Department of Computer Science

FLORIDA TECH
FLORIDA'S STEM UNIVERSITY™

CSE 4820: Wireless and Mobile Security

16. Z-Wave

Dr. Abdullah Aydeger
Location: Harris Inst #310
Email: aaydeger@fit.edu

Outline

- Z-wave
  - Overview
  - Protocol Stack
  - Security

Recall: Zigbee: Network Discovery

- First assessment is to discover networks within range and enumerate the configuration of devices
  - Simple way; mimic Zigbee network discovery process with Killerbee
- Part of network discovery process in Zigbee Standard, ZDEs transmit beacon request on a given channel
  - All ZR and ZCs receiving beacon -> respond by sending a beacon frame
    - Disclose PAN ID, ZC or ZR source address, stack profile/version, extended IEEE address information
- Using same technique to actively scan for the presence of Zigbee network

Recall: Zigbee: Network Discovery

- Killerbee tool zbstumbler (similar to Wifi discovery tool Netstumbler):
  - Channel hops and transmits beacon request frames
    - Every two seconds hopping to a new channel
  - Display useful information from response beacon frames

```
test@test-HP-EliteBook-840-G3:~/killerbee$ sudo zbstumbler
[sudo] password for test:
Warning: You are using pyUSB 1.x, support is in beta.
zbstumbler: Transmitting and receiving on interface '1:11'
New Network: PANID 0xC762  Source 0xE2DA
        Ext PANID: 79:21:70:53:a3:d7:fc:34      Stack Profile: ZigBee Enterprise
        Stack Version: ZigBee 2006/2007
        Channel: 11
New Network: PANID 0xC762  Source 0xFF4F
        Ext PANID: 79:21:70:53:a3:d7:fc:34      Stack Profile: ZigBee Enterprise
        Stack Version: ZigBee 2006/2007
        Channel: 11
```

Recall: DoS Zigbee

- Silva/Nunes attack exploits a flaw in how recipients process inbound packets with regard to the IEEE 802.15.4 frame counter (FC) value
- When a transmitting node sends a secure packet, it includes a sequential frame counter value in each frame with a range of 0 to 0xffffffff-1
  - FC value is not encrypted but it is included in the calculation of MIC (Message Integrity Check) for a packet

Z-Wave

- Low-energy, mesh-networking protocol
- Predominately used in home automation (locks, garage door openers, thermostats)
  - Over 100 million products in use in homes
- Proprietary design by Sigma Systems and governed by standards established by Z-Wave Alliance
  - Does not share details of protocol outside of NDA (nondisclosure agreement)
  - Controls all fabrication and delivery of Z-Wave chips to product manufacturers

Z-Wave

- Aggressive power conservation for long battery life
  - Like Zigbee
- Using a <u>mesh networking</u> model to accommodate greater device range
- Relatively simple protocol
- Support for positive acknowledgement and frame retransmission, self-forming and dynamic routing topology updates, and application-specific profiles

Z-Wave Overview

- Z-Wave is based on a mesh network topology
  - Each (non-battery) device installed in the network becomes a signal repeater
  - As a result, the more devices you have in your home, the stronger the network becomes
- While Z-Wave signals easily travel through most walls, floors and ceilings, the devices can also intelligently route themselves around obstacles to attain seamless, robust, whole-home coverage

