Mobile PPC における認証方式の実装に関する検討

瀬下　正樹*，竹内　元規，渡邊　晃(名城大学)

Researches about Implementation of Authentication Mechanisms in Mobile PPC

Masaki Sejimo, Motoki Takeuchi, Akira Watanabe (Meijo University)

１．はじめに

インターネットでは，端末が移動すると IP アドレスが変化し，通信が切断されてしまうという問題がある．そこで，端末の移動による IP アドレスの変化を隠蔽し，通信を継続できるようにする移動透過性の研究が盛んに行われている．

我々は，移動透過性の一方式として，P2P で移動透過性を実現する Mobile PPC(Mobile Peer to Peer Communication) [1]と，その認証機構である Mobile PPC における認証方式[2]の研究を行なっている．Mobile PPC は既に実装済みであるが，Mobile PPC における認証方式は未実装である．そこで，本研究では Mobile PPC における認証方式の実装に関する検討を行った．本稿ではその検討内容を報告する．

２．Mobile PPC とセキュリティ問題

Mobile PPC では，通信中に IP アドレスが変化しても通信を継続するために，エンド端末間に新旧の IP アドレスの対応関係を示すテーブル(CIT)を保持させ，IP アドレスが変化すると，その直後に移動端末（MN）から通信相手端末（CN）に対して新しい IP アドレスを CIT Update (CU)により通知する．CU により CIT が更新され，以後の通信ではパケット送受信時に IP 層で CIT を参照してアドレス変換を行う．これにより，IP 層より上位のソフトウェアに対し IP アドレスの変化を隠蔽し，通信を継続させることが可能となる．

しかし，CN が CU パケットを受信する際，セッションの乗っ取りを防ぐため MN を確実に認証する必要がある．

３．Mobile PPC における認証方式

Mobile PPC における認証方式は Diffie-Hellman 鍵交換(DH 鍵交換)を利用する．DH 鍵交換とは，離散対数問題を利用したアルゴリズムにしたがって生成した乱数を交換することにより，その乱数を盗聴されたとしても盗聴者には知ることのできない共有鍵を生成する鍵交換方式である．

Mobile PPC における認証方式では，通信に先立ってエンド端末間で DH 鍵交換を行うことにより MN と CN に共有鍵を保持させておき，移動時にこの共有鍵を用いて MN の認証を行う．

４．実装に関する検討

４．１．NIT(Node Information Table)

Mobile PPC における認証方式では DH 鍵交換を端末単位での通信に先立って実行する．そこで，出力されるパケットが端末単位で１回目であるかどうかの判断を行なう必要があり，この判断を行なうための情報を格納する NIT(Node Information Table)を Mobile PPC の仕様に追加する．NIT は，自端末/相手端末 IP アドレス，自端末/相手端末 DH 乱数，共有鍵情報，状態の 6 つのフィールドから構成され，端末単位での通信の有無を判断するための情報以外にも共有鍵に関連する情報も格納する．

４．２．モジュール構成

Mobile PPC は FreeBSD のカーネル部に既存の処理へ影響を与えないようにモジュールを組み込むことで実現されている．本実装は，これまでの Mobile PPC にモジュールを追加することにより，認証方式を実現する．モジュール構成を図 1 に示す．追加するモジュールには通信に先立ちネゴシエーションを行なう DH 鍵交換モジュール，DH アルゴリズムにより乱数および共有鍵の算出を行う DH 算出モジュール，NIT レコードの検索・生成・更新を行なう NIT 操作モジュール，認証データの生成・検証を行う認証処理モジュールがある．また，既存の CU 生成・送/受信モジュールから認証処理モジュールを呼び出せるように修正を加える．

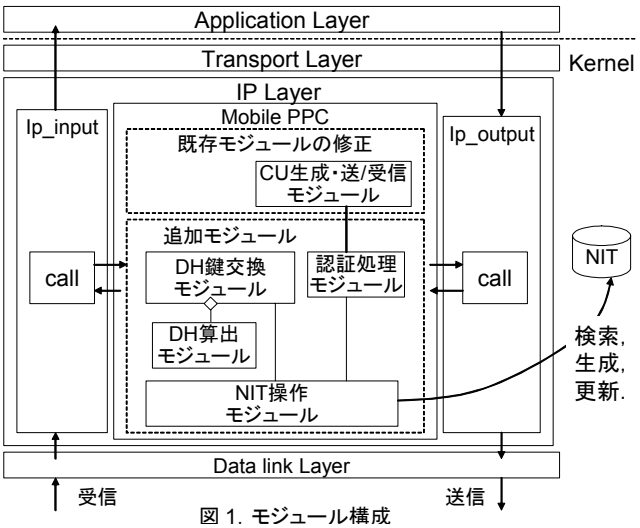


図 1. モジュール構成

５．むすび

Mobile PPC における認証方式の実装に関する検討を行った．今後は実装と有効性の確認を行う．

文　献

[1] 竹内元規，渡邊晃，“モバイル端末の移動透過性を実現する Mobile PPC の提案,”情報処理学会研究報告，2004-MBL-30, pp.17-24, Sep. 2004.

