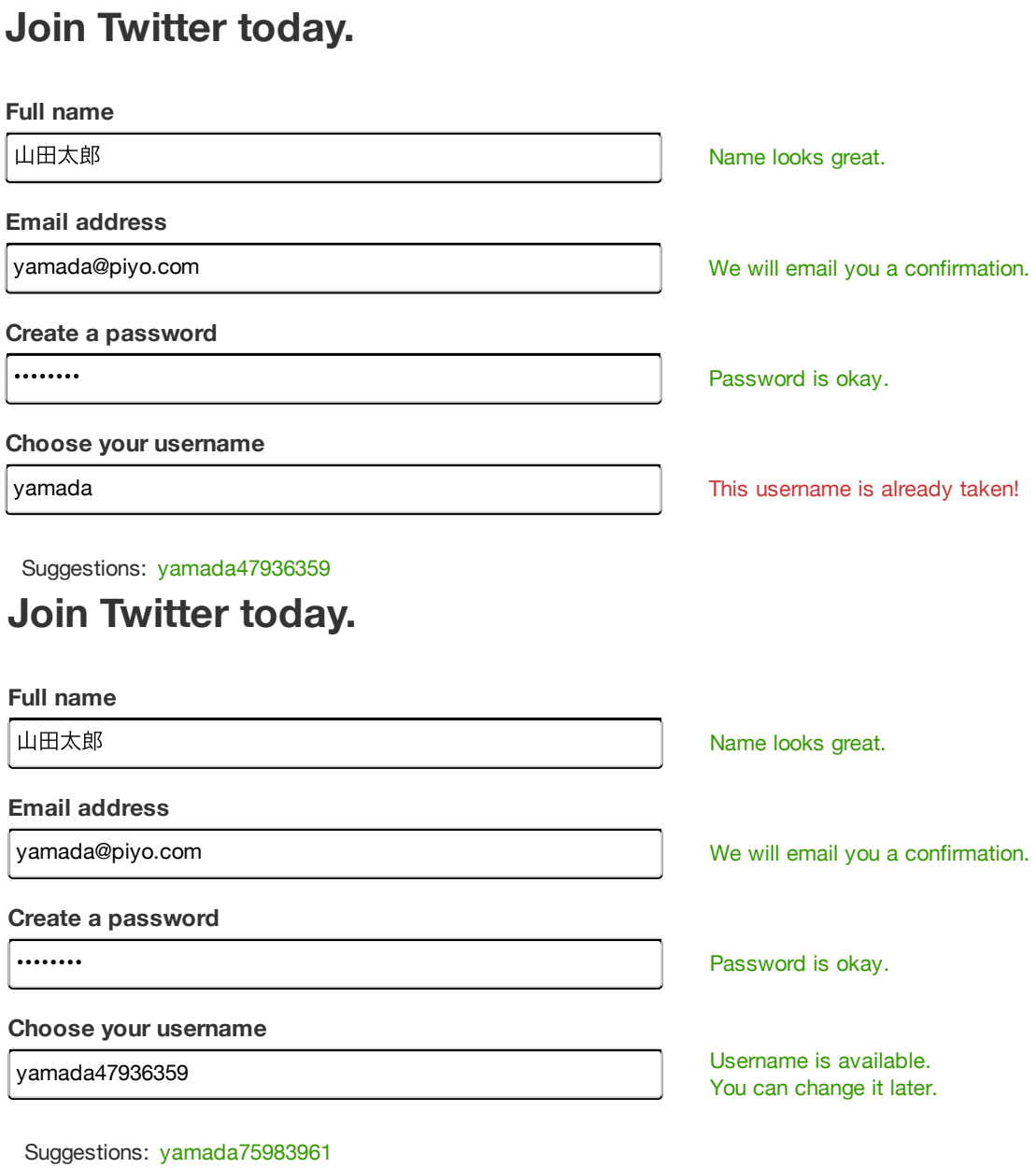


図 2.7: Twitter における ID 登録手続き

第3章

提案モデル

3.1　NDN ベース耐災害分散型携帯電話網

2.2 で述べたように，NDN は各ノードが分散的なルーティング機構を持つため，隣接するノード間が物理的に接続されていれば，ネットワークを構成することができる．災害時に NDN を利用するためには，バックホール障害が発生しても提供可能な物理的接続が必要となる．近接するデバイスを直接接続可能にする LTE Direct [4] や Wi-Fi Direct [6] などの Proximity Communication [14] がある．図 2.2(a) に示されるように，Proximity Communication は近接するデバイスを直接接続可能であるが，Point-to-Point の接続を確立するのみである．各ノードが自律的に動作し，災害時のようなインフラが破壊され利用できないような環境下でも利用可能である．Proximity Communication 上で NDN を動作させ，その上に ChronoSnyc による安否確認アプリケーションを動作させる図 2.2(b) に示すシステムを構築する [22]．NDN によって，分断ネットワーク，たとえば，基地局とそれに接続する端末からなるネットワーク内において，情報共有が可能となる．

しかしながら，その場合，情報共有が可能な範囲は同一の基地局に接続している端末間のみであり，その効果は限定的である．そこで，分断されたネットワークとその間を移動するユーザを活用して，Delay Torelant Network(DTN) を構成することで，より広範囲での情報共有が可能になる．DTN を構成するために NDN 上で動作する端末駆動型の同期システム ChronoSync の切断耐性を利用した [9]．平常時の利用における ChronoSync での同期頻度はノード間の Round Trip Time(RTT) 程度の間隔であることが想定され，災害時のような電源供給が満足に得られない状況では消費電力の観点から問題がある．以下では，ChronoSync のプロトコルを踏襲しつつ同期間隔を伸ばし，現状の携帯電話網における電子メールの転送遅延を満足する制約下で，どこまで消費電力を抑えられるか，シミュレーションにより示す．ここで転送遅延のレファランスに図 1.1 で示した携帯メールの災害時の性能を用いている．

3.2　Name トンネリングプロトコル

ChronoSync ではすべてのメッセージをすべてのユーザ間で共有するため無駄なトラヒックが大量に流れる．一方で，単純に NDN のルーティング機構を利用し FIB や PIT に従った通信を行った場合，NDN ではパケット単位での回線交換的制御により災害時の分断されたネットワーク間での通信に問題が生じる．まず，ネットワーク間をノードが移動するまでの時間は通常の回線速度より非常に遅く，各ノードの PIT エントリーがタイムアウトとなり経路が断絶する可能性が高い．また，リクエストである Interest Packet の通った経路しかコンテンツを運ぶ Data Packet は通ることができない制限もある．別のネットワークへ移動したノードが元のネットワークへ帰らない限り通信は完了しない．Name トンネリングではこの欠点を解決するために，Name 書き換えゲートウェイ機能を持つアプリケーションを各ネットワークに導入することで解決した．ゲートウェイは外部ネットワークへのパケットの送信を一旦各ネットワーク内のゲートウェイで終端させ，Name を書き換えた Interest/Data packet (Tunnel Object) に変換し移動ノードへ送り保存させる．移動ノードは他のネットワークへ移動した時，そのネットワークのゲートウェイが宛先である Tunnel Object を保存していれば転送する．これにより，各ネットワークのゲートウェイ間に通常の通信とは独立した仮想的な通信経路がゲートウェイ間に形成され，各ネットワークのユーザは切断を意識せず切断前と同様の通信を継続して利用できる．Tunnel Object はゲートウェイと移動ノード間で直接やり取りされるため，PIT によるタイムアウトの影響は受けない．また，Tunnel Object では Tunnel Interest と Tunnel Content Object はそれぞれ独立で送受され，さらに移動ノード間で

共有されるため，往復で移動するノードが異なっても通信は完了する．図 3.1 は Name トンネリングを導入した SNS のタイムラインサービスを提供するシステムの概要図である．

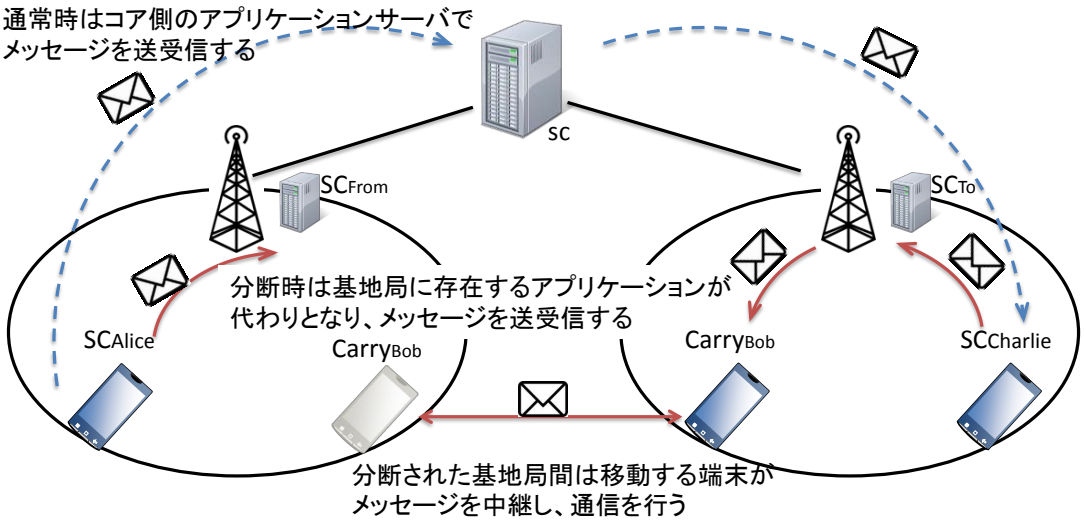


図 3.1: タイムラインサービスシステム概要図

通常時にはタイムラインサービスを提供するアプリケーションサーバ SC とユーザ端末間でメッセージの送受信を行う．災害時にネットワークが分断された場合は，各ネットワークの代表ノードがアプリケーションサーバの代替を担う．図 3.1 では携帯電話網を例に取っており，基地局がアプリケーションサーバ兼ゲートウェイとして動作する想定である．ユーザ端末におけるタイムラインサービスアプリケーション SC_{Alice}, $SC_{Charlie}$ と基地局におけるタイムラインサービスアプリケーション SC_{From}, SC_{To} 間の通信は各基地局ネットワーク内で一旦終端される．各基地局におけるアプリケーション SC_{From}, SC_{To} 間の通信は移動端末にインストールされるアプリケーション $Carry$ を介した Tunnel Object によって行われる．基地局における SC_{From}, SC_{To} とアプリケーション $Carry$ との通信は分断された各ネットワークで完了し，$Carry$ が保持することで他ネットワークへと運ばれる．メッセージの送信者と受信者が同じ基地局に所属している場合は，サーバへ接続している場合と同じプロセスでメッセージの送受信が完了する．タイムラインサービスアプリケーションによるメッセージの送受信は省略し，Tunnel Object を用いた分断された基地局ネットワーク間の通信フローについて述べる．

ネットワークが分断された場合，タイムラインサービスでのメッセージの保存先はユーザ端末がはじめに接続した基地局のアプリケーションである．別の基地局から移動したユーザがタイムラインサービスアプリケーションへメッセージの書き込みを行った場合，そのメッセージは初期基地局へ転送される必要がある．図 3.2 は Tunnel Content Object を用いたメッセージの基地局間転送フローである．ユーザ α は基地局 A から B へ移動し基地局 B からメッセージを送信したものとする．

(1) α のメッセージが基地局のアプリケーション内に Tunnel Content Object に変換され保存される．(2) 基地局は移動ノード δ へ基地局 A へ転送すべきメッセージを取得したことを Interest packet によって通知する．(3) 移動ノード δ はユーザ α のメッセージリストを取得する．新規メッセージがあればメッセージ本体を Tunnel Content Object として取得し，ストレージに保存する．(4) 移動ノード δ は基地局 A へ移動すると，自身の持つメッセージリストを基地局へ送信する．(5) 基地局は自身の管理するユーザのメッセージがあれば Tunnel Content Object として取得し