Z-Wave Overview

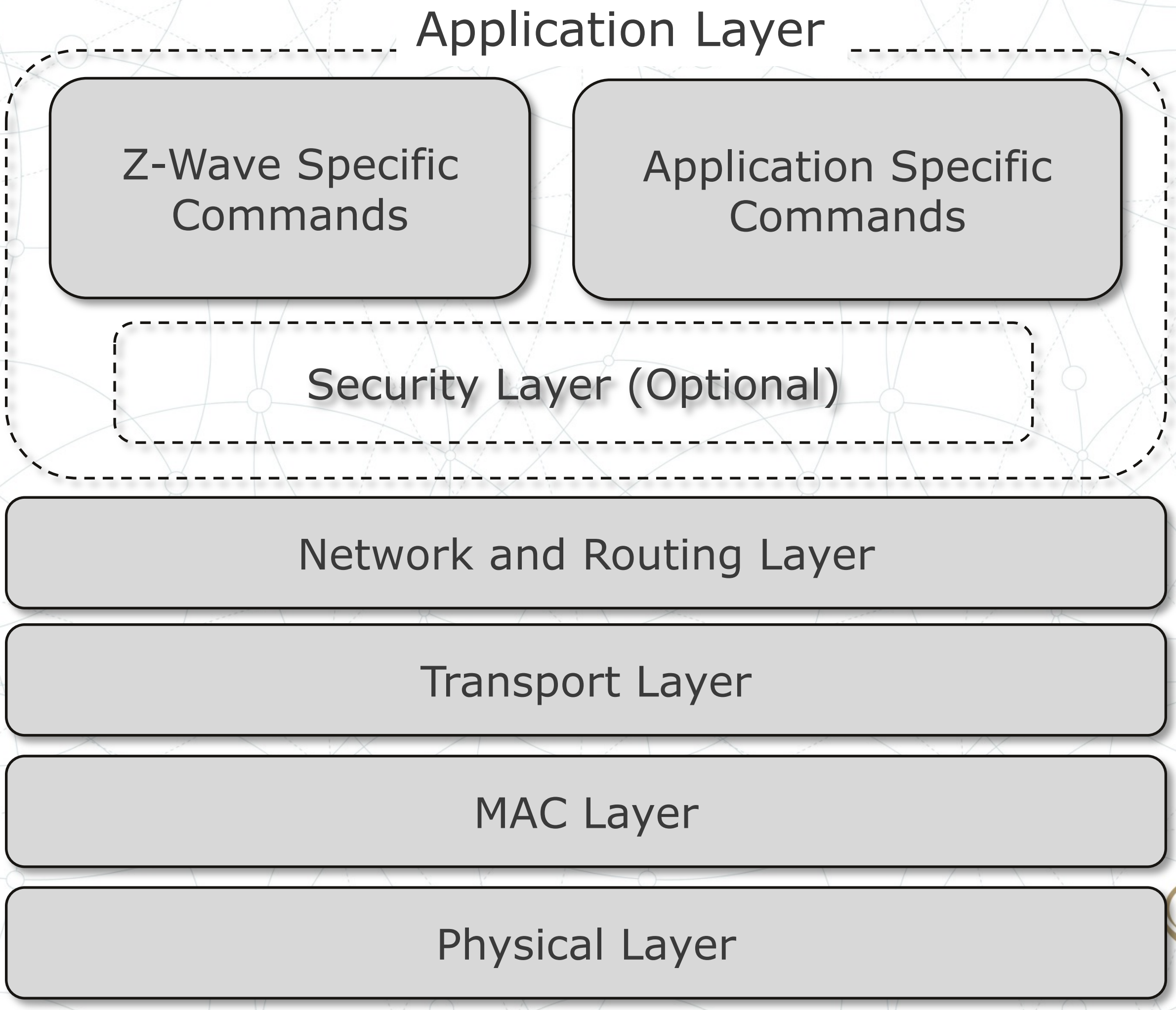
- While Z-Wave has a range of 100 meters (or 328 feet) in open air, building materials reduce that range (roughly every 30 feet)
  - Operates at 908.42 MHz in the United States and Canada
- The Z-Wave networks can be linked together for even larger deployments
- Each Z-Wave network can support up to 232 Z-Wave devices

Z-Wave Offers

- Extremely simple setup
  - Plug & Play
- Wireless Mesh Network
- Every non-battery node is a repeater
- Extremely robust
- Ultra-low power
  - Ideal for battery powered sensors
- Sub – 1GHz Frequency
- Multi speed: 40…100 kbps
- Low communication latency
- Interoperable
- Largest Home Control Community

Z-Wave Protocol Stack

- Uses structured protocol stack



Z-Wave PHY Layer

- Uses sub-1-GHz band to accommodate frequency variations in different countries

Profile	Data Rate	Encoding	Modulation	Packet Size
R1	9.6 Kb/s	Manchester	FSK	64 bytes
R2	40 Kb/s	NRZ	FSK	64 bytes
R3	100 Kb/s	NRZ	FSK	170 bytes

- Offers 3 different RF Profiles (R1, R2, and R3) with unique data rates, encodings, modulation, and packet frame sizes
  - R1 is deprecated by Z-Wave alliance but might be in use for some
- Range from 3 – 75 feet; depending on transmit power

