2L-04

Publish/Subscribe通信フレームワークにおける ハードウェアを用いた暗号処理高速化の検討

木戸　剛生 † 大川　猛 †† 大津　金光 †† 横田　隆史 ††
† 宇都宮大学工学部情報工学科　†† 宇都宮大学大学院工学研究科情報システム科学専攻

1　はじめに

IoT 機器が急速に普及しており，2014 年時点では 170.7 万台であった世界の IoT 機器の数は，2020 年には 403.0 万台にまで増加する見込みである [1]．これに伴いセキュリティが深刻な課題となっている．たとえば，IoT 機器搭載カメラによる盗撮や，第三者の攻撃によるスマートロックの解錠などが挙げられる．この様に，IoT 機器の多様化，高機能化によって悪意ある第三者による攻撃も多様化しているのが現状である．これらのリスクに対し，多様な IoT 機器にセキュリティ機能を追加することが要求される．その際に課題となるのが，消費電力の制限，及び要求される応答時間である．特に小型の IoT 機器において，セキュリティ処理を低消費電力で実現する必要がある．さらに，リアルタイム性を重要視する IoT 機器においては，低遅延での処理が望ましい．

もうひとつの課題は．上記のようなセキュアな IoT 機器の開発手法である．セキュリティ機能を追加するための開発が困難であると安全でない IoT 機器が世の中に増えることになる．そのため．低消費電力，低遅延のセキュリティ処理を IoT 機器に容易に組み込むことができる開発フレームワークが必要となる．開発フレームワークを用いることで，IoT 機器の開発者は専門的な知識を要求されずに，セキュアなデバイスを設計することが可能となる．

以上の背景から，本研究の目的は IoT 機器に用いられる通信フレームワークの暗号処理をハードウェアを用いて高速化を検討することである．本稿では，Publish/Subscribe 型通信フレームワークである Fast RTPS を対象とし，暗号化処理部分のソフトウェア性能の分析とハードウェア化の効果について検討する．

2　Publish/Subscribe 通信フレームワークにおける暗号化通信

DDS(Data Distribution Service) とは，Publish/Subscibe 型通信ミドルウェアの仕様である．DDS をはじめとする Publish/Subscribe 型通信では，通信を行うノード (ユーザプログラムに相当する) が，Publisher または Subscriber，或いはその両方の役目を果たす．Publisher はメッセージの送信を行い，Subscriber は受信を行う．Publisher と Subscriber は topic という概念を用いて，対応するメッセージのみをやり取りすることが可能である．また，ユーザアプリケーションが通信相手の情報を事前に知る必要がなく，実行時にフレームワークが通信相手を検出しメッセージ制御を行う．DDS のコア仕様においてはセキュリティ機能は定義されないが，追加の仕様である DDS Security においてセキュリティ機能が定義されている．[2]

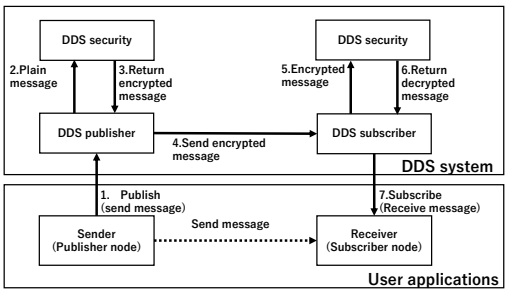

図 1: DDS とユーザアプリケーション概略

図 1 に DDS Security を用いた際の 2 つのユーザアプリケーションプログラム間の暗号化通信について概略を示す．ユーザアプリケーションの Sender(Publisher) が，Receiver(Subscriber) に対してメッセージを送る際の手順は以下のとおりである．(1) まず DDS システムに対して publish の API 呼び出しを行う．(2)DDS Security モジュールは平文のメッセージを受け取り，(3) 暗号文を返す．(4) 暗号文を通信し，(5)DDS Security モジュールは暗号文を受け取り，(6) 平文のメッセージを返す．(7) 最後にユーザアプリケーションの Reciever がメッセージを受け取る．

DDS Security においては，暗号化と認証の 2 つのセキュリティ機能が提供される．暗号化では，AES の GCM(Galois/Counter Mode) を用いて暗号化/復号の機能が定義されている．このときメッセージは 128bit ごとのブロックに分割され，暗号化の際に用いられる鍵は後述の認証機能 (PKI-DH) で共有されるものを用いる．認証では，PKI-DH として ECDH(Eliptic Curve Diffie-Helman key exchange) を用いて，2 者間の認証機能が定義されている．PKI-DH では Publisher ノードと Subscriber ノードの二者間の認証を行い，通信相手の公開鍵と自分の秘密鍵から共通鍵を生成する．

認証が通信開始時にのみ行われるのに対し，暗号化

Study on Hardware Acceleration of Cryptographic Processing for Publish/Subscribe Communication Framework
†Takao Kido,††Takeshi Ohkawa,††Kanemitsu Ootsu, and ††Takashi Yokota,
Department of Information Science, Faculty of Engineering, Utsunomiya University (†)
Department of Information Systems Science, Graduate School of Engineering, Utsunomiya University (††)

処理はPublish/Subscribe通信のたびに行われる．IoT機器の使われ方によって，認証と暗号化の頻度はさまざまであり，どちらも重要である．本稿では初期検討としてまずは暗号化通信について議論することとした．

