# How to Setup a Secured ZigBee Networks

ZigBee / IEEE 802.15.4

ZM101, ZM101PA, ZM102
EZport, SZport, ZIOport

**Version 1.0**
**2010 Jan**

# 1. ZigBee Network Security Overview

This guide explains the security features of EZport. ZigBee Network Layer Security and point to point (APS Layer) Security will be examined. Precise step by step guides of setting up Network Layer Security and point to point security will be discussed. All behaviors of the security Networks, data transmission rules, and security related ATCommands will be covered in detail.

## A Non-Secured ZigBee Network

By disabling the security options on all ZigBees, all device with any or none NwkKeySet1 could establish a network and all data transmission ATCommands such as ATTXDATAU, ATTXDATAB, ATTXEACK will function.

## Enabling Network Layer Security with Network Key

By setup Coordinator as Trust Center and enabling the security options on all ZigBees, all device with the same NwkKeySet1 can establish a secured network. All data transmission ATCommands within the network will function. Devices with different NwkKeySet1 will be blocked out by the Trust Center.

## Enabling Point to Point Security with Link Key

Begin with a secured ZigBee network which has Network Layer Security enabled, install a pair of LinkKeySet on any two ZDOs that need point to point security. Each LinkKeySet pair must have the corresponding target's MAC Address filled. Once LinkKeySet are established between the two devices, data transfered between point to point will be encrypted. For every point to point security between any two ZDOs, a pair of LinkKeySet is needed.

# 2. Security Keys

## Master Keys

Master Keys are used as a foundation for two devices when performing Symmetric-Key Key Establishment (SKKE) to generate Link Keys. They are not used to encrypt frames. They are most likely to be pre-installed.

In this application note, Key Transport method is used to setup a secured network.

Master Keys which are stored in the Trust Center are called Trust Center Master Keys. All other Master Keys are called Application Layer Master Keys.

## Network Keys

Network Keys functions as passports for entering a secured Networks. If there are no networks available only devices with the same NwkKeySet1 are allowed to establish a network.

It is also used to secure broadcast communications. It is shared amongst all devices in the network and it operates at the ZigBee Network Layer.

## Link Keys

Link-Keys are used to secure unicast communications. It is shared between two devices at the ZigBee Application Layer.

Link Keys which are stored in the Trust Center are called Trust Center Link Keys. All other Link Keys are called Application Layer Link Keys.

# 3. Network and Link Key Data Structure

## Network Keys

There are three sets of Network Keys. They are stored in “ATDUMP --> NWK KEY”. NwkKeySet1 functions as passport identification for Security Network Establishment. It also influence Data Transmission rules as that of NwkKeySet2 and NwkKeySet3.

ATDUMP A
NWK Key

| | |
|---|---|
| NwkKeySet1 | Key SeqNum: 00<br>ABCDEF0123456789000000000000000 |
| NwkKeySet2 | Key SeqNum: FF<br>00000000000000000000000000000000 |
| NwkKeySet3 | Key SeqNum: FF<br>00000000000000000000000000000000<br><br>Active Key SeqNum [00] |

## Link Keys

There are five sets of Application Link Keys. They are stored in “ATDUMP --> APS Pair Desc”.

ATDUMP 9
APS Pair Desc

| | |
|---|---|
| LinkKeySet1 | DeviceAddr 0000000000000000<br>Key 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000<br>Incoming 00000000<br>Outgoing 00000000 |

| | |
|---|---|
| LinkKeySet2 | DeviceAddr 0000000000000000<br>Key 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000<br>Incoming 00000000<br>Outgoing 00000000 |
| LinkKeySet3 | DeviceAddr 0000000000000000<br>Key 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000<br>Incoming 00000000<br>Outgoing 00000000 |
| LinkKeySet4 | DeviceAddr 0000000000000000<br>Key 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000<br>Incoming 00000000<br>Outgoing 00000000 |
| LinkKeySet5 | DeviceAddr 0000000000000000<br>Key 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000<br>Incoming 00000000<br>Outgoing 00000000 |

# 4. ZigBee Security ATCommands

## 4.1 ATSETNWKKEY

It sets NwkKeySet1. It needs to be saved in order to be effective. Use ATSAVE or in parameter window press read, apply, then reset.

NwkKeySet1 of a device can only be changed on the device with ATSETNWKKEY. In other words, even a Trust Center will not have the permission to change the NwkKeySet1 of another device (ATSENDNWKKEY can only send to NwkKeySet2 and NwkKeySet3).