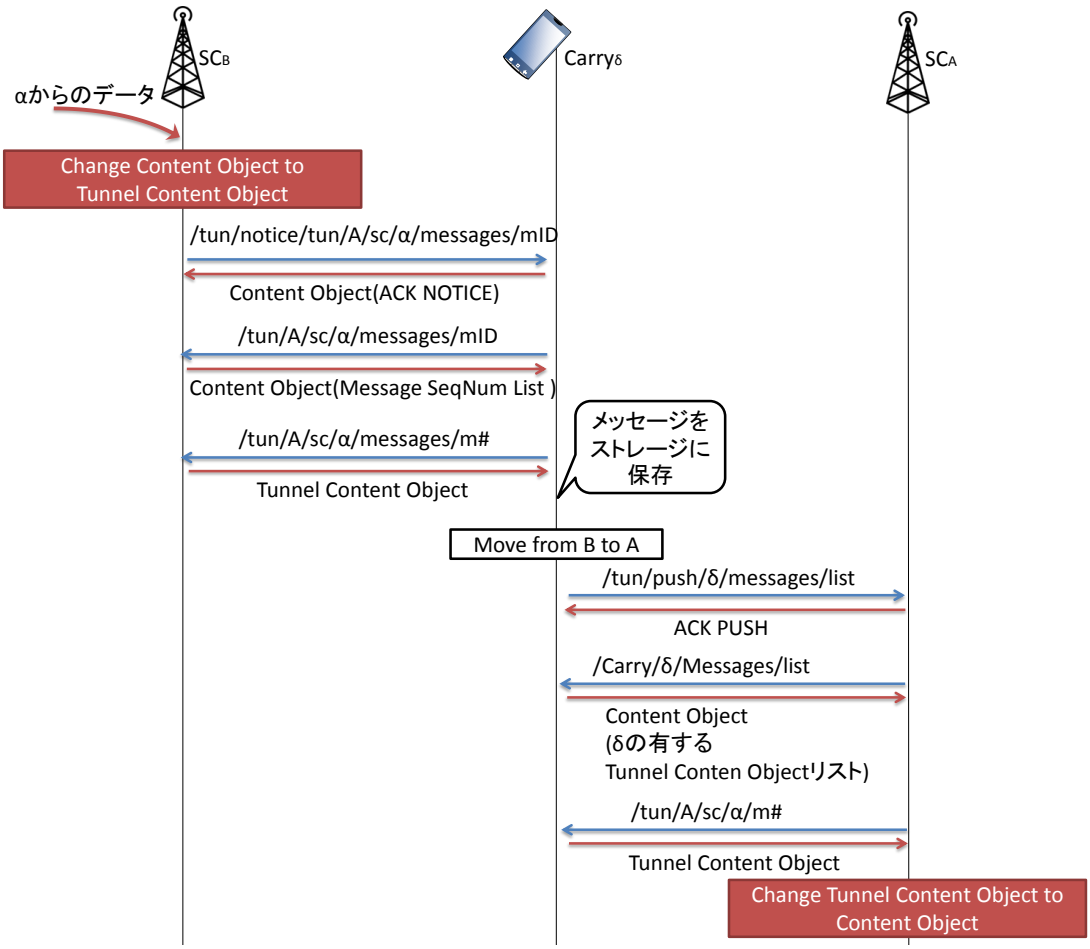


図 3.2: 基地局間でのメッセージ送信

Content Object へ変換しアプリ SC_A で利用する．管理下以外の Tunnel Content Object については，ルーティングテーブルを参照し基地局 B 経由でない配送先があれば取得し中継する．

次に，基地局間での Tunnel Interest の転送フローについて述べる．図 3.3 に異なる基地局に所属するユーザのメッセージのリクエストを送信しメッセージ取得するフローを示す．ここでは，基地局 A に所属するユーザ β が基地局 B に所属するユーザ α のメッセージを取得するものとする．基地局 A は移動ノードからの情報でユーザ α が基地局 B に所属するユーザであることがわかっているという前提である．

(1) 基地局 A のユーザ β がタイムラインサービスを利用して基地局 B に所属するユーザ α のメッセージの取得を試みる．この時，基地局 A にはユーザ α のメッセージはない．ユーザ β からの Interest packet は Tunnel Interest へと変換される．(2) 基地局から移動ユーザ γ へ基地局 B のユーザ α のメッセージの取得を Tunnel Interest により依頼する．(3) 移動ユーザ γ は基地局 A から B へ移動すると Tunnel Interst を送信し，基地局 B からのメッセージの要求を伝える．(4) 基地局 A は図 3.2 と同じ処理を基地局 A 内の移動ユーザに対して実行することで要求されたメッセージを Tunnel Content Object として基地局 B へメッセージを送信する．

上記の処理により，基地局間で Tunnel Interest を介してメッセージのリクエストが転送され，対応する Tunnel Content Object が返送される．先に述べたように，Tunnel Interest を運ぶ移動ユー

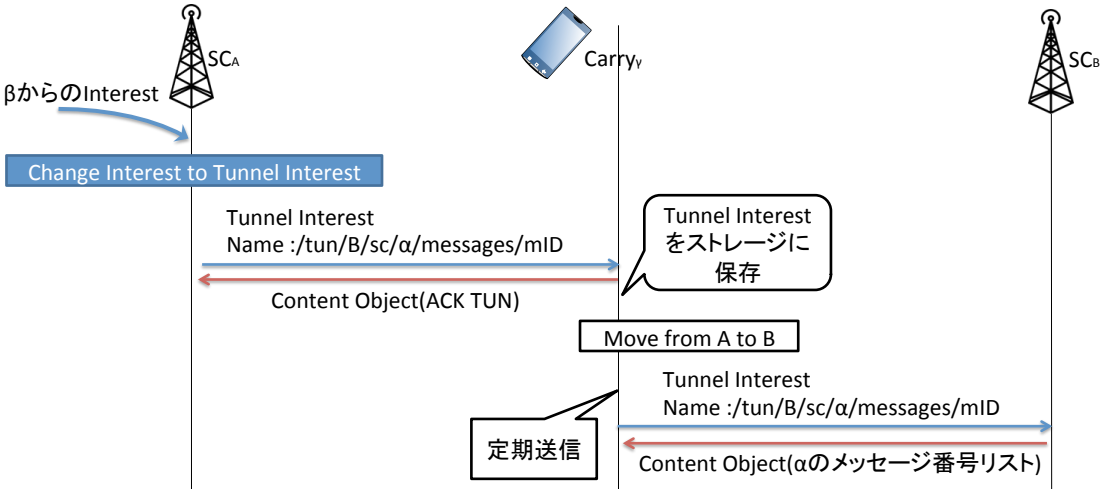


図 3.3: 基地局間でのメッセージリクエスト

ザと Tunnel Content Object を運ぶユーザは必ずしも一致する必要はない．これにより，NDN のルーティング機構で単純にタイムアウトまでの時間を伸ばした場合と比べて短い時間でメッセージの共有が可能となる．

3.3　階層型 IBE による端末認証とアプリケーション層におけるユーザ認証

本節では，本システムで利用する 2 階層の HIDE を利用した認証プロトコルについて述べる．

ネットワーク/端末認証

2.4 節で述べたように，現在の 3G/LTE におけるネットワーク/端末認証は AKA プロトコルが利用される．本システムでも認証には AKA を模したプロトコルを利用することを考え，図 3.4 にそのプロトコルを示す．AKA に由来するパラメータについては太字で表示している．前提条件として，Alice は Root KGC であるキャリアから自身の第 1 層の秘密鍵および公開鍵に用いられる System Parameters を取得している．(1) まず，Alice は基地局へ認証を要求する Interest Packet を送信する．AKA ではリクエストとして Alice の $IMSI$ を送信する．しかしながら，本システムでは認証に用いる ID は公開鍵として利用されるため，非公開情報の $IMSI$ は利用できない．$IMSI$ の代替として他の ID，携帯電話キャリアであれば電話番号を用いる．AKA では，ユーザと HLR/AuC 間で Sequence Number(SQN) の同期をとり，過去の認証手続きとの区別に SQN 用いている．基地局は HLR/AuC と異なり台数が多く，全体で同期をとることは不可能である．このため，Alice が保存している過去の SQN の最大値 SQN_{MS} を Alice が，目指す基地局のみが取得できるように暗号化して送信して共有する．(2) 基地局は AKA と同様に Authentication Reply を準備するが，基地局は計算に必要な Alice との共有秘密鍵 K を持たない．ここでは，LTE において AKA 実行後に基地局へ渡される K_{eNB} を代替として用いて算出する．次回以降の認証プロセスを簡略化するために SE-EPS AKA と同様に KSI_{ASME} と $S-TMSI$ を送る．(3) 基地局は $RAND$ と $AUTN$ を Alice の ID である $ID1_{Alice}$ で暗号化して返信する．ここで同時に Authentication Reply の計

算に利用した K_{eNB} を送信し共有する．(4)Alice は $XMAC$ を算出して MAC を検証し，SQN が SQN_{MS} より大きいことを確認する．このとき，返信された Data Packet には基地局による署名がなされているため，Alice は署名を検証することによっても，基地局およびネットワークを認証することができる．(5) 基地局は Alice を認証する要求を送る．この要求が一連の手続きの一部であることを示すために Name の末尾に $ID1_{Alice}$ で暗号化した SQN を付加する．(6)Alice は (3) で受け取った情報からレスポンス RES を計算する．(7) 基地局の ID で RES を暗号化して返信する．(8) 基地局は RES を検証することで Alice を認証する．同様に，基地局は，返信された Data Packet の署名を検証することで Alice を認証することができる．ユーザと基地局の相互認証が完了すると，基地局はユーザからおよびユーザへのパケットを転送することを許可する．

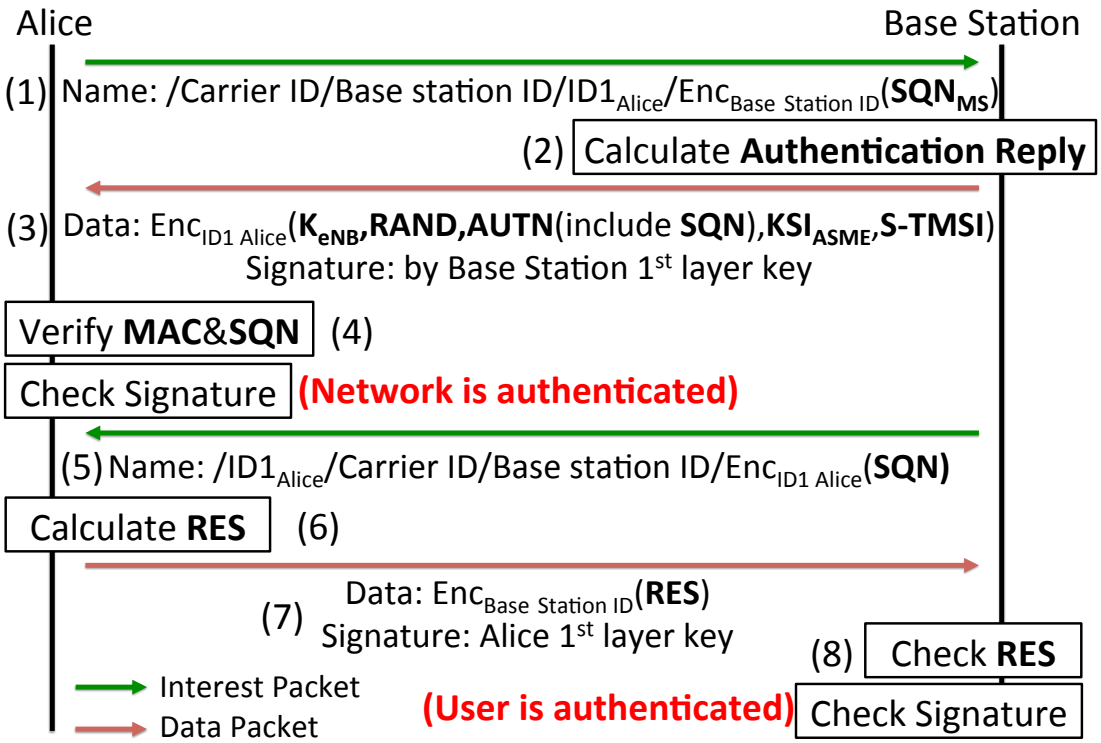


図 3.4: ユーザと基地局間の認証プロトコル

SE-EPS AKA での認証では，共通秘密情報 K を利用してキャリアにより認証されたユーザであることを証明し，同時にユーザの公開鍵の認証を行う．一方，本システムでは，ユーザの HIDE 鍵自体がキャリアから認可されていることを証明する．そのため，図 3.4 に示した認証プロトコルは，K を認証するための Challenge and Response に関連する計算を省略し，HIDE 鍵の認証のみに簡略化することができる．図 3.5 に簡略化した相互認証のプロトコルを示す．手続きを一連のものとしてまとめて他の認証手続きと区別するための SQN を残し，認証は Data Packet の署名によって行う．基地局とユーザ間で SQN を含む Interest Packet と Data Packet を送受信するだけで認証が完了する．

