LiKe: Lightweight Certificateless Key Agreement for Secure IoT Communications

Pietro Tedeschi, Savio Sciancalepore, Areej Eliyan, Roberto Di Pietro

Division of Information and Computing Technology
College of Science and Engineering, Hamad Bin Khalifa University - Doha, Qatar
email: {ssciancalepore, rdipietro}@hbku.edu.qa, {ptedeschi, aeliyan}@mail.hbku.edu.qa

IEEE Internet of Things Journal, November 2019

LiKe

LiKe is
a lightweight pairing-free[1] certificateless key agreement protocol

[1]Pairing-based cryptography: pairing between elements of two cryptographic groups to a third group with a mapping $e : G_1 \times G_2 \rightarrow G_T$.

LiKe Protocol Features

- ephemeral cryptographic materials
- support for intermittent connectivity with the Trusted Third Party(TTP)
- lightweight *re-keying* operations
- robustness against impersonation attacks (even when information stored on the TTP are leaked)
- formally secure (via the *ProVerif* tool)
- compatible with real IEEE 802.15.4 devices
- suitable for integration in Zigbee 3.0
- bandwidth and energy efficient

Open Issues

- Certification Management in traditional public key infrastructure (PKI) is inefficient
- Key-escrow problem in Identity Based Encryption

Certificateless Cryptography

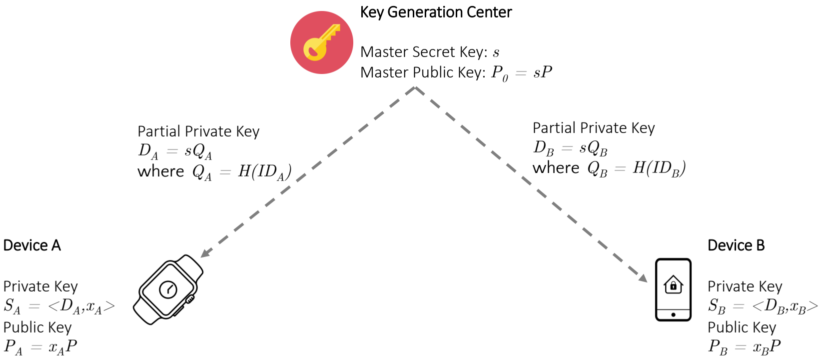


Figure: Certificateless Cryptography - An overview.

Scenario

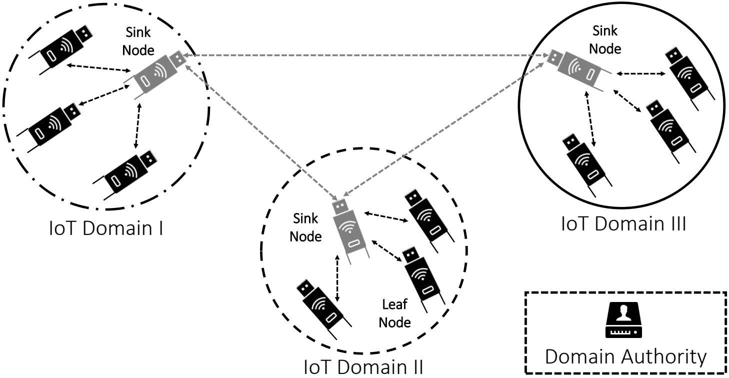


Figure: Reference Scenario: multiple IoT domains, managed by a unique Domain Authority (DA), where each domain is organized in a single sink IoT node and several leaf IoT nodes.

Pre-Deployment Phase

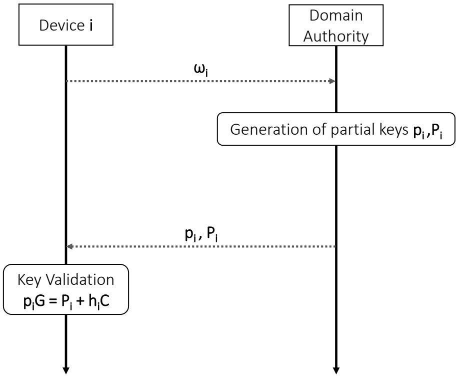


Figure: LiKe: Sequence Diagram of the Setup Phase.

$$\omega_i = (ID_i \parallel t_i \parallel X_i) \qquad P_i = r_i G$$
$$h_i = H(\omega_i \parallel P_i) \qquad p_i = r_i + h_i c \bmod n$$

Key Agreement Protocol

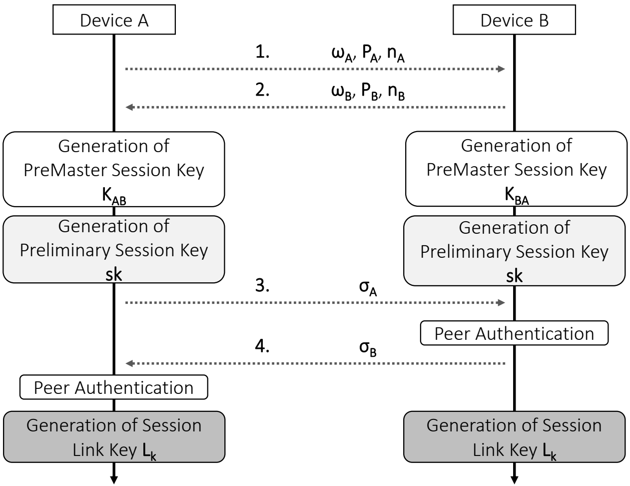


Figure: LiKe: Sequence Diagram of the Key Agreement Phase.