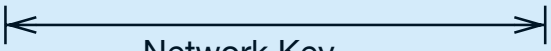
If a Trust Center decides to abort its current network and wants all members to move to a new network, all NwkKeySet1 on all the members must be changed individually.

Input:

| | |
|---|---|
| network key | 32 CHAR or 128-bit security |

Example:

*ATSETNWKKEY 12345678901234567890123456789012*



Network Key

## 4.2 ATSENDNWKKEY

It transport a Network-Key and its key-id to a destination device. In the same time it will store a copy of the same Network-Key into its own NWK Key Table. If input C's own mac address, the new Network-Key will be stored only to itself. ATSENDNWKKEY can only set NwkKeySet2 and NwkKeySet3.

Input:

| | |
|---|---|
| IEEE-64bit address | 16 CHAR |
| key-id | 2 CHAR or 8-bit |
| network key | 32 CHAR or 128-bit |

Example:

*ATSENDNWKKEY ccccccccc0c0c0c0c dd 55566666666666666666666666666655*

destination's IEEE adress | Key ID | Network Key

Storage Behavior:

It stores NwkKeySet2, if Active-Key-SeqNum is in NwkKeySet1 or NwkKeySet3. It stores in NwkKeySet3 if Active-Key-SeqNum is in NwkKeySet2. All Network Keys stored in NwkKeySet2 and NwkKeySet3 will be erased after power loss or reset.

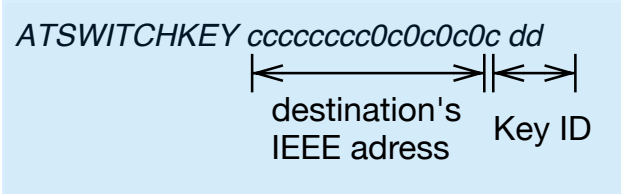
## 4.3 ATSWITCHKEY

It informs the specified device to switch to one of the three Network-Keys that are stored in its Network-Key table. It will change the Active-Key-SeqNum of the specified device. Only a trust center can use this function. Using this function the trust center will also automatically switch its own Active-Key-SeqNum to match the Key-ID that is being sent out.

Input:

| | |
|---|---|
| IEEE-64bit address | 16 CHAR |
| key-id | 2 CHAR |

Example:




## 4.4 ATCLRNWKKEY

It clears all of the Network Keys within the NWK Key Table.

## 4.5 ATSETLINKKEY

Link Key is used to secure unicast communications. It is shared between two devices for unicast communications.

It sets a Link Key for itself. Every time an unicast message is sent to this specified destination device, the message will be encrypted. In order for the destination device to understand the encrypted message, it must also have the same Link Key (with the IEEE address of the source device).

Therefore, to have encrypted messages understood both ways or sent encrypted messages both ways, ATSETLINKKEY must be done individually to both devices with destination address of the opponent.

Input:

| | |
|---|---|
| IEEE-64bit address (of the device that you are sharing the Link Key with) | 16 CHAR |
| link key | 32 CHAR or 128-bit |

Example:

*ATSETLINKKEY ccccccc0c0c0c0c 12345123451234512345123451234512*

IEEE address of partner device that shares the Link Key

Link Key

Storage Behavior:

It stores from LinkKeySet1 to LinkKeySet5 and then back to LinkKeySet1 (1, 2, 3, 4, 5, 1, 2, 3 etc...). There exist only one Link Key between any two devices. In other words, among all of the LinkKeySets of an device no two LinkKeySets should have the same IEEE address. Using ATSETLINKKEY by inputing an already existing IEEE address, the new Link Key will replace the old LinkKeySet.

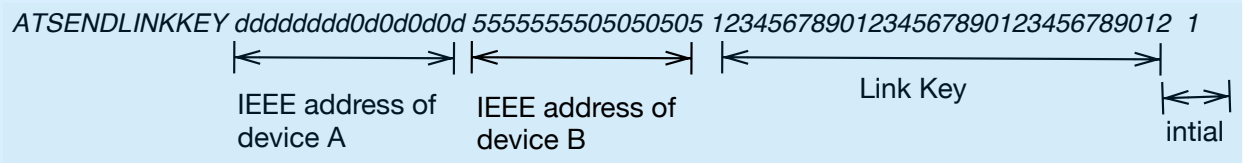
## 4.6 ATSENDLINKKEY

It transport a pair of Link-Key to two specified device that required to establish point to point security. If input Trust Center's own IEEE address as one of the specified device then point to point security will be establish between self (TC) and the other device.

