An Alternative Approach for Enhancing Security of WMANs using Physical Layer Encryption

By

Arpan Pal
Wireless Group
Center of Excellence for Embedded Systems
Tata Consultancy Services
India

Agenda

- Security Threats of Wireless MAN
- Proposed System Overview
- Proposed System Features
- How the proposed system mitigate the security threats
- Conclusion

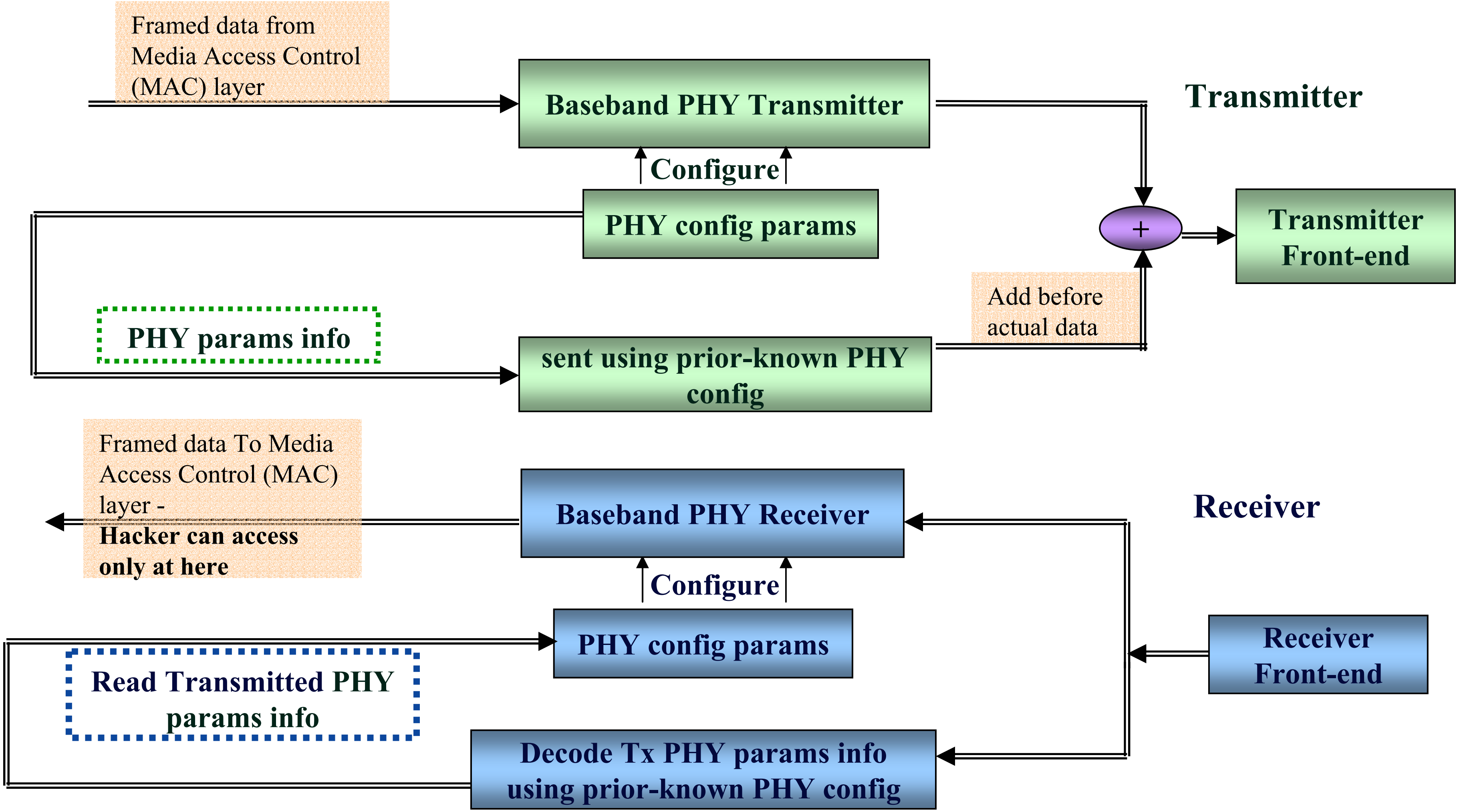
Security Threats of Wireless MAN

- Human Initiated Events
- Data Privacy
- Data Forgery
- Denial of Service
- Hardware Errors

Data Privacy, **Data Forgery** and **Denial of Service** are the main security events that need to be addressed

