NTMobile におけるグループ鍵を利用した相手認証の提案

右京　康也 †*，菅沼　良一 †，鈴木　秀和 †，内藤　克浩 ‡, 渡邊　晃 †
(† 名城大学,　‡ 愛知工業大学)

Proposal for Node Authentication with Group Key of NTMobile

Koya Ukyo†, Ryoichi Suganuma†, Hidekazu Suzuki†, Katsuhiro Naito‡, Akira Watanabe†
(†Meijo University, ‡Aichi Instiure of Technology)

1　はじめに

携帯電話やスマートフォン、タブレットなどのモバイル端末や無線インフラの普及によって、ネットワーク環境に関わらず通信を開始することができる通信接続性、通信中にネットワークが切り替わっても通信を継続することができる移動透過性が求められている。NTMobile（Network Traversal with Mobility）[1] は通信接続性と移動透過性を同時に実現することが可能な技術である。

NTMobile の通信パケットは、共通鍵によって暗号化され、MAC（Message Authentication Code）認証が行われるためセキュリティも高い。しかし、現在の NTMobile の役割はネットワークの制約を除去することであり、通信相手がグループメンバであることを確認する相手認証機能が提供されていない。本研究では、エンド端末間で事前にグループ鍵が共有されていることを前提にしたうえで、NTMobile でグループ認証を実現するための方式を提案する。

2　NTMobile の概要

NTMobile は、エンド端末（以後 NTM 端末）に NTMobile の機能を搭載することにより、セキュアなエンドツーエンドの通信を可能とする技術である。NTMobile は、DC（Direction Coordinator）と NTM 端末で構成されている。DC は NTM 端末の仮想 IP アドレスの管理と通信経路の指示を行う。NTM 端末はログイン時に DC に実 IP アドレスを登録し、DC から重複しない仮想 IP アドレスを受け取る。アプリケーションはその仮想 IP アドレスを用いてセッションを確立する。実際の通信は、実 IP アドレスで全てのパケットをカプセル化し UDP トンネルによる通信を行う。DC は通信開始時と NTM 端末が移動した時、両 NTM 端末に対して実 IP アドレスによる UDP トンネル構築の経路指示を行う。上記の動作により、移動透過性と通信接続性を実現することができる。

通信を行う NTM 端末はシグナリングの過程において安全に End Key を共有する。この共通鍵を用いてエンドツーエンドでパケットの暗号化と、送信元認証を行っている。

3　相手認証機能の実現方法

<3・1 >従来のシーケンス　MN は Direction Request を DC に送信して、経路指示を仰ぐ。Direction Request を受け取った DC は、MN と CN に対して Route Direciton で経路を指示する。経路指示を受け取った MN と CN は DC の指示に従って Tunnel Request/Tunnel Respose を交換し、End Key の共有と通信経路の確立を行う。これによりセキュアな通信は実現できるが、グループ認証機能がなかった。

<3・2 >提案方式のシーケンス　提案方式では、事前に共有されているグループ鍵 GK を利用することにより通信相手の認証を行う。Fig. 1 に提案方式のシーケンスを示す。提案方式は、Tunnel Request と Tunnel Respose に、GK と OTC（One Time Code）のハッシュ値、h（GK||OTC）と OTC を追加する。OTC は使い捨てで十分大きな乱数である。各端末は受け取ったハッシュ値を検証することにより相互認証を行う。MN、CN は同一グループのメンバであり、GK を事前に共有している。MN は、Tunnel Request において、自分が持つ GK と適当に生成した OTC1 のハッシュをとり、OTC1 とともに CN へ送信する。CN は自分が持つ GK と受信した OTC1 のハッシュをとり、受信したハッシュ値と一致するか検証する。一致すれば、Tunnel Respose において、自分が持つ GK と適当に生成した OTC2 のハッシュをとり、OTC2 とともに CN へ送信する。MN が CN から送られてきたハッシュ値の検証に成功すれば相互認証が完了する。Fig.2 に提案方式における Tunnel Request のヘッダフォーマットを示す。NTM Header は NTMobile 特有のヘッダー、E（End Key, TempKey）は End Key を DC から配布された TempKey で暗号化したもの、HMAC は認証コードである。ここに今回 h（GK||OTC1）と OTC1 を追加した。

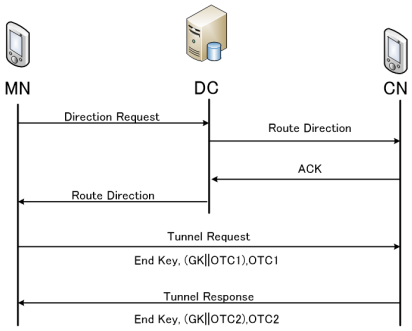


Fig. 1　提案方式のシーケンス図

HTM Header
E(End Key, TempKey)
h(GK||OTC1)
OTC1
HMAC

Fig. 2　Tunnel Request のヘッダフォーマット

グループ鍵の共有方法は、グループ管理サーバ GMS（Group Management Server）からの配送、もしくはパスワードの手入力等を選択できるようにする。そのためグループ鍵を格納する所定のファイルを各端末に持たせる。

4　まとめ

グループ鍵を事前に共有しているという前提で、NTMobile においてグループ認証を実現する方式を提案した。

文　献

[1] 鈴木秀和．他：NTMobile における通信接続性の確立手法と実装, 情報処理学会論文誌 Vol.54, No.1, pp.367-379, 2013.