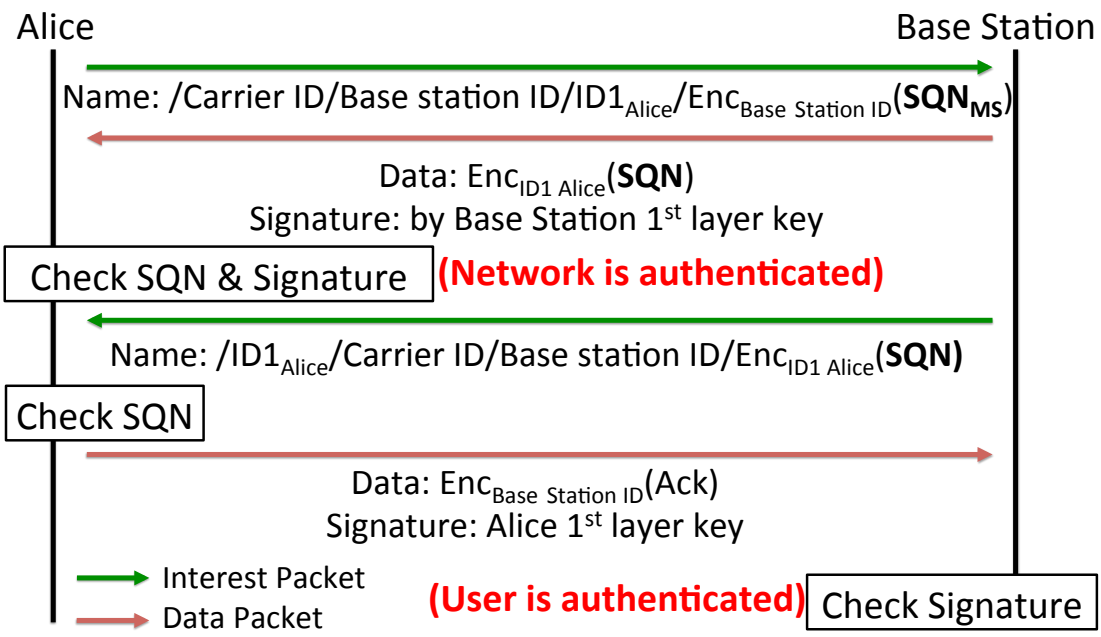


図 3.5: 簡略化したユーザと基地局間の認証プロトコル

3.4　アプリケーション層におけるユーザ認証

ユーザは，第 2 層のアプリケーション層における KGC を担う．各ユーザは，目的やアプリケーション毎に ID を設定し，キャリアから受け取った秘密鍵を用いて新たに秘密鍵を生成することができる．現在の Facebook や Twitter といったアプリケーションを利用するとき，ユーザにはアプリケーション毎に ID が割り当てられる．本システムにおいて，この ID を利用して第 2 層の HIDE の秘密鍵を生成する．さらに，アプリケーションにおいてユーザを認証するためのパスワード認証は，秘密鍵を使った署名によって置き換える．HIDE による認証は現在のシステムの自然な拡張となる．

現在のアカウント登録の実装に沿ったシステムにするために，2.6 節で述べた流れに沿ったアプリケーションにおけるユーザ登録の処理の流れを図 3.6 に示す．$Enc_{ID}(arguments)$ は HIDE を使って ID によって暗号化された $arguments$ を示す．

Alice と Application Server が異なるキャリア/プロバイダに所属する場合，HIDE を利用するためには互いの System Parameters を正確にそれぞれが取得する必要がある．そのための一案は，キャリアや ISP の上位に Root KGC を置いた 3 層の階層構造を導入することである．

(0)Alice と Application Server の所属する Root KGC が異なる場合，System Parameters を取得する．(1)Alice は $ID2_{Alice}$ としてユーザ登録を要求する．アプリケーションサーバは既存ユーザの ID と重複確認を行い，$ID2_{Alice}$ がすでに使われていれば NACK と代替 ID 案を返信する．さらに，以降の Interest/Data Packet を一連の手続きとして扱うためにシーケンス番号 Seq を Alice の 2 層目の HIDE 秘密鍵で暗号化して付加する．Application Server は 2 層目の HIDE 秘密鍵を利用した署名によって自身を証明する．(2)Alice は，代替 ID 案から選択した新しい $ID2_{Alice}$ として再度登録を要求する．この時，前回登録を要求した Alice であることを示すために Application Server から受け取った Seq を Application Server の ID で暗号化して Name の末尾に付加する．Application Server は Seq の値によって前回の Alice と同一のユーザであることを認証した後，ID の重複がな

ければ，ACK を返す．(1) と同様に 2 層目の HIDE 秘密鍵による署名によって正しい Application Server であることを証明する．(3)Application Server は新しい $ID2_{Alice}$ の登録要求を行ったユーザが Alice であるか確認する．確認を要求する Interest Packet には，一連の手続きを行っている Application Server と同一のものであることを証明するために Alice の 2 層目の HIDE 秘密鍵で暗号化した Seq を Name に付加する．Alice は Seq の値によって Application Server を認証した後，2 層目の HIDE 秘密鍵によって署名をした Data Packet を返信し，Application Server は Data Packet の署名を検証して Alice を認証する．以上でユーザ ID の登録および Alice と Application Server の相互認証が完了する．(4)Alice は Interest Packet を送信し，$ID2_{Alice}$ のコンテンツを要求する．Application Server は $ID2_{Alice}$ で暗号化したコンテンツを 2 層目の HIDE 秘密鍵で署名して返信する．復号可能なユーザは Alice のみであり，アクセスを Alice のみに制限可能である．Alice は署名を検証することで Application Server から送られたコンテンツであることを確かめる．

上記の認証は信頼できる Alice と Application Server が信頼できる Root KGC から認証されて秘密鍵を受け取っていることに依存している．そのため，前述した System Parameters の交換は非常に重要である．

Alice が図 3.6 の (2) で ACK を受信した後は，Application Server は Alice からの PULL リクエストに返信するのみではなく，Alice への PUSH 通知も可能となる．

第 1 層の ID はキャリアによって管理されているため，各ユーザに対して固有の ID である．第 2 層の ID についても，上記のプロトコルを利用することで各アプリケーション内では固有の ID であることが保証される．一方で，異なるアプリケーションにおける同一ユーザの ID については重複の可能性がある．この場合，アプリケーションが提供する ID(Account) をそのまま鍵生成の ID として用いた場合，異なるアプリケーションで同一の秘密鍵が生成されユーザによって利用されることになる．他のアプリケーションでの鍵の漏洩がその他のアプリケーションにも影響をあたえるという問題が生じる．そこで，本システムでは，第 2 層の鍵生成には，アプリケーションの ID をプレフィックスとして Account に付加して ID2 とし対応する秘密鍵を生成する．これにより，異なるアプリケーションで Account が同一であった場合にも，異なる秘密鍵を生成し利用できる．

3.5　認証システムの設計

3.5.1　HIDE 秘密鍵の保存

HIDE を利用するには PKI 同様に，秘密鍵を安全に管理し利用するシステムが重要である．スマートフォンでの利用を想定した本システムでは，USIM に保存することが望ましい．USIM 上に保存することで耐タンパ性を確保することができる．USIM において PKI 機能を利用するには PIN2 コードの入力が必要となる．HIDE についても同様に，PIN2 コードによって保護することで情報の漏洩を防ぐ．アプリケーション毎に新たに秘密鍵を生成した場合，PIN2 コードで暗号化し，PKI の秘密鍵を保存する領域に HIDE の秘密鍵を保存する．

3.5.2　USIM 上の HIDE 秘密鍵を利用するためのコマンド

USIM カードへ保存した鍵を利用するためのコマンドについて述べる．HIDE を利用する際，ユーザが実行するコマンドは下記の 5 つが考えられる．

Extract 特定の ID に対するユーザ秘密鍵の生成

Encrypt ユーザ ID による message の暗号

Decrypt ユーザ秘密鍵による ciphertext の復号

Sign ユーザ秘密鍵による message からの署名生成

Verify ユーザ ID による signature と message の照合による署名の検証

Root KGC 以外の KGC が Root KGC から System Parameters を取得する Lower-level setup も存在するが，これは 2 層目の KGC であるユーザが秘密鍵を取得した時に同時に取得していると考えられるため省略する．USIM における PKI 機能と同様に IC チップ上で演算が行われることを考えると，USIM カードへ送る引数としては下記が必要である．ここで IDs とは，1 層目の場合は {System Parameters, ID1} の配列，2 層目の場合は {System Parameters, ID1, ID2} の配列とする．

1. Extract (IDs, PIN2)
2. Encrypt(IDs, message)
3. Decrypt(IDs, ciphertext, PIN2)
4. Sign(IDs, message, PIN2)
5. Verify(IDs, signature, message)