**Ref:- Alan Chickinsky, “Wireless Security Threats”,
IEEE C802.20-03/06, January 2003**

System Overview – Traditional System



Framed data from Media Access Control (MAC) layer

Baseband PHY Transmitter

Transmitter

Configure

PHY config params

+

Transmitter Front-end

Add before actual data

PHY params info

sent using prior-known PHY config

Framed data To Media Access Control (MAC) layer -

Hacker can access only at here

Baseband PHY Receiver

Receiver

Configure

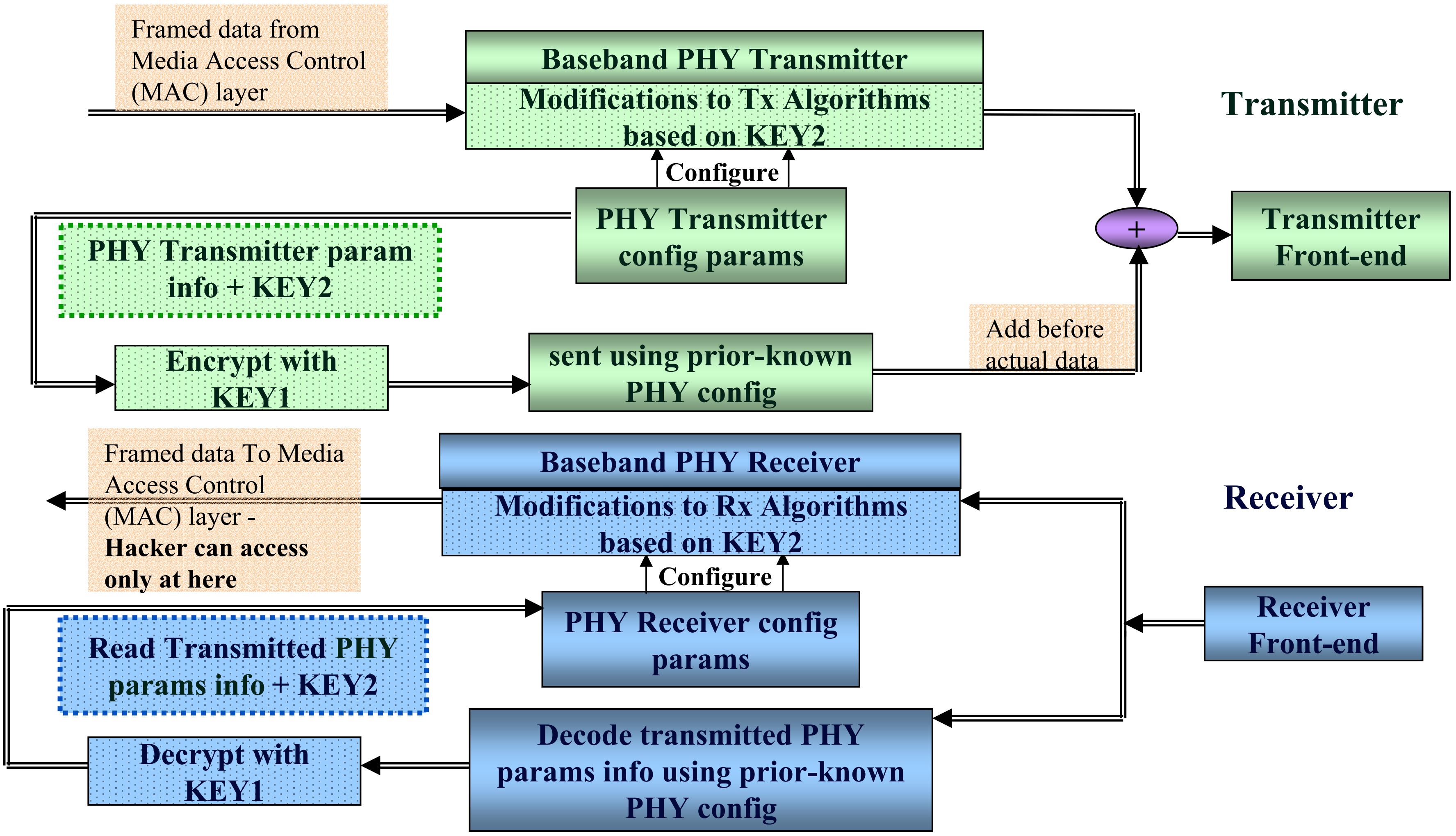
PHY config params

Receiver Front-end

Read Transmitted PHY params info

Decode Tx PHY params info using prior-known PHY config

System Overview – Proposed System

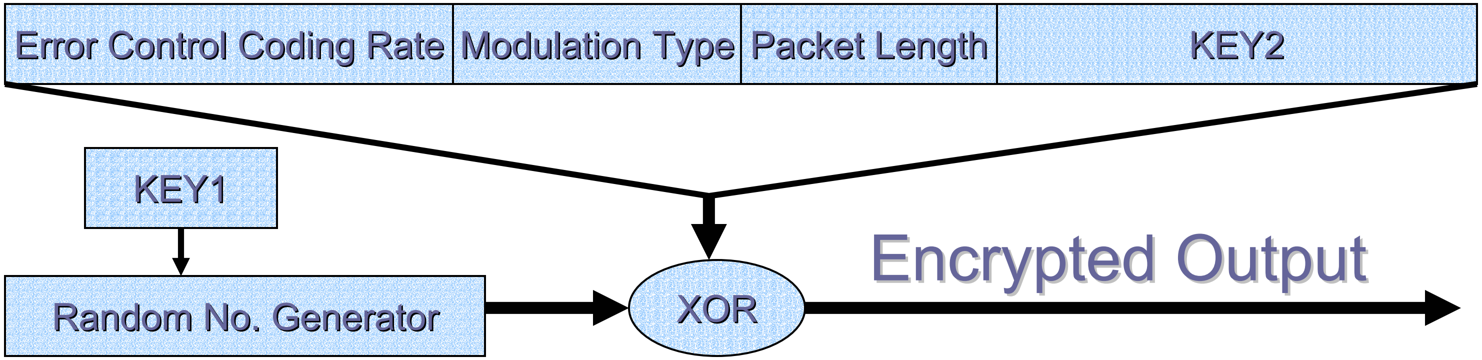


Framed data from Media Access Control (MAC) layer
Baseband PHY Transmitter
Modifications to Tx Algorithms based on KEY2
Transmitter
Configure
PHY Transmitter config params
+
Transmitter Front-end
PHY Transmitter param info + KEY2
Add before actual data
Encrypt with KEY1
sent using prior-known PHY config
Framed data To Media Access Control (MAC) layer - **Hacker can access only at here**
Baseband PHY Receiver
Modifications to Rx Algorithms based on KEY2
Receiver
Configure
PHY Receiver config params
Receiver Front-end
Read Transmitted PHY params info + KEY2
Decrypt with KEY1
Decode transmitted PHY params info using prior-known PHY config

Proposed System Features

- KEY1 delivered to valid users using some secure key distribution mechanism
- Possible Physical layer system parameters encrypted using KEY1
  - Error Control Coding Rate
  - Type of Modulation
  - Length of Packet
  - Second Level Key KEY2
- Possible Physical layer system parameters modified using KEY2
  - Interleaving Pattern
  - Phase offset of OFDM symbols
  - Constellation Mapping

Proposed System - Example



- ❑ KEY2 can be varied from packet to packet
- ❑ One may modify using random numbers seeded by KEY2
  - Phase offset of OFDM symbols at IFFT input

Note:- Phases of only data points (excluding pilots and zero padding) should be altered