Z-Wave MAC Layer

- Responsible for several attributes;
  - Packet framing and formatting
  - Positive ACK
  - Error detection
  - Retransmission of packets
  - Unicast, broadcast, and multicast processing
  - Address selection and allocation functions

Z-Wave MAC Layer

- Basic architecture of Z-Wave network: Controller device and slave devices
- Single primary controller device is responsible for establishing the network and selecting unique network identifier (i.e., HomeID)
- Controller devices are able to initiate a transmission on the network (polling or updating target devices) and responsible for maintaining network routing information
- Slave devices follow the instructions of controllers without dealing with how

Z-Wave MAC Layer

- Z-Wave controller;
  - Portable controller device; typically battery powered and is capable of relearning network topology as it moves about the home
  - Static controller device; powered through a consistent source and may also be connected to other networks, providing gateway services between the Z-Wave and IP network

Z-Wave MAC Layer Frame Format

- Varies depending on the RF profile
- Each Z-Wave network is uniquely identified by randomly selected value when the network is established, HomeID, that is transmitted as the first four bytes of each packet
  - Similar to IEEE 802.11 BSSID or Zigbee PAN ID
  - Used to differentiate Z-Wave networks in close physical proximity and associate all the nodes participating in the same network

Z-Wave MAC Layer Frame Format

- HomeID: Randomly selected 4-byte value chosen by controller
- NodeID: 1-byte value assigned to the node by the controller
  - Max 232 nodes (22 left for reserved, 1 for broadcast, 1 uninitialized)
- Frame Control: 16-bit field with several subfields

Z-Wave R1/R2 Frame Format

HomeID	Source Node ID	Frame Control	Length	Destination Node ID	Payload	FCS

Z-Wave R3 Frame Format

HomeID	Source Node ID	Frame Control	Length	Sequence number	Destination Node ID	Payload	FCS

Z-Wave MAC Layer Frame Control Format

- 16-bit frame control field represents several subfields with two reserved bits:
  - Routed; to indicate if packet <u>has been routed</u> by another node prior to delivery
  - Ack Request; to indicate that the receiving node <u>should ACK the packet</u>
  - Low Power; to indicate that the packet was transmitted <u>using low-power</u> output for reduced range
  - Speed modified (R1/R2 only); when a packet is transmitted at a <u>lower data rate than</u> what is supported by src/dst

Z-Wave MAC Layer Frame Control Format

- Header type; packet type (unicast/multicast/ACK/broadcast)
- Beam control; node shall be woken from power conservation state with continuous transmission
- Seq number (R1/R2 only); identify packet for subsequent ACK

Z-Wave R1/R2 Frame Control Format

Routed	Ack Req	Low Power	Speed Mod.	Header Type	Res.	Beam Control	Res.	Sequence Number

Z-Wave R3 Frame Control Format

Ack Req	Low Power	Res.	Header Type	Res.	Beam Control	Res.	Reserved

Z-Wave MAC Layer Fields

- Length field; indicates the length of the entire packet including the header, payload, and Frame Check Sequence (FCS)
- Destination NodeID is present in unicast and multicast frames to indicate the intended recipient
- Data payload; 0-54 bytes in R1/R2 nonmulticast, 0-25 bytes in multicast
  - R3; 0-158 bytes and 0-129 bytes
- FCS provides simple integrity check using XOR checksum for R1/R2 and CRC-16 for R3

Z-Wave R3 Frame Format

HomeID	Source Node ID	Frame Control	Length	Sequence number	Destination Node ID	Payload	FCS

Z-Wave Network Layer

- Defines device responsibilities and responsible for other network components such as HomeID selection and NodeID allocation process as well as network route establishment
- Z-Wave inclusion and exclusion for network connections

Z-Wave Network Layer: Inclusion

- Involves configuring the controller in inclusion mode (allowing it to accept new nodes) by pressing a physical button or choosing a menu item, and pressing a button on the new node to initiate an inclusion exchange
- When the new node initiates the inclusion process, it sends a Z-Wave node information frame using homeID of 0x00000000 and nodeID of 0x00 and a brodcast dest NodeID
  - Discloses the capabilities of the new device to the controller, which, in turn, allocates a NodeID to the new device for subsequent use on the network and updates routing tables to accommodate packet delivery to the new node