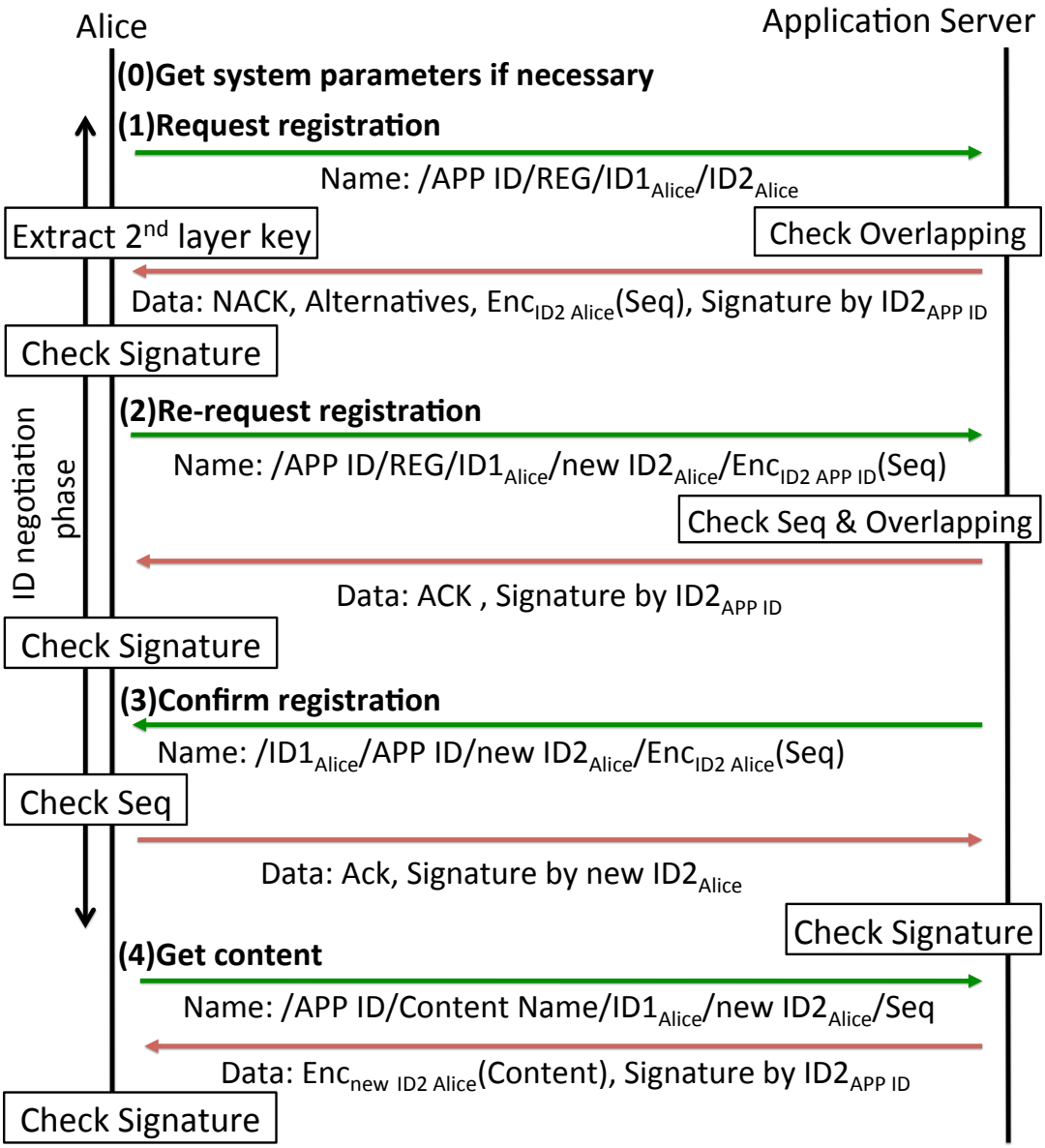


図 3.6: アプリケーションにおけるユーザ認証および ID 合意プロトコル

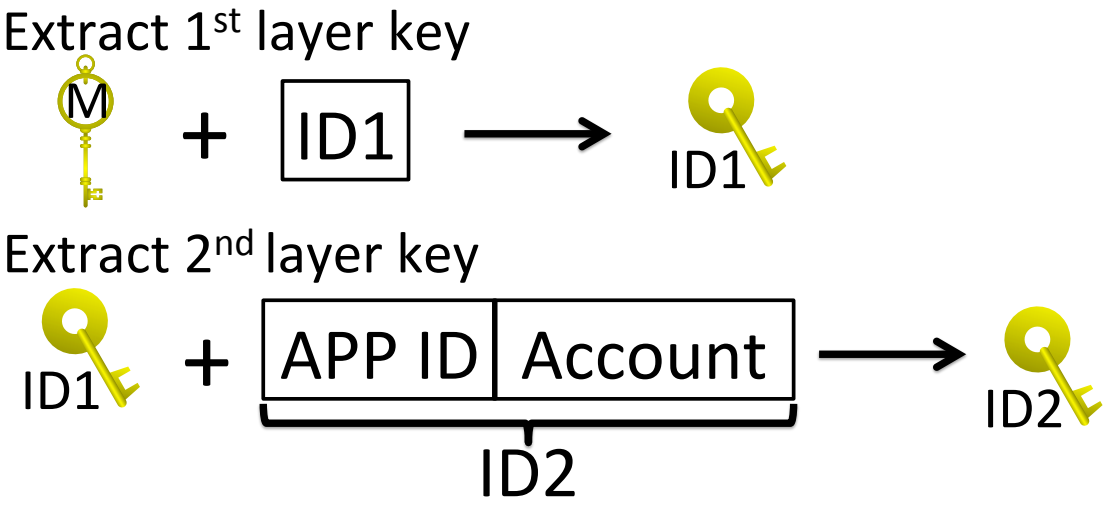

Extract 1st layer key
M
+
ID1
ID1
Extract 2nd layer key
ID1
+
APP ID
Account
ID2
ID2

図 3.7: 鍵生成

第4章

性能評価

4.1　ChronoSync による情報伝達性能および端末消費電力の評価

4.1.1　シミュレーション環境

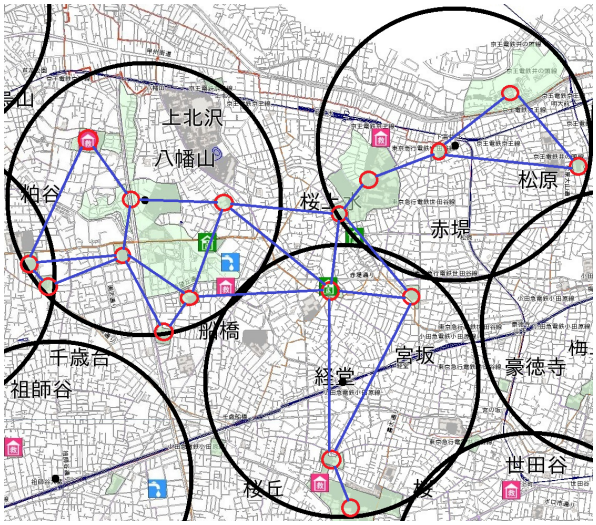
提案システムの情報伝達性能について下記の環境下でのシミュレーションにより評価を行った．シミュレーションソフトウェアは ns-3 上に実装された NDN のシミュレーションモジュールである ndnSIM を利用した [23]．ns-3 は ns-3.16 を利用し，ndnSIM は 2013 年 1 月 7 日時点で最新のものを用いた．実行環境は，CPU: Intel Xeon CPU E5540 @ 2.53GHz で，メモリ容量は 23.6GB のマシンである．

4.1.2　シミュレーションモデル

各データの Name は次のように定義した．

- sync Interest: /SNS/sync/RootDigest
- recovery sync Interest: /SNS/recov/UnknownDigest
- message: /SNS/UserID/SeqNo

シミュレーションモデルとして，図 4.1 に示すような東京都世田谷区の経堂・桜上水周辺の避難所配置を利用した．想定環境としては，各基地局はコアネットワークから完全に切断され，アプリケーションサーバやコアネットワーク内の各種サーバが利用できず，基地局同士は通信できない孤立した状態で動作しているものとしている．また，一部のユーザが避難所間および基地局間を移動し，直接的なアクセスパスが残されていないネットワーク間での情報伝達を担うものとした．



Affected Area	Setagaya Kyodo/ Sakurajosui
Shelters	17
UEs	100/shelter
Move Ratio	10, 20, 30, 50, 100%
Distance	1~2km
Move Interval	20~120min
Move	Walk(4km/h)
Message transfer interval	17 min[2,3]
Sync Interval	1~30min
Base station	radius 1km

図 4.1: 避難所および基地局の配置とシミュレーションパラメータ

黒い円は 1 つの基地局のセルを表し，それぞれのセル半径は 1km を想定した．赤い円は各避難所の位置を表し，避難している各ユーザはスマートフォンなどのモバイル端末を携帯しているものとした．初期状態では，各避難所にはそれぞれ 100 人のモバイル端末ユーザが存在する．それぞ

れのユーザは平均 t_m(Move Interval) のポアソン分布に従う間隔で避難所間を移動する．移動先は図 4.1 において青い線で接続された避難所の中からランダムに選択される．経堂・桜上水周辺の道幅は狭く，ユーザの移動手段は徒歩が想定される．そのため，ユーザは避難所間を Google マップの推奨ルートを時速 4km で移動するものとした．同一の基地局内に所属している各ユーザは，その基地局を介して通信することができる．本論文で挙げた ChronoSync ベースアプリケーションは t_s の平均送信間隔で Sync Interest を送る．2012 年の情報通信白書によると，年間の電話総呼数は 608.7 億回であり，契約者数は 11953.5 万人であったことから，通常時の 1 契約者あたりの平均呼間隔は約 17 時間である [11]．NTT docomo のデータによれば，東日本大震災後のトラヒック量は通常時の約 60 倍であった．これらのデータからユーザによるメッセージの平均送信間隔は 17 分とした [1].

4.1.3　シミュレーション結果

ユーザの移動度や移動するユーザの割合，同期間隔を変化させた時のメッセージ伝達時間について調査した．シミュレーションは各パラメータ設定に対して 1 回ずつ行った．メッセージ伝達時間は下記のように定義した．メッセージ伝達率 r をメッセージ msg を受信したノードの数 n_{msg} を全ノード数 N で割った値とする．

$$r = \frac{1}{M}\sum_{msg=1}^{M}\frac{n_{msg}}{N}$$

メッセージ伝達時間 T は r が 95%に達するまでの時間として定義した．また，95%以上のメッセージ伝達率であったメッセージについてメッセージ伝達時間を平均したものを平均伝達時間 ADT として定義した．

Content Store の最大エントリー数を 50 とし，t_s と t_m を変化させたときの平均伝達時間について調べた．パラメータ t_s および t_m は，$t_s = 1, 5, 10, 20, 30$ 分と $t_m = 1, 10, 30, 60, 120$ 分の値で変化させた．以降の図では，赤い水平線で平均伝送時間 80 分を示し，携帯電話のメール伝達時間との比較に使っている．

まず，ユーザ全員が移動する場合 (Move Ratio 100%)，図 4.2 のように平均伝達時間 $T_{100\%}$ はほぼ t_s に比例して増加している．一方，図 4.3 に示すように，平均伝達時間 $T_{100\%}$ は t_m に対して指数関数的に増加している．しかし，赤の水平線で示した携帯電話メールの転送遅延 80 分より，いずれの場合も小さく，移動間隔 120 分，同期間隔 30 分の最悪の場合でも 70 分以内の ADT に収まっていることがわかる．

図 4.3 は $y = a\mathrm{e}^{bx}$ の形で近似できる．図 4.4 は t_s と係数 a および b の近似値の関係を表す．a は t_s に対して線形な変化を示している．一方で b は t_s の値に依らずほぼ一定である．t_s による a の近似式は $a = 39.89t_s + 352.3$ であり，b の平均値は 0.0059 である．以上から，すべてのユーザが移動した時の平均伝達時間 $T_{100\%}$ は，t_s と t_m の関数として得られ，その近似式は下記である．

$$T_{100\%} = (39.89t_s + 352.3)\mathrm{e}^{0.0059t_m}$$

一方で，実際の災害時には，避難所間や基地局間を移動するのは一部のユーザであり，多くのユーザは 1 つの避難所に留まることが想定される．そのため，以下では移動するユーザの割合を変化させながら平均伝達時間の変化を調べる．図 4.5 は移動するユーザの割合と平均伝達時間の関係を示す．各グラフはそれぞれ 10% (図 4.5(a)), 20% (図 4.5(b)), 30% (図 4.5(c)), 50% (図 4.5(d)) のユーザが移動した時の平均伝達時間である．すべてのユーザが移動する場合と同様に，到着時間

は移動間隔に対して指数関数的に増加する傾向を示している．赤の水平線に示した携帯電話メールの転送遅延 80 分より平均伝達時間が小さくなるように推定 t_m に合わせて t_s を選べばよい．例えば，10%のユーザしか移動しない場合でも，同期間隔を 1 分にすれば，携帯電話メールの転送遅延 80 分より良い性能になることがわかる．

