Study and Application of Security based on ZigBee Standard

Paper Presentation

Presented by:

Archana Sreekumar (P2CSN18005)

Betrant Titus (P2CSN18006)

1.

Introduction

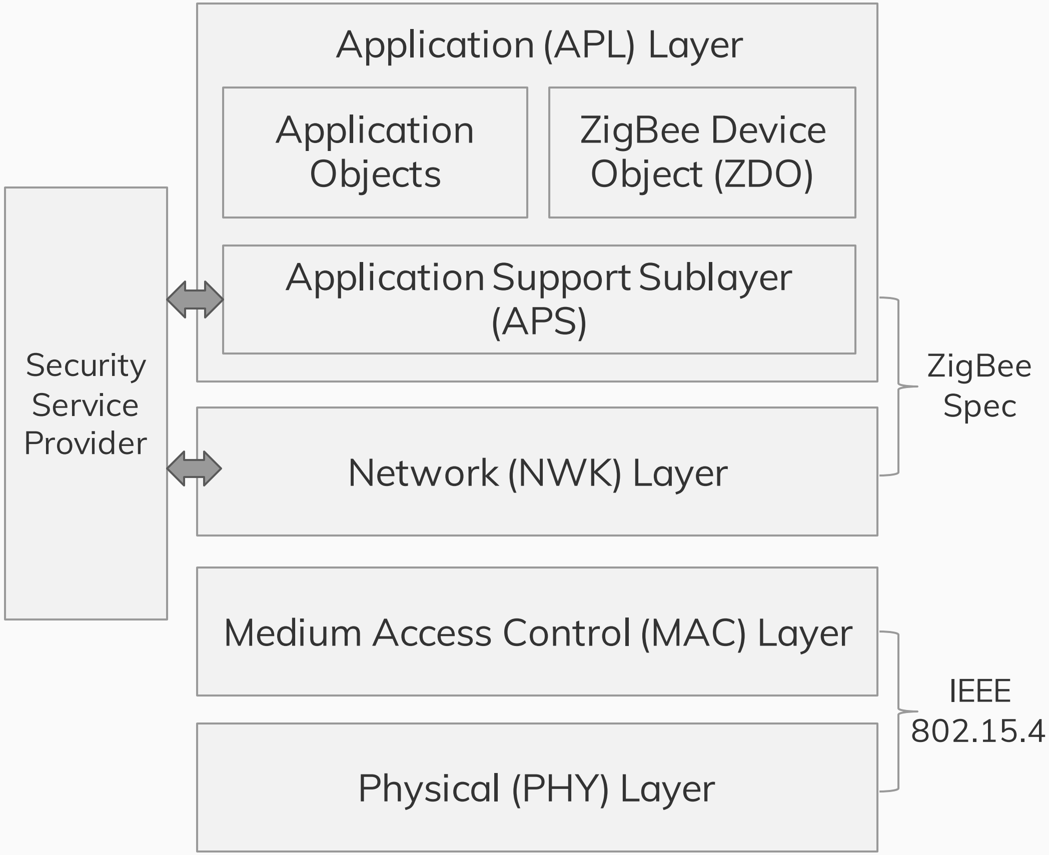
A quick overview of ZigBee and how it secures it’s communication

ZigBee: Advantages and Disadvantages

- ZigBee : Open WLAN communication technology standard for low data rate network.
- Advantages : low-complexity, low-cost, high reliability, etc.
- Restrictions : computing speed of nodes, memory space, limit of energy consumption etc.
- Unable to utilize a traditional security mechanism in a ZigBee network.
- Need to design a practical security scheme for the same.

The stack architecture of ZigBee

The ZigBee protocol stack consists of the given layers which provide one layer of abstraction over the other.


Application (APL) Layer
Application Objects
ZigBee Device Object (ZDO)
Application Support Sublayer (APS)
Security Service Provider
Network (NWK) Layer
Medium Access Control (MAC) Layer
Physical (PHY) Layer
ZigBee Spec
IEEE 802.15.4

ZigBee: Security Suites

Data Integrity Check

This uses message integrity codes (MIC) to prevent data from being modified by the attackers without secret key.

Support for identity authentication

This provides a safe means for a device to synchronize messages with another.

Presence of AES

ZigBee encryption utilizes AES algorithm.

It is approved by National Institute for Standards Technology.

ZigBee: Security Suites

Presence of Trust Center

Trust Center decides whether new devices are allowed to join the WLAN or not.

It stores the keys for the network.

Three-key network security

Master key : Basic key among communicating of nodes.

Link key : Secure unicast communication.

Network key : Secure broadcast communication.

ZigBee: Network Attacks

- Three kinds:
  - Sybil
  - Sinkholes
  - Wormholes
- Malicious node enters WLAN and acts as legitimate one.
- Destroy packets, altering, discarding etc.

