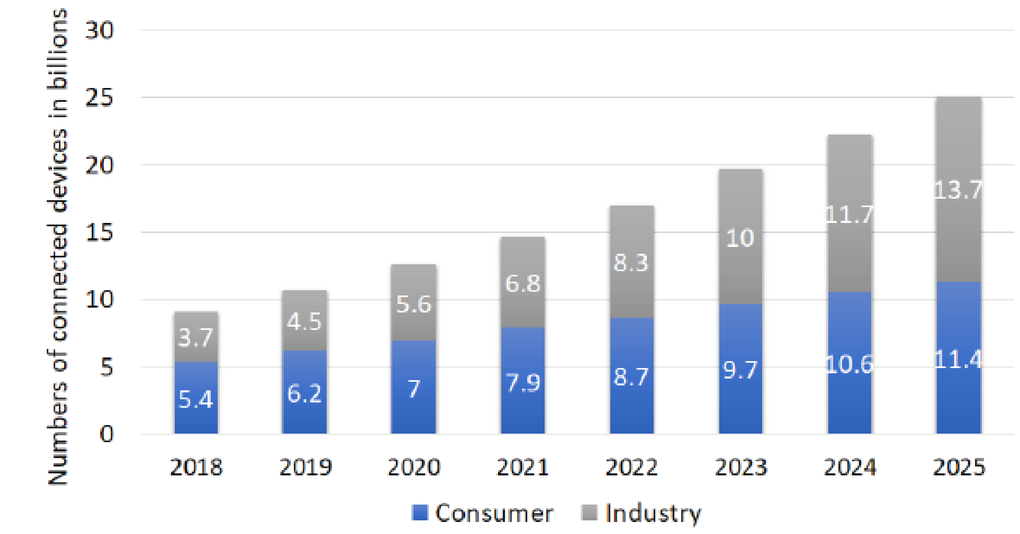
An Efficient Data Protection Scheme Based on Hierarchical ID-Based Encryption for Message Queueing Telemetry Transport

Hui-Chun Huang (黃彙淳)
Advisor: Chun-I Fan (范俊逸)
National Sun Yat-sen University

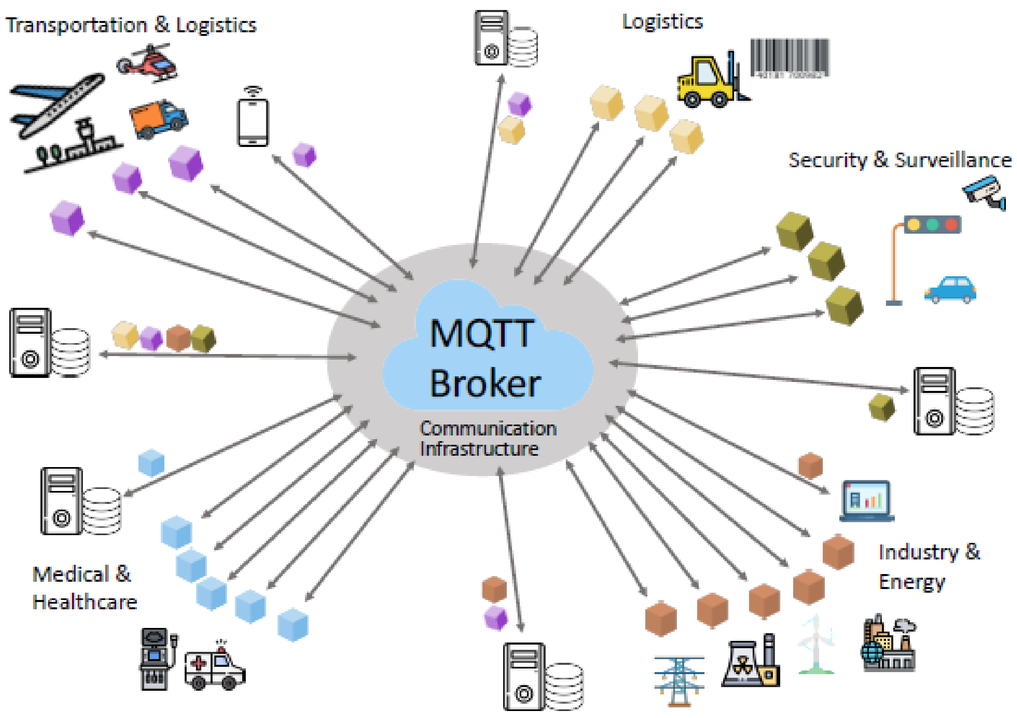
資訊安全實驗室 Information Security Laboratory 中山大學・資訊工程學系