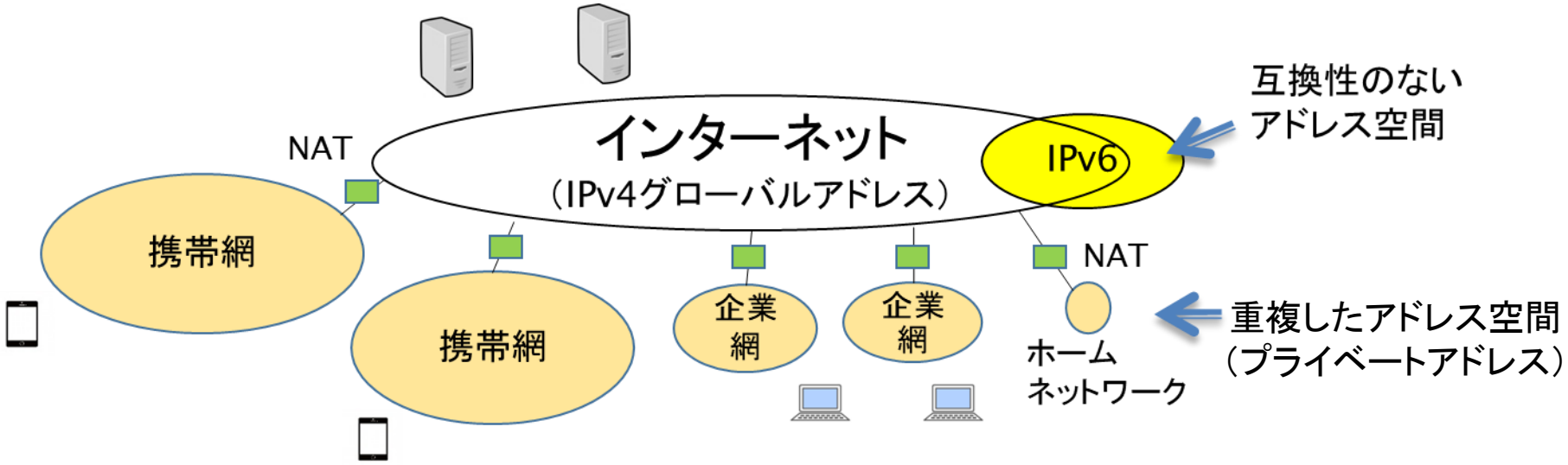
NTMobileにおけるグループ鍵を利用した相手認証の提案

右京 康也†, 菅沼 良一†, 鈴木 秀和†, 内藤 克浩‡, 渡邊　晃†
† 名城大学　理工学部　情報工学科
‡ 愛知工業大学　情報科学部

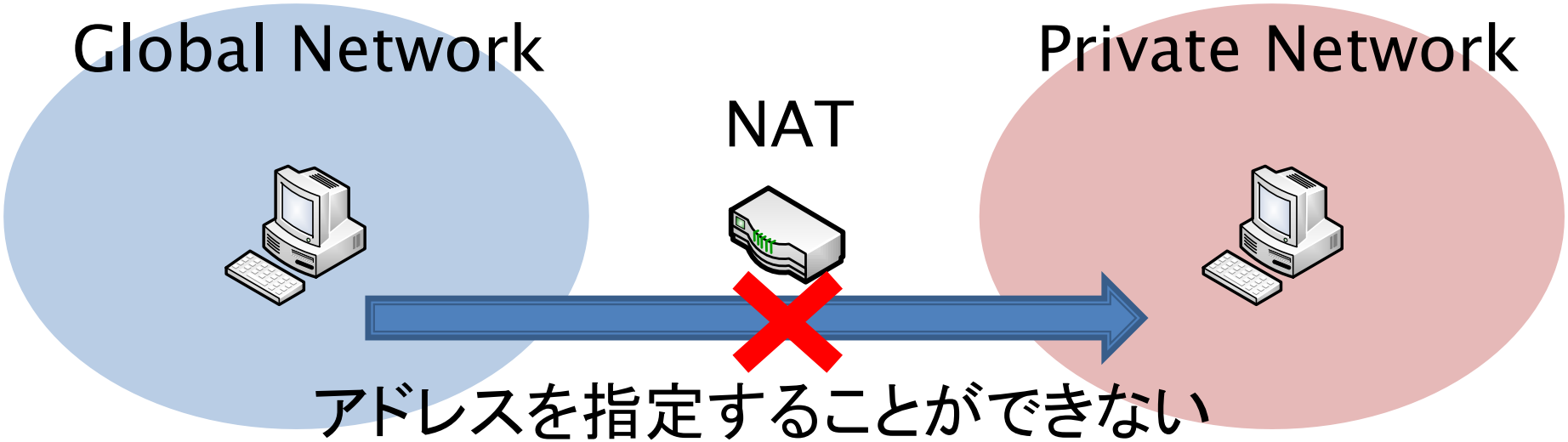
Watanabe Lab.

研究背景　－現状のネットワーク－

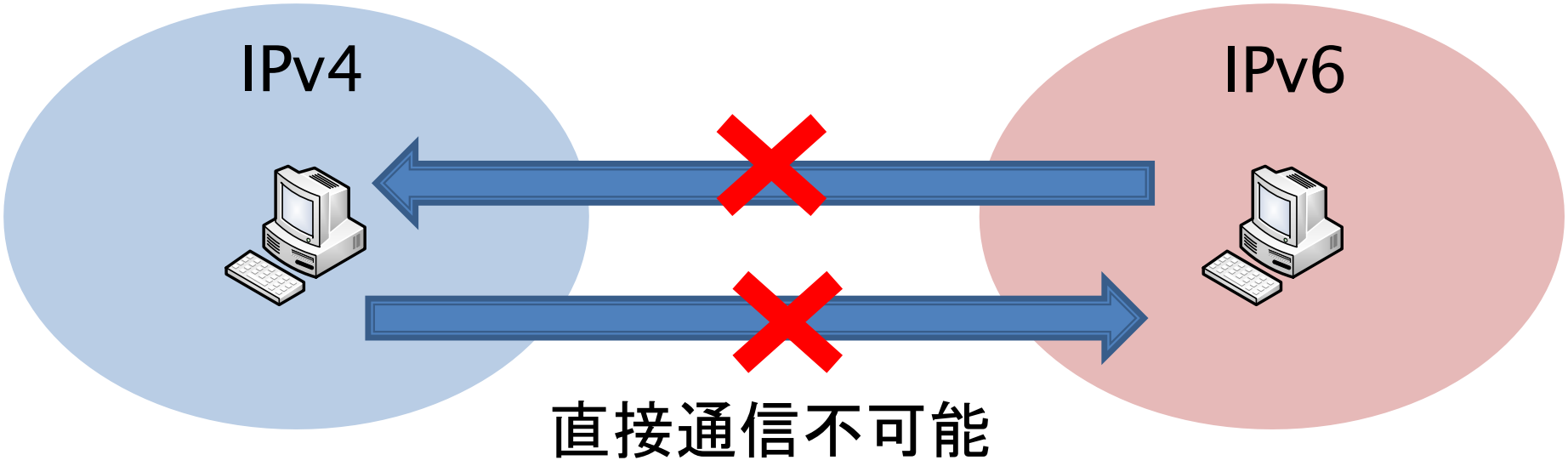
- IPv4グローバルアドレス枯渇問題
  - NATを利用したネットワークの構築
  - IPv6アドレスへの移行