Input:

| | |
|---|---|
| IEEE-64bit address (of device A) | 16 CHAR |
| IEEE-64bit address (of device B) | 16 CHAR |
| link key | 32 CHAR or 128-bit |
| initial value | 1 or |

Example:




## 4.7 ATCLRLINKKEY

It clears all of the Link Keys within the APS Pair Desc.

## 4.8 ATREQUESTKEY

If Key-Type = 1, ATREQUESTKEY request the Trust Center for the active network key that the coordinator is using at the moment. This NwkKeySet will automatically be transmitted to the requesting device.

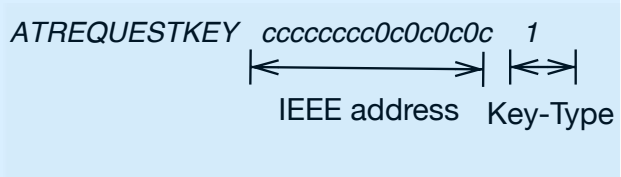
If device E1 wishing to establish point to point security with TC, input TC's MAC and Key-Type = 2. TC must already have a link key set against E1. Upon verification this LinkKeySet will be transmitted to E1.

If device E1 wishing to establish point to point security with device E2, the request will be sent to TC. After verification TC will automatically generate a new link key and send to both E1 and E2.

Input:

| | |
|---|---|
| IEEE-64bit address (get Active Network Key from this Device or get link Key for this Device) | 16 CHAR |
| Key-Type | 1 = Network Key, 2 = Link Key |

Example:



# 5. Procedures to Setup Network Layer Security

## *To setup a ZigBee Network with Network Layer Security*

*a. Verify NwkKeySet1 of all the ZigBees that are needed to establish network. Ensure they are identical. Use ATDUMP select NWK KEY to dump the Nwk Key tables, or in Parameter section view the Nwk Key directly.*

*b. If NwkKeySet1 not identical, use ATSETNWKKEY, or in Parameter section change to the correct NwkKeySet1, save and then reset.*

*c. Set the Coordinator as a Trust Center by using ATSTARTC or in Parameter section select Trust Center option, save and then reset.*

*d. Connect all ZigBee devices, allow to establish network*

*e. Test ATTXEACK, ATTXDATAU, and ATTXDATAB between devices within the network. All devices should be able to send and receive.*

## 5.1 Case Studies: NwkKeySet1's Influence on Network Establishment

In figure 1, C and E1 have the same NwkKeySet1, are security enabled and allowed to establish a secured network. All Data Transmission ATcmds between C & E1 will work.

