1Z-5

オープンフロースイッチを活用した高セキュアーなSDNサービス実現法の性能評価

古川　雅大† 宮保　憲治† 鈴木　秀一† 上野　洋一郎† 黒田　高希†

東京電機大学情報環境学部†

1. はじめに

近年，拠点間通信のセキュリティに対する関心が高まりつつある．現在，IP-VPN，インターネットVPN 等の複数の拠点間通信の実現方法が存在するが，サービス料金や暗号強度などの点で多くの課題が存在する．

本稿では，一体化処理と呼ばれる，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の後に，分散保存する DRT(Disaster Recovery Technology)技術[1]のSDN (Software Define Network)サービスへの適用方式を提案する．具体的には，当該手法を用いたセキュア拠点間通信を提案し，一体化処理のパラメータが，エンドツーエンドのスループットに与える影響について評価した結果を述べる．

2. 拠点間通信における課題

拠点間通信を実現する方法としては，IP-VPN 等の専用網を使用する方法と，インターネットVPN 等のインターネットを使用した方法が商用化されている．

IP-VPN は通信事業者が独自に構築した閉域 IP 網(専用網)を介して構築されているため，安全性は高い．しかしながら，遠距離，高スループットの IP-VPN を高負荷トラヒックの転送に利用する場合はコストが増加する課題を解決する必要がある．

一方，インターネットVPN では IPsec を用い，ネットワーク上で暗号化することにより，安全性を確保している．IPsec では暗号化アルゴリズムを選択できるが，一般的には AES が用いられることが多い．AES では計算量が鍵長，データサイズが増加するに従って指数関数的に増加することが知られており，現在は，鍵長として128bit，256bit が活用されている．暗号強度を更に高めるためには，鍵長を増やす必要があるが，データサイズを増加する場合には，天文学的な計算量が必要となり，処理時間が増加する課題が存在する．また IKE(Internet Key Exchange)を使用した鍵交換アルゴリズムでは，コネクション確立までのシーケンスが複雑であり，通信開始までの処理時間も長くなるという課題もある．

3. セキュア拠点間通信の提案

提案するセキュア拠点間通信の構成例を図 1 に示す．提案方式では，SDN 技術の一つである OpenFlow を使用する．OpenFlow は OFS(OpenFlow Switch)に到着したパケットの処理方法は OFC(OpenFlow Controller)が決定し，OFS にパケット制御用の指示を行う．提案方式では，OFS に一体化処理機構を組み込むことにより，OFS 間での通信を暗号化する．一体化処理に必要なパラメータ(以下，メタデータと呼称する)は OFC が管理し，OFCα，OFCβで共有する．一体化処理時はメタデータが暗号解読用の鍵となるため，メタデータの送信には安全性を考慮し，IP-VPN を使用する．メタデータのファイルサイズは送信データに比べて非常に小さいため，メタデータの送信経路である IP-VPN のスループットは低くても問題なく，コスト増加は抑えることができる．一方，OFS 間の通信にはインターネットの活用が適している．OFSαに到着した n 個のパケットに対し，高速ストリーム暗号を用いた暗号化と一体化処理を行い，パケットの順番をランダムに並び替え，別経路で OFSβに送信する．OFCαはメタデータを OFCβに送信する．OFSβは OFCβから受信したメタデータを用いて，逆一体化処理，復号を行う．上記の手順により OFSα，β間で，低コストでかつセキュアな通信が実現できる．