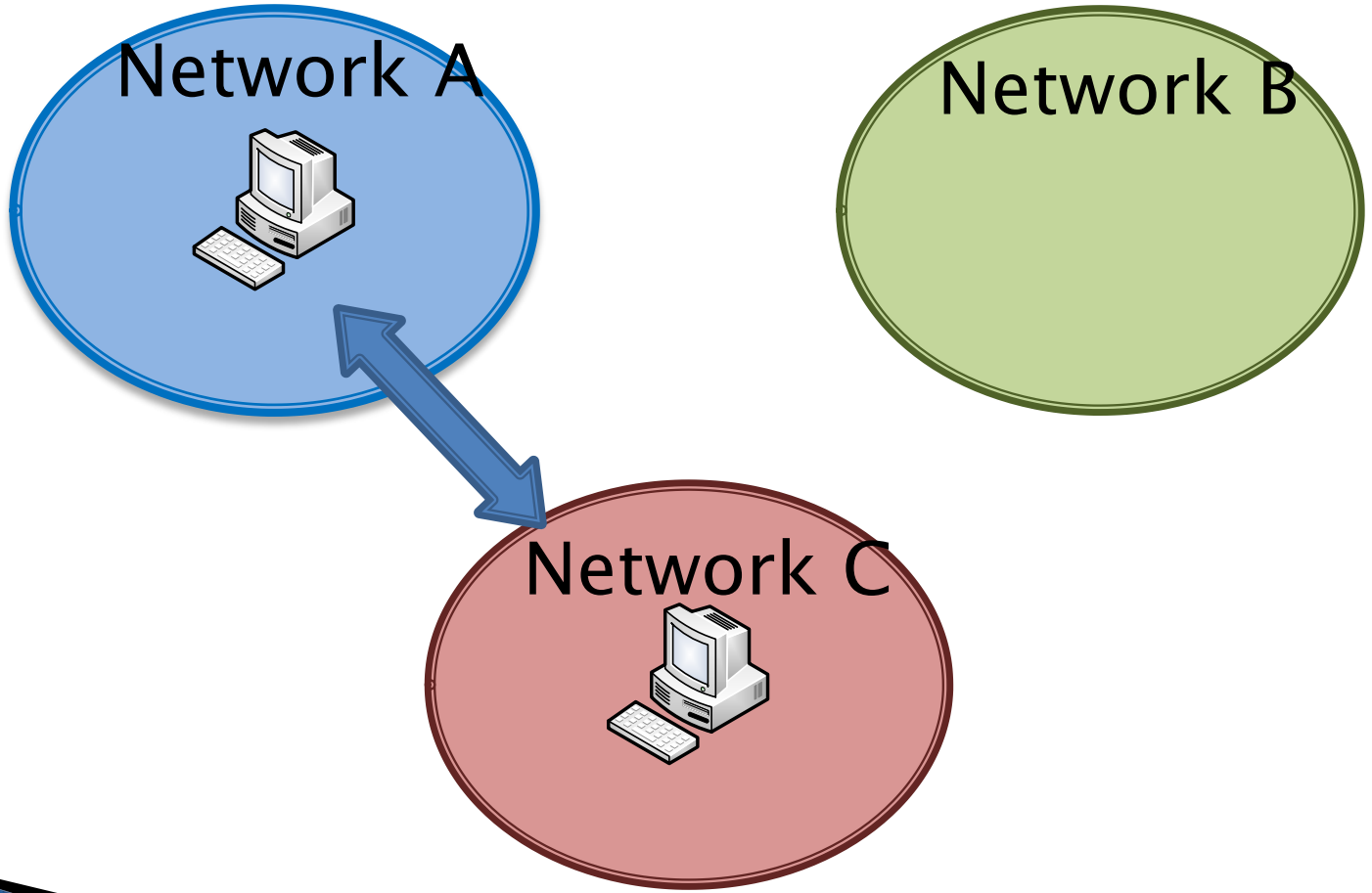
- NAT越え問題
  - インターネット側端末からプライベート側端末へ通信を開始できない