Z-Wave Network Layer: Exclusion

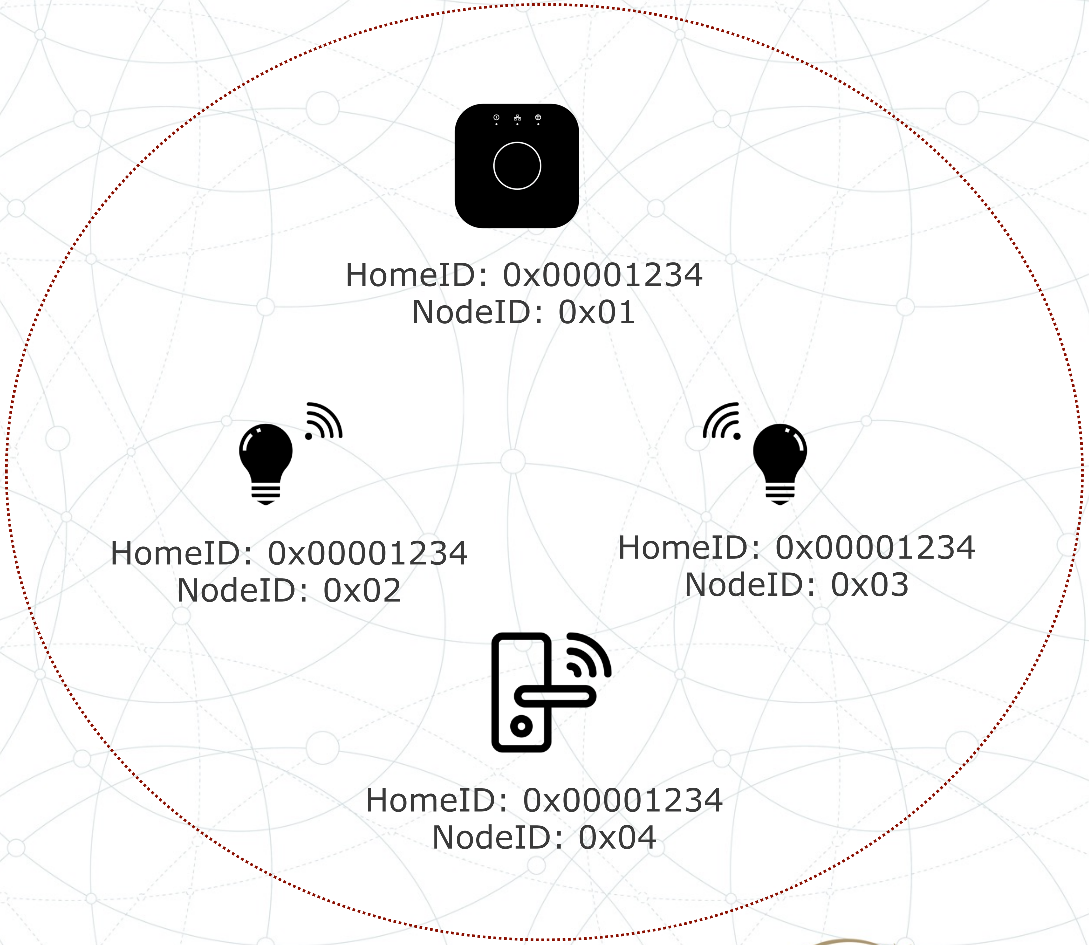
- Similar to inclusion but functionally opposite
- A node joined the Z-Wave network via inclusion <u>cannot leave</u> the network to join a different Z-Wave controller <u>without</u> completing the <u>exclusion process</u>
- Involves pressing a physical button on the controller and the device node, causing device to return to <u>unallocated nodeID 0x00</u>

Z-Wave Inclusion & Exclusion

- Strong component of the overall Z-Wave security
  - Requires <u>physical</u> access to the controller
- Is it secure enough?
  - What about spoofing?