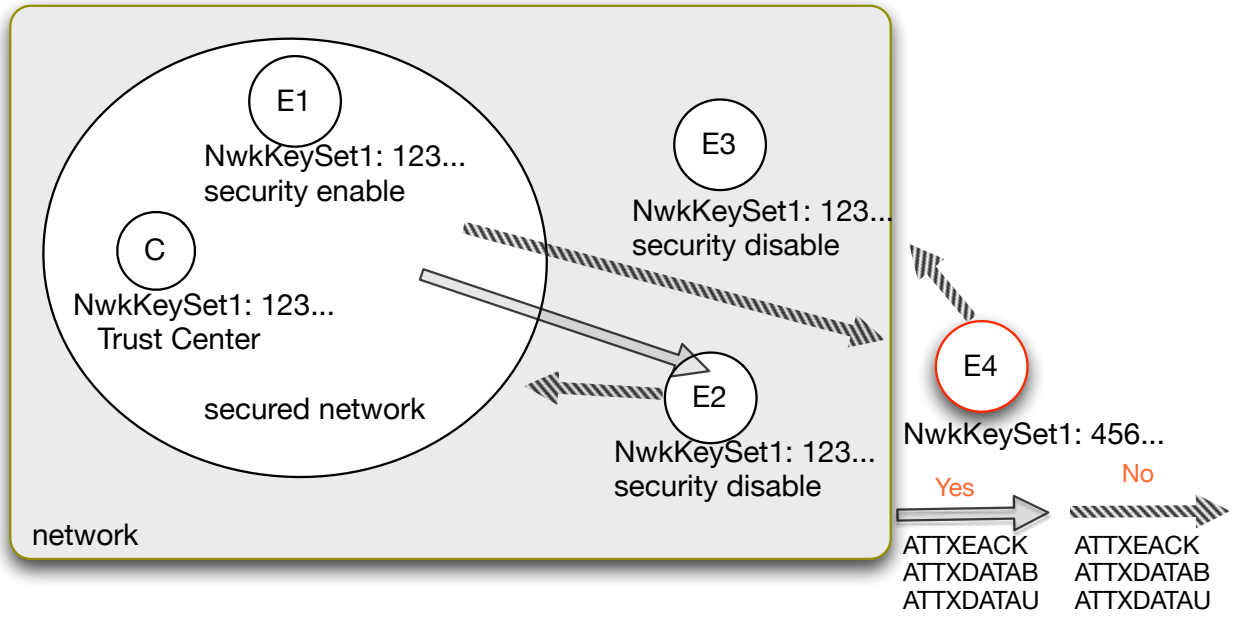


**Fig. 1**

E2 and E3 both also have the same NwkKeySet1 as C and E1. However, they are security disabled. They are not allowed to enter the secured network, but able to enter the network nevertheless.

When devices have the same NwkKeySet1, even a security disabled device could join the network, provided the Coordinator is setup as a Trust Center. Data Transmission ATCommands going outbound of the secured-network will work. This means E2 could receive from both C and E1. All Data Transmission in/out of network is not possible. All Data Transmission ATcmds between E2 & E3 will work.

E4 with a different NwkKeySet1 could be recognized by C and other devices in their ATNEIGHOR tables and vice versa. However, all Data Transmission in/out of network is not possible.

## 5.2 Case Studies: Network Key's Influence on Data Transmission

In figure 2, a secured network is established, with both Coordinator (C) and End Device 2 (E2) having three sets of Network Keys.

### *To setup Multiple NwkKeySets as Figure 2*

*a. After a secured network is established with the presence of identical NwkKeySet1 between the three devices, use ATSENDNWKKEY to transport NwkKeySet2 and NwkKeySet3 from C to E2.*

*note: The only way to set NwkKeySet2 and NwkKeyset3 is through ATSENDNWKKEY, since ATSETNWKKEY is only capable of setting NwkKeySet1.*

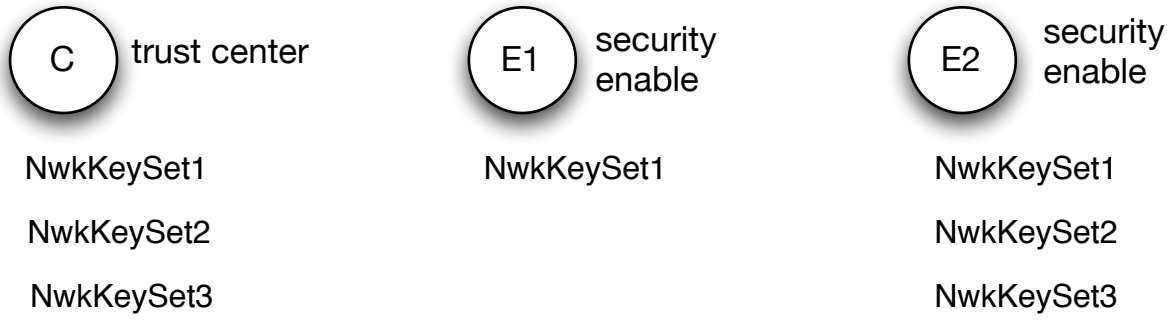



**Fig. 2**

## Data Transmission Rules and Network Keys

***C and E2***
***could receive any data that is ATTXDATAB, ATTXDATAU, or ATTXEACK from devices which has (key1 ,2, or 3). The Active-Key-SeqNum of the sending device does not matter.***

***E1***
***could only receive data that is ATTXDATAB, ATTXDATAU, or ATTXEACK from devices which the Active-Key-SeqNum is in key 1.***

❉ note: NwkKeySet1 not only influence Data Transmission Rules but also plays role in Security Network Establishment.

According to the Data Transmission Rules above, if E2's Active Key-SeqNum is in NwkKeySet3 and wants to send data to E1. E1 will not be able to receive. Therefore, C must use ATSWITCHKEY to inform E2 to change its Active Key-SeqNum to NwkKeySet1. Other ways of changing the Active Key-SeqNum is shown in figure 3 below.