すべてのユーザが移動する場合と同様に近似式の推定を行った．以下がその近似式である．10%, 20%, 30%, 50%のユーザが移動するとき，平均伝達時間は $T_{10\%} = (332.02t_s + 76.23)\mathrm{e}^{0.0126t_m}$, $T_{20\%} = (130.69t_s + 322.65)\mathrm{e}^{0.0135t_m}$, $T_{30\%} = (76.471t_s + 401.49)\mathrm{e}^{0.0125t_m}$, $T_{50\%} = (50.721t_s + 416.95)\mathrm{e}^{0.00823t_m}$ である．

移動ユーザの割合を x%として，メッセージの平均伝達時間 $T_{x\%}$ は以下の式で近似できる．

$$T_{x\%} = (\alpha(x)t_s + \beta(x))\mathrm{e}^{\gamma(x)t_m}$$

図 4.6 は α, β, γ と移動するユーザの割合の関係を示すグラフである．α, β は 10%から 20%で大きく変化し，それ以上では大きな変化は見られない．移動するユーザの割合が大きくなると，t_s が平均伝達時間に与える影響が小さくなることがわかる．一方，γ は 30%から 50%の間で大きく変化している．50%を超えるユーザが移動したとしても，50%のユーザが移動する場合と，平均伝達時間は大きく異なることはないことを示している．

図 4.7 に移動時に端末の電源を切った場合の平均伝達時間に与える影響を示す．各グラフの黒い点線は，常時電源オンである場合を 1 とした時の移動時に電源を切ることによる平均端末駆動時間の増加量である．その他の点は常時電源オンの場合の伝達時間を 1 とした時の，移動時に電源を切った場合の平均伝達時間の伸びを示す．平均伝達時間の伸びを表す式は下記である．常時電源オンの場合の平均伝達時間を T_{on}，移動時に電源を切る場合の平均伝達時間を T_{off} として，

$$\text{平均伝達時間の伸び} = \frac{T_{off} - T_{on}}{T_{on}}$$

である．平均端末稼働時間の伸びは移動間隔 $t_m = 20$ のとき 37.4%，$t_m = 40$ のとき 25.2%，$t_m = 60$ のとき 19.0%，$t_m = 100$ のとき 12.2% であり，バッテリーのみの電力で 1 日稼働する端末であれば，3 時間から 9 時間程度の稼働時間の延長が可能となる．一方で平均伝達時間は，同期間隔の短い領域においては数倍にもなっている．平均伝達時間の伸びは大きく，所望の伝達時間が得られるような電源管理の手法に調整する必要がある．

4.1.4　端末消費電力の推定

今回のシミュレーションでは，同期間隔 1 分の場合，東日本大震災時の携帯電話メールの平均伝達時間より短い時間で安否確認ができる．そのため，このときの端末の消費電力についてトラヒック量の概算から以下に見積る．ユーザによるメッセージ生成間隔は平常時の電話の 60 倍として 17 分とした．このような場合はショートメッセージが多いと考え，各メッセージサイズは災害伝言板に残せるメッセージの最大サイズである 200Byte で十分とした．Sync Interest や Recovery Interest によって返される各メッセージの情報はユーザ ID と Sequence Number であるため 12Byte とした．また，各パケットのヘッダーサイズは ndnSIM の実装内容から 50Byte とした．この仮定のもとに 1 ユーザが送受信する 1 時間あたりのトラヒック量を計算する．1 メッセージあたりのトラヒックはメッセージ本体 200Byte とメッセージ交換のための Interest および Data packet のヘッダー 50×2Byte, Sync/Recovery Interest によるメッセージ情報の交換 12Byte が生じることから 200+50×2+12Byte となる．Sync Interest と Recovery Interest 各 1 メッセージによるトラヒックは，ヘッダーサイズか

ら 50×4Byte である．メッセージは 17 分毎，Sync Interest は 1 分毎であるから，1 時間あたりのトラヒック量は，$60/17 \times (200 + 50 \times 2 + 12) + 60/1 \times (50 \times 4)$Byte である．これが 1 ユーザによる 1 時間あたりのトラヒック量である．避難所は，小学校や中学校が想定されるが，世田谷区における小学校の平均児童数は約 500 人 である．また，世田谷区における各世帯の平均人数は 1.9 人であることから，各避難所におけるユーザ数はおよそ 1,000 人 と推定される．今回のシミュレーションでは 17ヶ所の避難所を考えているため，総ユーザ数は 17,000 人である．よって 1 ユーザが送受信する 1 時間あたりのトラヒック量は $\{60/17 \times (200 + 50 \times 2 + 12) + 60/1 \times (50 \times 4)\} \times 17,000 \approx 206$MB である．平常時の実際のスマートフォン 1 台のトラヒック量は 6.4 時間の計測で 42MB であることが報告されている [24]．今回のシミュレーションによる 6.4 時間のトラヒック量は約 1.32GB でありおよそ 30 倍のトラヒック量になる．概算ではあるが，平常時 1 日動作するような端末であっても，この実装では災害時には 1 時間も動作しない計算になる．災害時に利用するアプリケーションとしては，より消費電力の少ないプロトコルおよび運用手法が必要である．

4.2　Name トンネリングによる消費電力および情報伝達性能評価

本節では，ChronoSync と Name トンネリングのそれぞれの性能を消費電力と情報伝達性能の観点からシミュレーションにより比較し評価を行う．シミュレータは ns-3 上に実装された NDN のシミュレーションモジュール ndnSIM を利用した．ns-3 はバージョン 3.18 であり，ndnSIM は 0.2.8 である．

4.2.1　シミュレーション構成

シミュレーションモデルとして，図 4.8 に示した世田谷区経堂・桜上水周辺の実際の避難所配置を用いた．各赤い円がそれぞれ避難所の位置を表す．青い線で結ばれた避難所をユーザが徒歩で移動するものとした．黒い円は基地局を介して直接通信可能な範囲である．すべての通信は基地局を介した LTE Direct によるものであり，Wi-Fi Direct による通信は行わないものとした．各ノードの PIT のエントリー数は無制限とし，Content Store の最大エントリー数は 100 とした．

表 4.1: シミュレーションパラメータ

想定被災地域	世田谷区経堂・桜上水
避難所数	13ヶ所
端末数	避難所当たり 100 台
メッセージ生成間隔	平均 17 分 [1,11]
メッセージサイズ	200Byte
移動手段	徒歩 (時速 4km)
移動するユーザの割合	10%
移動間隔	平均 1, 2, 3 時間
移動距離	1〜2km
基地局による通信可能範囲	半径 1km
タイムラインサービスの更新間隔	1 回/分
タイムラインサービスの起動間隔	平均 30 分 ON/1 時間 OFF

シミュレーションに用いたパラメータを表 4.1 に示す．各避難所に避難しているユーザ数は 1ヶ所の避難所当たり 100 人である．各ユーザの平均メッセージ生成間隔は平常時のユーザの呼の間隔の 60 倍である 17 分のポアソン生起とした [1, 11]．移動するユーザは全体の 10%であり，青い線で結ばれた避難所のうちからランダムに選択し移動する．移動間隔は平均 1〜3 時間のポアソン生起であり，Google Map による推奨ルートを時速 4km の徒歩で移動するものとした．タイムラインサービスは Twitter の API 1.1 と同様に 15 分間当たり 15 回のアクセス制限があるものとし，タイムラインの更新は 1 分間に 1 回であるとした [21]．ユーザによるタイムラインサービスの起動および終了の間隔は平均 30 分のオンラインと平均 1 時間のオフラインをポアソン生起で繰り返すものとした [25].

SNS でのユーザのグループ分けを考えた場合に，大規模災害時を想定すると基本的に家族間での連絡が主になることから，メッセージ送信先ノードは世田谷区国勢調査から世田谷区の世帯構成を参照し，本シミュレーションの 1300 ノードをそれと同一割合になるようにグループ分けした．その際，世帯構成において世帯構成人数が 1 人である端末は世帯構成人数が 2 人以上である端末へと均等に割り振ることで，全ての端末が 2 つ以上の端末からなるグループに割り振られるようにした．各ノードは新規メッセージ要求を自身が属するグループの他の全ての端末宛に送信することとした．

Name トンネリングのシミュレーションでは，各ユーザが移動するかどうかは事前にわかっているものとして，移動するユーザにのみアプリケーション *Carry* をインストールした．ChronoSync のシミュレーションでは移動するユーザと避難所に留まるユーザは区別せず，すべてのユーザに対して ChronoSync ベースの SNS アプリがインストールされているものとした．ただし，ChronoSync は常時オンラインであり，同期間隔も ChronoSync で制御されるため，Name トンネリングによるタイムラインサービスのようなオンラインとオフラインの切り替えは導入していない．

4.2.2　シミュレーション結果

シミュレーション結果は以下の通りである．Name トンネリングは各移動間隔に対して 12 回ずつ ChronoSync については各移動間隔に対して 10 回ずつ行いそれらの平均をとった．

図 4.9 にメッセージ生成からの経過時間とメッセージの伝達率の関係を示す．ここで，メッセージ伝達率を以下のように定義する．ChronoSync でのメッセージ伝達率はこの間の全送信メッセージに対して “メッセージを受信したノード/全ノード数” の平均で算出した．一方，Name トンネリングでのメッセージ伝達率は各送信メッセージが家族構成員数だけマルチキャストされていることを考慮して，この間の全送信メッセージに対して “メッセージを受信したノード/家族構成員数” を平均して算出した．

Name トンネリングにおいて，図 4.9(a)，4.9(b) に示す平均移動間隔 2 時間まででは送信相手数によって性能の変化はほとんど見られない．今回のシミュレーションは 2 基地局間のみの通信である．したがって，同一基地局内に全ての端末が集中する確率とそうでない場合の確率を比較した場合，送信先数が多くなるほど前者の確率が小さくなり，平均伝送時間の増加につながる．この効果は平均移動時間が 3 時間になった図 4.9(c) に至って現れている．

メッセージ伝達率 0.6 で ChronoSync と Name トンネリングを比較すると，ChronoSync に比べて Name トンネリングが 1700 秒から 3000 秒程度遅いことがわかる．この差は，Name トンネリングではユーザは 30 分のオンライン時間と 1 時間のオフライン時間を繰り返すが，ChronoSync では常時オンラインとしたことによると考えられる．メッセージが到着した瞬間にオフラインになったとすれば 1 時間 (3600 秒) の遅延が生じることになるが，これはグラフから読み取れる遅延と同

程度のオーダーであり伝達性能の差の原因として十分に考えられる．Name トンネリングを利用したタイムラインサービスアプリが常時オンラインであったとすると，ChronoSync とほぼ同程度の伝達性能と考えられる．

図 4.10 および図 4.11 に ChronoSync と Name トンネリングそれぞれによる 12 時間のアプリケーションのトラヒック量を示す．ここで，Carry(MOVE), Carry(STAY), SC(MOVE), SC(STAY) はそれぞれ移動端末の Carry，非移動端末の Carry，移動端末の SC，非移動端末の SC が送受信したトラヒック量である．図 4.10 が示すように，Carry, SC アプリのトラヒック量は ChronoSync よりも大幅に少なく，ChronoSync の 8%から 14%程度にまで削減できている．アプリケーション SC によるトラヒック量は非常に少ないが，これは ChronoSync と Name トンネリングの差ではなく Name トンネリングのシミュレーションが移動ユーザが既知であると仮定したところが大きい．ChronoSync でも移動ユーザのみ ChronoSync を導入し非移動ユーザは SC のみをインストールするようにすれば同等の結果を示すと考えられる．トラヒック量の内訳を Interest/Data packet の送受信量別に分けて見ると，受信 Data packet の量は Name トンネリングが 10 分の 1 以下のトラヒック量であるのに対し，送信した Interest packet の量は Name トンネリングが ChronoSync の 10 倍程度になっている．これは，Name トンネリングでは Interest packet による push 通知などで Interest packet の数が多くなっている一方で，返信される Data packet は ACK のみであるなど容量が小さいことが影響している．ただし，受信 Data pakcet のサイズが Interest packet と比べて非常に大きく支配的であるため，総トラヒック量では Name トンネリングのほうが小さくなっている．