Security Properties

Protection Against Leakage of Secret DA Information

Ephemeral Cryptography Materials

Protection Against Man-in-the-Middle Attacks

Protection Against Replay Attacks

Protection Against Known-Key Attacks

Formal Verification

```
:~$ proverif LiKe_test_1.pv | grep "RESULT" | nl
1  RESULT not attacker(xA[]) is true.
2  RESULT not attacker(xB[]) is true.
3  RESULT not attacker(pA[]) is true.
4  RESULT not attacker(pB[]) is true.
5  RESULT inj-event(end_LiKe_B(x)) ==> inj-event(begin_LiKe_A(u,v_13,y,w,n)) is true.
6  RESULT inj-event(end_LiKe_A(x_14)) ==> inj-event(begin_LiKe_B(u_15,v_16,y_17,w_18,n_19)) is true.
```

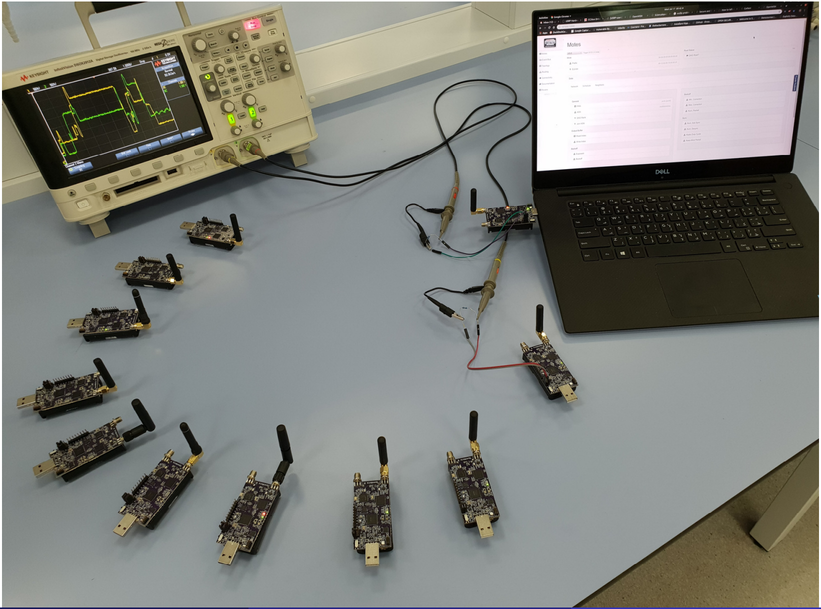
(a) Test 1: Security Verification of LiKe when the private keys of the involved devices are assumed to be secret.

```
:~$ proverif LiKe_test_2.pv | grep "RESULT" | nl
1  RESULT not attacker(xA[]) is true.
2  RESULT not attacker(xB[]) is true.
3  RESULT not attacker(pA[]) is false.
4  RESULT not attacker(pB[]) is false.
5  RESULT inj-event(end_LiKe_B(x)) ==> inj-event(begin_LiKe_A(u,v_13,y,w,n)) is true.
6  RESULT inj-event(end_LiKe_A(x_14)) ==> inj-event(begin_LiKe_B(u_15,v_16,y_17,w_18,n_19)) is true.
```

(b) Test 2: Security Verification of LiKe when the partial private keys of the involved devices maintained by the DA are assumed to be leaked to the adversary.

Figure: Output provided by *ProVerif*.

Experimental Testbed



Temporal Results

- LiKe Protocol Duration: 340.478ms
- Preliminary Session Key Generation: 243.392ms
- Mutual Authentication and Session Key Generation: 97.086ms

