5W-3

iSCSIターゲットにおける安全な通信を行うシステムの実装と性能評価

神坂 紀久子† 山口 実靖‡ 小口 正人†
†お茶の水女子大学 ‡東京大学生産技術研究所

1. はじめに

近年，ストレージシステムに格納するデータ量と管理コストが急増しているため，ストレージ群とサーバ群を高速なネットワークで接続し，ストレージ統合と集中管理が可能なSAN(Storage Area Network)への関心が高まっている．現在では，TCP/IPネットワークを介したSAN接続を可能にするIP-SANが提案されており，そのIP-SANで用いられる主要なプロトコルとして，iSCSIが有力視されている．iSCSIでは，SCSIコマンドをTCP/IPパケットにカプセル化することで，サーバ(イニシエータ)とストレージデバイス(ターゲット)をIPネットワーク経由で接続する．これにより，安価なコストでSANを導入，管理することが可能になる．

iSCSIは通信の性能に関していくつかの課題を持つ．広帯域のネットワークでストレージアクセスを行う際には，TCPプロトコル処理がサーバの負荷を増大させる．また，iSCSIネットワークでセキュアな通信を行うためにはIP層で認証と暗号化を行うセキュリティ技術であるIPsecを用いることができる．しかし，IPsecを利用すると，主に用いられる暗号化アルゴリズムである3DES(Triple Data Encryption Standard)の暗号化処理の計算量が多いだけでなく，非効率的な処理を行うことによって，性能低下につながり，高いCPU負荷の原因となる．セキュリティとパフォーマンスはトレードオフの関係にあるため，暗号化などのセキュアな通信を行いながら可能な限り性能を落とさないように工夫する必要がある．

そこで本稿では，IP-SANを利用した安全なストレージアクセス実行時の性能低下に関する問題点について述べ，その解決手法を提案し，実装方法，スループットのモデリングについて議論を行う．

2. IP-SANにおける暗号化の問題点と解決手法の提案

2.1 IPsecの問題点

iSCSIネットワークにおいてIPsecを利用したシーケンシャルリードアクセスの評価実験を行った．その結果，スループットが大幅に低下し，CPU負荷が非常に高くなることがわかった．解析した結果として，IP層と同位のIPsec層において，小さなサイズに分割されたデータブロックごとに暗号化をしてから転送する処理が性能に大きな影響を与えていることがわかった[1][2].

IPsecを用いる場合には，IPsecはTCPなどの上位層における処理を知ることができないため，効率的な暗号化処理を行うことは困難である．大規模なデータをシーケンシャルにアクセスする場合には，IPsecは上位層であるTCP層などから，データブロックを受け取った時点で，順次暗号化処理を行い，そのまま下位層に渡す．この際，上位層で分割された小さなパケットごとに暗号化処理を行うため，効率的な処理をしているとはいえない．

2.2 予備評価実験

IPsecを用いる方式と上位層で暗号化する提案手法の簡易実装を用いた予備評価実験を行った[3][4][5]．まず，基礎実験として，iSCSIを用いない単純なソケット通信による実験を行った．次に，iSCSIネットワークでイニシエータからターゲットのrawデバイスに対してシーケンシャルリードアクセスを行った場合の性能を評価した．予備評価実験においては，Target側の実装は簡易実装であり，暗号化を行ったデータをあらかじめディスクに格納し，シーケンシャルリードアクセスを行う際に，その暗号化されたデータをディスクから読み出している．予備評価実験における提案手法の上位層における暗号化には，OpenSSLのcyrptoライブラリで実装されている3DESを用いた．これはIPsecで用いられているものと同じ暗号化アルゴリズムであり，実装コードもほぼ同様である．

iSCSIを用いない単純なソケット通信においては，提案方式である上位層における暗号化の際には，スループットが30%向上し，CPU負荷も約3%軽減されるという結果が得られた．

また簡易実装を用いた実験においては，理想的なケースをモデル化した場合における比較であるが，提案方式はIPsecを用いた方式に比べ，スループットが約17%の性能向上がみられ，全体のCPU使用率が平均で8%減少した．

2.3 提案手法

本稿では，安全なiSCSIストレージアクセスにおける性能を向上させるため，従来のIPsec層で暗号化を行う代わりに，ミドルウェアとしてより上位層で暗号化，復号化処理を行う手法を提案する．提案手法の実現方式を図1に示す．提案方式の場合には，IPsec層より上位で暗号化，復号化を行うため，まとまったブロックを処理することができ，IPsecを用いて小さなパケットごとに暗号化を行うよりも効率的であると考えられる．

また，上位層で暗号化，復号化処理をすることによって，柔軟な処理が可能になり，ユーザ空間で並列プロセスを起動させ，前のパケットの暗号化・復号化サイクルが完了しないうちに次のパケットの処理を始めるという最適化を行うことできる．暗号化処理時間を通信処理の待ち時間に隠蔽することによって，効率的な暗号化を行

Implementation and Performance Evaluation
of Secure Communication System in iSCSI Target
† Kikuko Kamisaka, Masato Oguchi
‡ Saneyasu Yamaguchi
Ochanomizu University (†)
Institute of Industrial Science, The University of Tokyo (‡)

