Dynamic Secure Mesh for Collaborative Nodes of IoT devices

Who? Sylvia Entcheva, Sharil Tumin

From? Western Norway University of Applied Sciences (HVL.no)

Trimensity Tech (trimensity.eu)

When? CDVE 2023 (cdve.org)

Introduction

- Dynamic Mesh
- Secure Mesh
- Collaborative Nodes
- Stationary and roaming devices
- Dynamic routing
- No centralized controller
- IoT

IoT Architecture

1. Device Layer
2. Communication Layer
3. Security Layer
4. Application Layer
5. Cloud/Server Layer

Dynamic Mesh

- Two or more nodes can connect to form a mesh network
- A node send a `HEY` broadcast packet to join a mesh
- A node send a `BYE` broadcast packet to exit a mesh
- All nodes within the radio broadcasting range should react to these packets
- A node send a `HEY` at boot time and at regular intervals
- A node can send a `BYE` before going down
- All nodes do automatic cleanup of peer nodes

Secure Mesh

- When a node `X` receives the `HEY` packet from a node `Y` then `X` will send a unicast packet `AUQ` (authentication query) to `Y`
- When the node `Y` receives the `AUQ` packet from `X` then it will respond by sending unicast packet `AUR` (authentication response) to `X`
- The `AUQ` and `AUR` are authentication handshake.
- After authentication handshake `X` will have `Y` key and address likewise `Y` will have `X` key and address
- `X` and `Y` can now send encrypted unicast packet `MSG` to eachother

Collaborative Nodes

- All nodes listen and respond to broadcast packets `HEY` and `BYE`
- All nodes do authentication handshake
- All nodes forward `MSG` packets to all registered nodes in its list
- A `MSG` packet addressed to itself is not forwarded.
- A node with a plan shutdown or *deep-sleep* sends the `BYE` packet before doing so.
- All nodes are well-behave
- All nodes provide data and services to other nodes

Stationary and roaming devices

- Nodes are mostly stationary but some are mobile devices
- Stationary nodes join and rejoin the same mash
- Mobile nodes can be members of multiple mash-networks
- A mobile node act as a bridge between different mash-networks