Z-Wave Network Topology

- Nodes in a Z-Wave have a 1-byte NodeID, which must be different than every other node in the network
- Nodes in a Z-Wave network have a 4-byte HomeID, assigned by the controller at the time of inclusion
- Nearby networks must have different HomeIDs



Z-Wave Application Layer

- Responsible for <u>parsing</u> and <u>processing the data requests</u> and responses in the packet payload
- Handles both application-specific and Z-Wave application control data
- Basic application payload format:

Header	Command Class	Command	Command Class Data

Z-Wave Application Layer

- Z-Wave uses application command classes to differentiate actions and responses on the network
- Each command class supports one or more commands within the class that define the basic functionality of the application layer
  - For ex., CLASS_SWITCH_ALL command class is used to control multiple network devices for power on/off control so that the user can shut them all of with one single button

Z-Wave Application Layer

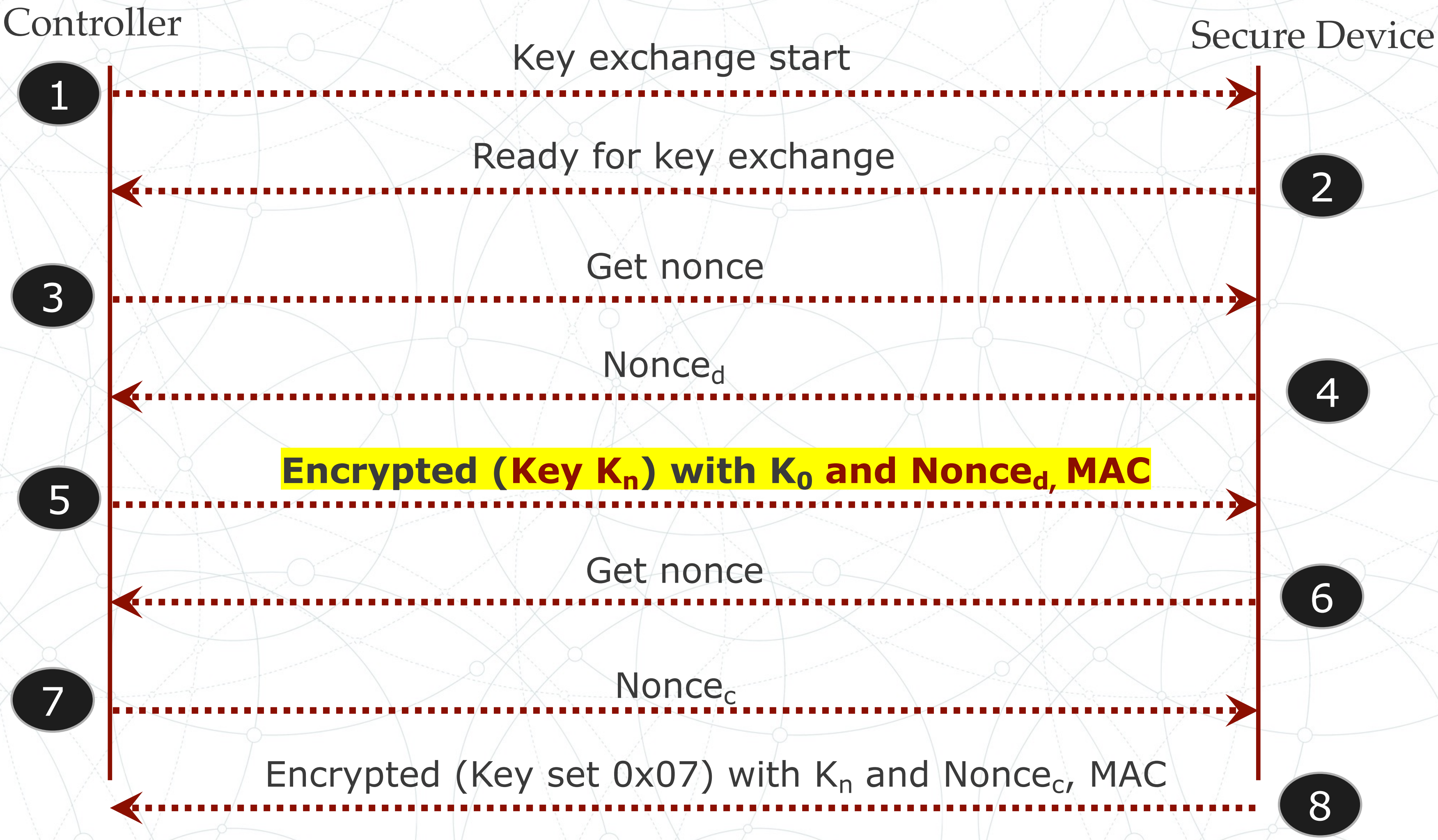
- Each Z-Wave application has well-defined set of functionality based on the device type and manufacturer application command class support
- At the application layer, Z-Wave uses command classes specified in ITU-T G.9959
  - Open source project such as OpenZWave are instrumental to understand and document the proprietary Z-Wave