[2] 瀬下正樹，竹内元規，渡邊晃，“Mobile PPC における認証方式の提案”，情報処理学会 第 67 回全国大会，Mar.2005.

Mobile PPCにおける認証方式の実装に関する検討

名城大学大学院　理工学研究科
瀬下正樹　竹内元規　渡邊晃

研究背景

➢ 研究背景

- Mobile PPC
  - 移動中にIPアドレスが変化しても通信を継続するノード移動透過性の実現
- Mobile PPCにおける認証方式
  - Mobile PPCが提供する移動透過により新たに発生する通信の乗っ取りを防止

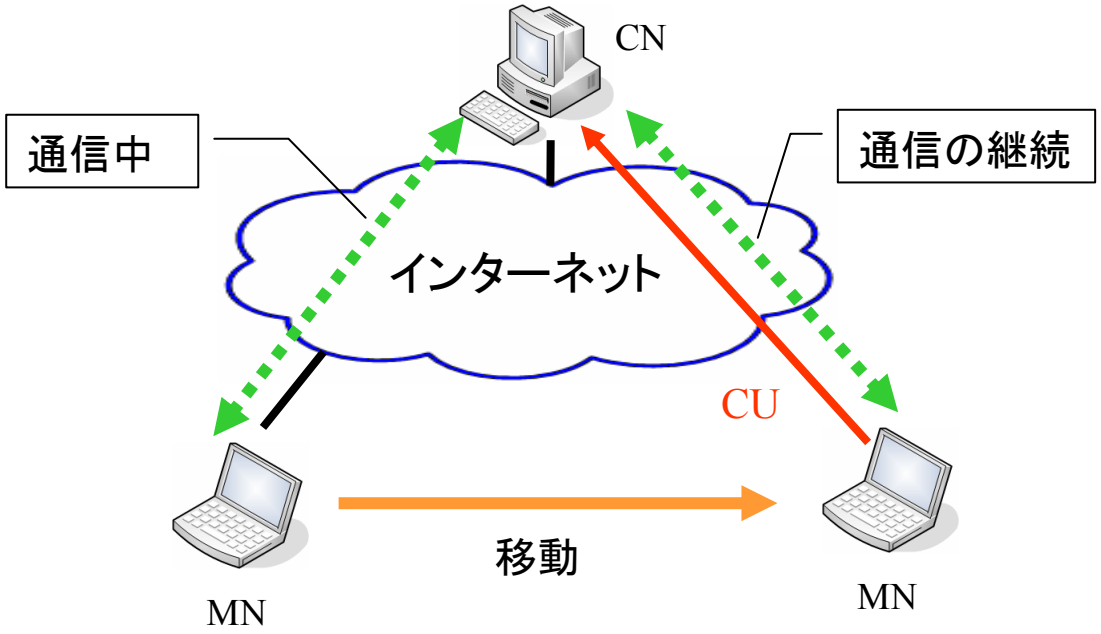
✓ Mobile PPCは実装済みであるが，Mobile PPCにおける認証方式は未実装

Mobile PPCにおける認証方式の実装に関する検討

➢ 動作概要

- 通信中のIPアドレスの変化
  - CU(CIT Update)を用いて新しいIPアドレスを通知
  - 移動前後のIPアドレスの対応関係を示すテーブル(CIT)を生成
  - パケット送受信時にIP層でCITを参照し，アドレス変換を行う

