TECH OFFER

# Mutual Authentication And Key Exchange Protocol For Peer-To-Peer Iot Devices

## KEY INFORMATION

TECHNOLOGY CATEGORY:
**Electronics** - Embedded Systems
**Infocomm** - Wireless Technology
**Infocomm** - Internet of Things & Wearable Technology

TECHNOLOGY READINESS LEVEL (TRL): TRL4
COUNTRY: SINGAPORE
ID NUMBER: TO174411

## OVERVIEW

In database-driven Internet of Things (IoT), the connection between two IoT devices is performed indirectly through a server. Data collected on one IoT device needs to flow to the server before reaching another IoT device. By contrast, Peer-to-Peer (P2P) IoT enables direct connection between two IoT endpoints. IoT data is shared directly between two 'peers' and a server is only needed to enroll the devices in the P2P network for a direct connection. P2P IoT has much lower latency and higher privacy than database-driven IoT. However, current practices of addressing the wireless vulnerability by using the server to mediate a direct end-to-end encrypted connection between two IoT endpoints is too complex and inefficient.

This technology offer is a lightweight and secure protocol for mutual authentication and key exchange directly between two endpoints in P2P IoT. The protocol exploits physically unclonable function (PUF) derived from manufacturing process variations of integrated circuits as device "biometrics". The PUF circuit is lightweight and can be embedded in an endpoint device to generate unique, unpredictable, and unforgeable identity only upon query. PUF-based device identity is tamper-aware and hence more secure than hardcoded or memory-based identity. This PUF-based protocol is significantly more efficient and secure than cryptographic-key based protocols for P2P IoT applications. It enables any pair of IoT devices after enrollment to directly authenticate each other. Upon successful authentication, a secure and fresh shared session key is automatically established for encrypted communication, which directly overcomes the existing key distribution and management problem in P2P IoT.

## TECHNOLOGY FEATURES & SPECIFICATIONS

This protocol uses hardware-intrinsic root of trust to achieve robust security and privacy protection against impersonation attacks. Existing protocols rely mainly on public and private key cryptographic algorithms, which require the secret keys to be stored locally on device's memory. Secret keys stored persistently on IoT devices are vulnerable to memory, side-channel, and tamper attacks. This protocol creates puzzles that can be solved only by the genuine interlocutors using their respective PUFs ("silicon biometrics") without storing any secrets on device. The secret required to solve the puzzle can be generated-upon-request by the device PUF and cannot be tampered.

This protocol has the following unique advantages:

1. Secure: IoT devices, either prover or verifier, do not have to store any secrets locally. Device-to-device mutual authentication and key exchange can be achieved directly without involving a server, after the devices have been enrolled.
2. Flexible: "Silicon biometrics" can be realized in several ways, e.g., memories or ring oscillators, based on the resources of each device.
3. Efficient: Only require three handshakes to establish the mutual authentication and key exchange.
4. Low-cost: Computational complexity on each device is very low. For each pair of devices, the total communication cost is only around 300 bytes and the storage cost on each device is only around 150 bytes.
5. Generic: The handshake messages are generic. Its binaries can be adapted to any payload of gateway or network communication package specifications. No complicated controller is required to execute the protocol operations on the device.

## POTENTIAL APPLICATIONS

The proposed protocol can be used to benefit smart home and secure peer-to-peer communications in IoT applications, e.g.,

1. Secure remote control of smart locks/printers/water heaters and so on.
2. Drone remote control and surveillance.
3. Secure communication between a window actuator and its external weather station.
4. Safe and secure P2P video live streaming between security cameras and phones.

By eliminating the need for a relay server, this protocol greatly reduces an expensive and long-term cost of server traffic. Besides, the proposed protocol enables end-to-end data encryption, which can protect information like video streaming from being leaked. Unlike existing hardware-based or software-based solutions, no secret is required to be stored in those IoT devices, which greatly reduces the risk of tampering attacks. Knowing authentication handshake messages and states of the device in each authentication session will not help the adversary to gain any useful information and advantage for attacking any other sessions. The protocol can work with any PUF design that suit the endpoint and have the right quality and performance for the end point.

The technology owner is keen to license this protocol to IoT device developers and IoT service providers who are developing

P2P IoT devices.

## UNIQUE VALUE PROPOSITION

IoT devices appear in every aspect of modern living, and typically work as data-collector and controllers. For efficiency and privacy reasons, these intelligent devices should to "talk" to each other directly without involving a server in each communication. On the other hand, it is desirable that the direct communication in the public channels is secure even though the IoT devices themselves cannot provide much protection due to their resource constraint and limited computing power. This protocol can perfectly help with these requirements. Using this technology, customers can:

1. Enjoy lower latency for secure remote control.
2. Ensure privacy for data-transmission applications like video streaming.

Tampering of IoT devices for impersonation can be detected.