## 5.3 Automatic Change of Active-Key-SeqNum

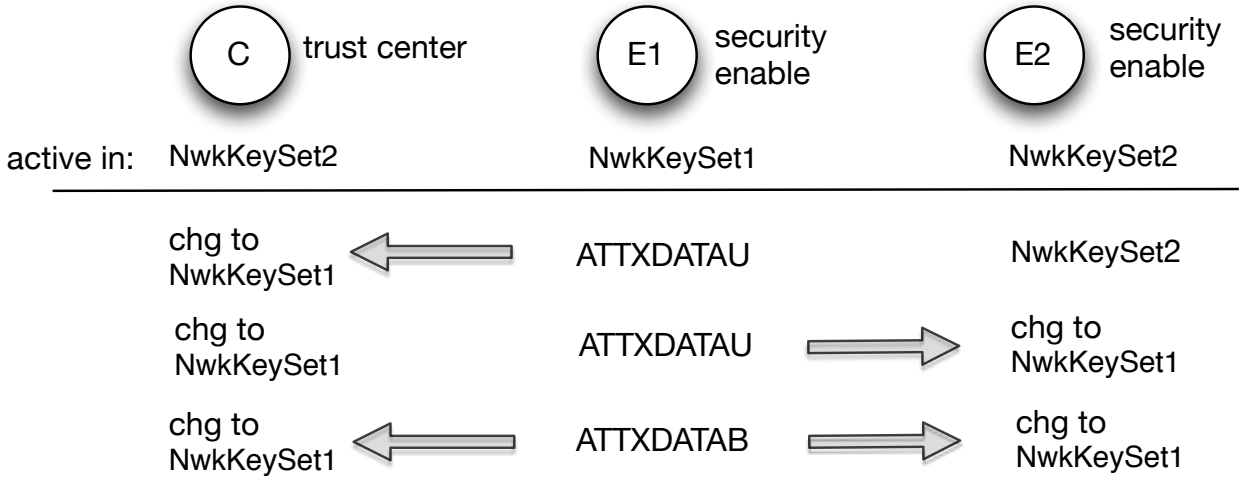



**Fig. 3**

Figure 3 shows the interesting behaviors of the Active-Key-SeqNum. Assuming that C, E1, and E2 all have the same NwkKeySets as in figure 2. Both C and E2 are currently active in NwkKeySet2 while E1 are active in NwkKeySet1. If E1 ATTXDATAU to C, C's

Active-Key-SeqNum will automatically change to NwkKeySet1 to match that of E1's while E2's Active-Key-SeqNum remains the same. If E1 ATTXDATAU to E2, both E2 and C will change its Active-Key-SeqNum to NwkKeySet1 to match that of E1's. In the third case, E1 will ATTXDATAB, both C and E2 will change its Active-Key-SeqNum to NwkKeySet1 again.

# 6. Procedures to Setup Point to Point Security

## *To setup secured unicast communications with Link Keys*

*Begin with a secured ZigBee network which has Network Layer Security enabled; Within this network we wish to setup three secured-unicast communications: C & E1, C & E2, and E1 & E4 (**Fig. 4**). The two possible procedures are as follows:*

*Using ATSETLINKKEY to set the Link Keys individually.*
*a. use ATSETLINKKEY in C, filing in E1's mac address and Link Key content (123...).*

*b. use ATSETLINKKEY in C, fililng in E2's mac address and Link Key content (12345...).*

*c. use ATSETLINKKEY in E1, filling in C's mac address and Link Key content (123...).*

*d. use ATSETLINKKEY in E1, filling in E4's mac address and Link Key content (14444...).*

*e. use ATSETLINKKEY in E2, filling in C's mac address and Link Key content (12345...).*

*f. use ATSETLINKKEY in E4, filling in E1's mac address and Link Key content (14444...).*

*OR*

*Trust Center use ATSENDLINKKEY to transport the blue LinkKeySets to E1 and self, green LinkKeySets to E2 and self, and purple LinkKeySets to E1 and E4.*

*a. C use ATSENDLINKKEY, input E1's mac address, C's own mac address, Link Key content (123...), initialize setting = 1*

*b. C use ATSENDLINKKEY, input E2's mac address, C's own mac address, Link Key content (12345...), initialize setting =1*

