講演番号： 85

SDN を活用したセキュアなデータセンタ間通信の性能評価

B－6 Performance Evaluation in Secure Communication service based on SDN

古川 雅大† 黒田 高希† 上野 洋一郎 宮保 憲治†
Masahiro FURUKAWA† Kouki KURODA† Youichirou UENO† Noriharu MIYAHO†
† 東京電機大学大学院情報環境学専攻
† Tokyo Denki University, Graduate School of Information Environment

1. はじめに

近年，データセンタ間通信におけるセキュリティが注目されている．既存のデータセンタ間通信手法として，IPsec を用いたVPN技術が存在するが，一つの経路を盗聴することにより、暗号化したパケットが解読される危険性があった．

筆者らは，DRT(Disaster Recovery Technology)技術[1]でパケットデータの断片を暗号化し，SDN(Software Define Network)技術を活用して各々の断片を別経路で送信することにより，盗聴に対してセキュアな通信法を検討した．

提案手法に基づいて，パケットの暗号化と転送に要するSDN スイッチ内処理時間を評価している[2]． 本稿では，提案手法で，転送に用いる複経路選択手法とエンドツーエンドのスループットを比較し，性能評価した結果を報告する．

2. 提案手法の概要

提案手法は，SDN スイッチで受信したパケットを，DRT による独自の暗号化処理を施し，暗号化されたパケットを複数のパケットに分割し，別経路で転送する．分割された断片パケットは，全ての断片が揃わないと復号が不可能である．そのため，断片を2つ以上の経路で分散転送することにより，1つの経路の盗聴では，通信データが復号できない，セキュアなデータセンタ間通信を可能にすることができる．

3. 実験概要

実験環境の概要を図 1 に示す．Linux サーバにパケットの暗号化と分割後に，トンネリング処理を行う DRT ブリッジを実装し，OpenFlow を用いて経路制御を行った．

Open vSwitch 間は，3 つのリンク(route①～③)を張った．Open vSwitch 間の 3 つの経路には，表 1 に示すように経路ごとの遅延時間を 4 パターン設定し，±5ms のゆらぎを設定した．3 つの経路から以下に示す経路制御方式 A～B の 4 つのルーティング方式により，2 つの経路を決定した．また，どの経路制御方式も，5 秒間隔で経路を更新した．

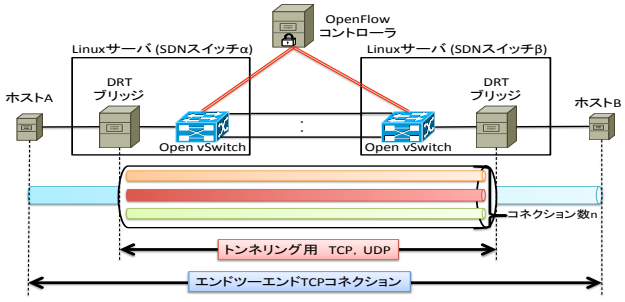

図 1 実験環境の概要

A) ラウンドロビン方式
B) RTT の平均時間が少ない 2 経路を選択する方式
C) ジッターの平均が小さい 2 経路を選択する方式
D) 経路遅延の差が小さい 2 経路を選択する方式

表 1 経路遅延時間の設定パターン

	Delay 1	Delay 2	Delay 3	Delay 4
route①	0ms	30±5ms	30±5ms	30±5ms
route②	0ms	0ms	30±5ms	30±5ms
route③	0ms	0ms	0ms	30±5ms

経路制御方式，遅延時間設定毎の，ホスト A，B 間のスループットを計測した実験結果を図 2 に示す．どの経路遅延パターンに対しても，経路制御方式 D が他の方式に比べて，スループットが安定的に高い値となることが判明した．特に，経路遅延時間の設定パターン 3 では，route①，②の経路遅延時間の差が少ない 2 経路を選択する経路制御方式 D が一番高いスループットを得られることが判明した．すなわち，DRT 用のアプリケーションでは，2 経路選択時に，スループットに与える影響が大きいメトリックは個別経路の遅延時間ではなく，選択経路の遅延差であることが分かった．

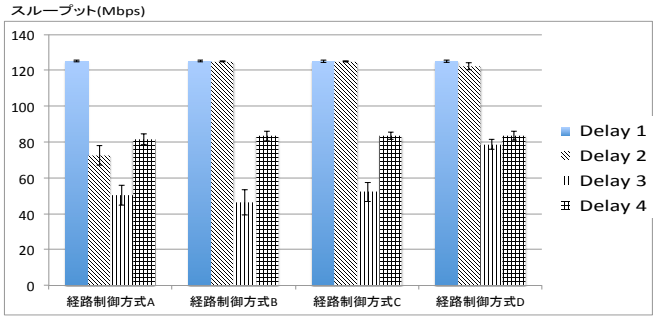

図 2 実験結果

4. まとめと今後の予定

提案したセキュアなデータセンタ間通信における経路制御手法では，選択する経路遅延時間の差がスループットに影響を与えることを示した．今後は，パケットロス率を考慮した経路選択手法の検討と性能評価を行う予定である．

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, vol.3, no.1,pp. 266-278, 2010.

[2] M.Furukawa, K.Kuroda, T.Ogawa, and N.Miyaho , “Highly Secure Communication Service Architecture using SDN Switch,” EICE 10th APSITT, 2015