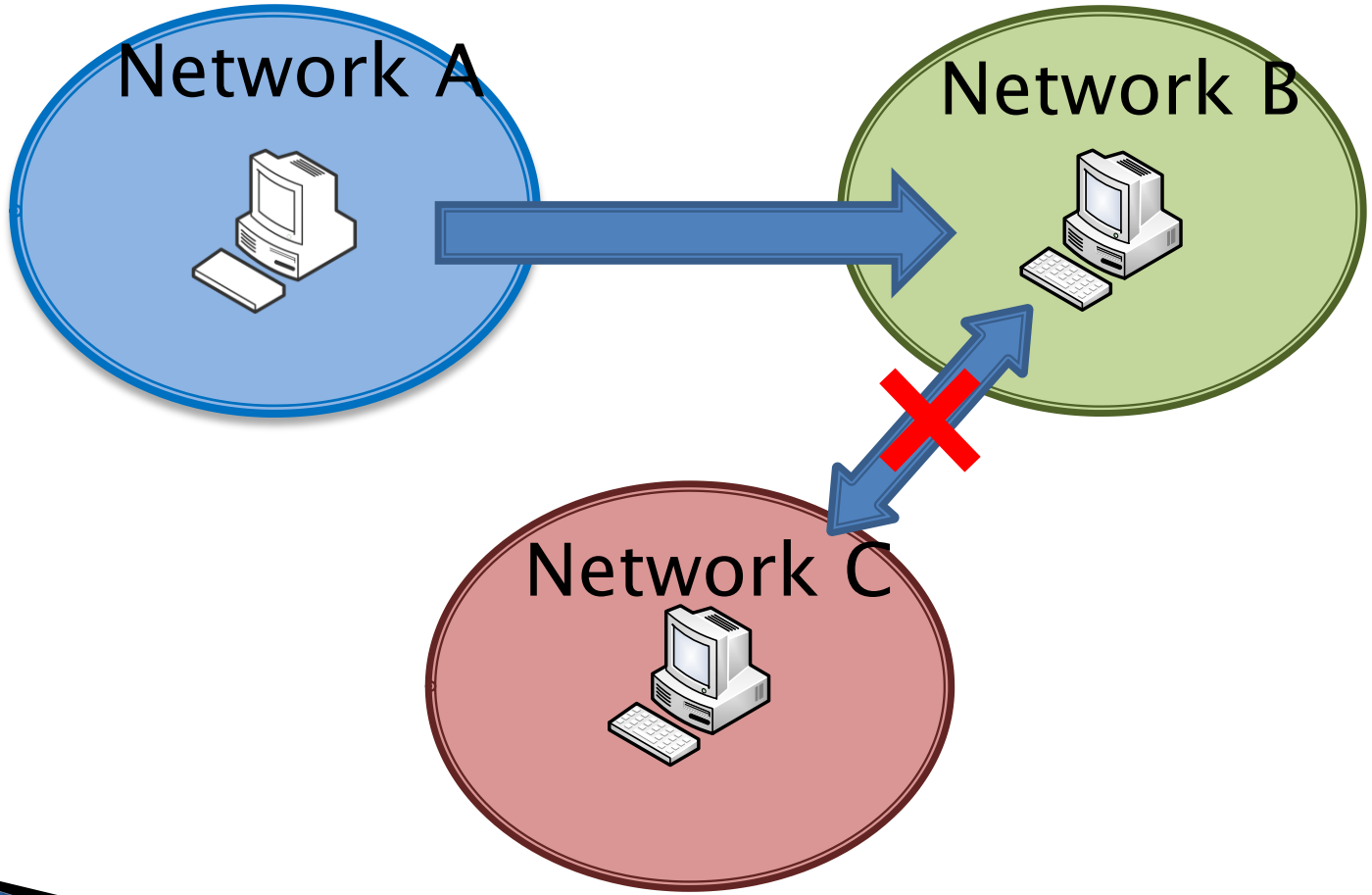
- IPv4/IPv6の非互換性
  - IPv4とIPv6には互換性が無い



- 移動透過性が必要
  - ネットワークが切り替わると通信を持続することができない

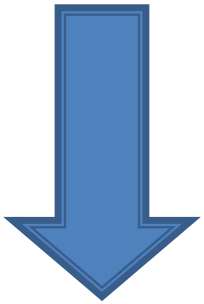


- 移動透過性が必要
  - ネットワークが切り替わると通信を持続することができない



インターネットの問題点

- NAT越え問題
- IPv4/IPv6の非互換性
- 移動透過性が必要



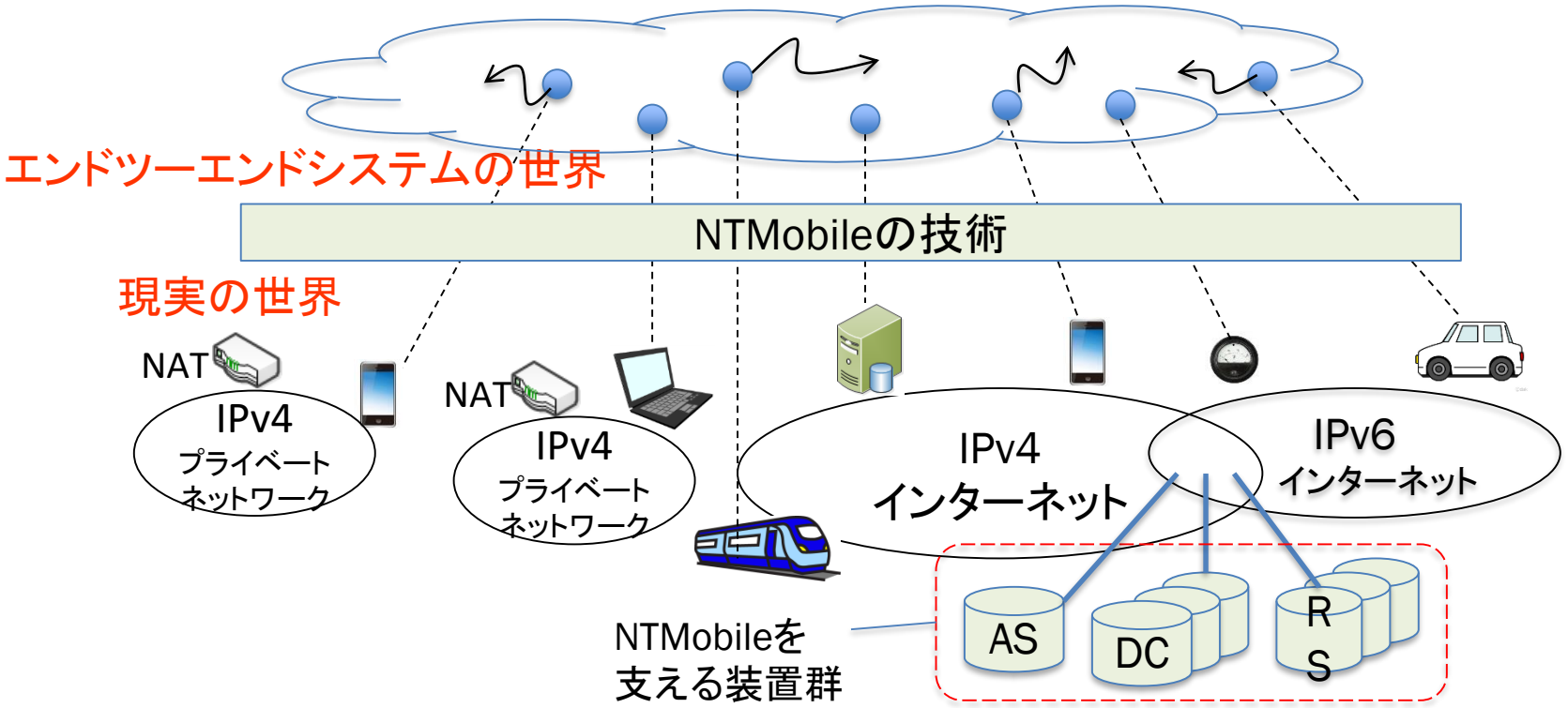
NTMobile（Network Traversal with Mobility）

NTMobileの概要

- 移動透過性の実現
  - 仮想IPアドレスを使用し通信を行う
    - すべてのパケットをUDPでカプセル化
- 通信接続性の実現
  - DC(Direction Coordinator)による経路指示
  - 両NTM端末が異なるNAT配下、もしくはIPv4-IPv6通信の場合はRS (Relay Server)を利用

NTMobileの構成

エンド端末にNTMobile用アプリケーションをインストールすることによりエンドツーエンドシステムの世界に移行できる。
NTMobileをサポートする装置群（AS,DC,RS）をインターネット上に配置する必要がある（ユーザは意識しなくてよい）。



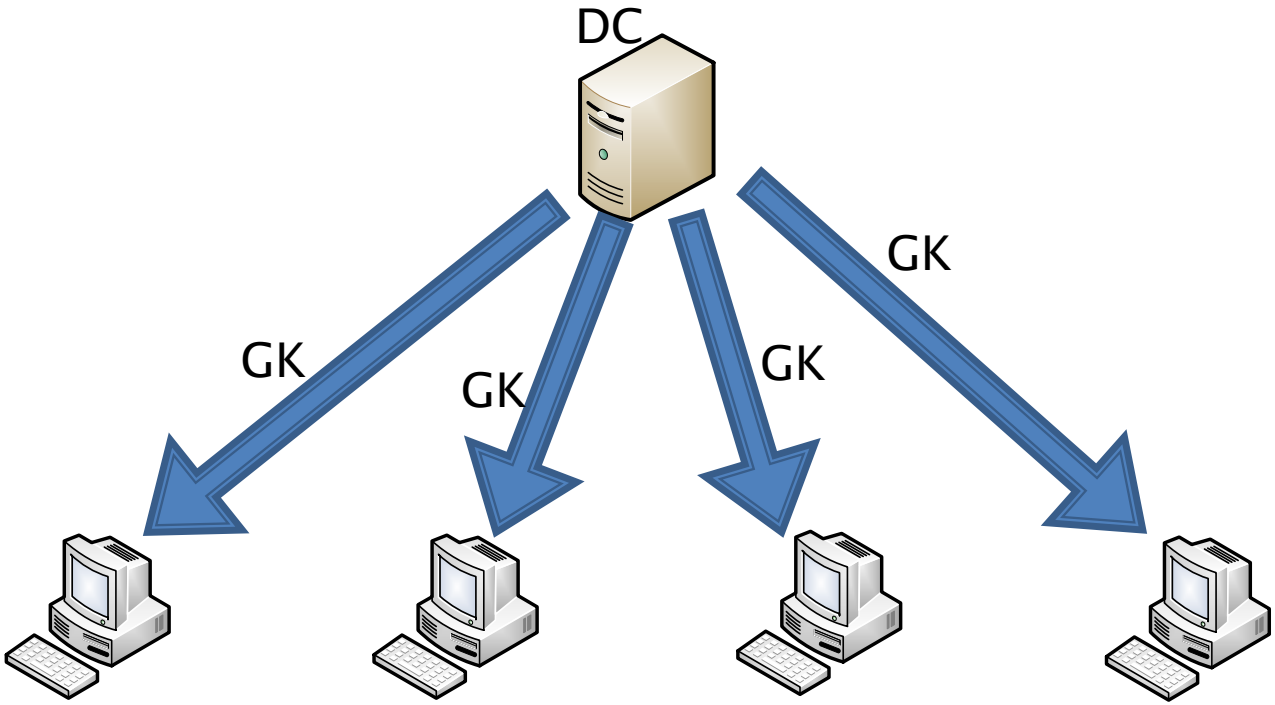
AS (Account Server): NTM端末のアカウントを管理する装置
DC (Direction Coordinator) : 仮想アドレスの配布と通信経路を指示する装置
RS (Relay Server) : 必要に応じてパケットを中継する装置