Mobile node and mash-networks bridge

Mobile node M
MESH-1
MESH-2
MESH-3

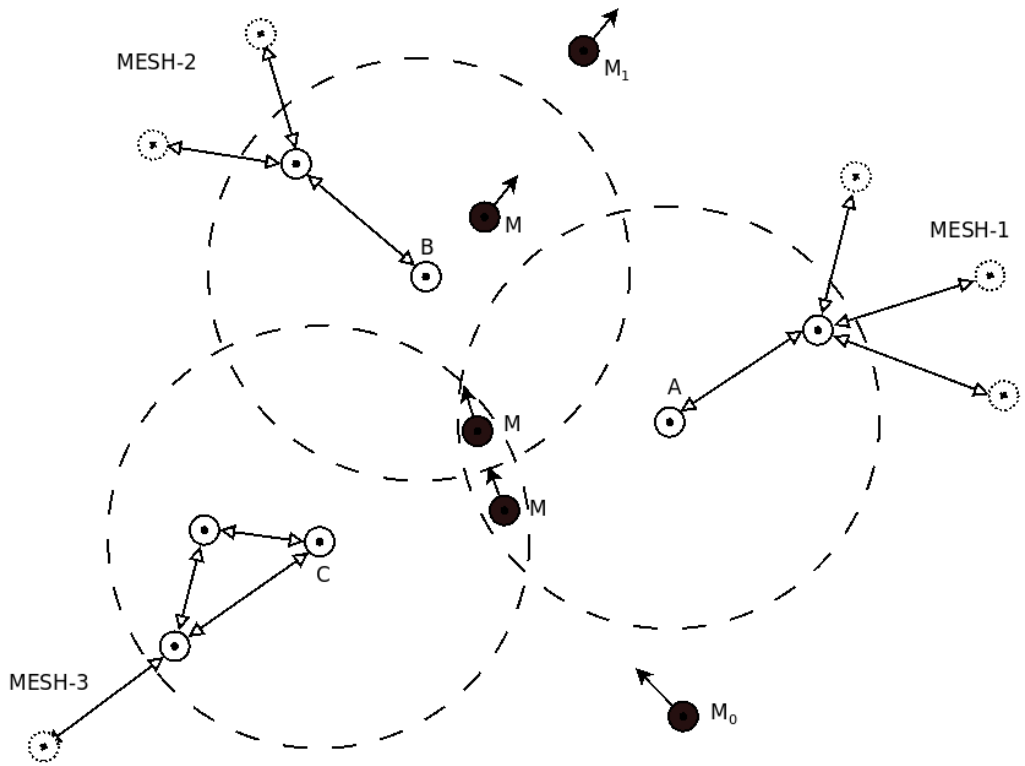

Figure 1: Mobile node bridging mash-networks

Mobile node positions

1. M0 out of range
2. M connects with A and C, bridging MESH-1 and MESH-2
3. M connects with A, B, and C, bridging all mash-networks
4. M connects with B only
5. M1 out of range

Dynamic routing

- Each nodes keeps a list of autenticated peer-nodes
- All `MSG` packets are forwarded to peer-nodes, except packet addressed to the node
- If `MSG` forwarding fail then delete the fail node from peer-nodes list
- At regular interval send `HEY` broadcast packet

No centralized controller

- No central broker
- All nodes can send `MSG` as published data
- All nodes can *subscribe* to any `MSG` packet
- Data and control packets flow freely and up to each node to process these packets according to its business logic.