Proposed System – Application to 802.20

- Physical Layer of 802.20 is evolving
- OFDM could be an integral part of PHY given the operational scenario
- The proposed scheme can easily be adapted to the 802.20 OFDM PHY
- The proposed scheme is not limited to OFDM PHY only

Mitigation of Security Threats - Data Privacy

- Known-Plaintext Attack
- Recording of encrypted data at MAC level
- Key can be found out if Data is known

- Proposed Scheme prevents hackers from recording correct encrypted data at MAC level

  (wrong FEC rate, wrong modulation, unknown phase offset, unknown interleaving pattern etc.)

Mitigation of Security Threats - Data Forgery

- Unauthorized users insert data into network as valid user
  - Replay
  - Mimicking

- Proposed Scheme prevents hackers from both Replay and Mimicking
  - Replay is not possible as the data recorded at MAC layer is totally wrong and hence cannot be replayed
    to generate a valid message
  - Mimicking is not possible because this needs finding out the key first (using Known-Plain-Text attack)

Mitigation of Security Threats - Denial Of Service

- Intruder can flood network with valid and invalid messages
- Channel jamming at RF level

- Proposed Scheme prevents hackers from sending valid messages as they don't know the Key
- Invalid messages can be filtered out in the PHY level as the encryption is taking place in PHY layer itself
- Channel jamming at RF level cannot be prevented

Conclusion

- Data Privacy, Data Forgery and Denial-of-Service (valid messages) at MAC layer (software) can be prevented
- Denial-of-Service (invalid messages) can be prevented using PHY layer message integrity check
- Denial-of-Service (Channel jamming at RF level) cannot be prevented
- To break into the proposed security scheme, hackers need costly hardware set-up
- Even with Hardware set-up, breaking the system in Real-time is extremely difficult – the PHY level ciphering substantially increases the entry barrier for break-in
- A good KEY distribution scheme need to be explored

Thank You

Email: arpan_pal@tcscal.co.in