高セキュアーな SDN サービスを実現ディザスタリカバリ（HS-DRT）の研究

Study of the HS-DRT for realizing high secure SDN services

（HS-DRT：**H**igh **S**ecurity – **D**istribution and **R**ake **T**echnology for Disaster Recovery）

○古川雅大　三石広樹　鈴木秀一　上野洋一郎　宮保憲治

○M. Furukawa, K. Mitsuishi, S. Suzuki, Y. Ueno, N. Miyaho

東京電機大学大学院　情報ネットワーク環境研究室

Tokyo Denki University, Department of Information Environment School

Graduate School of Information Environment Technology

〒270-1382　千葉県印西市武西学園台 2-1200　電話/FAX(0476-46-8632/ 0476-46-8449)

〒270-1382, 2-1200 MuzaiGakuendai, Inzai, Chiba, Phone/Fax (0476-46-8632/ 0476-46-8449)

E-mail address: 14jkm16@ms.dendai.ac.jp

近年，災害時に無線基地局や，キャリアの局社が破壊された場合等の緊急の通信手段として，アドホックネットワークを利用する研究が注目されている．通常はインフラストラクチャモードで，基地局と通信しているモバイル端末は，基地局が倒壊等で被災した場合には，アドホックモードでネットワークを構築して通信再開を実現する技術が提案されている．しかしながら，アドホックネットワークでは，ユーザ端末がパケットデータを中継するノードの役割も同時に担うため，盗聴や改竄が比較的容易に実施できる問題点がある．

本稿では，送信パケットデータを一体化処理（データを空間的に撹拌してビット列をランダム化する処理）後に，分散保存する DRT(Disaster Recovery Technology)技術[1]を用い，上記のアドホックネットワークにおいて，セキュアー通信を実現する方式を提案する．

提案技術の概要を図 1 に示す．例えば局舎 A と無線基地局 X を結ぶ回線が災害等で遮断された場合には，通常は無線基地局 X,Y 間でアドホックネットワークを構築する．一方，アドホックモードが可能な場合には，モバイル端末 **a** は無線基地局 X から局舎 A を経由したインターネットには接続せず，無線基地局 X から無線基地局 Y，局舎 B を経由してインターネットに接続することも可能である．ここで，ルーチング制御等を行うコントローラは，クラウド等の設備を活用し，冗長化して無線基地局 X,Y に接続され，災害時にはアドホックネットワークを使用した通信への切り替え，経路情報の制御，暗号鍵の管理等を行う．コントローラと無線基地局間の通信は制御パケットの流通に対応するだけで十分なため，高速回線の確保は不要である．制御パケットには暗号鍵情報，経路情報等の重要データが含まれるため，データパケット送信用ネットワークと分離して運用することが望ましい．従来はモバイル端末 a から送信する際に AES 等の暗号化を施し，AODV 等で決定された単一経路を使用して無線基地局 Y にデータを送信する．この場合，悪意あるユーザのモバイル端末が中継ノードであると，送信されたパケットデータを全て盗聴し，保存することが可能になる．当該信号は AES 等で暗号化されているため，暗号鍵を時間帯で変化できる場合には，リアルタイム解読は困難である．しかしながら，保存されたデータを，後で解析できる可能性は存在する．本提案技術においては，AES 等で暗号化されたデータ

パケットを無線基地局 X で, 複数の受信データパケットに対して一体化処理，分割，シャッフリングによる再暗号化を施し，同時に複数の中継経路を使用して当該パケットを送信する特徴を備えている．暗号化に使用する分割数等の鍵情報(メタデータ)は, コントローラが作成し，無線基地局 X，Y に通知する．無線基地局 Y では，暗号化されたパケットをコントローラから通知されたメタデータを用いて復号化し，局舎 B に送信する．この仕組みにより復号化を行うため，メタデータと全ての暗号化されたデータパケットが揃わない限り，第三者による復号化は不可能となる. 例えば，図 1 の場合には，3 つの経路上の全てのデータの盗聴を行わない限り, 復号化は不可能である．

