7J-06

マルチノードコンピューティング(MEC)における SmartNIC への暗号化処理のオフロードの実装

宮川大輝† 李彦志† 深井貴明‡ 広渕崇宏‡ 菅谷みどり†
芝浦工業大学† 産業技術総合研究所‡

1. 背景

第 5 期科学技術基本計画において，2016 年に Society 5.0 が提唱された [1]．Society 5.0 では，サーバーが大量のデータを処理し，人間中心の社会の様々な活動を支える高度な AI 処理を行う．これにより，低遅延・高性能な計算資源を必要とするアプリケーションを提供することが可能になる．

Society 5.0 アプリケーションの要件を満たすために，高性能な計算資源を活用したマルチノードコンピューティングシステムが議論されている [2, 3]．マルチノードコンピューティングシステムの一つとして，Society 5.0 アプリケーションを低遅延で利用するために，GPU や FPGA などのアクセラレータを用いた高性能なハードウェアを統合したマルチノードエッジコンピューティング (MEC) システムも期待されている [4]．このシステムでは，複数のコンピュータ (ノード) のそれぞれにアクセラレータを搭載し，アクセラレータの特性を活かして大量の演算を行う．これらのノードは，図 1 で示すようにネットワークで接続され，一つの大規模なシステムを形成している．高い計算能力と応答性を持ち，Society 5.0 アプリケーションで要求されるような高い処理能力を提供するエッジコンピューティングに適している．

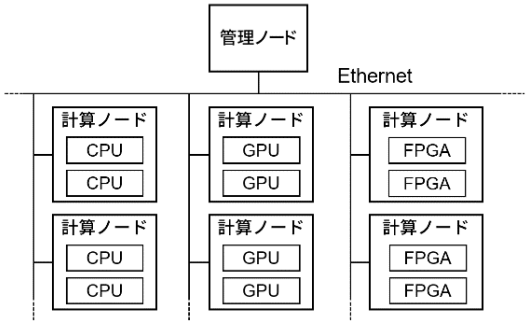

図 1：MEC システムの構成

2. 課題

Li らは，MEC の効率的なリソース管理のための MEC-RM を提案した [4]，MEC-RM は，各計算ノードへ効率的にジョブを割り当てる管理ノードのミドルウェアを提供している．ジョブのアロケーションを担っていることから，計算ノードの数の増加に伴い管理ノードの負荷は高くなる．また，MEC はエッジサーバーとしてセキュリティやプライバシーを考慮したデータの送受信を担う必要があることから，MEC-RM は通信を暗号化している．そのため，接続する多数のクライアントに対して，受信時は復号，送信時は暗号化しなければならない．Pismenny 氏らは，暗号化・復号処理に多くの CPU サイクルを費やすことを指摘した [5]．この点を踏まえると，ノード数が増え，もしくはデータ量が増大するごとに，管理ノードへの負担の増大が考えられる．

3. 目的

本研究では，MEC-RM において，計算ノードを管理するサーバーの処理の一部をオフロードし，負荷を軽減することを目的とする．

オフロード先のデバイスとして，SmartNIC の利用を検討した．SmartNIC は暗号化処理や圧縮処理など，ネットワークに関連する機能をサポートしており，CPU に代わって SmartNIC がこれらの処理を行うことで，CPU の負荷を軽減できる．今回は，前章の課題で述べたように，暗号化処理が負担となっている可能性を考慮し，暗号化処理のオフロードを実装し，性能評価を行う．

4. 提案実装

本研究では，SmartNIC (BlueField DPU) を使用し，MEC-RM [4]でも用いられている Nginx の暗号化処理のオフロードの実装を行った．図 2 の右側に実装の構成を示した．

Nginx の暗号化・復号処理を SmartNIC にオフロードするための手順は次の通りである．まず OS カーネルで Kernel TLS (kTLS) が有効であり，SmartNIC への暗号化・復号処理のオフロードに対応していることを確認する．次に OpenSSL を，kTLS を有効にするオプションを付けてビルドする．そしてその OpenSSL をリンクさせて Nginx をビルドする．

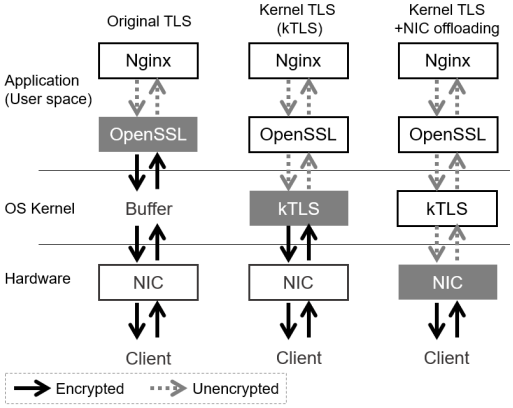

図 2：TLS 実装方法の比較
(灰色部分で暗号化・復号処理を行う)

5. 評価

評価実験では，実験用システムに Nginx をインストールし，HTTP サーバー機能を使用して行った．

実験では，あるファイルを wget コマンドで取得する操作を，100 ミリ秒の間隔で 100 回行った．操作にかかった時間を計測し，100 回分の値の平均値と標準偏差を算出した．この実験を，(1) TLS を使用しない場合，(2) OpenSSL を標準の状態 (TLS をユーザー空間で処理) で用いる場合，(3) kTLS を有効にした場合，(4) kTLS と SmartNIC へのオフローディングを有効にした場合の，4 つの形態で行い，比較を行った (以下，(1) 〜 (4) と示す)．また，サイズの異なる 2 つのファイルを用いた場合で比較した．なお，(3) kTLS のみの評価は，(2) と (4) の比較において，kTLS を使用したことによる変化か，もしくは SmartNIC へのオフローディングを行ったことによる変化かを判断するために行っている．