https://github.com/openzwave/

Z-Wave Security

- Uses AES-OFB (Output Feedback Mode) to provide data confidentiality on the network
  - Conserve the amount of payload content transmitted in Z-Wave frames while being NIST (National Institute of Standards and Technology) approved
- AES CBC-MAC (cipher block chaining message authentication code) for data integrity protection
- CLASS_SECURITY command; key exchange process to derive keys

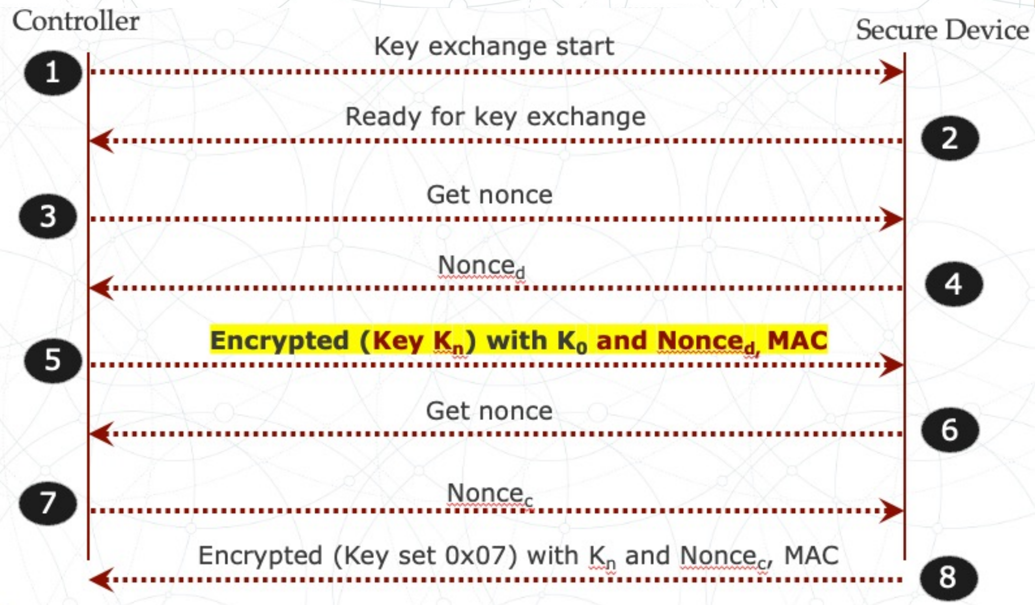
Z-Wave Key Exchange Process



Temporal Key
$K_0 =$ 16 bytes of 0x00

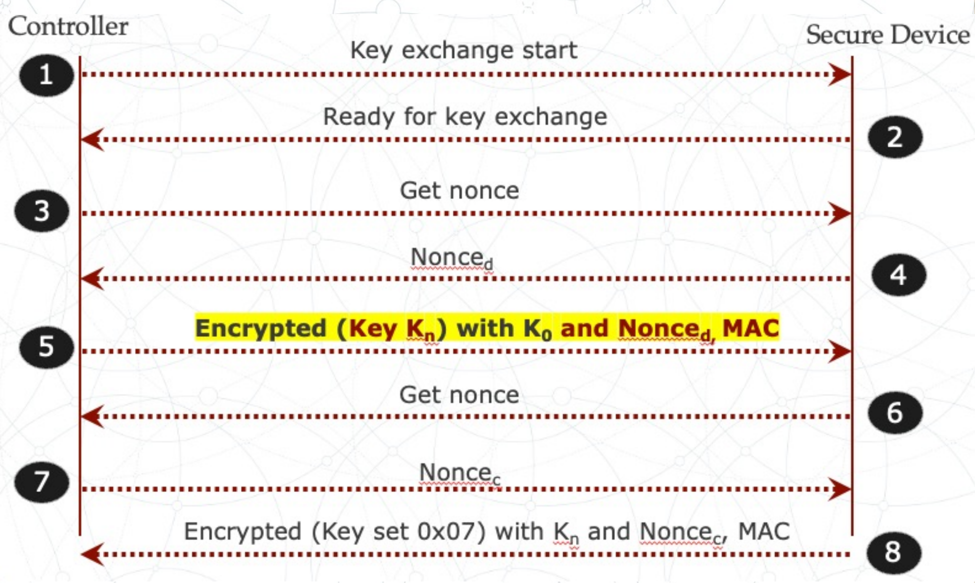
Network Key
$K_n =$ Chosen by controller