*c. C use ATSENDLINKKEY, input E1's mac address, E4's mac address, Link Key content (14444...), initialize setting =1*

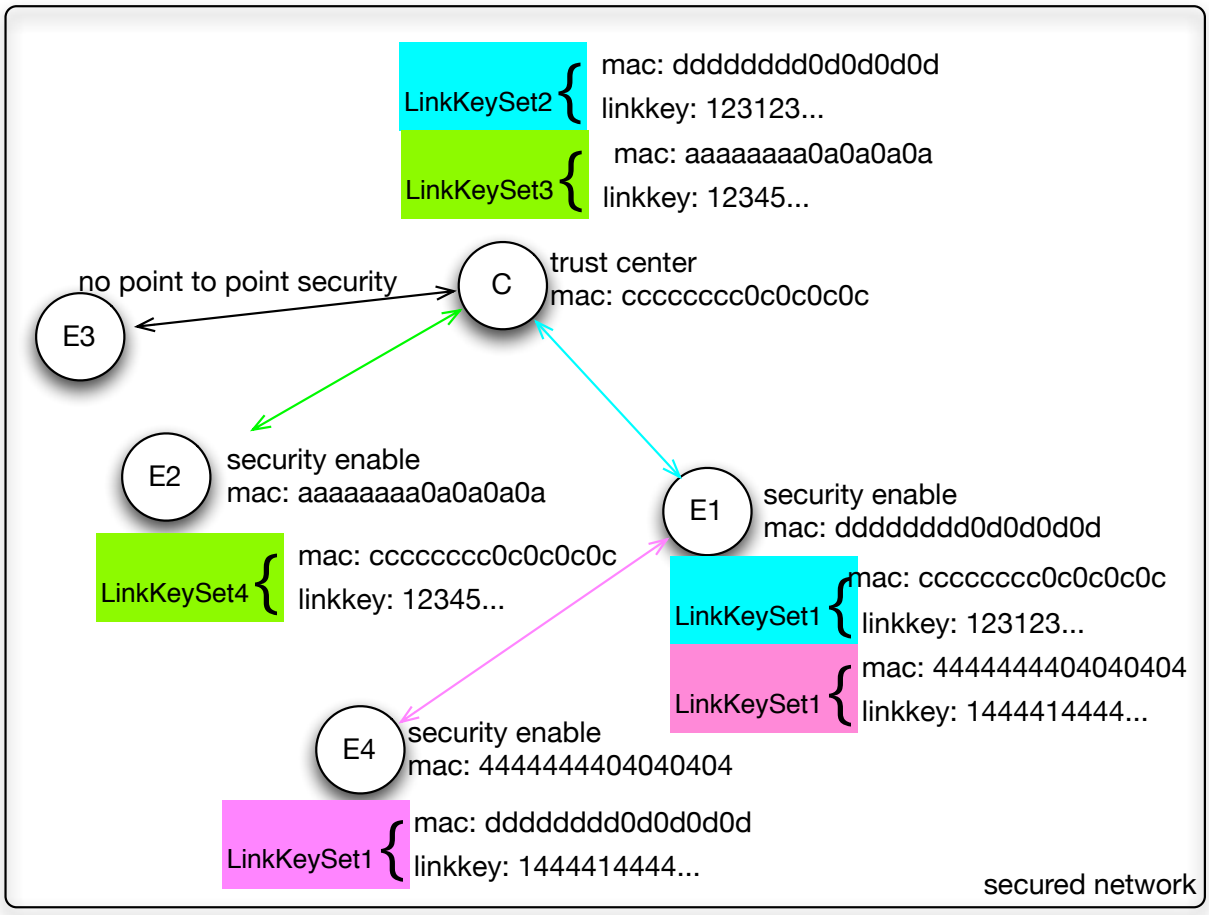



**Fig. 4**

All unicast communications between C and E1 are encrypted by the blue LinkKeySets. All unicast communications between C and E2 are encrypted by the green LinkKeySets. All unicast communications between E1 and E4 are encrypted by the purple LinkKeySets. E3 does not have any LinkKeySet established with C. Therefore, any ATTXDATAU between E3 and other devices will not be secured at the APS Layer level.

# 7. Abbreviations

**APS** - Application Support sublayer

**NWK** - Network

**TC** - Trust Center

**ZDO** - ZigBee Device Objects, defines the role of a device within the network (coordinator, router, or end device).