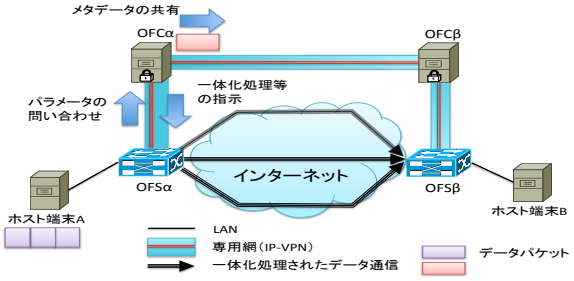

図 1:セキュア拠点間通信の構成例

4. 実験環境

本手法を高速で実現するには，OFS にストリーム暗号や一体化処理機構を実装する必要があるが，現状では実際のスイッチに早期に実装することが困難である．このため，第一段階としては，機能検証，特に一体化処理に主眼を置き，それぞれのホスト端末と OFS の経路上にストリーム暗号，一体化処理，シャッフリングを行うソフトウェアブリッジを配置し，一体化処理がエンドツーエンドのスループットに与える影響の実験・評価を行った．

実験環境の全体構成を図 2 に示す．本実験では OFC からパラメータの通知，メタデータの共有は行わず，データ処理用のパラメータは事前にソフトウェアブリッジに配置した．また，OFS はラーニングスイッチと同様の処理を行うように OFC を設定した．

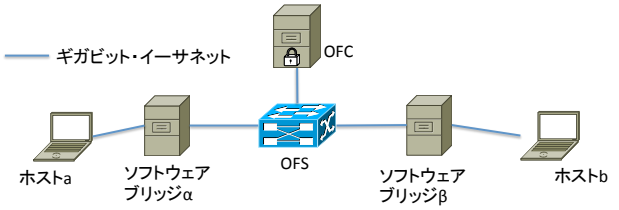

図 2:実験環境の全体構成

5. 実験方法

本実験では，ソフトウェアブリッジα，βにおける一体化処理のパラメータを変動させ，ホスト a，b 間の TCP

Evaluate of the high security SDN service by making use of OpenFlow Switch

† Tokyo Denki University School of Information Environment

通信のスループットを iperf[2]を使用して計測した．

一体化処理のパラメータは，バッファリングパケット数 N と，演算回数 M の 2 つを変動させた．バッファリングパケット数 N は，受信パケットをすぐには中継転送せずに，バッファ内に一旦，保存する際のパケット数を示す．N 個のパケットデータが集まった段階で，一つのデータとしてストリーム暗号，一体化処理を行い，N 個のパケットに再分割した後，ランダムな順に送信する．演算回数 M は，全ビット列を対象としてランダム化する処理の繰り返し演算回数を示す．

一体化処理フローを図 3 に示す．本実験では N 個のパケットのペイロードを 4 バイト毎に一体化処理された直前のブロックと次ブロックの排他的論理和演算を行い，これら一連の処理を M 回繰り返す．

バッファリングパケット数 N=10 のとき演算回数 N を 1～20 まで変動させた場合(実験 1)と，演算回数 M=6 のときバッファリングパケット数 N を 1～15 まで変動させた場合(実験 2)のホスト a，b 間の TCP 通信のスループットを計測・評価した結果を次章に述べる．

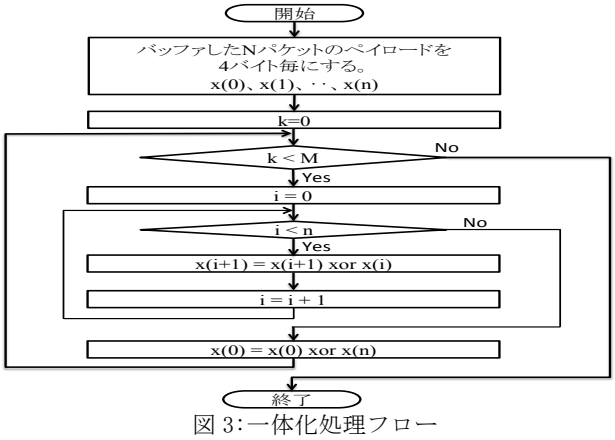

図 3:一体化処理フロー

6. 結果と考察

実験 1 の結果を図 4 に示す．実験 1 では演算回数 M が 3 回まではスループットが低下せず，それ以降は，演算回数が増加するに従って，スループットが低下し，収束傾向を示す結果が得られた．演算回数 M はスループットに影響を与えるため，M の選定に当たっては通信に必要なスループットと，セキュリティ強度の双方を考慮する必要がある．