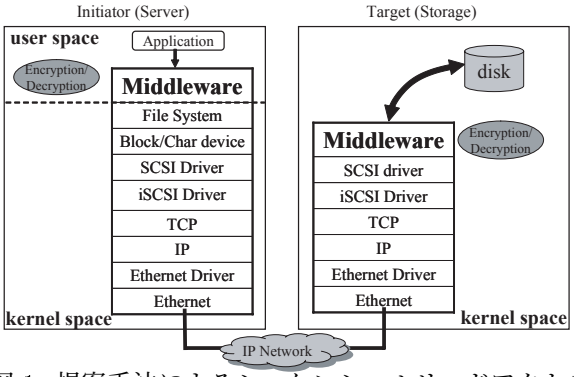

図 1: 提案手法によるシーケンシャルリードアクセス

うことができ，性能を向上させる手法として有効である．

3. 提案手法のターゲット側における実装

iSCSI イニシエータにおいては，提案手法をユーザ空間で実装し，ターゲット側においては，カーネル空間で実装している．本節では，ターゲット側における実装方法について説明する．

SCSI デバイスドライバはカーネル空間で処理を行うため，提案手法である上位層における暗号化・復号化処理をカーネル空間で実行する必要がある．そこで，提案手法のターゲット側では，3DES アルゴリズムを使用した暗号化，復号化処理を実装し，それをカーネルモジュールとして提供してカーネル空間での処理を行っている．

カーネルモジュールとして提供することにより，カーネルを再コンパイルすることなく，暗号化，復号化の機能を利用することができ，また，SCSI デバイスドライバからの独立性を高めることによって，提案手法をミドルウェアとして提供することが可能になる．さらに，上位層で処理を行うことによって，下位層の処理内容を把握して，柔軟な処理を行うことが可能になる．

従来のターゲット側の実装を図 2 に，提案手法であるミドルウェアとして暗号化・復号化処理を提供する実装を図 3 に示す．ミドルウェアとして自作モジュールを起動し，SCSI デバイスドライバから暗号化，復号化ルーチンを呼び出すことにより，上位層における処理が可能となった．

4. スループットモデル化

提案手法の性能評価を行う際の指標として，シーケンシャルリードアクセスにおけるスループットのモデリングを行った．

イニシエータから SCSI Read コマンドをターゲット側に転送し，暗号化されたデータが復号化されるまでを 1 サイクルとすると以下のようになる．

1 サイクルに要する時間
$= RTT(RoundTripTime) +$ データ転送時間 $+$ 暗号化時間 $+$ 復号化時間

$$\text{データ転送時間} = \frac{\text{データサイズ}}{\text{下位層のスループット}}$$

$$\text{暗号化時間} = \frac{\text{データサイズ}}{\text{暗号化速度}}$$

である．下位層のスループットとは，提案手法を使用せずに測定した iSCSI のスループットである．よって，スループットは，次の式でモデル化することが可能である．

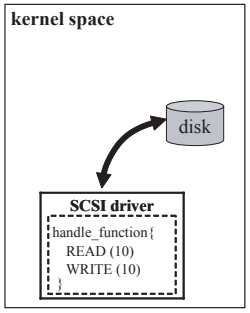

図 2: 従来の Target 実装

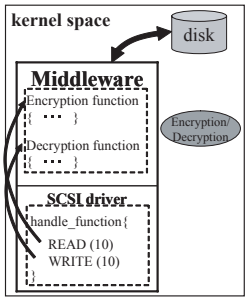

図 3: 提案手法の Target 実装

スループット

$$= \frac{\text{ブロックサイズ}}{RTT + \frac{\text{ブロックサイズ}}{\text{下位層の速度}} + \frac{\text{ブロックサイズ}}{\text{暗号化速度}} + \frac{\text{ブロックサイズ}}{\text{復号化速度}}}$$

一方，最適化を行った後のスループットモデルは，

スループット

$$= \frac{\text{ブロックサイズ}}{RTT + \frac{\text{ブロックサイズ}}{\text{下位層の速度}} + \frac{\text{ブロックサイズ}}{\text{暗号化速度}}}$$

とモデル化することができる．

5. まとめと今後の課題

本稿では，IP-SAN を利用した安全なストレージアクセスを実現するために，IPsec の代わりにその上位層で暗号化する方式を提案し，iSCSI ターゲット側での提案手法の実装を行った．また，提案手法のスループットのモデル化について議論した．今後の課題としては，われわれの実装において，総合的な性能評価を行う．また，並列プロセスを利用することによって，通信の待ち時間に次のパケットの暗号化処理を行う最適化などの場合における性能を評価する．

参考文献

[1] 山口 実靖，小口 正人，喜連川 優: “iSCSI 解析システムの構築と高遅延環境におけるシーケンシャルアクセスの性能向上に関する考察”, 通信学会論文誌, Vol. J87-D-I, No. 2, pp. 216–231, 2004 年 2 月

[2] 神坂 紀久子，山口 実靖，小口 正人: “IPsec を利用した iSCSI ストレージアクセス時の TCP パケット転送の解析”, 情報処理学会研究報告, 2004-HPC-97, HOKKE2004, pp. 145–150. 2004 年 3 月.

[3] 神坂 紀久子，山口 実靖，小口 正人：“IP-SAN を利用したセキュアなストレージアクセスにおける性能向上手法の提案と検討”, 第 3 回 情報技術レターズ, Vol. 3, LD-003, pp. 59–61，2004 年 9 月.

[4] 神坂 紀久子，山口 実靖，小口 正人: “iSCSI ストレージアクセスにおける安全な通信を行うシステムソフトウェアの検討”, 情報処理学会研究報告, 2004-OS-97, SWoPP2004, pp. 97–104. 2004 年 3 月.

[5] K. Kamisaka, S. Yamaguchi and M. Oguchi: “Performance improvement of an iSCSI-based secure storage access”, *Proc. the 16th IASTED International Conference on Pararellel and Distributed Computing and Systems (PDCS 2004)*, pp. 522–527. Nov. 2004.