このホワイトペーパーは、以下のサイトの英文のホワイトペーパーの日本語翻訳です。

For MQTT Smarter is Better

March 29, 2022/by Bob McIlvride

https://skkynet.com/for-mqtt-smarter-is-better/

よりスマートな MQTT へ

March 29, 2022/by Bob McIlvride

MQTT は、特に石油およびガスの多くの産業用通信タスクで使用されているプロトコルです。効率的に、高速で、そして安全に利用できるよう開発されています。フィールドデバイスをセントラルシステム SCADA に接続し、それらの間でデータを受け渡しできるように設計されています。

産業用 IoT（IIoT）の出現により、MQTT 支持者は、生産データをクラウドに接続する方法として MQTT を提案するようになりました。また OT（オペレーションテクノロジー）を IT に接続することへの関心が高まるにつれ、MQTT は現場のセンサーやアクチュエーターだけでなく、エッジデバイス、SCADA システム、IoT ゲートウェイなどにも接続することが求められるようになりました。これらは、企業の IT 部門で使用されているヒストリアンやデータレイク、AI エンジン、その他の分析機器などのさまざまなツールと繋がっています。

より大きい課題

このような幅広いアプリケーションスペース（応用空間）に適用することは、高速性と柔軟性を確保するために意図的にシンプルに開発された MQTT プロトコルにとっての課題です。各接続が単一のデバイスからのデータを送信する代わりに、MQTT はデータ値のコレクションを送信するように要求されるようになりました。かつてはすべてのデバイスが同一のものであったかもしれませんが、今ではさまざまなデバイスが異なるデータ形式を使用して互いに通信する必要があります。DMZ を使用してネットワークを分離し、マルチホップ接続を必要とする場合、デバイスからクライアントへの単純で直接的なセキュリティモデルでは十分ではありません。このような課題に対応するために、新しい仕様である Sparkplug B が導入されましたが、この仕様も更に強化できる点があります。

よりスマートに

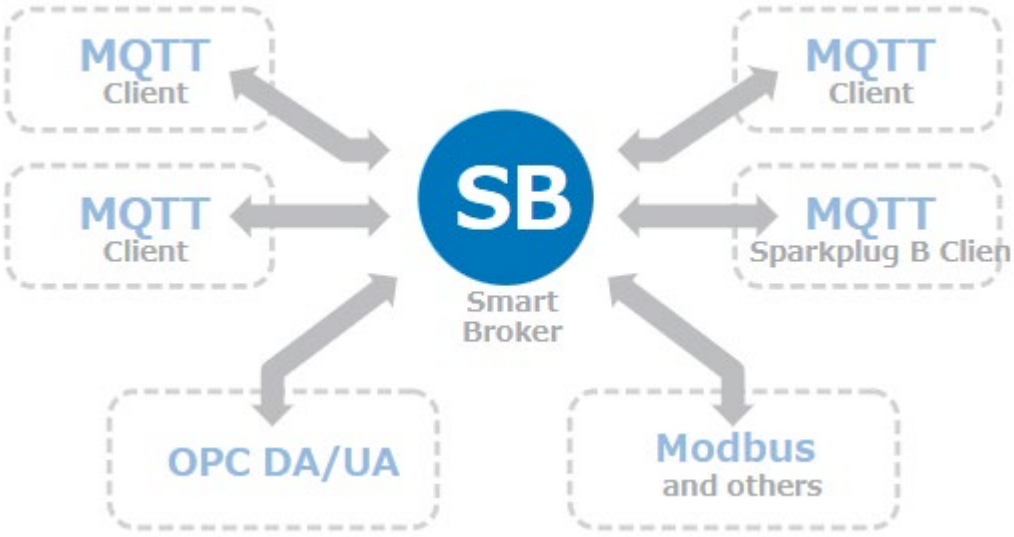
これらの課題は、MQTT がよりスマートになることを要求しています。設計上、MQTT は手紙を運ぶ郵便サービスのようなトランスポート・プロトコルです。このサービス（の配達人）は、手紙の中身を知りませんし、気にもしないし、手紙を送ったり受け取ったりする人の私生活には全く興味がありません。ただ、手紙を運び、届けるだけなのです。同様に、MQTT ブローカーは、メッセージの内容や、送信者と受信者の状態を知らないのです。