図 2 に，具体的な無線基地局 X での一体化処理に基づく暗号化手順を示す．無線基地局 X は受信した N 個のパケットをバッファに格納する．バッファリングされたパケット内のペイロードは, 一体化処理による可逆演算が施され，データビット列はランダム化される．具体的には, N 個のパケットのペイロードを 4 バイト毎に排他的論理和演算を行い，最後の 4 バイトと最初の 4 バイトを排他的論理和演算することにより，N 個のパケットデータはペイロードがランダムなビット列に変換される．その後，パケットを受信順とは異なる順番にランダムに並び替えて，データパケットを送信する．無線基地局 Y では，メタデータを元に受信したパケットの順番をもとの状態に戻し，復号化を行う．

本提案技術の実現に当たっては, 以下に述べる課題を解決する必要がある．まず, アドホックネットワーク上で活用可能な複数形路を決定するルーティングアルゴリズムを開発する必要がある．ルーティングアルゴリズムは経路探索の際に，電波強度，回線帯域などをメトリック値として用いて優先順位を決めることが望ましいこのように，幾つかの解決課題が存在するが，本技術はアドホックネットワークにおける第三者による盗聴を困難にするための有用な手段を提供できると考えられる．

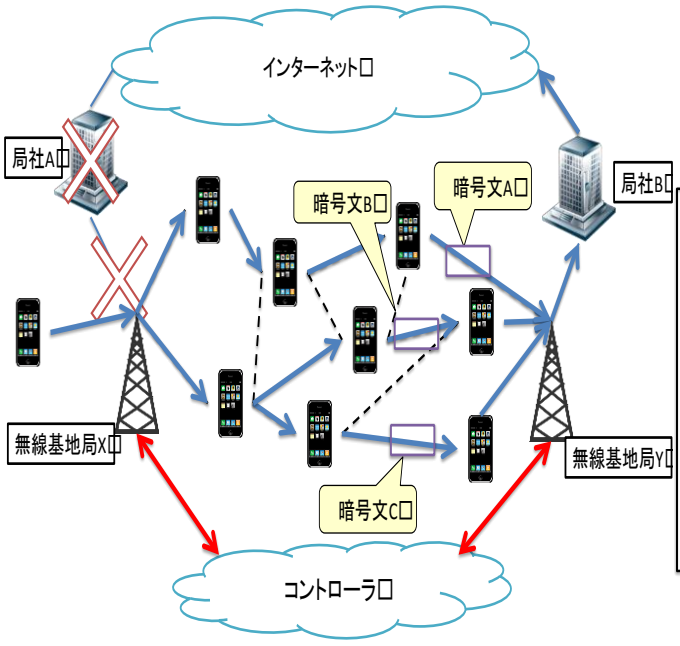

図 1.セキュアなアドホックネットワーク通信の概要

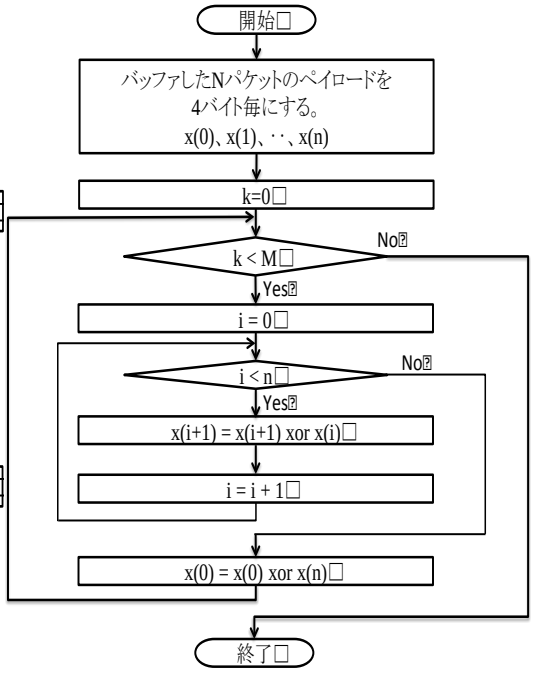

図 2. 無線基地局における一体化処理フロー

参考文献

[1] N.Miyaho, S.Suzuki, Y.Ueno, K.Mori, and K.Ichihara,"Study of a Secure Backup Network Mechanism for Disaster Recovery and Practical Network Applications" IARIA Journals, vol3, no.1, pp. 266-278, 2010.