Z-Wave Key Exchange Process



- Step 1,2; controller and secure device prepare for the key exchange
- Step 3; controller requests nonce
- Step 4; with the nonce value, controller encrypts the network key K_n, using temporary key K_0
  - Network key is randomly selected by controller when the network is established and is unique for each Z-Wave network
  - Temporary key is an array of 16 bytes 0x00

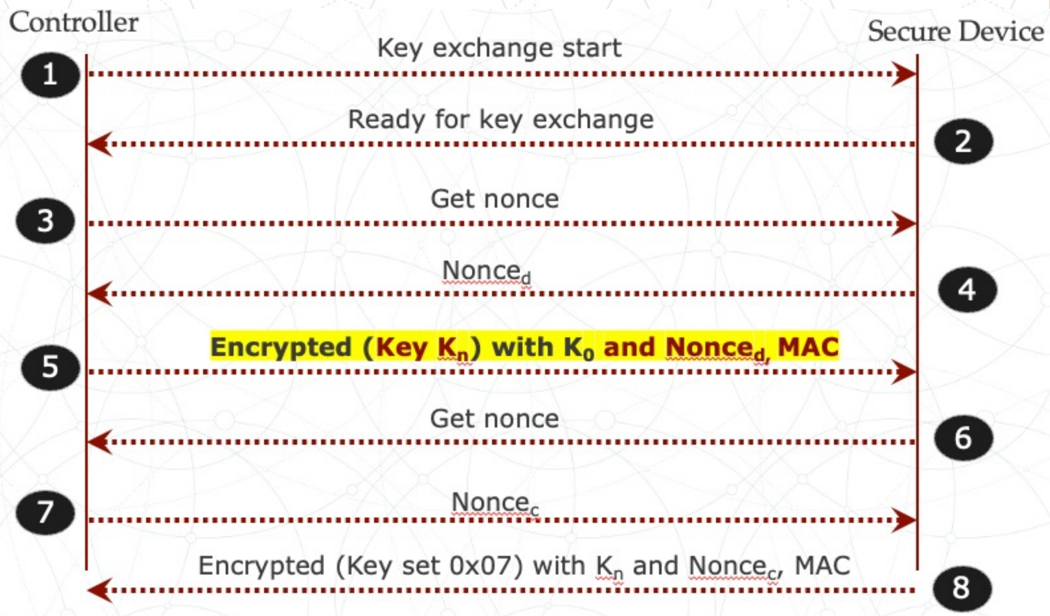
Z-Wave Key Exchange Process



- When the secure device receives encrypted network key K_n, and MAC from the controller, it validates the MAC and decrypts the message with K_0
  - Secure device then registers the decrypted K_n as the current key
- Next, step 6, secure device requests nonce from the controller

Z-Wave Key Exchange Process

- With the nonce value, secure device encrypts a "key set OK" message (hex 0x07) with K_n
- The controller receives the "key set OK" message validates that the packet was encrypted using K_n by validating MAC



Z-Wave Key Exchange Vulnerabilities

- MitM:
  - The secure device does not validate the identity of controller other than validating the MAC of encrypted Kn message using the temporary key K_0
  - Attacker can use any Z-Wave controller that support CLASS_SECURITY command class to intercept the inclusion process with a target device
    - Causing victim to associate to a malicious network

Z-Wave Key Exchange Vulnerabilities

- Key recovery attack:
  - There is no confidentiality protection in the delivery of the Kn key over the network since the K_0 is well known
  - Attacker passively observing the inclusion process can recover the network key K_n
    - Use it later to decrypt or forge arbitrary packets on the network

Z-Wave Key Exchange's Solution

- Low power inclusion mode
  - Controller and secure device transmit using minimal power capabilities
  - Require no more than 3 feet apart to complete the process
  - Also infrequent practice of adding new devices
  - Results in less opportunity for the attacker

Thank you.
Questions?

Dr. Abdullah Aydeger