表 1：評価実験用システム構成

CPU	Intel® Core™ i7-6700K
メインメモリ	64GB DDR4 SDRAM
OS	Ubuntu 22.04.1 LTS
NIC	NVIDIA BlueField-2 P-Series DPU MBF2H332A-AECOT 25GbE

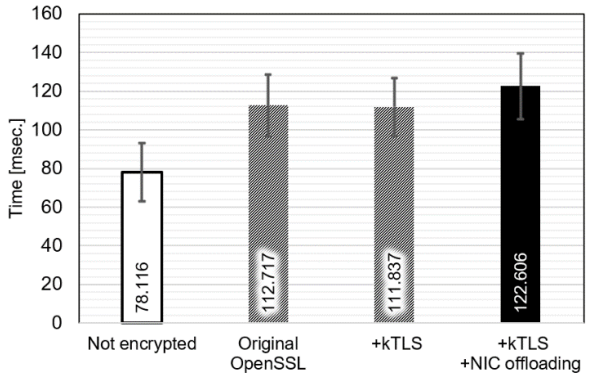

図 3：64MB ファイル受信　経過時間

図 3 では，64MB のファイルで実験を行った結果を示している．左から順に (1) から (4) の結果である．(2) は (1) と比較して平均値が約 44% 増加しており，暗号化処理により大きく時間が増加することが分かった．また，(3) は (2) と比較して約 0.8% 減少で，ほぼ差がなかった．(4) は (3) と比較して約 9.6% 増加しており，SmartNIC へのオフローディングにより時間が増大したことが分かった．

図 4 では，2KB のファイルで実験を行った結果を示している．(2) は (1) と比較して約 3 倍に増加しており，比較的小さなファイルの送受信においては暗号化により時間が増大することが分かった．(3) は (2) と比較して約 6.2% 増大した．(4) は (3) と比較して 13% 増大した．以上の結果について，MEC-RM への活用を考慮すると，時間の増大は MEC-RM のジョブ処理の遅延につながるものであり，無視できない新たな課題事項となった．

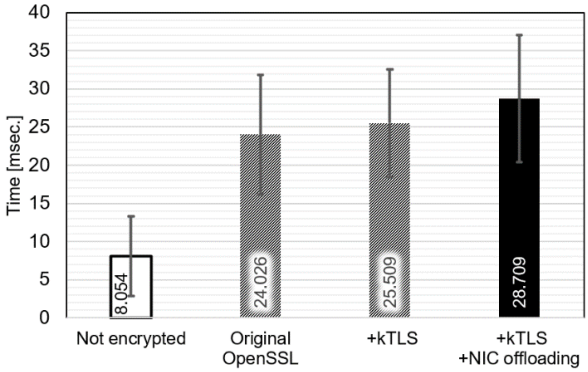

図 4：2KB ファイル受信　経過時間

6. まとめと今後の展望

本研究では，MEC-RM での活用を念頭に置き，暗号化・復号処理の SmartNIC へのオフローディングの実装を行った．評価実験での結果より，提案実装によってファイル送受信の時間は増大することが分かった．今後は，その原因の調査や，提案した実装により CPU の負荷がどの程度軽減するか，その影響でサーバーが処理可能な最大ジョブ数がどのように変化したかを分析する．また，SmartNIC に搭載されている汎用プロセッサを活かし，暗号化処理以外の SmartNIC の活用方法の検討などを引き続き検討する．

謝辞

本研究は，JST，CREST，JPMJCR19K1 の支援を受けたものです．

参考文献

[1] 内閣府, “Society 5.0 - 科学技術政策 - 内閣府,” 内閣府, [オンライン]. Available: https://www8.cao.go.jp/cstp/society5_0/. [アクセス日: 24 July 2022].

[2] Z. Fan, F. Qiu, A. Kaufman and S. Yoakum-Stover, "GPU Cluster for High Performance Computing," in *SC '04: Proceedings of the 2004 ACM/IEEE Conference on Supercomputing*, 2004.

[3] Y. Miho, T. Ryousei, A. B. Ahmed, S. Midori and A. Hideharu, "A Multi-tenant Re-source Management System for Multi-FPGA Systems," in *IEICE Trans. Information and Systems*, 2021.

[4] Y. Li and M. Sugaya, "Resource management system for mixed multi-FPGA and GPGPU environments," in *SWoPP2022*, 2022.

[5] B. Pismenny, H. Eran, A. Yehezkel, L. Liss, A. Morrison and D. Tsafrir, "Autonomous NIC offloads," in *Proceedings of the 26th ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS '21)*, 2021.

Implementation of offloading encryption processing to SmartNICs in multi-node computing (MEC) systems

†Miyakawa Taiki, Li Yanzhi, Sugaya Midori, Shibaura Institute of Technology
‡Fukai Takaaki, Hirofuchi Takahiro, National Institute of Advanced Industrial Science and Technology