私たちは MQTT を、もっとスマートに活用できるように考えています。MQTT ブローカーに、伝送するメッセージを読み、理解する機能を持たせたらどうでしょうか？好奇心旺盛な郵便局員がハガキを読みながら配達するように、MQTT ブローカーはハガキを解析し、メッセージをよりインテリジェントに処理できるようになります。さらに、ブローカーが送信者や受信者自身と直接通信できたらどうでしょうか？その結果、ネットワークの状態や、どのクライアントが切断されたかを知らせることなどもできます。

このようなスマート・ブローカーは MQTT への要求が高まる中、非常に貴重な存在になっています。何が必要なのか、そして MQTT をよりスマートにすることでどのような改善ができるかを詳しく見ていきましょう。

データ収集

多くの IoT および OT-to-IT アプリケーションでは、単純なデバイスとブローカーの MQTT 接続ではもはや不十分です。数百または数千の接続デバイスを持つ大規模システムでは、データストリームを数個または 1 つの MQTT 接続に統合しなければならない場合があります。これは、1 クライアント接続を 1 つしか受け付けないクラウドサービスや、接続ごとに課金されるクラウドサービスに特に当てはまります。



このようなデータストリームの集約に伴い、異なるデバイスやデータソースを統合しなければならない場合があります。すべてのデバイスが MQTT を使用している可能性があり、異なるメッセージタイプを使用している可能性は十分にあります。また、多くのシナリオでは、MQTT は OPC UA などの他の産業用プロトコルと統合されています。

ネイティブ接続と OPC UA からのデータ変換を提供するスマート・MQTT・ブローカーは、このように受信データを収集して集約するのに非常に役に立ちます。すべての受信メッセージを解析することで、様々な MQTT のメッセージタイプ間を変換し、単一のアウトバウンド MQTT メッセージタイプにして提供することができます。また、OPC のような他の一般的なプロトコルでデータを読み取ることができれば、そのデータを同じ MQTT メッセージタイプに変換させることはそれほど難しいことではありません。

データの一貫性

リアルタイムの産業用システムでは、データの一貫性が非常に重要です。HMI や SCADA システムを監視しているオペレーターは、物理デバイスで何が起こっているかを正確に把握する必要があります。古いデータや、時系列が正しくないデータは、誤った判断につながる可能性があります。また、切断やネットワークの異常も把握する必要があります。スマート・MQTT・ブローカーは、メッセージを解析する機能とスマート・メッセージ・キューイングを活用して、データの一貫性を確保します。

リアルタイムシステムでは、メッセージの過負荷を処理するために、**スマート・メッセージ・キューイング**が必要とされています。これは、センサーやその他のデバイスのようなデータプロデューサー（送信者）が、コンシューマー（受信者）がデータを受信するよりも速くデータを送信したときにキューイング機能が作動します。慢性的な過負荷は、ブローカーがメッセージをドロップすることを必要とします。

スマート・MQTT・ブローカーは、インテリジェントなメッセージ・キューを実装し、メッセージの内容を解析し、以前の値が削除された場合でも、すべてのデータ項目の最新値が配信されるようにすることができます。これにより、コンシューマー側（受信側）のデータとプロデューサー側（送信側）の物理的な現実との一貫性を保つことができます。

最新値－産業用システムでは、データを最新値の状態に保つことが重要です。例えば、ポンプが何度もオンとオフを繰り返し、最終的に「オフ」になったとします。もしその最後の MQTT メッセージが、ブローカーによってドロップされたとした場合、HMI や SCADA システムはポンプを「オン」と表示することになります。このような一貫性のないデータは、コストのかかるエラーやシステムの誤動作につながる可能性があります。スマート・メッセージ・キューイングを持たない通常の MQTT ブローカーは、最終的に最新の値をドロップする可能性がありますが、スマート・メッセージ・キューイングを持つブローカーは、確実にその値を配信することができます。