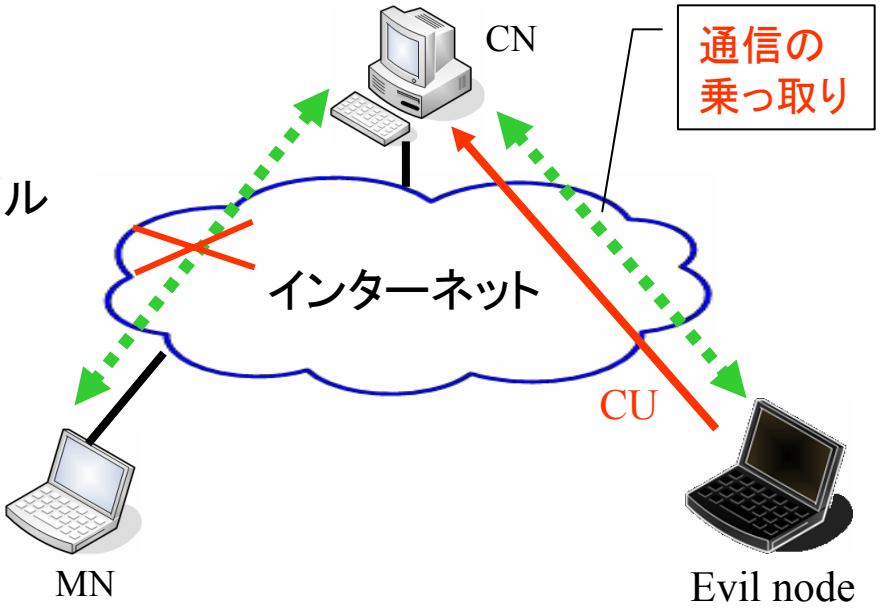
⇒IP層より上位層に対してIPアドレスの変化を隠蔽，パケットは移動先のMNへ正しく配送



CUにおけるセキュリティ課題

- MNとCNが通信中
  - 悪意を持ったノードがCNへCUパケット送信
    - 移動前後の対応関係を示すテーブル(CIT)が不正に書き換えられる

⇒ 通信の乗っ取りが発生



- CNにアクセスしてくるMNは不特定多数
  - CNは事前に認証に必要なMNの鍵を持つことは難しい
  - PKI の利用は現在の普及状況では現実的でない

⇒ 新たな認証機構が必要

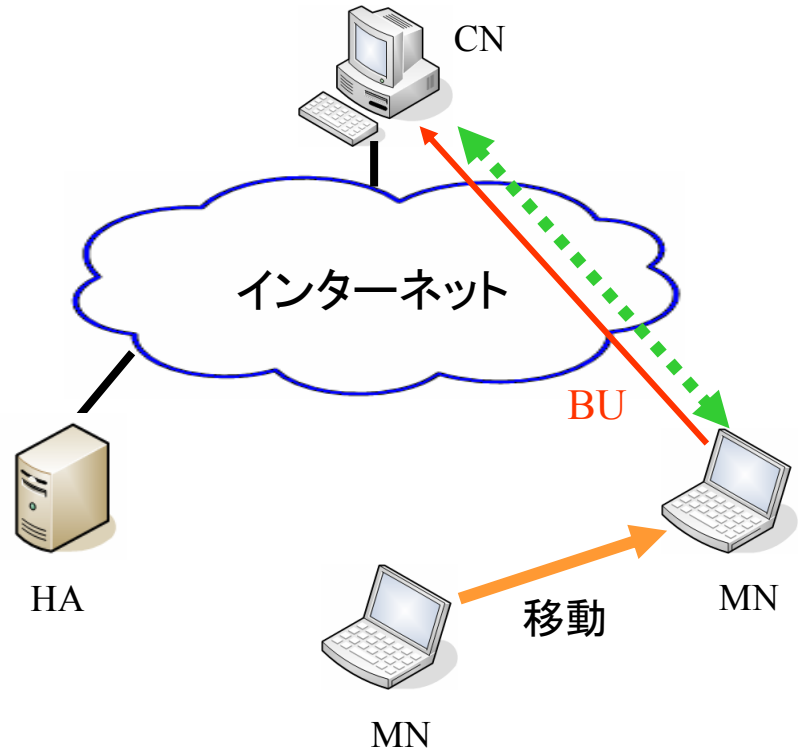
関連研究： Return Routability

➢ Return Routability
  – **Mobile IPv6**の**経路最適化時**に使用される認証機構

✓ Mobile IPv6
  – IPv6においてノード移動透過性を保証するプロトコル

✓ 経路最適化
  – Mobile IPv6において，通信中の移動透過をP2Pで行うための仕組み
    - IPアドレスの変更をBU (Binding Update)で通知
    - 移動前後の対応関係を示すテーブルを生成
    - パケット送受信時にIP層でテーブルとIPv6拡張ヘッダを利用したアドレス変換