IoT

Mesh To Cloud

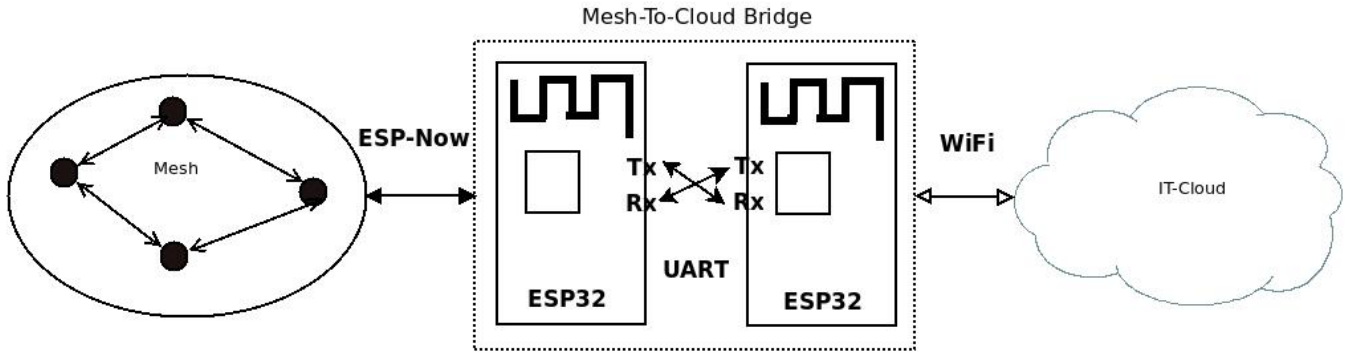

Figure 2: Two ESP32 with UART perform a Mesh-To-WiFi Bridge

Implementation

- ESP MCUs
- ESP-NOW
- MicroPython

ESP32 MCUs

ESP32
ESP32-C3
ESP32-S2
ESP32-S3

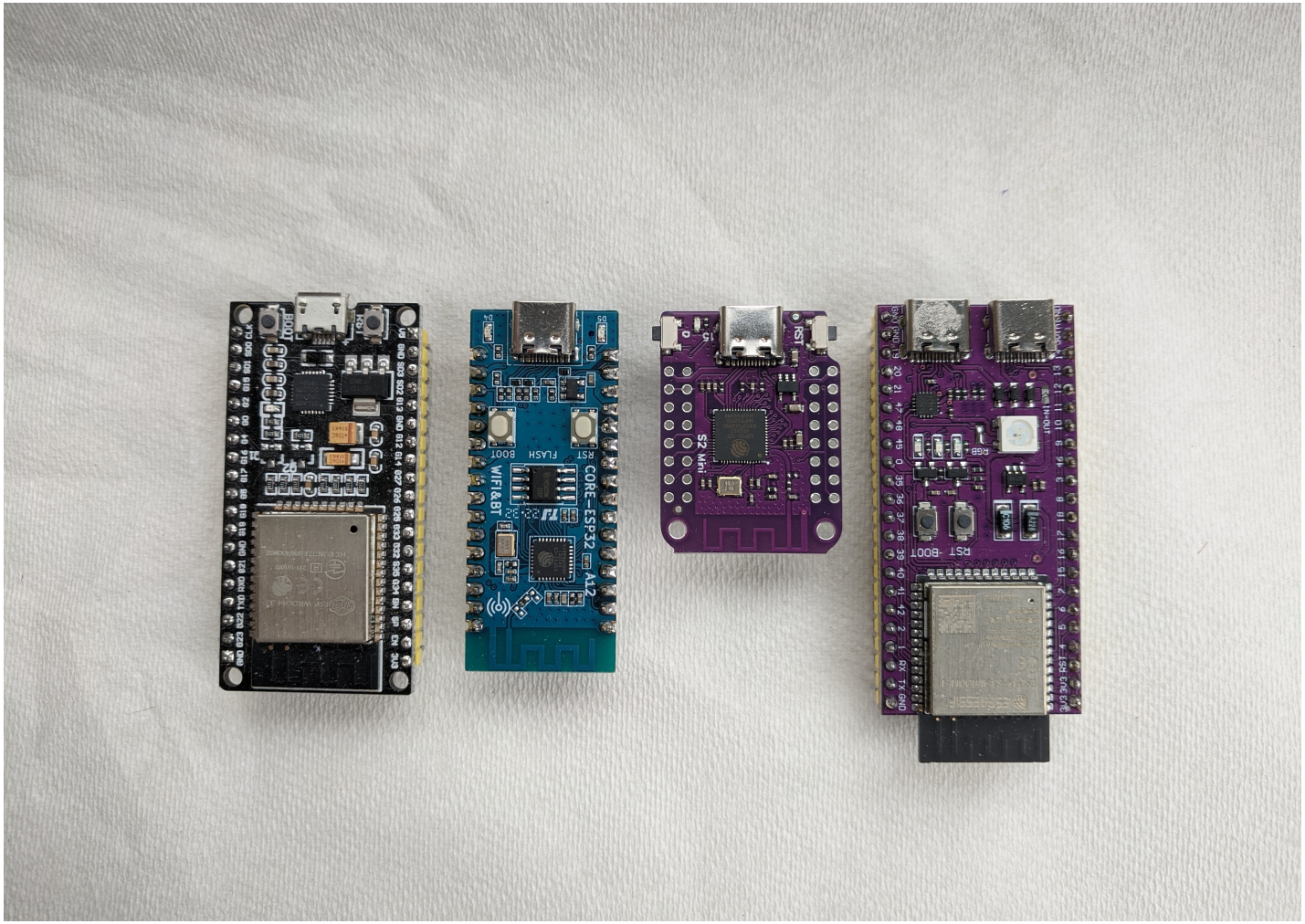

Figure 3: (L-to-R) ESP32 ESP32-C3 ESP32-S2 ESP32-S3

ESP32 Types

ESP32 MCUs Resource Table

Soc	MCU	Speed	Memory (KB)			GPIO	Radio Chip	
	32Bits Core	MHz	RAM	RTC	ROM	Pins	WiFi	Bluetooth
ESP32	2 Xtensa LX6	240	448	16	448	34	2.4GHz	Classic, BLE
ESP32-C3	1 RISC-V	160	400	8	384	22	2.4GHz	BLE5
ESP32-S2	1 Xtensa LX7	240	320	16	128	43	2.4GHz	-
ESP32-S3	2 Xtensa LX7	240	512	16	384	45	2.4GHz	BLE5