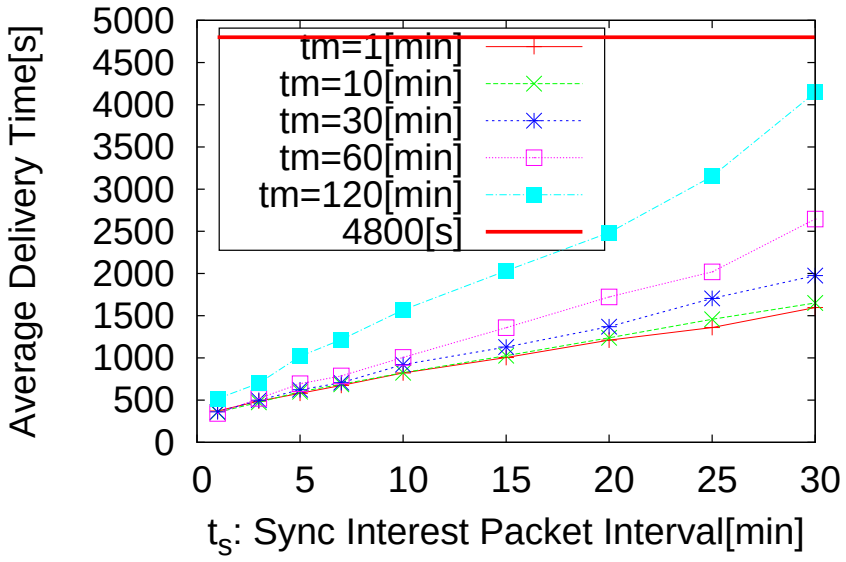


図 4.2: t_s と平均伝達時間の変化 (全員が移動)

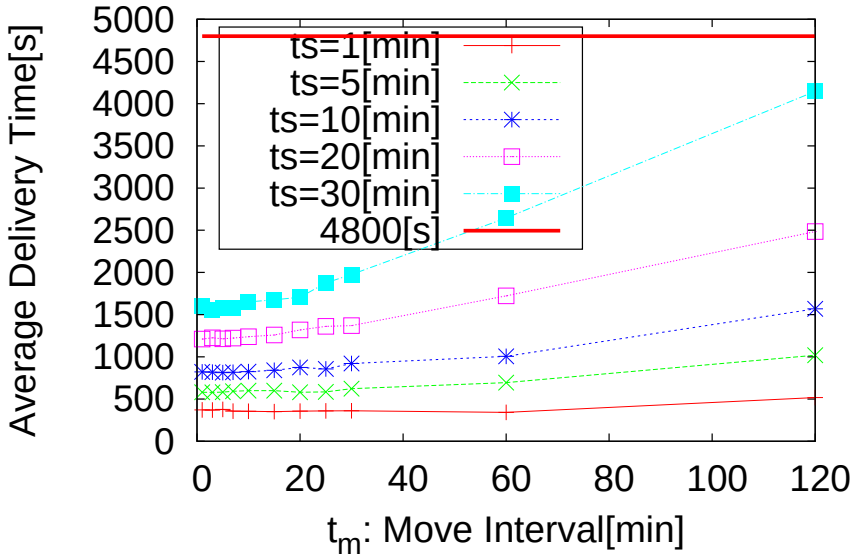


図 4.3: t_m と平均伝達時間の変化 (全員が移動)

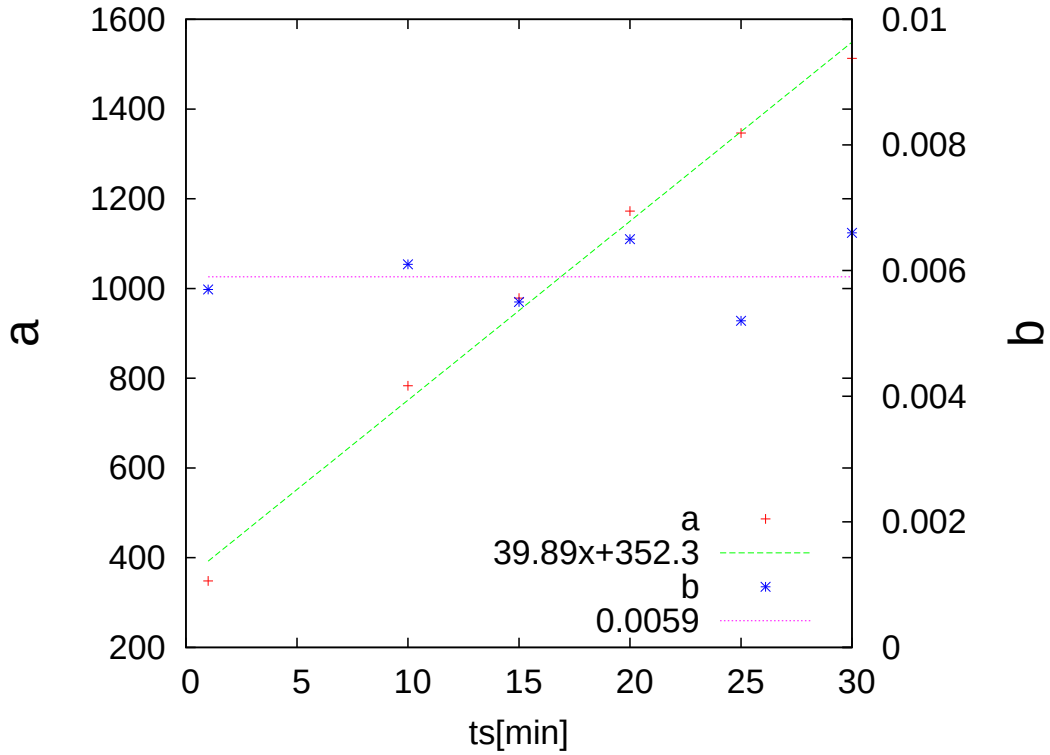
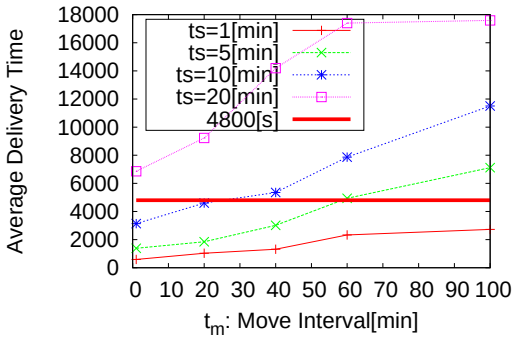
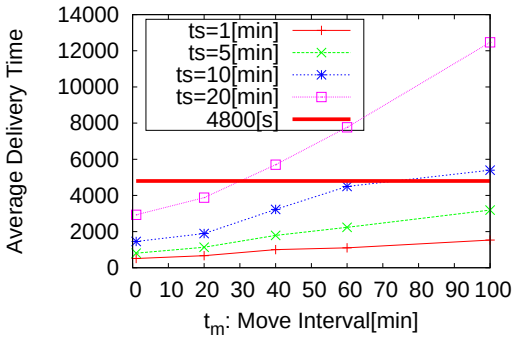


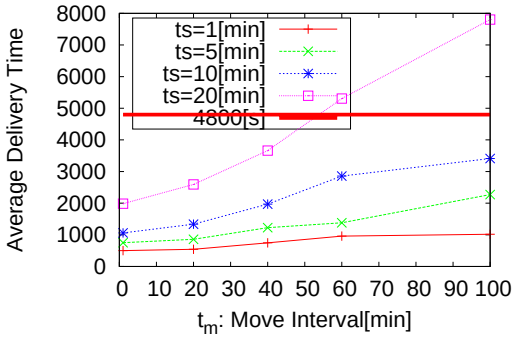
図 4.4: 係数 a および b の近似値



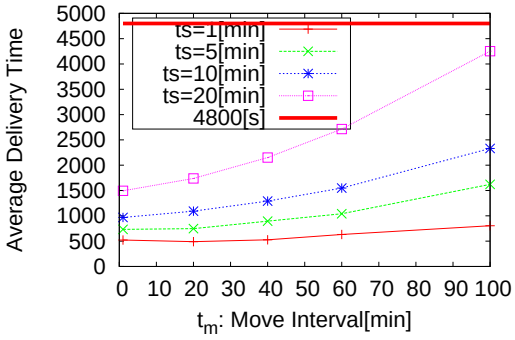
(a) 10%



(b) 20%



(c) 30%



(d) 50%

図 4.5: 移動するユーザの割合による平均伝達時間の変化

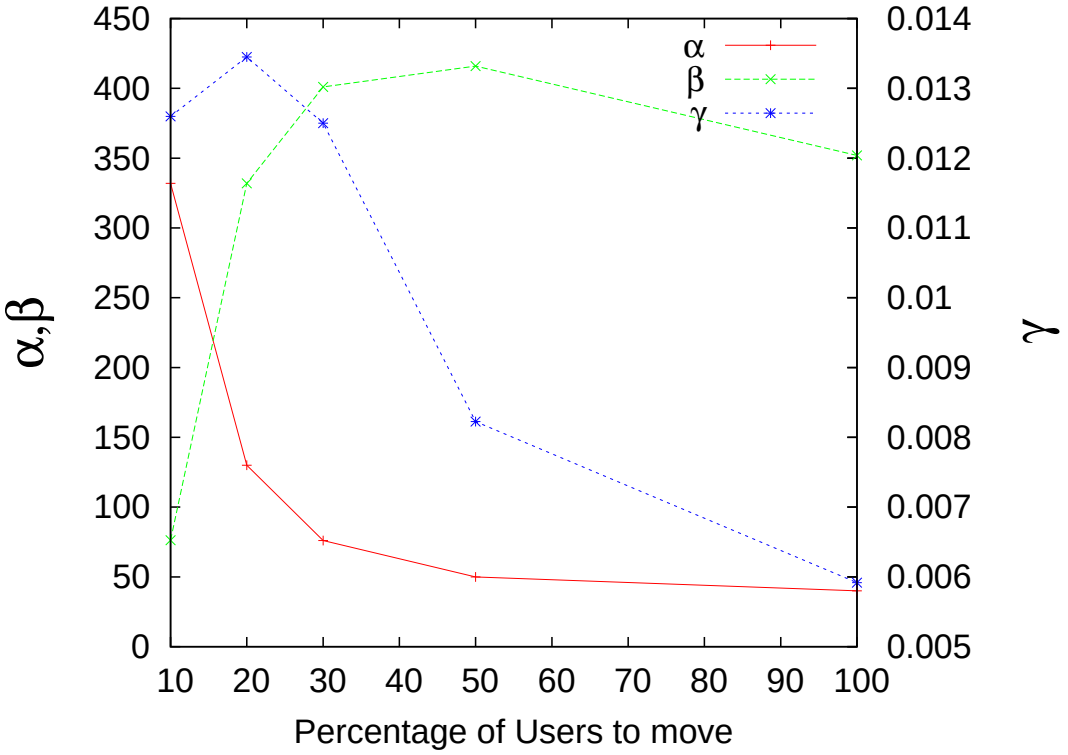
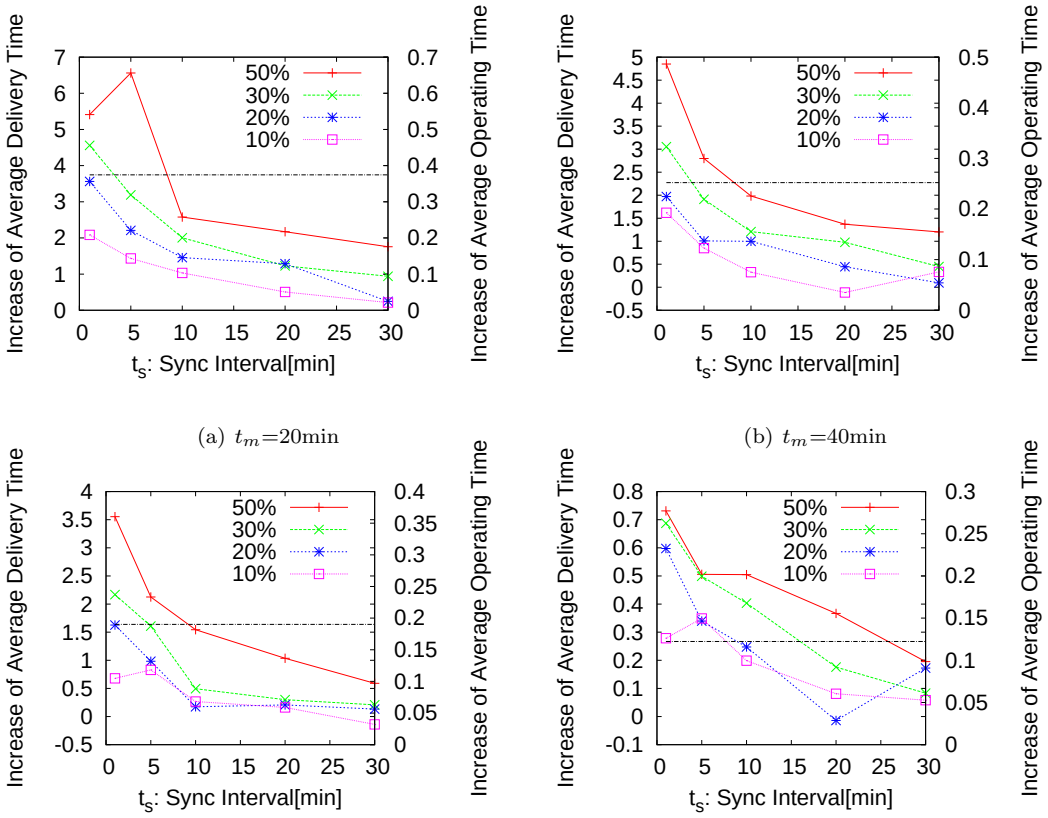