  ⇒移動透過を実現

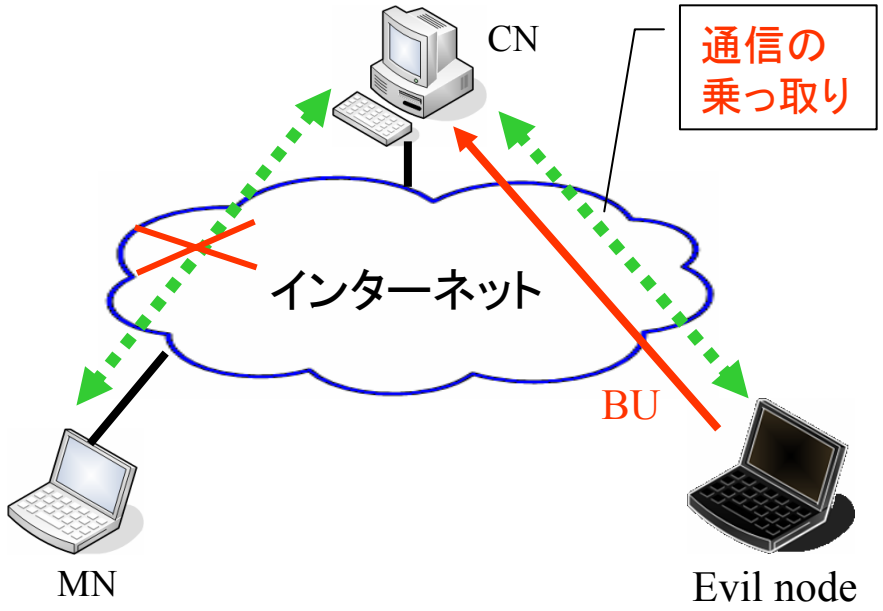


経路最適化の課題

- 経路最適化の課題
  - Mobile PPCと同様の課題を持つ

- MNとCNが通信中
  - 悪意を持ったノードがCNへBUパケット送信
    - 移動前後の対応関係を示すテーブルが不正に書き換えられる

通信の乗っ取りが発生



Mobile IPv6では，この問題をReturn Routabilityで解決

Return Routabilityの仕組み

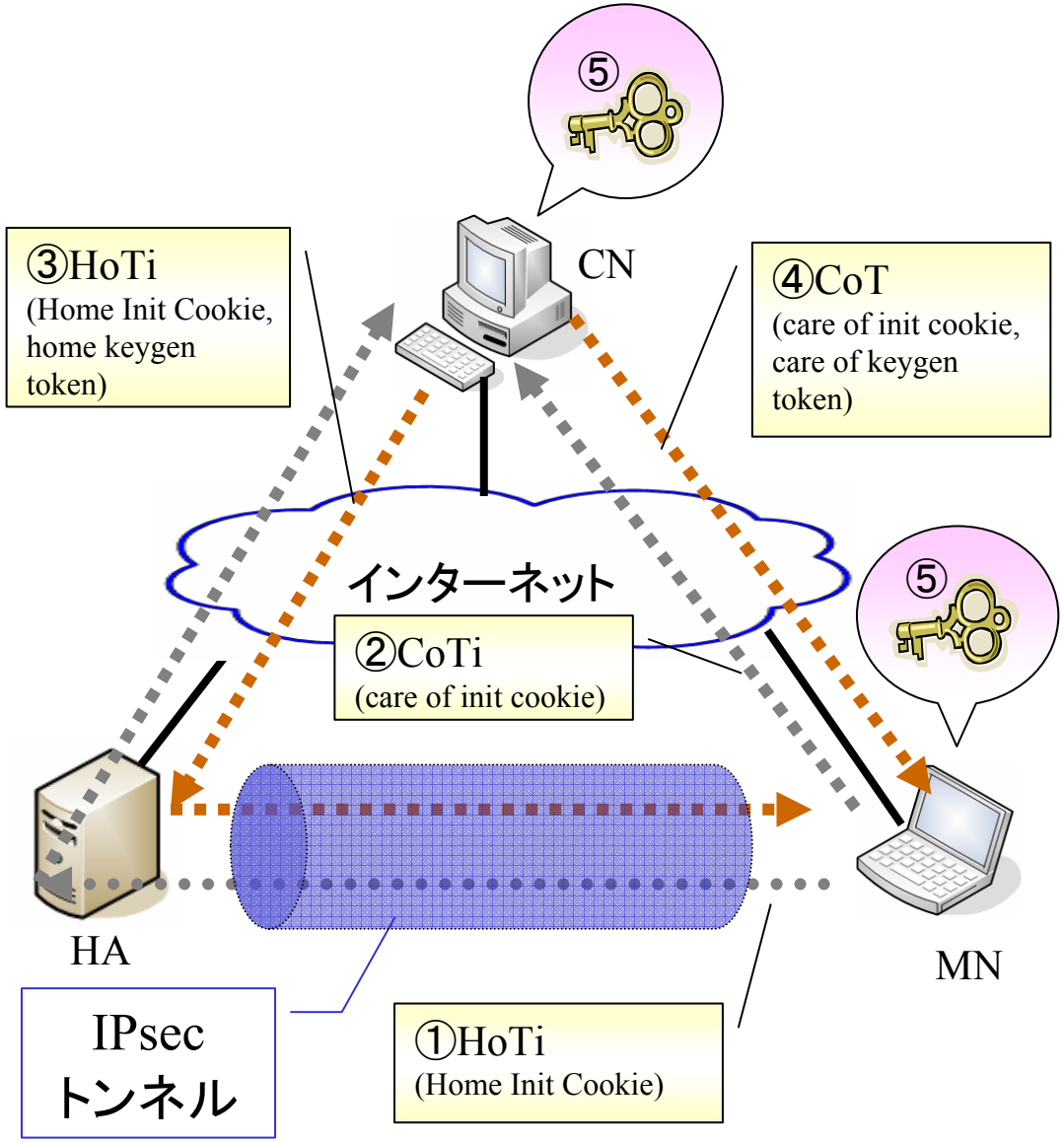
- Return Routability
  - 前提条件
    - HA(Home Agent)と呼ぶ第三の機器の導入
    - HAとMNは信頼関係にあることが前提