Abstract

- As time goes by, to meet people's needs, more and more IoT devices and functions have emerged. Therefore, data transmission protocols have been derived, and MQTT is one of them. MQTT is a many-to-many message transmission protocol based on the "publish/subscribe" mechanism. It has been widely used for data transmission in many industries such as the energy industry, chemical engineering, self-driving. Because of this, MQTT security has become a hot topic. In general, it is transmitted without encryption. While transporting important messages, MQTT specification recommends the use of TLS protocol. However, computation and time cost of TLS is too high. Since topics in a broker are stored with a hierarchical structure, we propose to use a hierarchical ID-based encryption system for message protection, and with a constant size key that is independent of depth in hierarchical structures. At the same time, the proposed scheme presents a formal security model to prove the security of the mechanism, which achieves chosen-plaintext attack security under the wBDHI assumption.

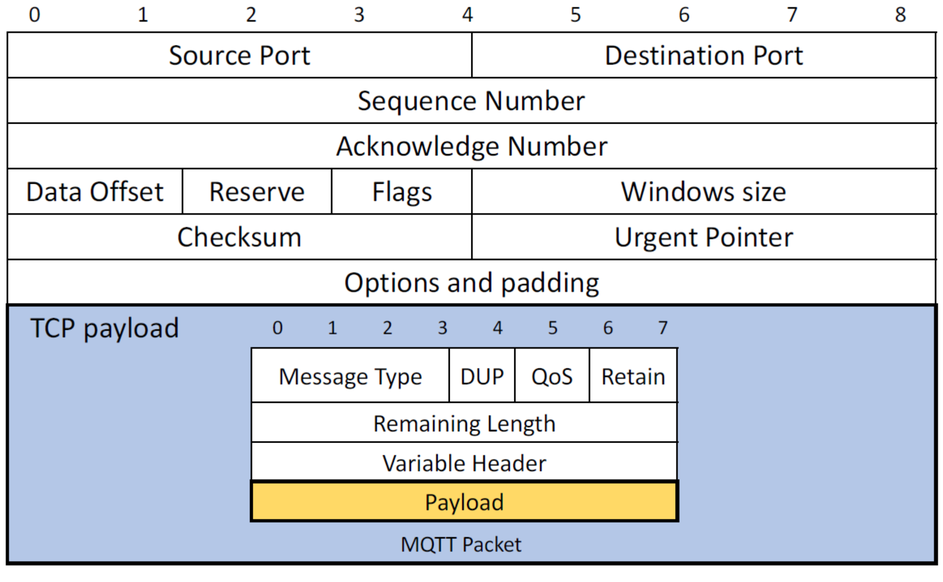


- Forecast Numbers of Internet of Things (IoT) Connected Devices Worldwide from 2018 to 2025 (in billions)