研究目的

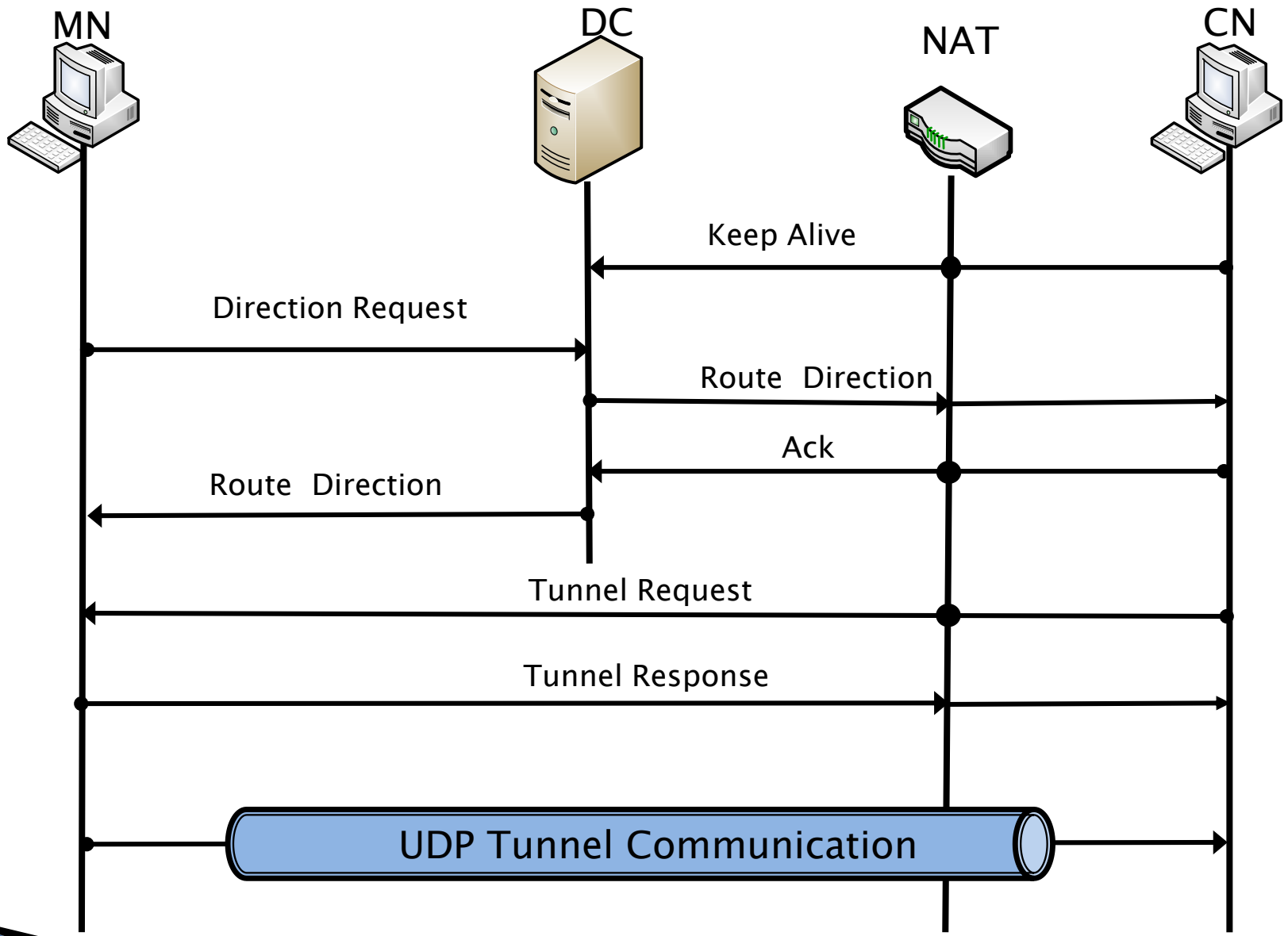
- NTMobileへグループ鍵を利用した相手認証機能を追加
  - 現状のNTMobileには相手認証機能がない
    - NTMobileをより安全にする