    ⇒ HAとMN間はIPsecで保護できると考える

「動作概要」

  - BU直前
    - 共有鍵を二つに分け，異なる経路から配送（①から④）

    ⇒ 共有鍵を生成（⑤）
  - BU時
    - 共有鍵を用いた認証を行う



Return Routabilityの問題点

- 問題点
  - HAのような特殊な第三の装置を利用する
  - 盗聴の問題
    - CNと同一セグメント上
      - 2つの鍵が平文のまま流れる

      ⇒容易に共有鍵の盗聴が可能
    - CNからHA間，MNからCN間
      - 2点を同時に盗聴した場合，共有鍵の盗聴可能

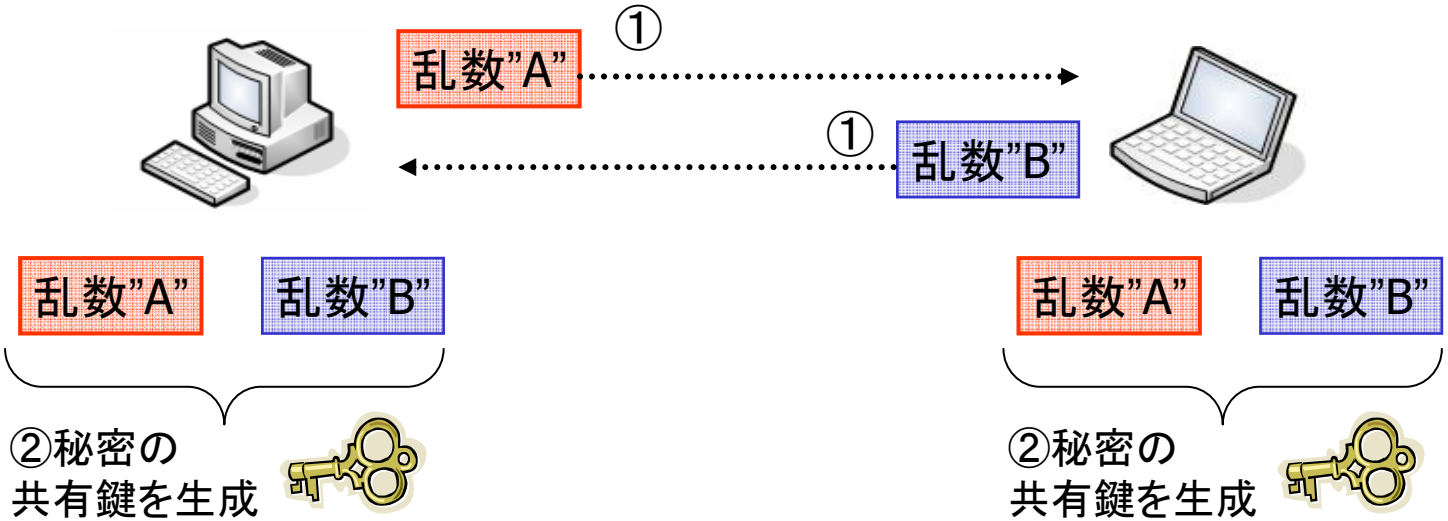
Mobile PPCのようにエンドエンドで移動透過性
を保証するプロトコルには適していない