図 4.6: α, β, γ の近似値



(a) t_m=20min

(b) t_m=40min

(c) t_m=60min

(d) t_m=100min

図 4.7: t_m と移動時オフラインの影響

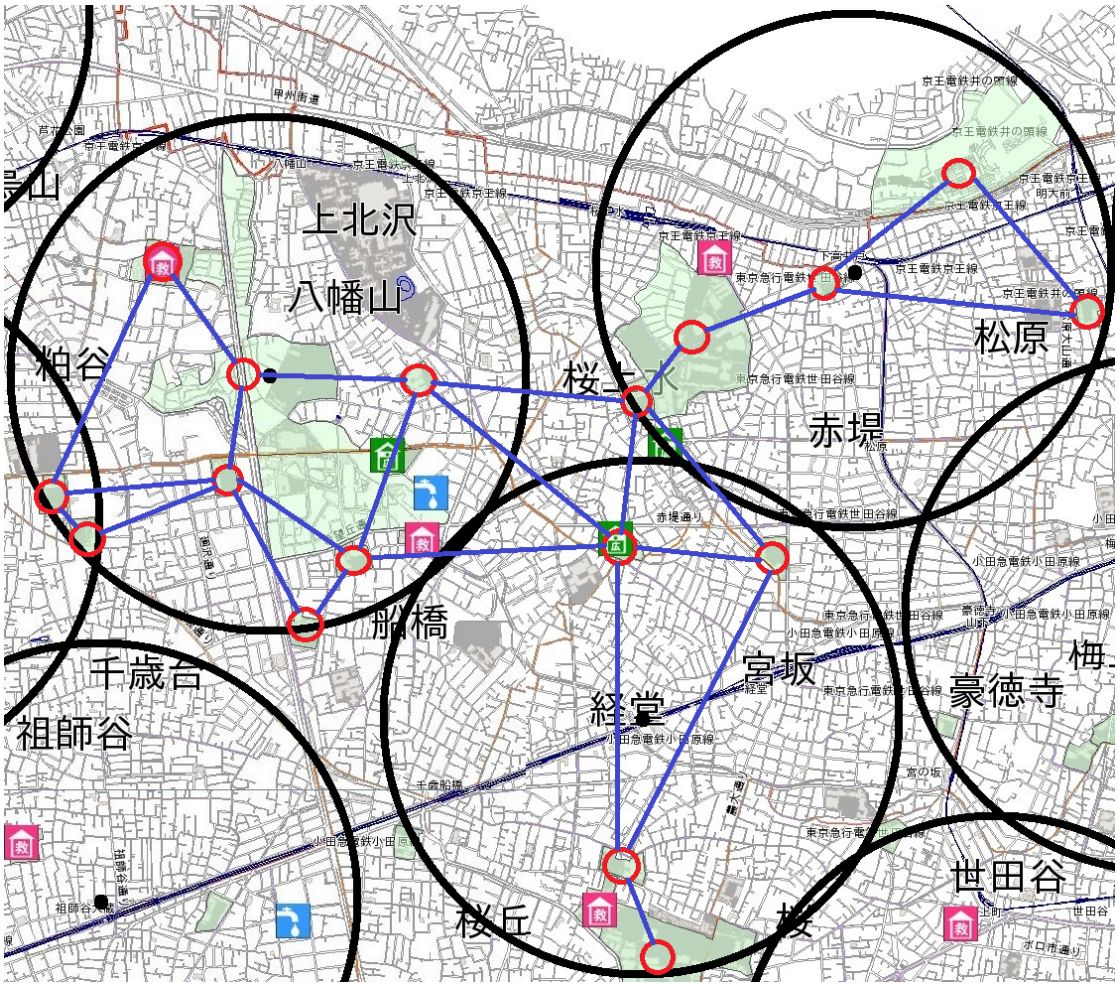
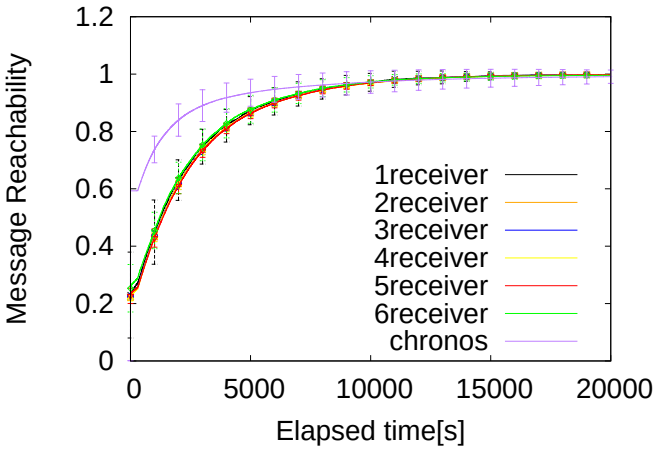
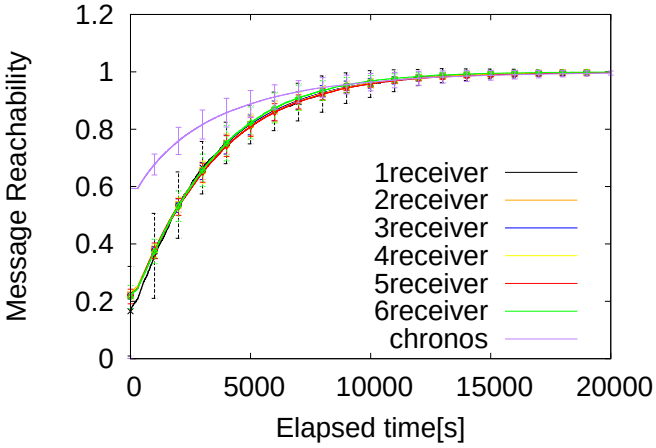


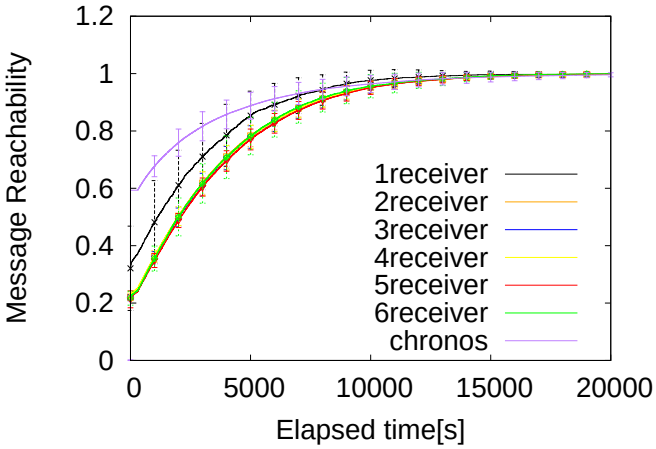
図 4.8: 経堂・桜上水周辺における避難所配置



(a) 平均移動間隔 1 時間



(b) 平均移動間隔 2 時間



(c) 平均移動間隔 3 時間

図 4.9: 経過時間とメッセージ伝達率の関係

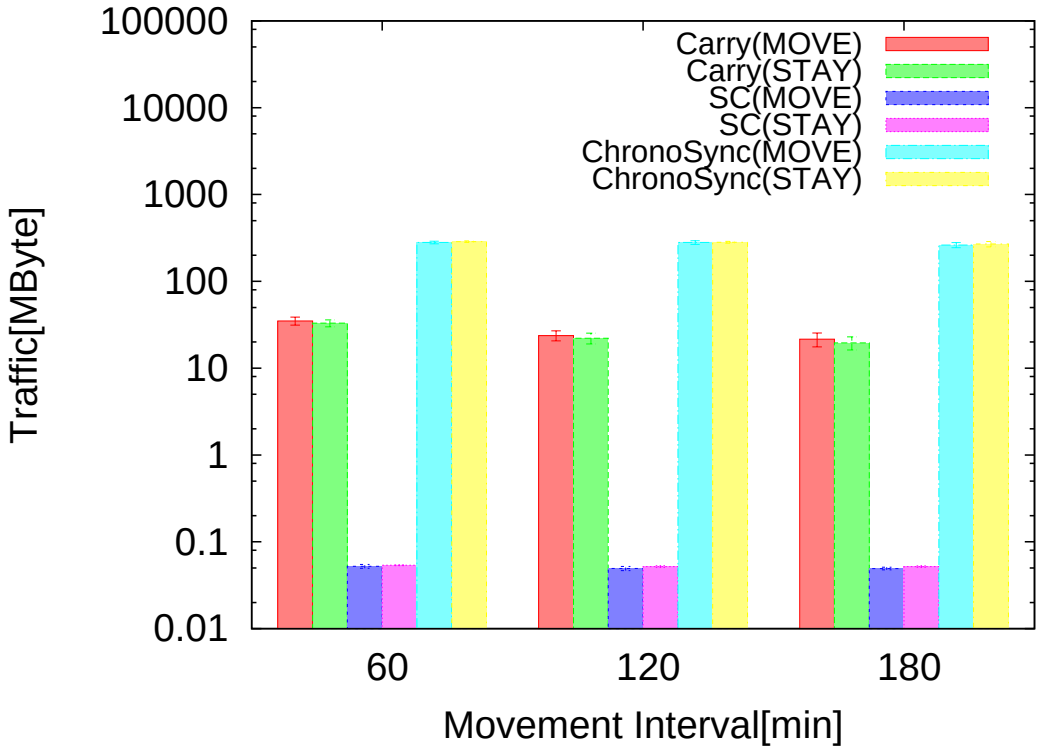
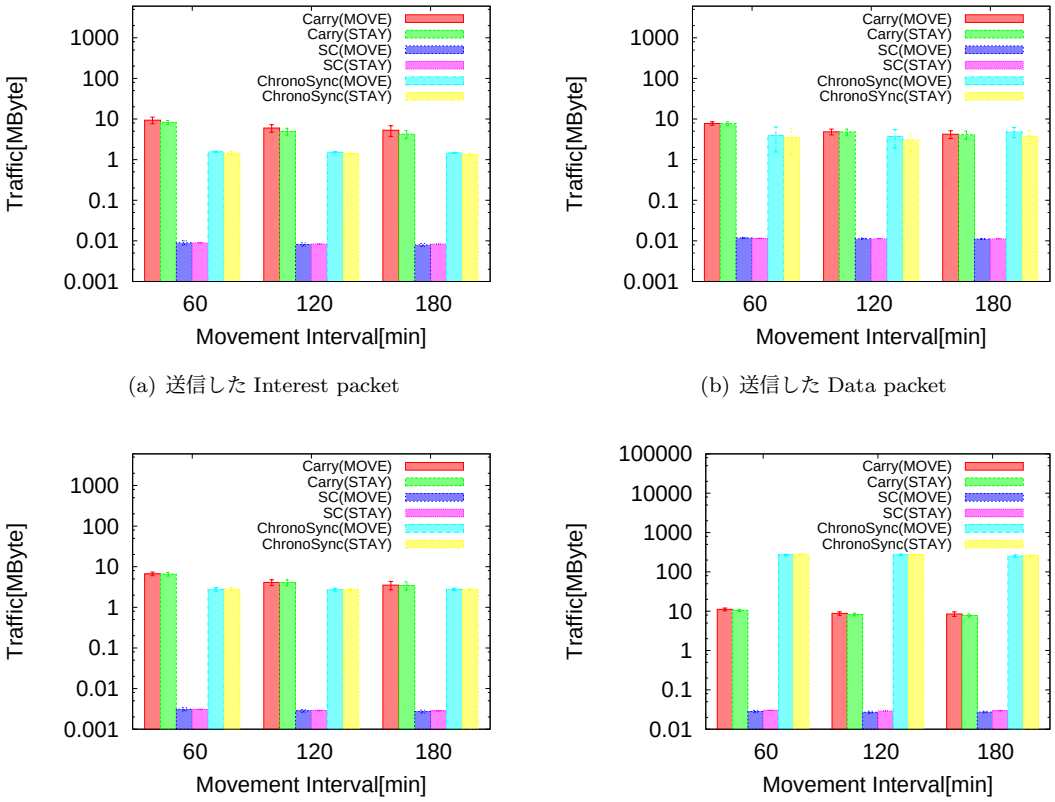