Figure 4: ESP32 Chipsets

ESP-NOW

OSI vs
ESP-NOW

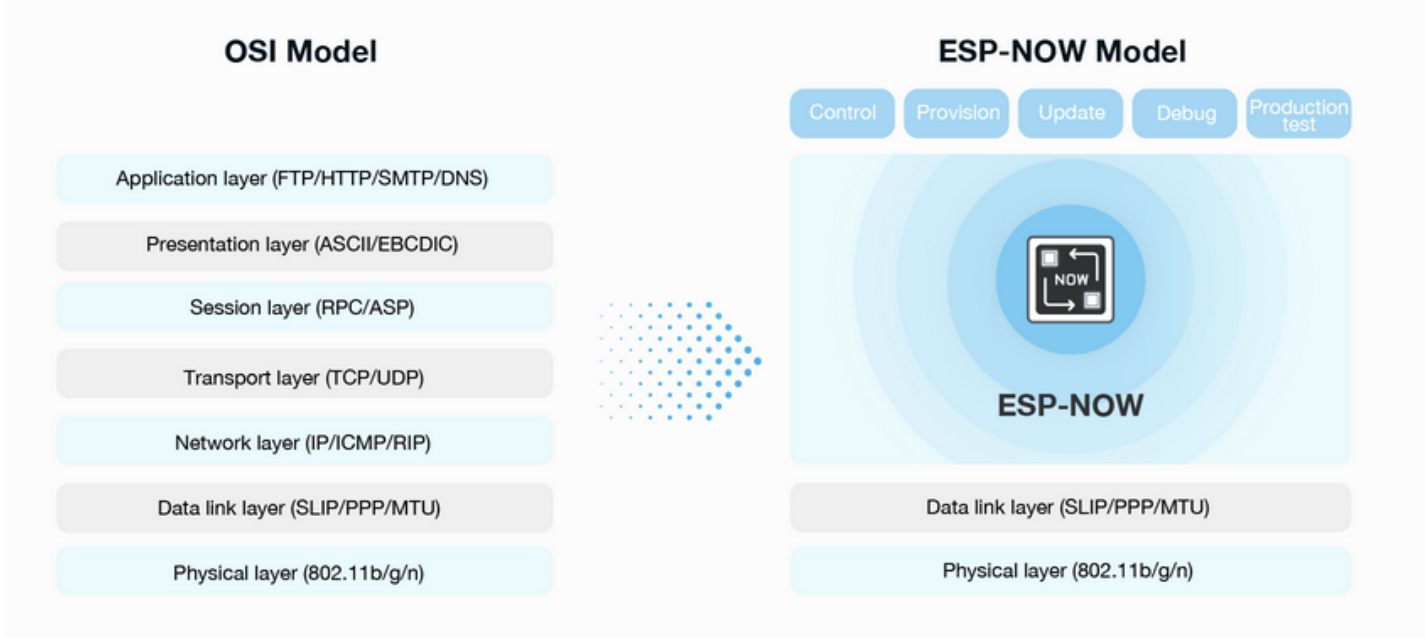

Figure 5: ESP-NOW Model

ESP-NOW

- Operate at network layer
- Connectionless communication protocol defined by Espressif
- Max 20 devices can be paired (17 with encrypted mode)
- Use MAC to address devices
- Data size is limited to 250 bytes (IEEE 802.11 vendor-specific element field of action frame which is only 1 byte 0xff = 255)

ESP-NOW Transmission Modes

1. one-to-one
2. one-to-many
3. one-to-all

Protocol		MAC		Accessible nodes	Message Type
Mode	Transmission	Source	Destination		
one-to-one	unicast	a2b388991111	17ef23de3434	(3)	AUQ, AUR, MSG
one-to-many	multicast	a2b388991111	a2b388ffffff	(2)	-
one-to-many	multicast	a2b388991111	a2b3ffffffff	(2, 4)	-
one-to-all	broadcast	a2b388991111	ffffffffffff	(2, 3, 4)	HEY, BYE
one-to-all	broadcast	17ef23de3434	ffffffffffff	(1, 2, 4)	HEY, BYE

With 4 nodes with these MAC addresses: (1) a2b388991111, (2) a2b388122222, (3) 17ef23de3434, and (4) a2b389ba4545

MicroPython

Time for DEMO

Conclusion

- ESP-NOW is a non-standard protocol run on Espressif MCU
- MicroPython is an open-source high level language for MCU
- Dynamic mesh is usefull for
  - smart home automation,
  - smart cities,
  - smart grid,
  - smart healthcare,
  - IIoT (Industrial IoT),
  - environmental monitoring,
  - disaster response and recovery,
  - smart agriculture and farming,
  - smart transportation, wildlife
  - tracking and conservation

Thanks

Preparation	This presentation is the work of Sharil Tumin and Sylvia Encheva.
Presented	This paper was presented by Petra, an AI virtual assistant.
Recorded	Presentation recorded for presentation at CVDE2023.
Contact	Any question please submit as an issue at github repository
Github repository	`https://github.com/shariltumin/mesh-espnow-micropython`

CDVE 20th anniversary

Congratulation and celebration