Mobile PPCにおける認証方式

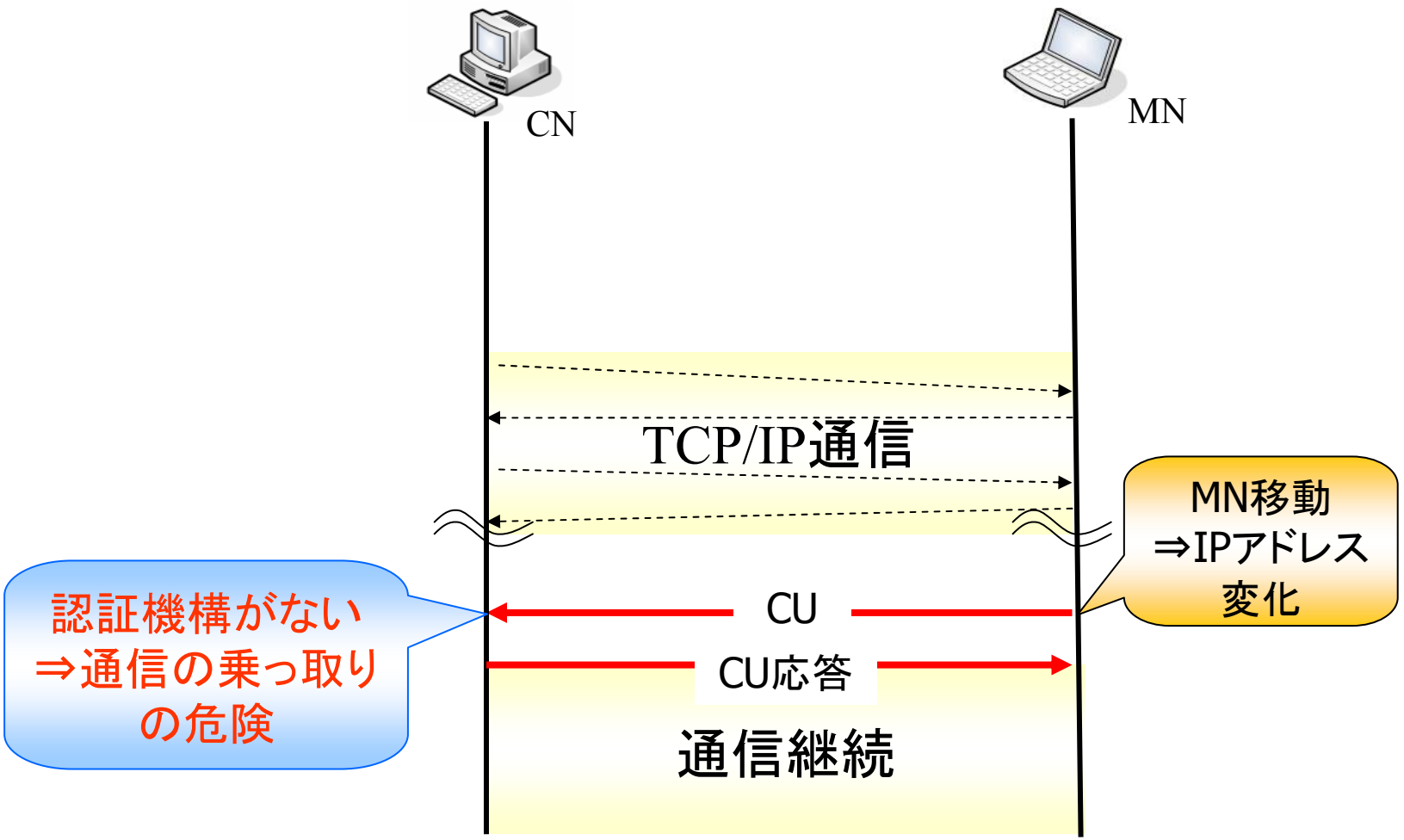
提案技術

- Diffie-Hellman鍵交換を利用した認証機構
  - Diffie Hellman鍵交換
    - ある乱数を交換することによって(①)
    - 盗聴者がいても端末間で共有鍵を安全に生成する(②)