提案方式の構成

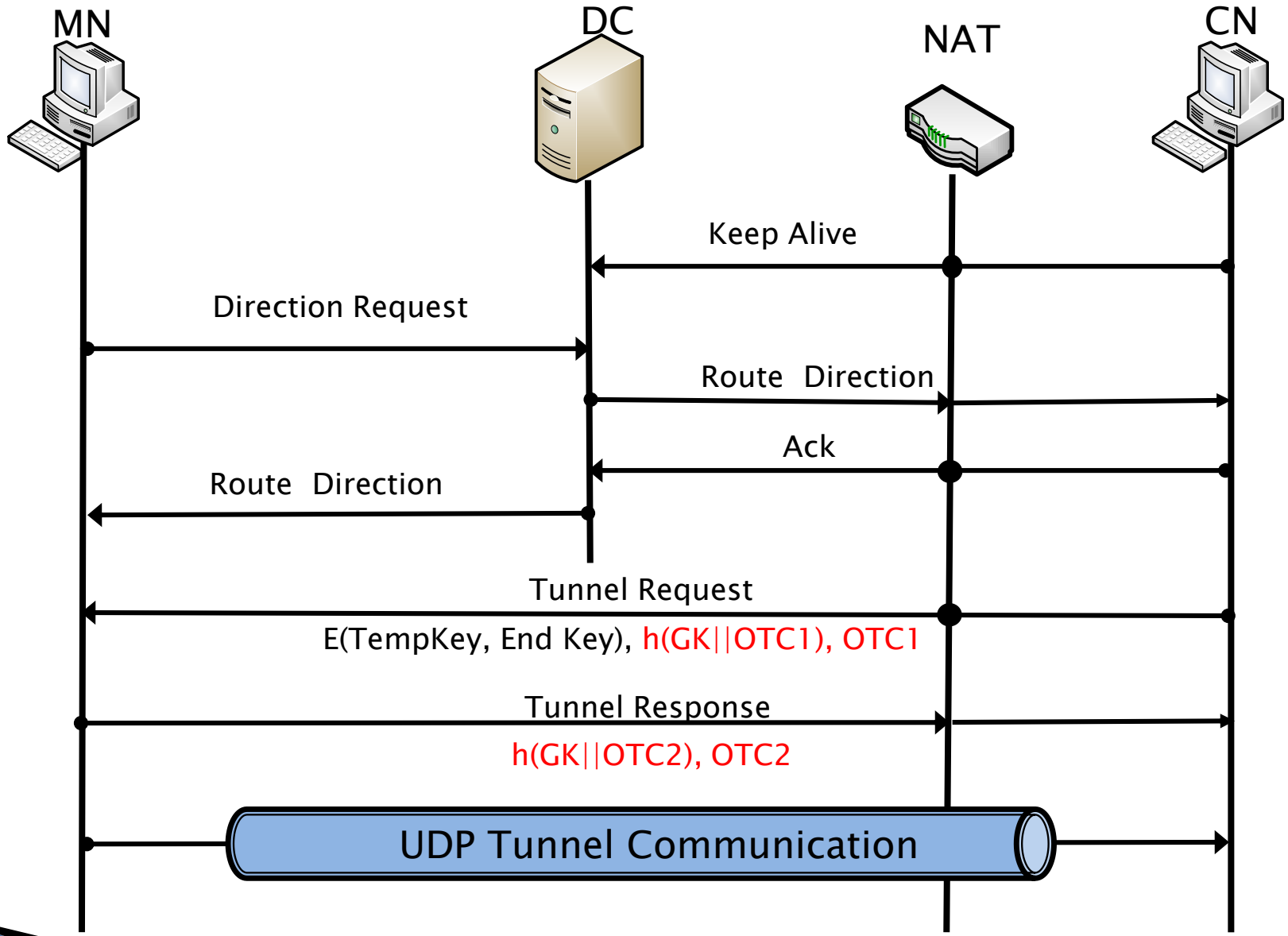
- エンド端末(MN,CN)
  - 事前にグループ鍵GKを共有している
    - グループ鍵はDCから配送
    - DCはすべての端末のIPアドレスを管理している



NTMobileのシーケンス



提案方式のシーケンス


MN
DC
NAT
CN
Keep Alive
Direction Request
Route Direction
Ack
Route Direction
Tunnel Request
E(TempKey, End Key), h(GK||OTC1), OTC1
Tunnel Response
h(GK||OTC2), OTC2
UDP Tunnel Communication