ZigBee: Security Mechanism

- Encryption mode : AES Counter mode with Cipher block chaining and Message authentication code (CCM*)
- Provides confidentiality and integrity.
- Same key used in all layers.

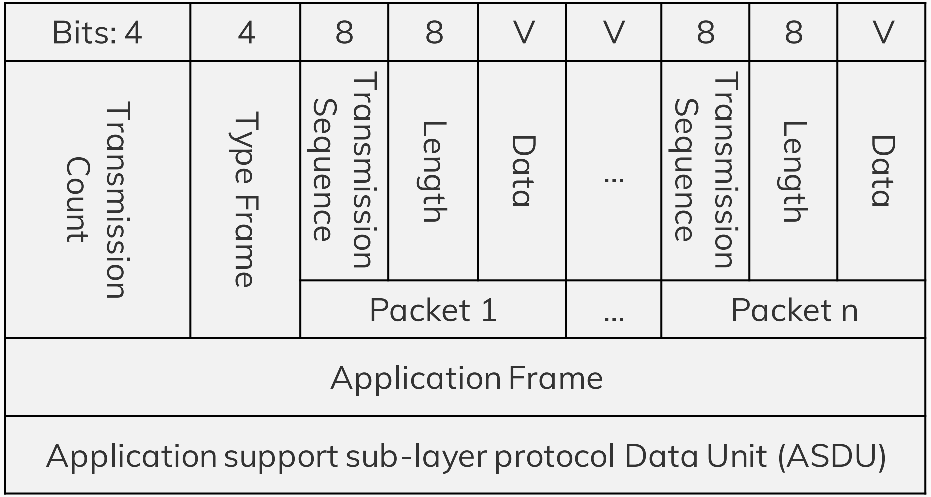
2.

Securing Application Layer

Proposing an idea to ensure integrity and confidentiality in the application layer

A regular ZigBee application frame

The ZigBee application layer data is transmitted via packets with the given frame structure.



<table>
<tr><td>Bits: 4</td><td>4</td><td>8</td><td>8</td><td>V</td><td>V</td><td>8</td><td>8</td><td>V</td></tr>
<tr><td rowspan="2">Transmission Count</td><td rowspan="2">Type Frame</td><td>Transmission Sequence</td><td>Length</td><td>Data</td><td>...</td><td>Transmission Sequence</td><td>Length</td><td>Data</td></tr>
<tr><td colspan="3">Packet 1</td><td>...</td><td colspan="3">Packet n</td></tr>
<tr><td colspan="9">Application Frame</td></tr>
<tr><td colspan="9">Application support sub-layer protocol Data Unit (ASDU)</td></tr>
</table>

The proposed secure ZigBee application frame

This revision of the packet frame structure introduces encryption along with message integrity.

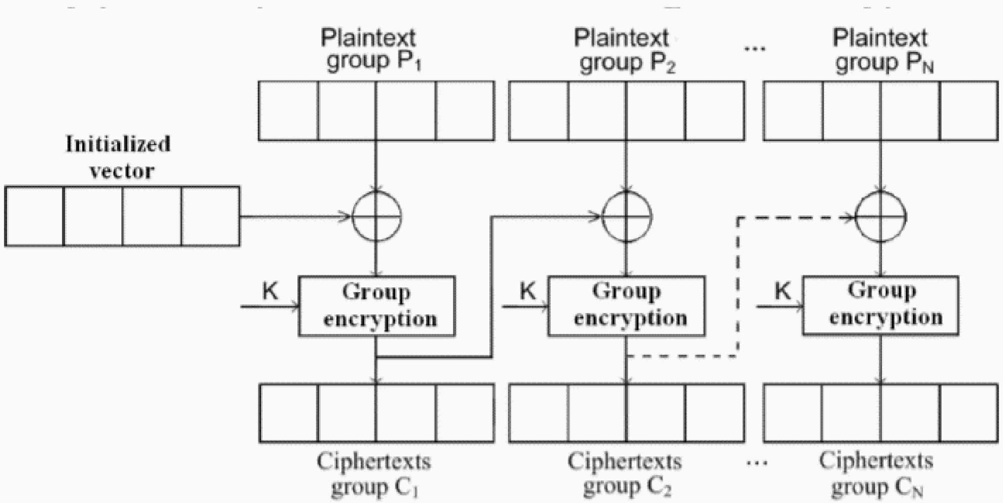
<table>
<tr><td>Bits: 8</td><td>8</td><td>8</td><td>8</td><td>V</td></tr>
<tr><td rowspan="2">Transmission Sequence</td><td rowspan="2">Length</td><td>Key Bit Sequence</td><td>MIC</td><td>Data</td></tr>
<tr><td colspan="3">Transmission Data</td></tr>
<tr><td colspan="5">Transmission packet 1</td></tr>
</table>

How is this realized?

