Security Considerations for IEEE 802.15.4 Networks

Eirik Klevstad

February 20, 2016

1 Abstract

IEEE 802.15.4 = Wireless radios and protocols for low power devices, personal area networks and sensor nodes.

Some of the optional features actually reduces security.

Highlight difficulties in security.

2 Introduction

802.15.4 = Common platform for devices to communicate with each other and share components to lower costs.

Personal Area Networks, used by sensor network communities.

Wireless game controllers, environmental, medical, building monitor instruments, heating, ventilation, smart homes, smart cities.

Such devices = embedded devices controlled by a micro controller operating without human intervention.

Because of no human contact, two demands:

1) Software = simple and correct.

2) Devices must make efficient use of their limited energy.

two heaviest components = micro controller and wireless chip.

Link-layer security package: confidentiality and data integrity

Three problems:

1) IV Management

2) Key management

3) Insufficient integrity protection

3 802.15.4 Security Overview

Link layer security: Four different basic security services:

1) Access Control

2) Message Integrity

3) Message Confidentiality
4) Replay Protection

3.0.1 Access control and message integrity

Access control: Link layer should prevent unauthorized parties from participating in the network. Detect and reject messages from unauthorized nodes.

Message integrity protection: Able to detect that a message was modified while in transit. Include a MAC with each message.

MAC = Cryptographic secure checksum. Requires both parties to have a shared secret.

3.0.2 Confidentiality

Keeping information secret from unauthorized parties. Use encryption.

Semantic security: Not possible to learn anything about the plaintext. E(m1) != E(m1) by using a random nonce. Add variation to the encryption process when there is little variation in the set of messages. Usually sent public.

3.0.3 Replay protection

Prevents attacks where someone can replay / inject a valid frame into the network. Frame counters (sequence numbers) are the solution. Discard older packets.

3.1 Protocol Description

3.1.1 802.15.4

Addressing: 64-bit node identifier, 16-bit network identifier.

Packets relevant to security: Data packets and acknowledgement packets

Data packets: Variable length, used to send a message to a single node or broadcast. Flags indicate packet type, security enabled, addressing mode, request ACK. Sequence number.

Acknowledgement packets: Sent by recipient if not broadcast and sender requested an ACK.

3.1.2 Security

802.15.4 security layer is handled at the media access control (MAC) layer. Application must explicitly enable security.

Four packets: Beacon, Data, Acknowledgement, Control for MAC layer

Application has a choice of security suits that control the security properties and guarantees. 802.15.4 has eight different suites.

Classify by properties: No security, encryption only (AES-CTR), authentication only (AES-CBC-MAC), encryption and authentication (AES-CCM).

Length of MAC = 4, 8 or 16 bytes.

Tradeoff: Packet size for authenticity attacks

Application indicates security suite based on source and destination address.

Access Control List (ACL): Controls security suite and keying information. 255 entries.

If security is enabled, look up address in ACL and apply security suite on the message.

Reception: Check if flags is packet has been exposed to security. MAC uses ACL with senders address to find suite and extract message.

3.2 Keying Models

Symmetric key: Both parties use the same key, but when using keying model, it governs what key a node uses to communicate with another node.

Keying model chosen based on application's threat model and how complex key management the application can handle. Network shared key model: All nodes uses same key. Easy key management.

3.2.1 Network Shared Keying

Each node possesses the same key.

Trivial key management.

Minimal memory requirements.

Vulnerable to insider attacks. If one node gets compromised, the whole network gets compromised as the attacker can forge valid messages to all nodes and decrypt all traffic.

3.2.2 Pairwise keying

Limited scope of each key. Each node pair share a symmetric key. Memory consumption is higher, but the compromise affects just that particular node pair.

3.2.3 Group keying

Compromise between network shared keys and pairwise keys. Create groups within the network that share the same key and communicate between each other using this key, while still maintaining pairwise keys with some other nodes.

3.3 Implementations

Not aware of any wireless chip that fully supports the security detailed in the 802.15.4 standard.

4 Problems

Found several vulnerabilities in 802.15.4. Danger zones for application developers where is possible to configure so much that the security is reduced.

4.1 IV Management Problems

4.1.1 Same Key in Multiple ACL Entries

Up to 255 ACL entries to store different keys and their associated nonce.