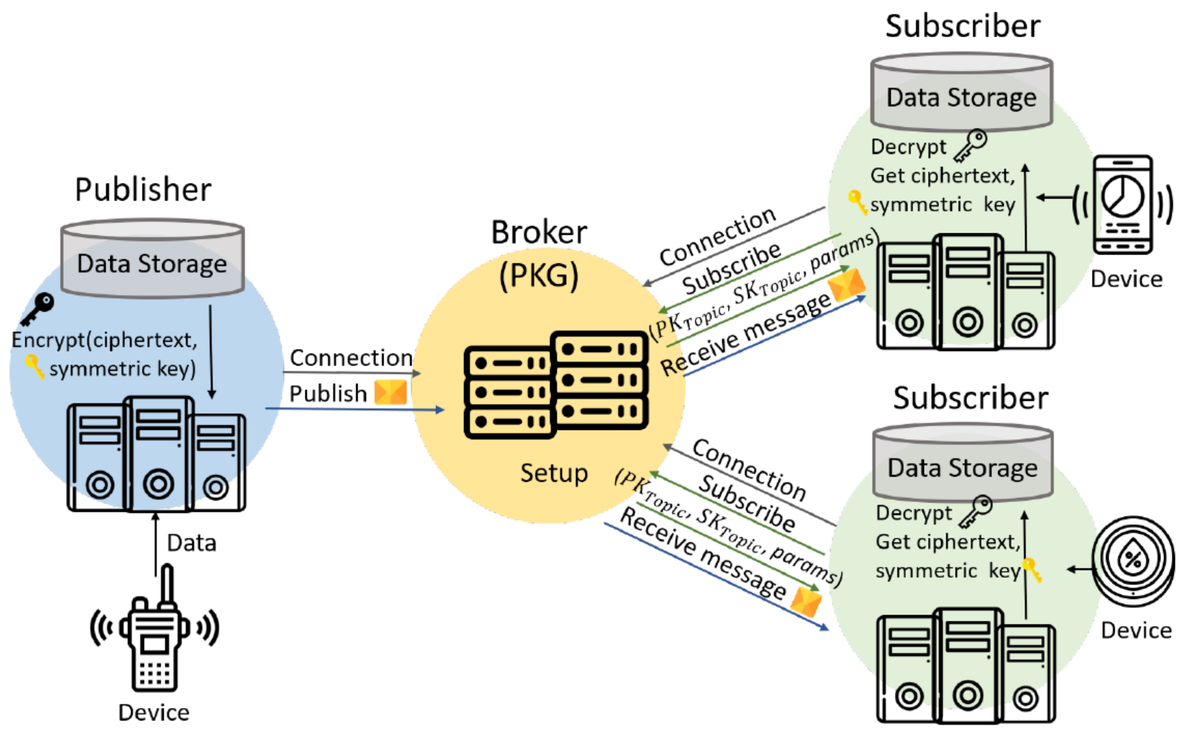
- MQTT in the IoT M2M Industry

Preliminaries



- An MQTT Packet on a TCP Network

Scheme



- The System Model of the Proposed MQHIBE Scheme

Comparison

Notation	Meaning	Key size	Cost
$T_{AES-GCM_{Enc}}$	the cost of an AES-GCM encryption	256 bits	0.003 ms
$T_{AES-GCM_{Dec}}$	the cost of an AES-GCM decryption	256 bits	0.231 ms
T_{ECDHE}	the cost of an ECDHE operation	-	62.972 ms
$T_{RSA_{Enc}}$	the cost of an RSA encryption	2048 bits	2.903 ms
$T_{RSA_{Dec}}$	the cost of an RSA decryption	2048 bits	109.462 ms
$T_{h_{384}}$	the cost of a 384 bits hash operation	-	0.001 ms
T_p	the cost of a pairing operation	-	33.524 ms
T_m	the cost of a modular multiplication in $\mathbb{Z}_q$	-	0.001 ms
T_s	the cost of a scalar multiplication in an additive group or an exponentiation in a multiplicative group	-	0.019 ms
T_a	the cost of an addition in an additive group or a multiplication in a multiplicative group	-	0.025 ms

- Computation Costs of Cryptographic Primitives in Millisecond (ms)

Scheme		Key generation	Encryption cost	Decryption cost
Singh *et al.*	CP-ABE	0.252 ms	33.728 ms	101.054 ms
	KP-ABE	0.08 ms	0.123 ms	67.43 ms
The MQHIBE scheme		0.214 ms	0.085 ms	67.329 ms

- Performance Comparison with Related Works

Scheme	Hierarchical	Encryption	Assumption	Security proof
Singh *et al.* [10]	No	CP-ABE [12]	None	ROM/CPA
		KP-ABE [11]	DBDH	STD/CPA
The MQHIBE scheme	Yes	HIBE	wBDHI	STD/CPA

- Properties Comparison with Related Works

Conclusion

- A novel MQTT encryption scheme has been designed by hierarchical ID-based encryption during the communications. In the MQTT protocol, every message belongs to a topic which is a hierarchical namespace stored in the broker. This is the reason why the proposed scheme utilized hierarchical ID-based encryption to protect the messages. Furthermore, the proposed scheme meets the need of the subscription by a multi-level wildcard character. The most significant feature of HIBE is that the root node can hierarchically generate the private keys of the descendants, and the private key of the node can be generated from the private key of the parent node. As a result, we took the advantage and used it in a multi-level wildcard character when subscription.
- With the advantages mentioned before, the proposed MQHIBE scheme is suitable for the MQTT environment and guarantees secure message transmission. In the future, how to achieve the IND-sID-CCA security will be a further study. In addition, the quality of service and quality of message transmission (such as data recovery) in MQTT are the exciting challenges to be investigated in the near future.