✧離散対数問題を利用



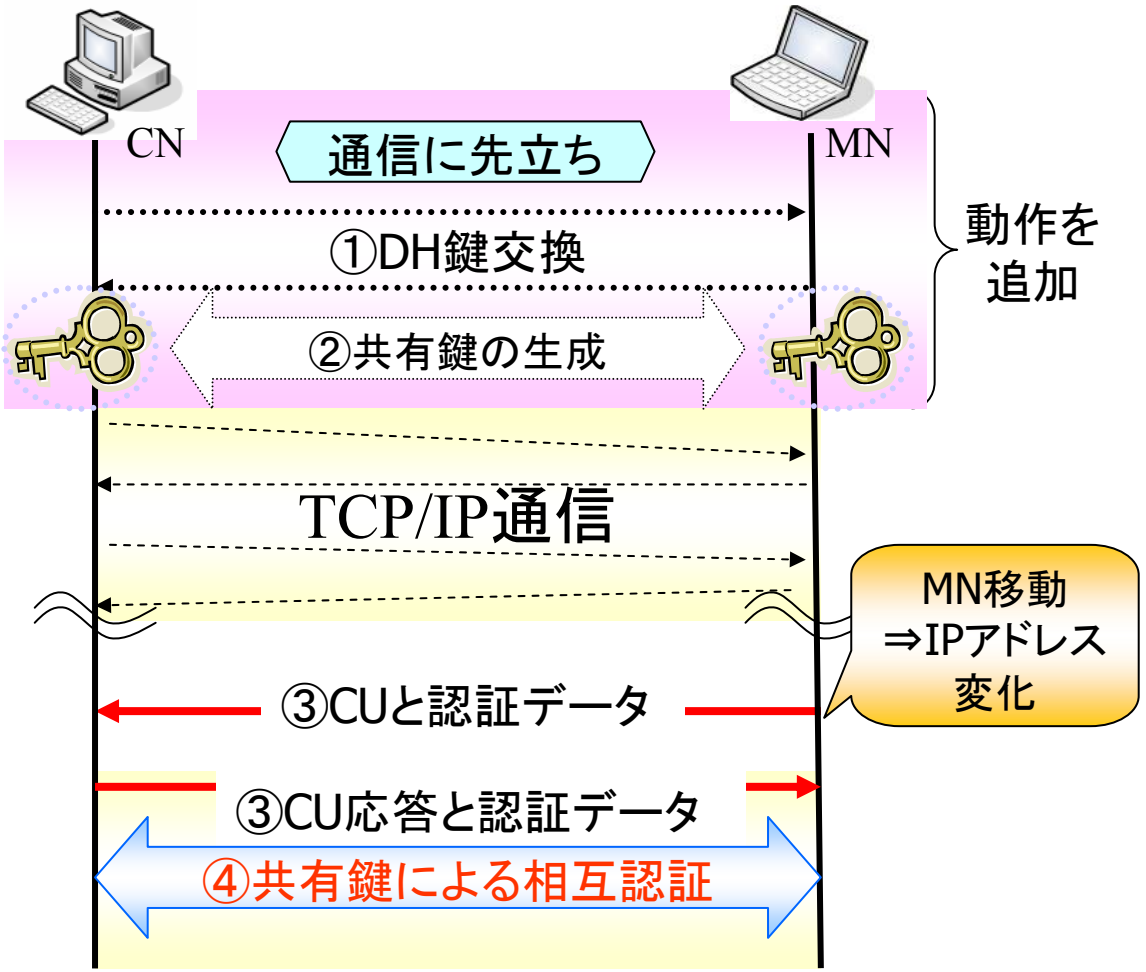
Mobile PPCのシーケンス



提案方式を追加したMobile PPCのシーケンス

動作概要

- 通信に先立ち
  - ①Diffie-Hellman鍵交換
  - ②共有鍵を生成
- *その後，通常のTCP/IP通信*
- MN移動
  - ③MNはCUと認証データをCNへ送信，CNはCU応答と認証データをMNへ送信
  - ④共有鍵を使用して相互認証



CUにおける通信の乗っ取りを防止することが可能

実装

- 現状のMobile PPC
  - FreeBSDのカーネルにモジュールを組み込むことで実現
    - IP層の入出力時に呼び出し，処理を終えたら差し戻す
    - IP層で行われる既存の処理へ影響を与えない
- Mobile PPCにおける認証方式
  - これまでのMobile PPCにモジュールを追加することで認証方式を実現