[Comparison] - MAC-Layer Exchanged Messages

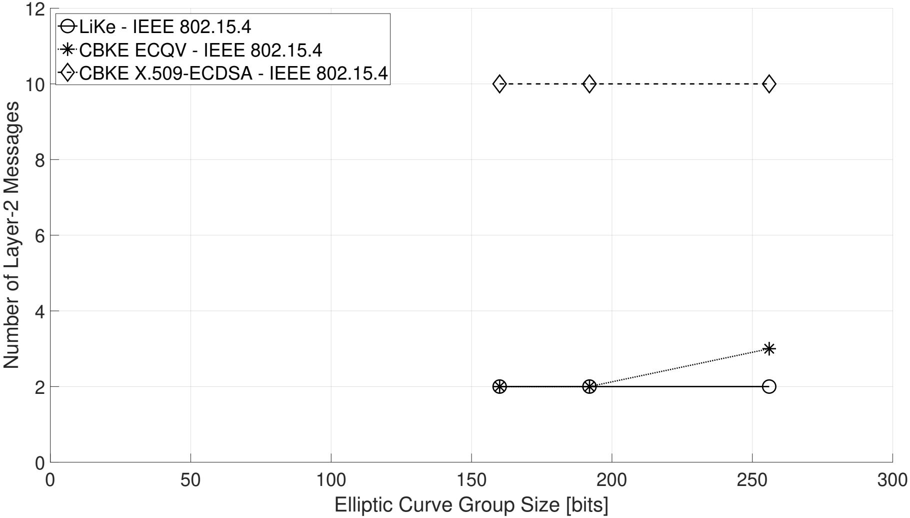


Figure: MAC-layer messages required to complete the key agreement, considering X.509-ECDSA, ECQV, and LiKe.

[Comparison] - Other Approaches

Feature	**X.509-ECDSA**	**ECQV**	**LiKe**
Robustness to Man-In-The-Middle	✓	✓	✓
No. of messages to detect an attack	9	2	2
Message Overhead per Key Agreement Instance	10	3	2
Energy Consumption per Key Agreement Instance (mJ)	$38,953$	$36,080$	$35,726$
Robustness to DA Secret Information Disclosure	✗	✗	✓

Figure: Comparison of LiKe against CBKE Approaches based on X.509-ECDSA and ECQV, assuming a 256-bit Elliptic Curve.

Energy Consumption

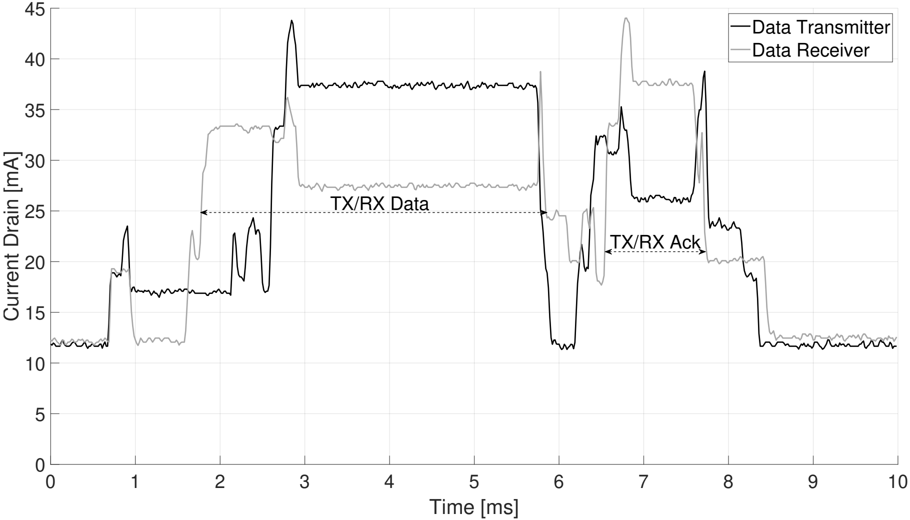


Figure: Current Consumption of a Data Transmission and a Data Reception Operation within the duration of a IEEE 802.15.4 time-slot (10 ms).

Related Work

Feature	[17]	[18]	[19]	[20]	[21]	[22]	[23]	[24]	LiKe
Pairing-free	✗	✗	✓	✗	✓	✓	✗	✓	✓
Non-persistent Connection with Domain Authority	✗	✗	✓	✗	✗	✓	✓	✓	✓
Ephemeral Cryptograhy Material	✗	✗	✓	✗	✓	✓	✗	✗	✓
Integration in a Real IoT Enabling Technology	✗	✗	✗	✗	✗	✓	✗	✗	✓
Implementation on Real IoT Devices	✗	✗	✗	✗	✗	✓	✗	✗	✓
Real Performance Evaluation	✗	✗	✗	✗	✗	✓	✗	✗	✓
Energy Friendly Approach	-	-	-	-	-	✗	-	-	✓
Suitability for Autonomous IoT Domains	✗	✗	✗	✗	✗	✗	✗	✗	✓
Lightweight Re-Keying	✗	✗	✗	✗	✗	✗	✗	✗	✓
Open-Source Code	✗	✗	✗	✗	✗	✗	✗	✗	✓

Figure: Comparison of LiKe against state-of-the-art approaches using **CL-PKC** techniques. A ✓ symbol indicates the fulfillment of a particular feature, a ✗ symbol denotes the miss of the feature, while the symbol – indicates that the feature is not applicable.

Questions?

Any Questions?
Thank you!