時間順序－時間の順序は、1 つの MQTT メッセージトピック内では保たれますが、複数のトピック間では必ずしも保持されるとは限りません。A→B→C の順で発生する異なるデバイスからのイベントは、C→B→A などの順序でアプリケーションに配信される可能性があり、多くの産業制御のユースケースではエラーになります。スマート・ブローカーは、制御システムへの送信やネットワーク上での再送信のため、メッセージを他のプロトコルに変換する際に、時間の順序を保持することができます。

接続状態－通常の MQTT ブローカーには、データソースが切断されたことを示す方法がありません。受信側のアプリケーションは、故障したセンサーからの古い値と、単に最近更新されていない現在の値との違いを見分けることができません。これに対処するために設計された MQTT の "last will "メカニズムは、データのプロデューサー（送信者）とコンシューマー（受信者）の間のデータの不整合によって発生する、構成の重複、統合とメンテナンスのコスト増加の問題に対処します。データプロデューサー（送信者）とネットワークの状態を監視するスマート・ブローカーは、各メッセージに品質コードを割り当て、値が変わるたびにそれを更新することができます。この情報（品質コード）は、 MQTT の送信メッセージに含めることができ、その結果、データコンシューマー（受信者）は、値が変化しない理由を知るための何らかの方法（手がかり）を手に入れることができます。

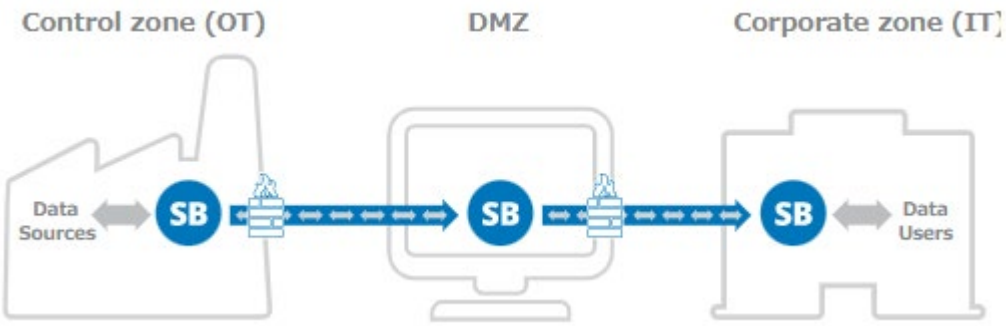
データーセキュリティー

産業セキュリティの専門家や政府機関は、OT と IT システムを接続する際には、ネットワークを分離することを推奨しています。望ましいアプローチは、DMZ を使用することです。NIST の文書 SP-800-82 は、次のように要約しています。「最も安全で、管理しやすく、拡張性のある制御ネットワークと企業ネットワークの分離アーキテクチャーは、通常、1 つまたは複数の DMZ を組み込んだ、少なくとも 3 つのゾーンを持つシステムに基づいています。」

この 3 つのゾーンとは、コントロールゾーン (OT)、コーポレートゾーン (IT)、そしてその中間にある DMZ です。DMZ を使用することで、企業ネットワークと制御ネットワーク間に直接のリンクがなくなり、既知の認証された関係者のみがシステムに入ることができます。SP-800-82 ドキュメントでは、ファイアウォールを使用して、これらのゾーンを分離し、正しいデータのみが一方から他方に渡されるようにすることの価値と使用方法について解説しています。

マルチホップデイジーチェーン

DMZ を経由したデータフローを満たすには、MQTT では問題があります。この種の接続には通常、2 台以上のサーバーを必要とし、デイジーチェーンで次々にリンクさせる必要があります。MQTT の QoS 保証はチェーンを介して伝搬することができないため、チェーンの端のデータは信頼性が低くなります。



信頼性の高いソリューションの 1 つは、MQTT メッセージを別のフォーマットに変換し、サーバーからサーバーへ、目的地に到着するまでネットワークを受け渡すことができるようにすることです。MQTT データを生成するデバイスは、スマート・ブローカーのインスタンスに接続されます。データ変換可能なブローカーは、品質情報とともにデータを安全なプロトコルを介してスマート・ブローカーの別のインスタンスに渡し、ブローカーは、データを再び MQTT に変換します。