Tunnel Requestのパケットフォーマット

従来のパケットフォーマット

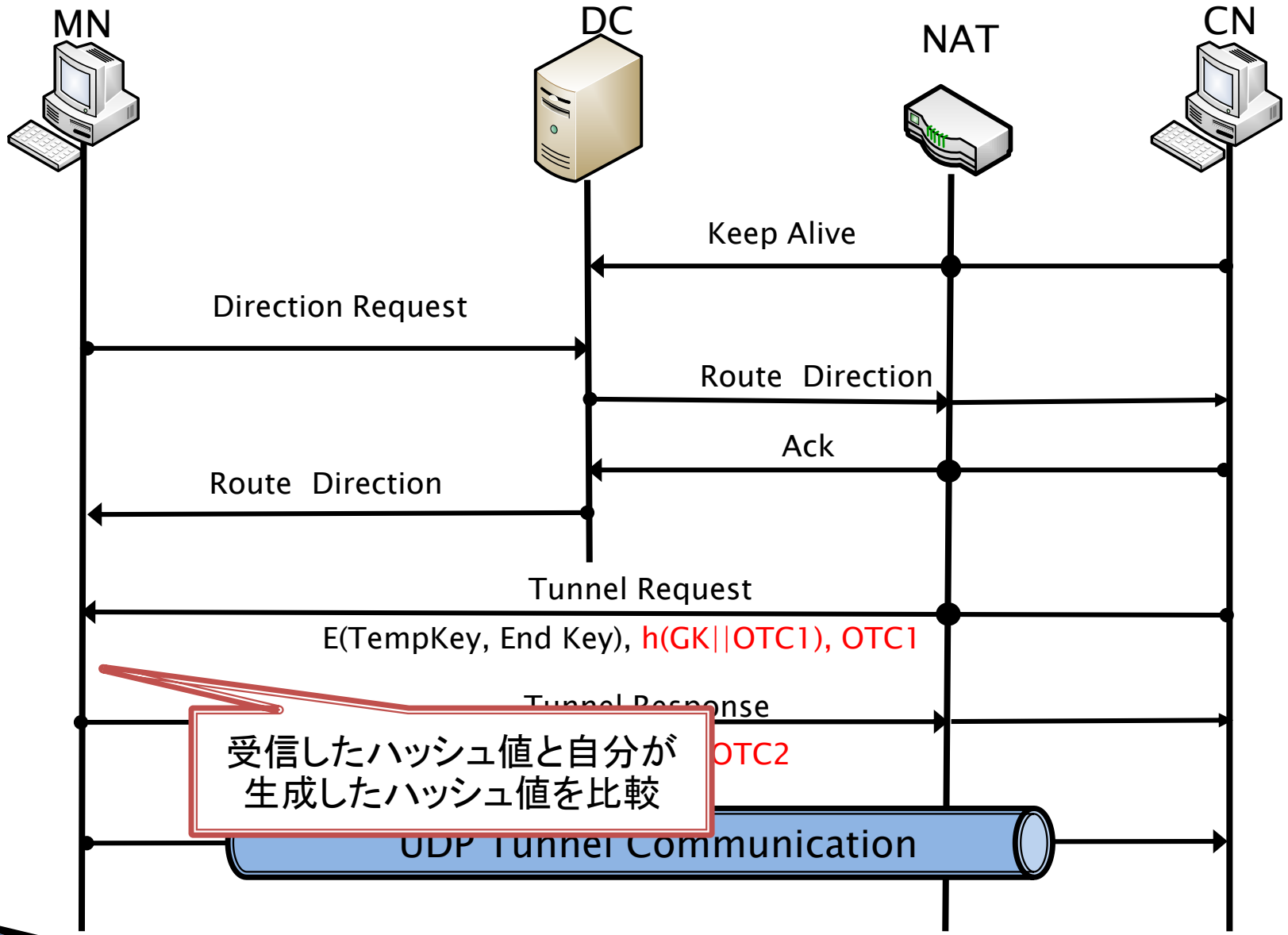
NTM Header
E(End Key, TempKey)
HMAC

提案方式のパケットフォーマット

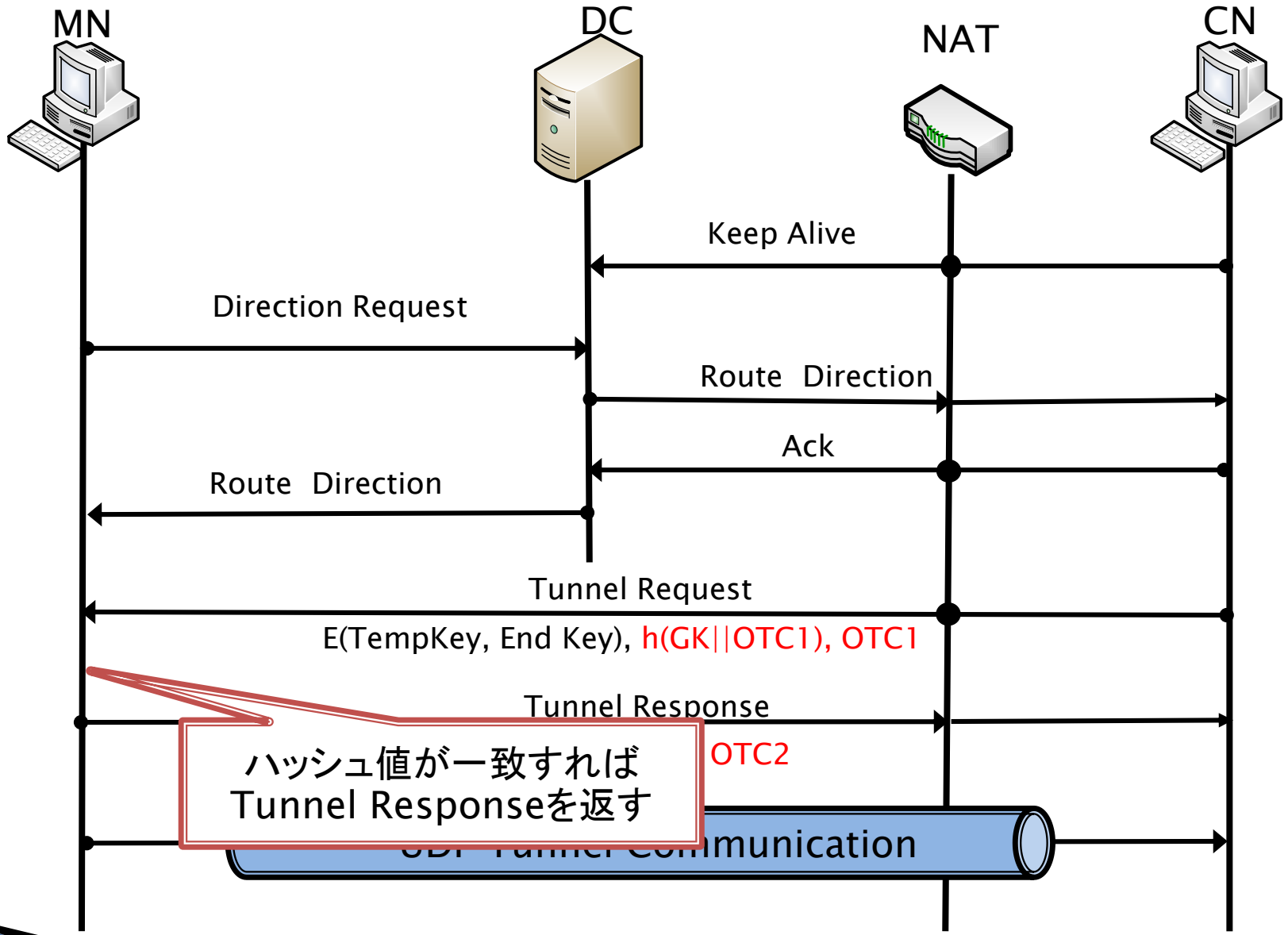
NTM Header
E(End Key, TempKey)
h(GK||OTC1)
OTC1
HMAC

- 従来のパケットにh(GK||OTC1)、OTC1を追加した
  - OTC1(One Time Code)は使い捨てで十分大きな乱数
  - h(GK||OTC1)はGKとOTC1のハッシュ値