3 暗号処理の課題

DDS SecurityをIoT機器に適用する際の課題を明らかにするため，通信性能評価実験を行った．実験に用いたDDS実装はロボット向けソフトウェアプラットフォームであるROS2で用いられるFast RTPSである．実験では，ユーザアプリケーションとして2つのROS2ノード間で暗号化通信を動作させた．

ROS2ノードはpublisherノードとsubscriberノードを同一のマシンで実行し，メッセージの送信時から受信時までの時間 (ROS2ノード間通信時間) と，暗号化に要した処理時間 (暗号化処理時間) を計測した．尚，ROS2ノード間通信時間は暗号化処理時間を含む全体の時間である．使用したマシンは，Raspberry Pi 3 Model B+ (CPU:Cortex-A53 (ARMv8)@1.4GHz, メモリ:1GB LPDDR2) 及び，ノートPC (CPU:Intel Core i7-4217MQ@2.2-3.3GHz，メモリ:8GB DDR3L) である．計測したROS2ノード間通信時間と暗号化処理時間を図2に示す．

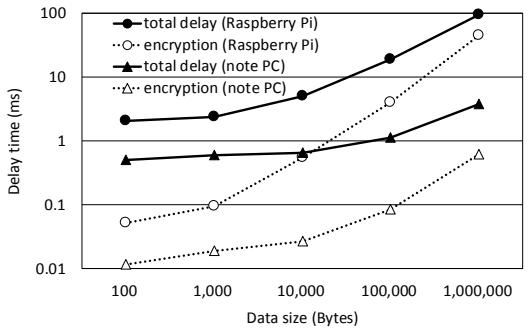

図 2: ROS2ノード間通信時間と暗号化処理時間

RaspberryPiを用いた場合，ノートパソコンを用いた場合に比べROS2ノード間通信時間及び，暗号化処理時間がかかることが分かる．RaspberryPi，ノートPC両方の場合において100KBを超えると暗号化処理時間が大きく増加する（RaspberryPiで約3.72倍，ノートPCで約1.72倍）．これは，Fast RTPSの暗号化処理において，データサイズがおよそ85KB〜90KB毎に暗号化のための関数を呼び出すためである．100KB以上のデータサイズとなった場合，暗号化処理のための関数が複数回呼ばれる．データサイズが増えるにつれ，ROS2ノード間通信時間全体に占める暗号化処理時間の割合が増加する傾向にあり，Raspbery Piでの1MBのときでは約47 %が暗号化処理時間であることがわかる．

4 性能試算:ハードウェアを用いた暗号処理

IoT機器で用いられる，ARMプロセッサのような組み込み向けプロセッサでは暗号化処理に時間がかかることが，ROS2ノード間通信性能評価実験で明らかとなった．多様なIoT機器にセキュリティ機能を追加するためには，ROS2-DDSのようなフレームワーク上で暗号化処理を加速する必要がある．本研究では，FPGAを用いてハードウェアを用いた暗号化処理方式について性能を試算した．ARMプロセッサ搭載のRaspberry Piを用いてソフトウェアで暗号化処理を行った場合のスループットは，データサイズが1MBのとき約22.53MB/sである．一方，FPGAを用いてAESの暗号化処理を行った場合，実装する回路の規模，及び実装方式によって違いがあるが，0.76GB/sから23.57GB/s程度のスループット性能が報告されている[3]．参考文献中で最も規模の小さい回路でスループットが (387 Slices)1.41Gbps 176MB/sであることから，Raspberry Piを用いた場合よりも高いスループットでの処理が期待できる．図2のRaspberry Piで1MBのデータを通信した場合において，暗号化の処理を，FPGAを用いて参考文献中の387 Slicesの回路を用いたときの期待値を試算すると，ROS2ノード間通信時間は約55,69msとなり約41.0 %，暗号化処理時間は87.2 %の処理時間の短縮になる．

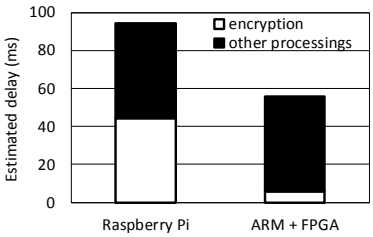

図 3: FPGAを用いたときのROS2ノード間通信時間

5 結論

ROS2ノード間通信時間及び，Fast RTPSの暗号化処理時間を測定し，ハードウェアを用いた暗号化処理を行った場合の性能向上を試算した．試算した結果，暗号化処理時間は87,2 %削減可能であり，ROS2ノード間通信時間全体においても約41 %削減可能である．小型のIoT機器でもセキュリティ処理を専用のハードウェアを用いてオフロードすることによって，高速化することが可能であると考えられる．

謝辞

本研究は，一部日本学術振興会科学研究費補助金 (基盤研究(C)17K00072, 17K00265, 16K00068,)，Intel University Programの援助による．

参考文献

[1] 総務省: “平成30年版情報通信白書”, pp.7, 2018.

[2] OMG: “DDS Security specification”, 2018, https://www.omg.org/spec/DDS-SECURITY/

[3] Joseph Zambreno, David Nguyen, Alok Choudhary: “Exploring Area/Delay Tradeoffs in an AES FPGA Implementation”, Intl. Conf. on Field Programmable Logic and Applications, pp.581-582, 2004.