- Variable number frame changed to one single frame.
- The transmission sequence, length and data fields are replaced with key-bit sequence, MIC and encrypted data.
- Since there are no multiple frames, transmission count is replaced with the required sequence number of the packet.

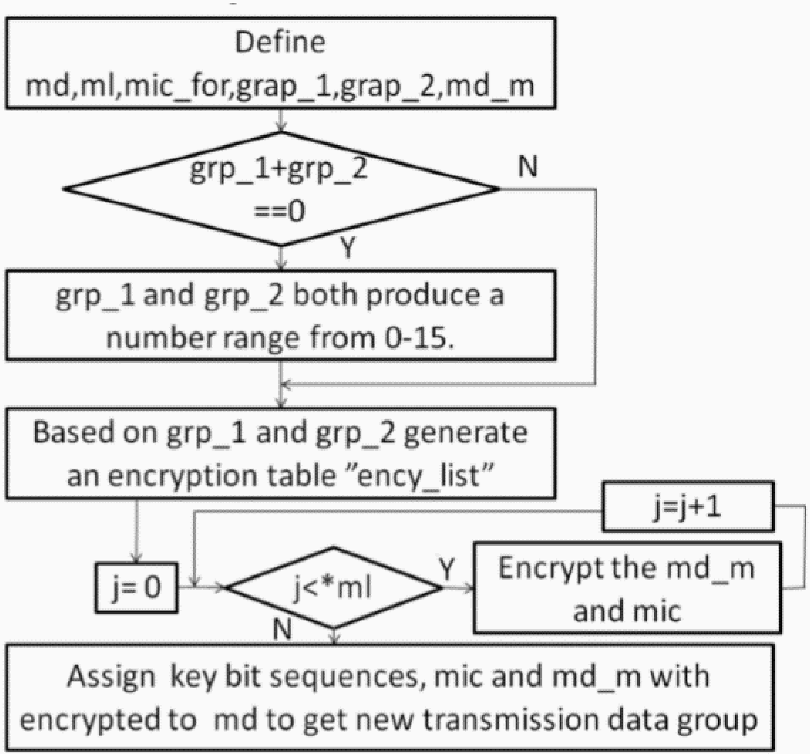
The Cipher-Block-Chaining method of AES

The AES-CBC-128 method is utilized to generate the encrypted data as shown in the schematic.



The proposed encryption method

The proposed AES-CCM* implementation is shown here.



Define md,ml,mic_for,grap_1,grap_2,md_m

grp_1+grp_2 ==0

N

Y

grp_1 and grp_2 both produce a number range from 0-15.

Based on grp_1 and grp_2 generate an encryption table ”ency_list”

j=j+1

j= 0

j<*ml

Y

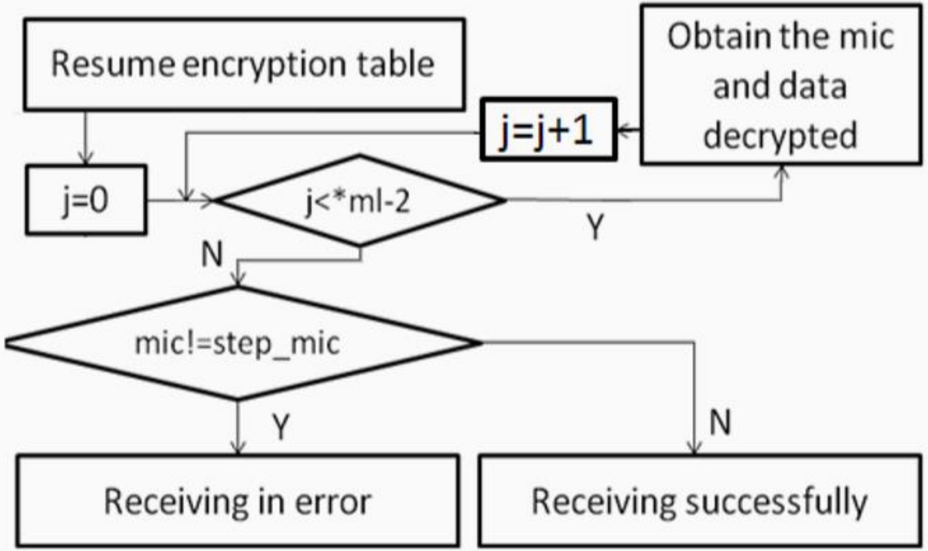
N

Encrypt the md_m and mic

Assign key bit sequences, mic and md_m with encrypted to md to get new transmission data group

The proposed decryption method

The proposed AES-CCM* implementation is shown here.



Conclusion

- Proposed system helps secure application data and reduces overhead and complexity.
- CCM* mode also helps assure message integrity along with confidentiality.
- Resistant toward internal cryptanalysis attacks as well.

Thank You!

Any questions?