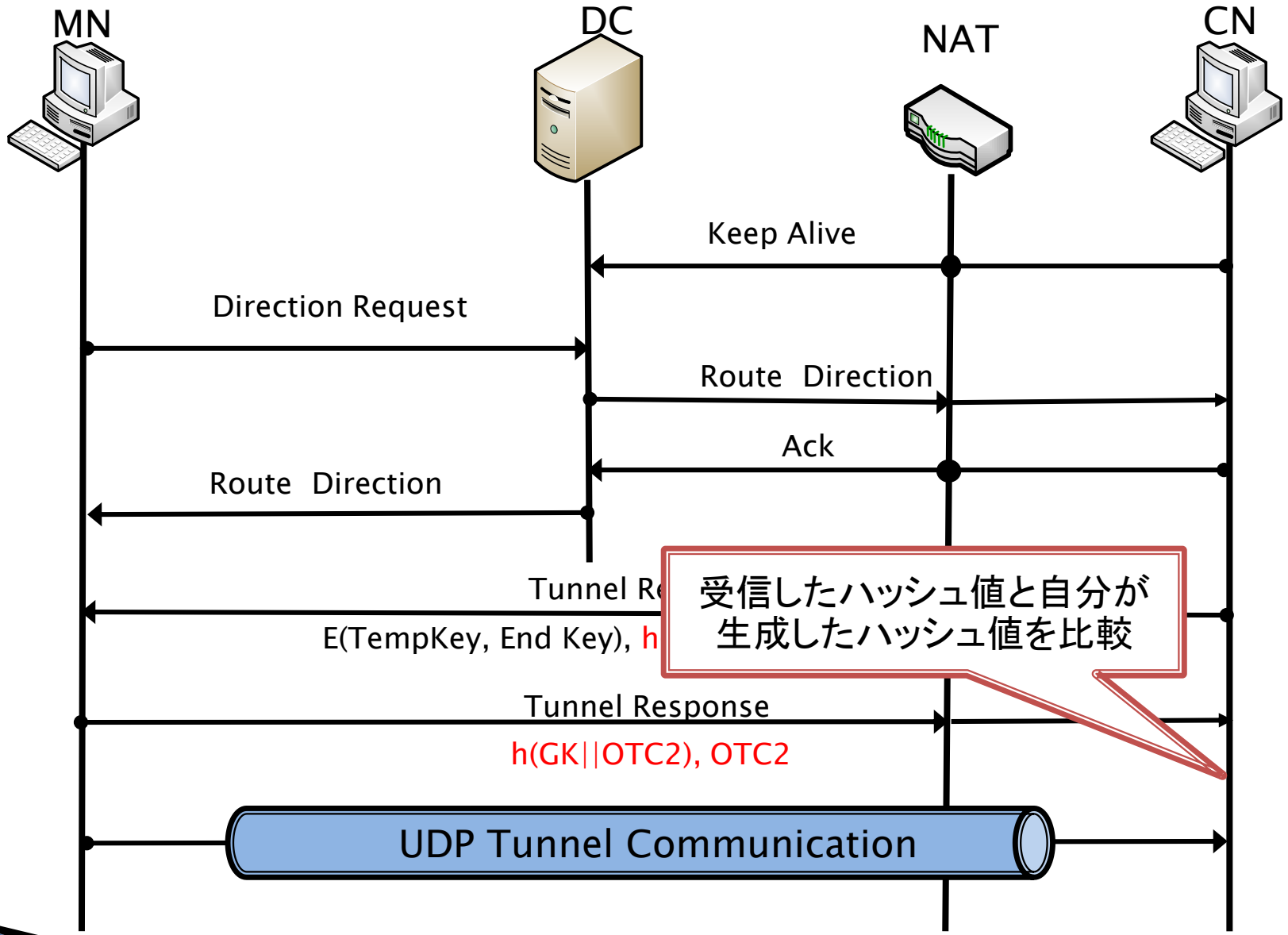
提案方式のシーケンス


MN
DC
NAT
CN
Keep Alive
Direction Request
Route Direction
Ack
Route Direction
Tunnel Request
E(TempKey, End Key), h(GK||OTC1), OTC1
Tunnel Response
OTC2
受信したハッシュ値と自分が
生成したハッシュ値を比較
UDP Tunnel Communication

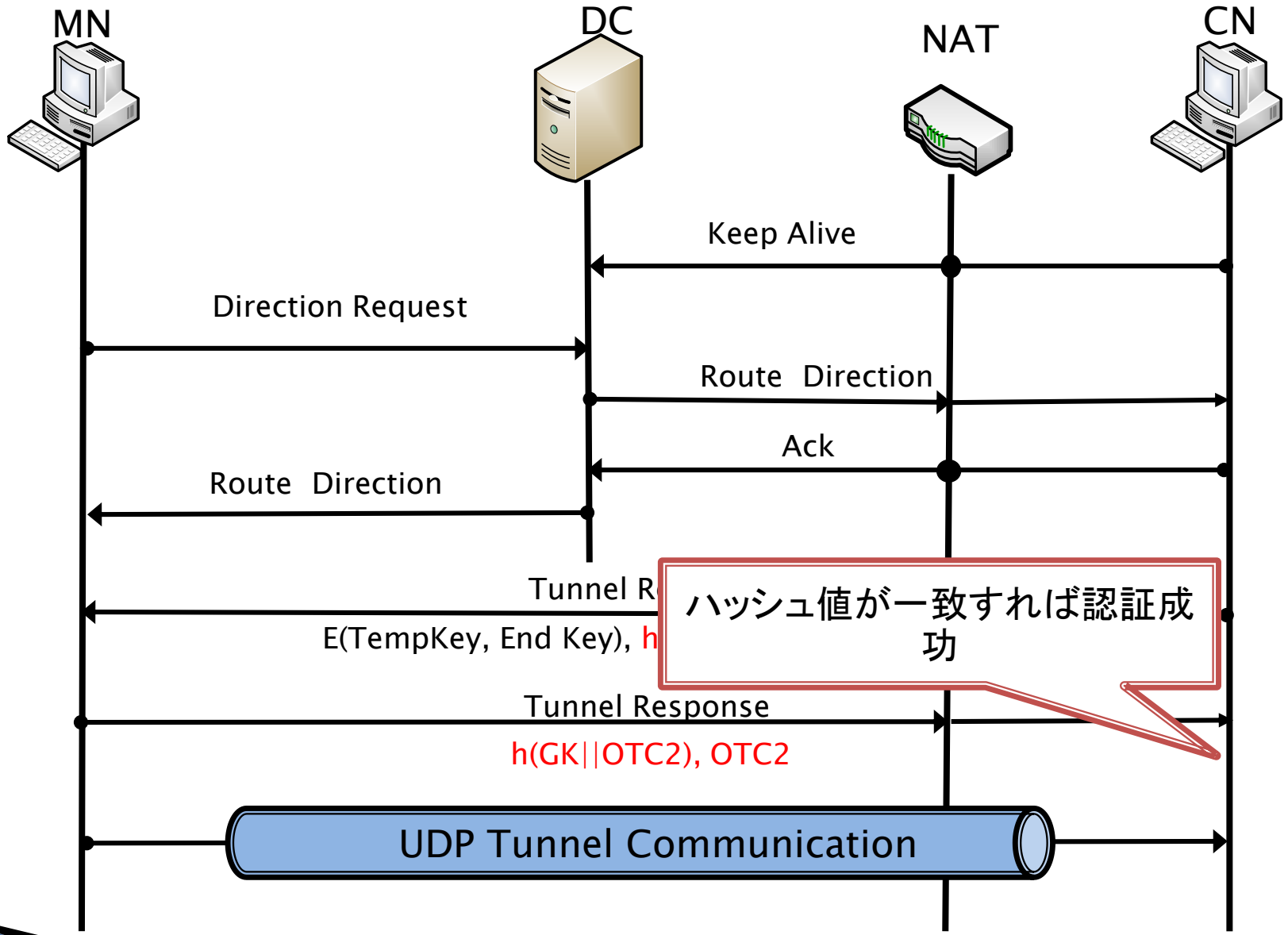
提案方式のシーケンス


MN
DC
NAT
CN
Keep Alive
Direction Request
Route Direction
Ack
Route Direction
Tunnel Request
E(TempKey, End Key), h(GK||OTC1), OTC1
Tunnel Response
OTC2
ハッシュ値が一致すれば
Tunnel Responseを返す
UDP Tunnel Communication

提案方式のシーケンス


MN
DC
NAT
CN
Keep Alive
Direction Request
Route Direction
Ack
Route Direction
Tunnel Re
E(TempKey, End Key), h
受信したハッシュ値と自分が
生成したハッシュ値を比較
Tunnel Response
h(GK||OTC2), OTC2
UDP Tunnel Communication

提案方式のシーケンス


MN
DC
NAT
CN
Keep Alive
Direction Request
Route Direction
Ack
Route Direction
Tunnel R
E(TempKey, End Key), h
ハッシュ値が一致すれば認証成功
Tunnel Response
h(GK||OTC2), OTC2
UDP Tunnel Communication

まとめ

- NTMobileへグループ鍵を利用した相手認証機能の追加を検討
  - 事前に共有されているグループ鍵を利用
- 今後の方針
  - 実装評価を行う