実装

- Mobile PPCにおける認証方式
  - Diffie-Hellman鍵交換を端末単位での通信に先立ち実行

⇒ 出力されるパケットが端末単位で1回目であるかどうかの判断が必要

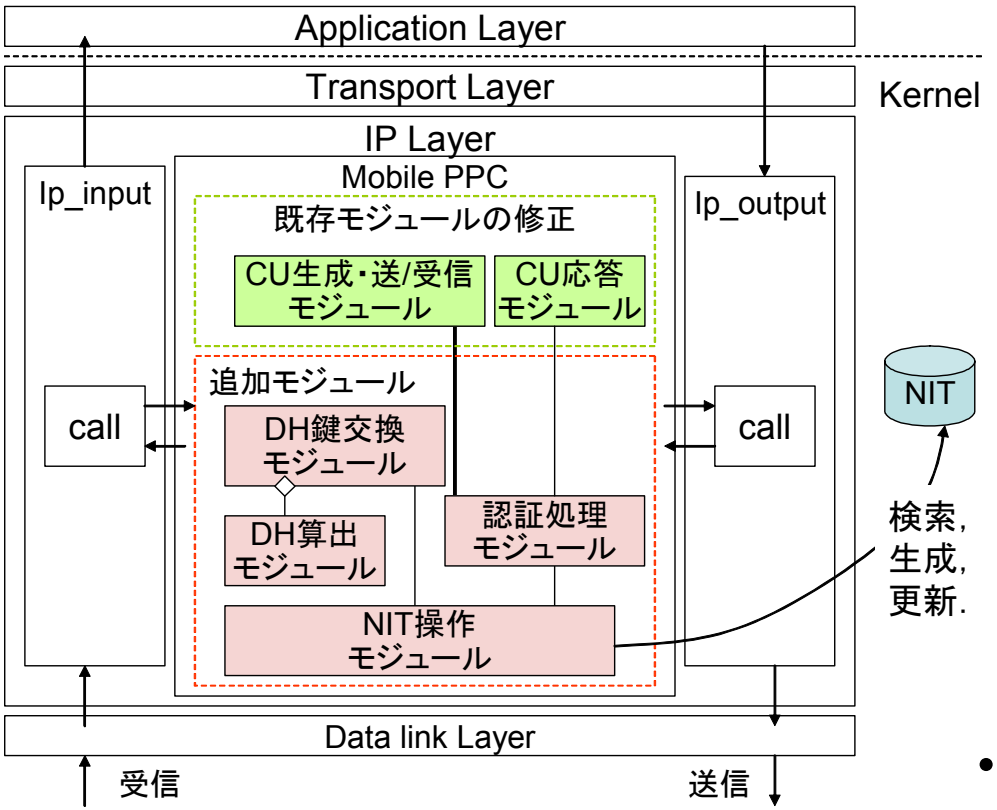
- NIT (Node Information Table)
  - 端末間での通信の有無を判断する情報を格納
  - 共有鍵に関連する情報も格納

- NITフォーマット

検索キー

自端末 IP	相手端末 IP	自端末DH 乱数	相手端末 DH 乱数	共有鍵
CN	MN1	A	B	Key1
CN	MN2	C	D	Key2

モジュール構成



- 追加するモジュール
  - DH鍵交換モジュール
    - 通信に先立ちネゴシエーションを行なう

    ⇒当研究室で別途研究しているDPRPを流用
  - DH算出モジュール
    - DHアルゴリズムにより乱数と共有鍵の算出

    ⇒オープンソースライブラリであるOpenSSLを利用
  - NIT操作モジュール
    - NITレコードの検索・生成・更新を行なう
  - 認証処理モジュール
    - 認証データの生成・検証を行う
    - CU応答の生成・送/受信を行う
- 修正するモジュール
  - CU生成・送/受信モジュール
  - CU応答モジュール
    - 認証処理モジュールを呼び出すように修正

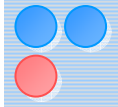
Mobile PPCにおける認証方式の評価

- 共有鍵の生成を通信に先立ち行なう.
  また，すべての処理をIP層で行なう.

  ⇒ 既存の処理に影響を与えない

- HAのような特殊な第三の装置を必要としない

  ⇒ 導入が容易



むすび

- Mobile PPCにおける認証方式を説明し，実装に関する検討を行なった
- 今後は提案方式を実装し，有効性の確認を行う

おわり