SecHack365

MQTTブローカーを狙う未知の攻撃を封じる 2段階分類侵入検知モデル

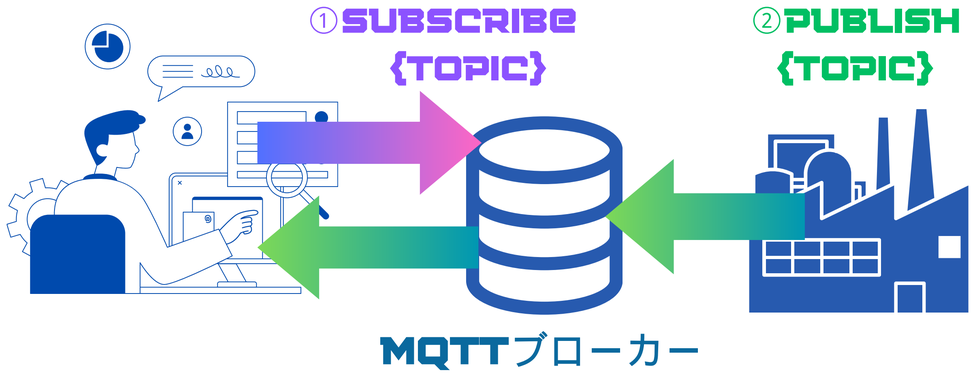
研究駆動コース
35R宮澤昌子

MQTTってなに？

軽量・省電力なIOT向け通信プロトコル

- IOTデバイス向けに設計された、軽量な通信プロトコル
- 低帯域のネットワークでも効率的にデータをやり取り
- FACEBOOK MESSENGERや自動車にも利用

PUB/SUBモデルでシンプルな通信



MQTTのセキュリティリスク

517,776※

※インターネットに晒されたMQTTブローカーの数【2025年2月11日SHODAN検索】

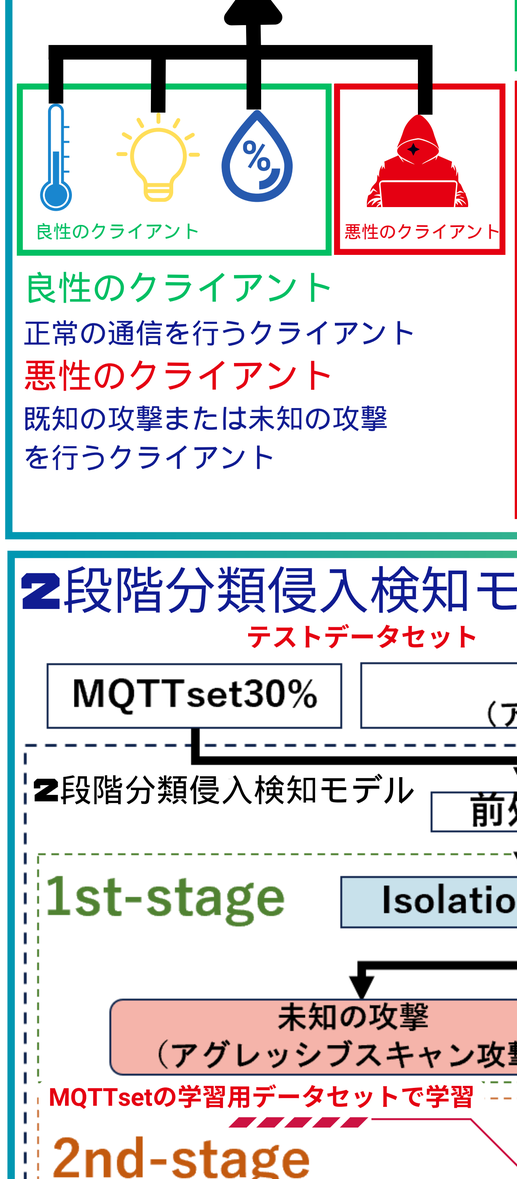
- **強力な認証機能や暗号を実装していない**
- **リソース制約のあるデバイスではTLSや非対称暗号化が困難**

既存の侵入検知は何がダメなのか？

「既知の攻撃」または「未知の攻撃」のどちらか一方にしか対応できない

攻撃パターンをもとに侵入検知	正常パターンをもとに侵入検知
シグネチャ型IDSや教師あり学習	アノマリ型IDSや教師なし学習
✅既知の攻撃を高精度で検知	✅未知の攻撃を検知
⚠️未知の攻撃には対応できない	⚠️攻撃を詳細に識別できない

想定するMQTTのIoTシステム



良性のクライアント
正常の通信を行うクライアント

悪性のクライアント
既知の攻撃または未知の攻撃を行うクライアント

良性のクライアント

正常の通信
- IDSが学習済みの正常パターン

悪性のクライアント

既知の攻撃
- IDSが学習済みの攻撃パターン

未知の攻撃
- IDSが未学習の異常通信

提案手法：2段階分類侵入検知モデルとは？

既存の侵入検知の欠点を補完しあう仕組み

前処理
MQTTのIDS手法における有益な特徴量を抽出する

1ST-STAGE
教師なし学習に基づく1クラス分類器で未知の攻撃を検知

2ND-STAGE
教師あり学習に基づくマルチクラス分類器で正常の通信と既知の攻撃を検知

2段階分類侵入検知モデルは本当に機能する？

テストデータセット

MQTTset30% / MQTT-IoT-IDS2020（アグレッシブスキャン攻撃）

2段階分類侵入検知モデル

前処理

1st-stage（MQTTsetの学習用データセットで学習）

Isolation Forest

- 未知の攻撃（アグレッシブスキャン攻撃）
- 既知の通信

2nd-stage（MQTTsetの学習用データセットで学習）

Decision Tree

- 正常の通信
- フラッディング攻撃
- MQTTパブリッシュフラッディング攻撃
- SlowIte攻撃
- ブルートフォース
- 不正なパケット

実験結果

- 各既知の攻撃を約81%識別できる（2ND-STAGEに渡された既知の攻撃データで評価）
- 未知の攻撃を100%検知できる
- 正常な通信を97%識別できる（2段階分類侵入検知システム全体の通信データで評価）

ステージ	評価指標	値
1st-stage	Accuracy	0.9102
	Recall （既知）	0.8072
	FPR	0.0000
	F1 Score	0.8933
	ROC-AUC	0.9036
2nd-stage	Accuracy	0.9187
	Precision	0.9171
	Recall	0.9187
	F1 Score	0.9156
	ROC-AUC	0.9586
	$Accuracy_{known\ attack,\ 2nd\text{-}stage}$	0.8102
全体	$Accuracy_{legitimate,\ overall}$	0.9785
	$Accuracy_{known\ attack,\ overall}$	0.5048
	$Accuracy_{unknown,\ overall}$	1.0000

考察

- 「未知の攻撃」を約100%検知できる
- 「正常の通信」を約97%適切に正常として識別できる
- 2ND-STAGEに渡された「既知の通信」のうち、各「既知の攻撃」を約81%識別できる

→ 従来よりも攻撃の解析にかかる時間や費用の発生を抑えられる

外部発表：宮澤昌子ほか，未知の攻撃に対するMQTTブローカーの2段階分類侵入検知モデル，
電子情報通信学会，インターネットアーキテクチャ研究会，2025年3月．