図 4.10: アプリ毎の総トラヒック量



(a) 送信した Interest packet

(b) 送信した Data packet

(c) 受信した Interest packet

(d) 受信した Data packet

図 4.11: アプリ毎の Interest/Data packet 送受信量

第5章

結論

本論文では，Proximity Communication 上に NDN を動作させることで災害時に分断された基地局配下の端末と基地局を使って，災害時以前と同じアプリケーションを提供することができる可能性を示した．また，現在提案されている NDN 上でのデータ同期アプリケーション ChronoSync を災害時の安否確認に利用する場合について，同期間隔を変化させて，そのメッセージ伝達時間について評価を行った．その結果，全体の 10%のユーザが移動する場合についても，同期間隔を 1 分に設定することで，現在の携帯電話メールサービスよりも良い性能が得られることを示した．一方，消費電力は現在の携帯電話サービスにおけるスマートフォンの平常時消費電力の 30 倍になることがわかった．NDN 上でのアプリケーションによる情報伝達性能は既存のメールサービスと同等以上にできることがわかったが，消費電力については課題が残されている．

また，ChronoSync と Name トンネリングをベースとした安否確認システムについてシミュレーションで評価を行った．Name トンネリングは Epidemic routing 型の ChronoSync と同等の情報伝達性能を示すことが予想され，かつ，トラヒック量を 8%から 14%まで削減でき，消費電力の観点から優れている．ただし，今回の Name トンネリングでは，基地局は 2 台だけなので，ルーティングは考慮していない．基地局が 3 台以上ある場合にはルーティング情報も Carry アプリケーションやゲートウェイを利用して共有する必要がある．その場合のプロトコルやトラヒック量の削減については今後の課題である．

ID-based Encryption を Named Data Networking 上で利用することを前提に，端末とネットワークの相互認証手続き，ユーザとアプリケーションサービスプロバイダ間でのサービス利用時の ID の生成 (ID 合意)，相互認証手続きについて提案した．オープンソースとなっている NDNx 上のチャットアプリケーションを対象に本提案を実装し有効性を証明することが次の課題である．

謝辞

本研究を進めるにあたり，ご多忙にもかかわらず，熱心にご指導くださいました浅見徹教授，研究内容について多くのアドバイスをくださいました川原圭博准教授に深く感謝いたします.

また，株式会社 KDDI 研究所杉山浩平様，栗原淳様，田上敦士様，日本電気株式会社柳生智彦様，大阪大学長谷川亨教授には本研究にご協力いただきましたことを，この場をお借りしてお礼申し上げます.

本研究成果は, 独立行政法人情報通信研究機構（NICT）の委託研究 167 課題ウ「コンテンツ指向ネットワーキングによる省エネルギーコンテンツ配信の研究開発」により得られたものです.

参考文献

[1] 入江　恵. 大規模災害等緊急事態における大規模災害等緊急事態における通信確保の在り方に関する検討会 (ネットワークインフラ wg). http://www.soumu.go.jp/main_content/000117676.pdf, June 2011.

[2] 南本, 保谷早苗. UIM バージョン 3 の開発. NTT DoCoMo テクニカルジャーナル, 第 15 巻, pp. 24–29, April 2007.

[3] Li Xiehua and Wang Yongjun. Security Enhanced Authentication and Key Agreement Protocol for LTE/SAE Network. In *Wireless Communications, Networking and Mobile Computing (WiCOM)*, pp. 1–4, Wuhan, September 2011.

[4] Qualcomm. LTE Direct Operator enabled proximity services. http://www.qualcomm.com/solutions/wireless-networks/technologies/lte/lte-direct, 2013.

[5] 3GPP. 3GPP TR 22.803 V12.2.0, June 2013.

[6] Wi-Fi Alliance. Wi-Fi CERTIFIED Wi-Fi Direct, 2013.

[7] Van Jacobson, Diana K. Smetters, James D. Thornton, Michael F. Plass, Nicholas H. Briggs, and Rebecca L. Braynard. Networking named content. In *Proceedings of the 5th international conference on Emerging networking experiments and technologies*, CoNEXT '09, pp. 1–12, New York, NY, USA, 2009. ACM.

[8] Z.Zhu, C.Bian, A. Afanasyev, V.Jacobson, and L. Zhang. Chronos:Serverless Multi-User Chat Over NDN. Technical Report Technical Report NDN-0008, NDN, Oct. 2012.

[9] Z.Zhu and A. Afanasyev. Let's chronosync- decentralized dataset state synchronization in named data networking. In *IEEE ICNP 2013*, Goettingen, Oct. 2013. to appear.

[10] 川本 貴史, 小河原 健生, 川原 圭博, 浅見 徹. Name トンネリングを用いた耐災害タイムラインサービス. 信学総大, 2014. to appear.

[11] http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h24/pdf/index.html, 2012.

[12] C. Gentry and A. Silverberg. Hierarchical id-based cryptography. In *Proceedings of Asiacrypto 2002*, Vol. 2501 of LNCS, pp. 548–66, 2002.

[13] 小河原健生, 川原圭博, 浅見徹. 耐災害 NDN ベース分散型アプリケーションの情報伝達性能に対するユーザ移動モデルの影響評価. マルチメディア, 分散, 協調とモバイル (DICOMO2013) シンポジウム, pp. 34–42, July 2013.

[14] 羅耿介.　標準現況：Proximity Communication. http://std-share.itri.org.tw/Content/Files/Event/Files/%E6%A8%99%E6%BA%96%E7%8F%BE%E6%B3%81%20Proximity%20Communication.pdf, 2012.

[15] V.Jacobson, D.K.Smetters, N.Briggs, M.Plass, and P.Stewart. VoCCN:Voice Over Content Centrin-Networks. In *Rearch'09 in CoNext 2009*, pp. 1–6, Rome, Italy, Dec. 2009.

[16] Lan Wang, A K M Mahmudul Hoque, Cheng Yi, Adam Alyyan, and Beichuan Zhang. OSPFN: An OSPF Based Routing Protocol for Named Data Networking. Technical Report Technical Report NDN-0003, NDN, July 2012.

[17] 3GPP. 3G security;Security architecture. TS 33.102, 3rd Generation Partnership Project(3GPP), June 2008.

[18] 青野博. SAE/LTE を実現するセキュリティ技術. Technical report, 株式会社 NTT ドコモ, September 2012.

[19] 石川秀俊, 高橋和彦, 能川千晶, 古瀬正浩. UIM バージョン 2 の開発. NTT DoCoMo テクニカルジャーナル, 第 11 巻, pp. 35–41, April 2007.

[20] D. Boneh and M. Franklin. Identity-Based Encryption from the Weil Pairing. In *SLAM Journal of Computation*, Vol. 32, pp. 586–615, 2003.

[21] Twitter. https://twitter.com/.

[22] 小河原　健生, 川原　圭博, 浅見　徹. Proximity communication 上での chronosync ベースアプリケーションの災害時情報伝達性能の評価. 信学技報, 第 113 巻, pp. 75–80, Jan. 2014.

[23] A. Afanasyev, I. Moiseenko, and L. Zhang. ndnSIM. http://ndnsim.net/, 2012.

[24] 高木雅, 川原圭博, 浅見徹. アプリ単位の動的な通信制御 を用いた Android 端末の 3G 制御信号と消費電力の削減 手法. 信学総大, No. No.B-15-8, March 2013.

[25] Giuliano Mega, Alberto Montresor, and Gian Pietro Picco. Modeling heterogeneous user churn and local resilience of unstructured p2p networks. In *ICNP*, pp. 32–41, Nov. 2006.

発表文献

国際会議 / International Conferences

[P1] T.Ogawara, Y.Kawahara, and T.Asami, “Disaster Tolerant Authentication System for NDN using Hierarchical ID-based Encryption, ” IEEE ICNP 2013, pp.1-2, Goettingen, Germany, Oct. 2013.

[P2] T.Ogawara, Y.Kawahara, and T.Asami, “Information Dissemination Performance of a Disaster-tolerant NDN-based Distributed Application in Disrupted Cellular Networks, ” IEEE P2P, pp.1-5, Trento, Italy, Sept. 2013.

全国大会

[P3] 小河原健生, 川原圭博，浅見徹, “ハンドオーバ機構を利用した NDN ベース耐災害ネットワークの情報伝達性能の向上手法，” 信学ソ大，B-7-23, Sept. 2013.

[P4] 小河原健生，川原圭博，浅見徹，“耐災害 NDN ベース分散型アプリケーションの 情報伝達性能に対するユーザ移動モデルの影響評価，” DICOMO2013，1B-2, pp.34-42, July 2013.

[P5] 小河原健生，川原圭博，浅見徹, “Proximity Communication 上での ChronoSync ベースアプリケーションの災害時情報伝達性能の評価，” IN 研究会，信学技報, vol. 113, no. 389, IN2013-130, pp. 75-80, Jan. 2014.

[P6] 小河原健生，篠田詩織，川原圭博，浅見徹，“Named Data Networking 上での ID-based Encryption による ID 合意および相互認証プロトコルの設計，” IN 研究会，信学技報, vol. 113, no. 389, IN2013-131, pp. 81-86, Jan. 2014.

[P7] 小河原健生, 川本貴史, 川原圭博, 浅見徹，“Name トンネリングを用いた耐災害タイムラインサービスの情報伝達性能評価，” 信学技報，Vol.113, No.473, IN2013-183, pp.235-240, March 2014.