Sender choses appropriate ACL entry based on destination address.

Vulnerable if same key is used in two different ACL entries. Highly likely that user will reuse nonce. Independent nonce in two different entries will be reused. Can xor messages to break confidentiality.

Two ways for recipient to end up with same keys:

1) Implementing group keys by using two separate ACL entries sharing the same key. Works, but not secure.

2) Two keys. One for parent nodes and one for all others. When switching parent node(s), the same key will be stored in two separate ACLs.

Never separate nonce state from key.

4.1.2 Loss of ACL State Due to Power Interruptions

Expect many devices to run on solar power / battery.

Power Failure

If no precautions: ACL entries will be empty after reboot on power outage. Can be repopulated with the keys, but there is no specification on what to do with the nonces. Can not be reset to a given value.

Developer can avoid by

1) Establish new keys after outage. Eliminate the possibility for reusing nonce with same key.

2) Store key counter in non-volatile memory. This is slow and energy inefficient. "Lease" in flash memory. Update with the current block.

Low Powered Operation

How to preserve nonce state when node goes into low powered operation.

4.2 Key Management Problems

4.2.1 No Support for Group Keying

Because of each ACL can only be associated with one address, not possible to establish a group key for a group of nodes.

By creating n entries all containing the same key: Too dangerous. highly chance of nonce reuse.

Another approach: modify the address in ACL for each packet sent. Too much processing and loss of energy. Also; receiver must known which is the sender of a packet BEFORE it arrives. Like.. whaat. Many constraints, not gonna work in practice.

No simple way for using group keys. If you try, you're gonna fail and weaken the security of the network.

4.2.2 Network Shared Keying Incompatible with Replay Protection

With Network shared key: No way to protect against replay attacks.

Replay protection: Use frame counter. Reject messages containing frame counter lower than the last observed. Will not work in a network of many nodes. Need to coordinate the counter use.

4.2.3 Pairwise Keying Inadequately Supported

The specification could include stronger support for pairwise communication.

No minimum size requirement of the ACL entry.

Can not share ACL entry between multiple nodes.

Limit of number of nodes in network utilizing pairwise keying is defined by the number of ACL entries.

If the manufacturer of a radio chip has only two ACL entries, you can wave goodbye to pairwise keying.

4.2.4 Discussion

difficulties is result of confusion between the role of nonces and replay counters.

Nonce in outgoing packages serves two purposes: Non-repeating value that provides confidentiality. Counter that prevents replay attacks.

Replay attacks: Ensure that the nonce value on this key is larger than the previous observed key.

problem: Nonce is not able to serve both purposes while under the constraints of the ACL structure.

None of the three most important key models are well supported in 802.15.4:

1) Network Shared Keying
2) Pairwise Keying
3) Group Keying

4.3 Insufficient Integrity Protection

4.3.1 Unauthenticated Encryption Modes

AES-CTR: Too dangerous to ever be used. Unauthenticated encryption is stupid.

CRC is not enough. Should use MAC.

Failures of integrity can affect confidentiality.

4.3.2 Denial of Service Attacks on AES-CTR

AES-CTR with replay protection.

No message authentication: Can send garbage with HIGH frame count. Will be decrypted. And the watermark will be updated to HIGH, and impossible for real users to get their packets accepted.

Attacker can permanently disrupt a 802.15.4-link.

4.3.3 No Integrity on Acknowledgement Packets

No integrity or confidentiality checks for ACKs.

Sender can request ACK by flag in request.

ACK contains the packets sequence number.

No authentication. Adversary can generate ACK on any package.

Can jam a package, and send a ACK tricking the sender into believing that the package was correctly received at destination.

5 Recommendations

5.1 Application Designers

Do not use AES-CTR security suite.

Do not rely on acknowledgements.

5.2 Hardware Designers

Include support for 255 ACL entries. Gives pairwise keying model.

Do not reset the list of ACL when entering low power mode.

Expose nonce for each received packet. Replay does not work in a network shared key system. Replay protection should be implemented on application level.

Eliminate support for AES-CTR

5.3 Specification Writers

Warn against dangerous ACL configurations.

Better support for keying models

Remove AES CTR Suite

Support authenticated Acknowledgements

Eliminate difference between key and frame counter

6 Conclusion