使用するプロトコルは、できれば TLS1.2 や TLS1.3 などの最新バージョンの SSL 暗号を提供し、サーバー証明書を使用または強制することが理想的です。また、スマート・ブローカーは、MQTT クライアントがインバウンドポートを公開することなく、ファイアウォールからデータをアウトバウンドで送信する機能を複製できる必要があります。MQTT のこの貴重なセキュリティ機能を維持することが重要です。

Sparkplug B の機能強化

MQTT における Sparkplug B 仕様は、データの送受信方法を定義することにより、ベンダー間の相互運用性の問題を解決するために導入されました。Sparkplug B では、MQTT クライアントをデータ生成する EoN (Edge of Network) デバイスとデータを消費するアプリケーションのいずれかに分類します。各 Sparkplug B デバイスは、オンラインになったとこを示す BIRTH メッセージ、データを送信する DATA メッセージ、オフラインになった

ことを示すDEATHメッセージなど、様々な種類の「メッセージを生成します。オンライン中のSparkplug Bアプリケーションは、これらのメッセージを受信し、どのデータがどのデバイスから送られてきているのか知ることができます。

これまで説明してきたスマート・MQTT・ブローカー機能は、すべてSparkplug Bベースのシステムに適用されます。さらに、スマート・MQTT・ブローカーは、Sparkplug Bの接続性を強化する他の機能を提供することができます。

すべてのアプリケーションを同期—スマート・ブローカーは、すべての接続を認識しているため、新しいアプリケーションがオンラインになるたびに、接続されている各デバイスのBIRTHメッセージを統合することができます。これにより、そのアプリケーションは、現在接続されているすべてのデバイスからDATAメッセージを受信できるようになり、起動順序に関わる問題が解消されます。

エラーへの対応－MQTTメッセージの異常や紛失を特定する機能に加えて、スマート・ブローカーは、この種のエラーが発生した時にSparkplug Bデバイスを自動的に切断し、再接続できるようにする必要があります。こうすることにより、デバイスは、BIRTH（起動）メッセージを再送信し、受信するすべてのアプリケーションを再同期させ、データの一貫性を保持することができます。

デバイスへの書き込み失敗の解決－もう一つの有用な機能は、アプリケーションからデバイスへの書き込み要求をすべてチェックし、指定されたデータ値がデバイスに書き込まれたかどうかを確認することです。スマート・ブローカーは、デバイス上の値が変化していないことを検知すると、デバイスを強制的に切断し、BIRTHメッセージの再送信を行います。これにより、そのデバイスをリッスンしているすべてのアプリケーションが再同期されます。データの一貫性を保持するためのもう一つの方法となります。

データ品質情報の追加－Sparkplug Bデータを他のプロトコルに変換する必要があるシステムに対し、スマート・ブローカーは、品質情報を追加することができます。例えば、Sparkplug Bのデータを OPCに変換する場合、OPCのデータ品質を追加することができます。BIRTHまたはDATAメッセージには、OPCのデータ品質である“Good”の品質が割り当てられ、一方、DEATH（シャットダウン）メッセージには、“Not Connected”の品質が割り当てられます。

より良いものにするために

MQTTは、デバイスとサーバー間のデータ通信だけではなく、OT/IT、Industry 4.0、産業IoTの課題に対処するために、さらに改善することができます。スマート・MQTT・ブローカーは、複数の受信メッセージタイプ、さらには他のプロトコルからのデータを収集することができます。データプロデューサー（送信者）からメッセージの経路全体にわたって、データの一貫性を保つことができます。データプロデューサー（送信者）からデータコンシューマー（受信者）へのメッセージの全経路において、データの一貫性を保ち、コンシューマー（受信者）は、常に最新の値とデータ品質の指標を持つことができます。適切に設計されたスマート・ブローカーは、DMZや他のマルチホップ・ネットワーク構成を介して、MQTTデータプロデューサーとコンシューマーを安全に接続するために使用することもできます。これらの利点は、 Sparkplug Bの実装においても同様に提供することができます。MQTTがよりスマートになればなるほど、今日求められている要件も今後求められる要件もより良いものになります。