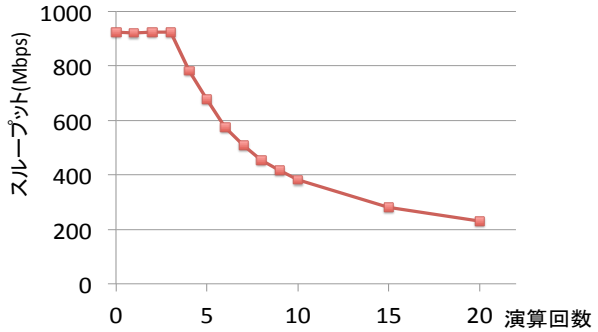

図 4:演算回数が変化した場合のスループット(実験 1)

実験 2 の結果を図 5 に示す．実験 2 では，バッファリングパケット数 N が N=1～15 までの間はバッファ処理時間の変動はあるものの，エンドツーエンドのスループットは変化しない結果が得られた．N>=16 の環境ではエンドツーエンドの通信が不安定となり，計測を実施できなかった．実験 2 での N>=16 の際に正常通信が実施できなかった理由は，エンドツーエンドで TCP を使用してスループット測定を行ったため，パケットバッファリング処理の間に，ホスト a の最初のパケットがタイムアウトする頻度が増え，TCP の再送制御が多発したことが原因と考えられる．

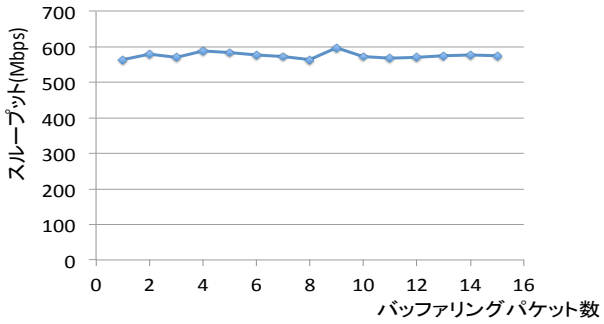

図 5:バッファリングパケット数の変化時のスループット(実験 2)

N<=15 ではエンド・エンドのスループット変動がほとんど無いことから，適切な制御を行えば，バッファリングパケット数 N はスループットに影響を与えない通信環境が実現できると思われる．N 個のパケットデータを一つのデータとしてストリーム暗号処理後に，一体化処理を行い，N 個のパケットに再分割した後，ランダムな順に送信するため，第 3 者による暗号解読には，バッファリング パケット数 N が偶然に知られた場合においても，N!個の組み合わせ検証が必要となる．このため，スループットに影響を与えることなく，セキュリティ強度の向上が図れる通信方式を実現できると考えられる．ただし，復号の際にはすべてのパケットが必要なため，一つのパケットが紛失した場合には，全パケットの再送が必要になり，スループットが低下することが考えられる．従って，ネットワークの品質とセキュリティ強度の双方を考慮し，パケットバッファリング N を設定する必要がある．加えて，本手法に適したタイムアウト処理，パケットロス時の高率的な再送制御を新たに検討する必要がある．

7. むすび

本稿では高セキュアな SDN サービスの提案と，高セキュアな通信を実現するための一体化処理に必要なパラメータがエンドツーエンドのスループットに与える影響を評価した．

本実験により，スループットを下げることなくセキュリティ強度を向上できる可能性を示したが，現状の TCP 通信におけるフロー制御では，対応が困難となる場合があることが判明した．今後は，本手法に適したフロー制御方式とインターネットを介した性能評価，および複数形路を使用したデータ配送方式の検討を進める予定である．

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, vol3, no. 1, pp. 266-278, 2010.

[2] iperf (https://code.google.com/p/iperf/) 2014.1.10 取得