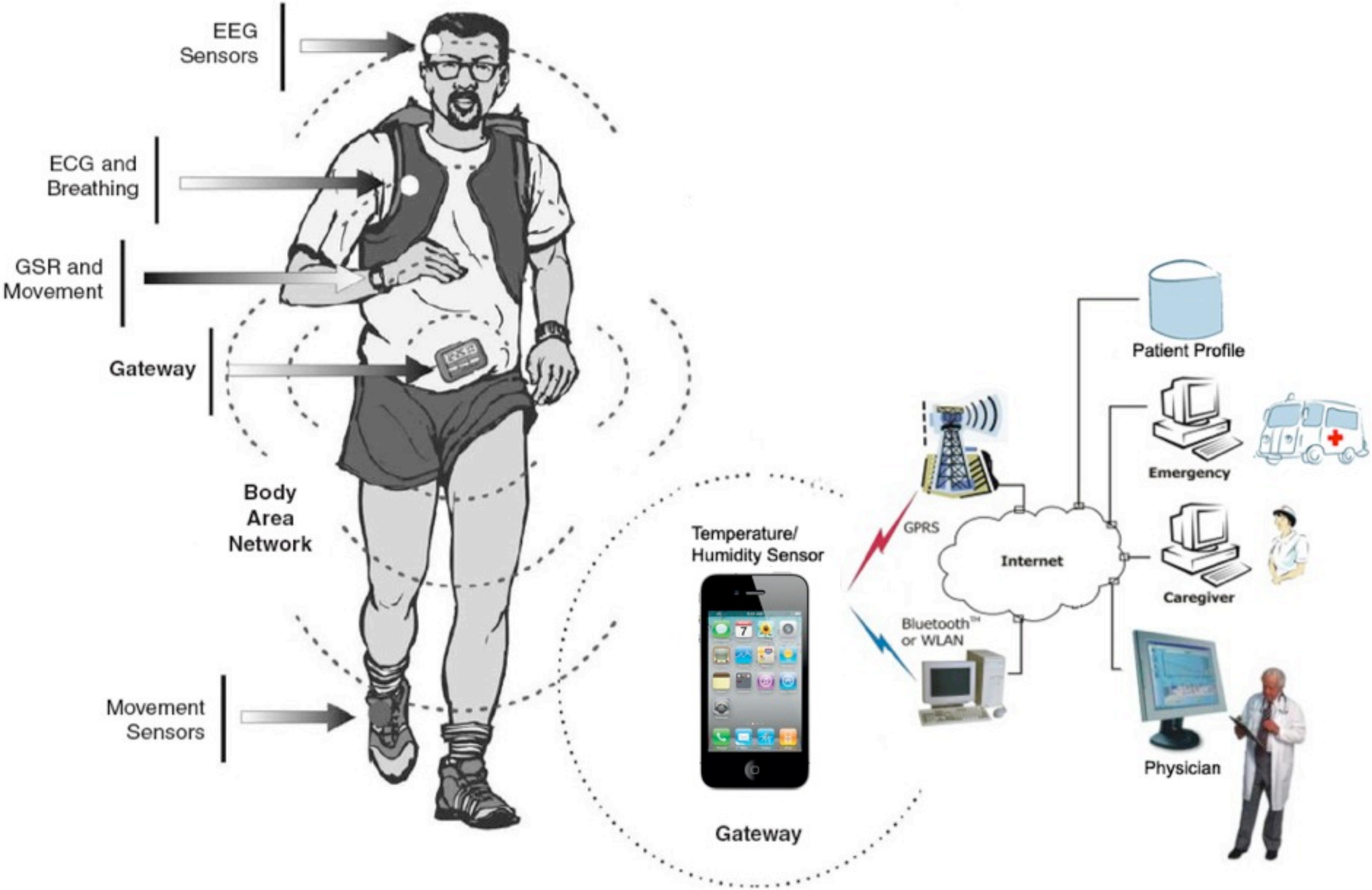
# Adaptive security and privacy for mHealth sensing

**Shrirang Mare[1],** Jacob Sorber[1], Minho Shin[2], Cory Cornelius[1], and David Kotz[1]

[1] Dartmouth College, USA
[2] Myongi University, South Korea




Source: Javanov et. al., *Stress Monitoring Using a Distributed Wireless Intelligent Sensor System*,


Source: Javanov et. al., *Stress Monitoring Using a Distributed Wireless Intelligent Sensor System*,


Source: Javanov et. al., *Stress Monitoring Using a Distributed Wireless Intelligent Sensor System*,


**Secure, private, and efficient**
protocol

Source: Javanov et. al., *Stress Monitoring Using a Distributed Wireless Intelligent Sensor System*,

# Wireless protocols

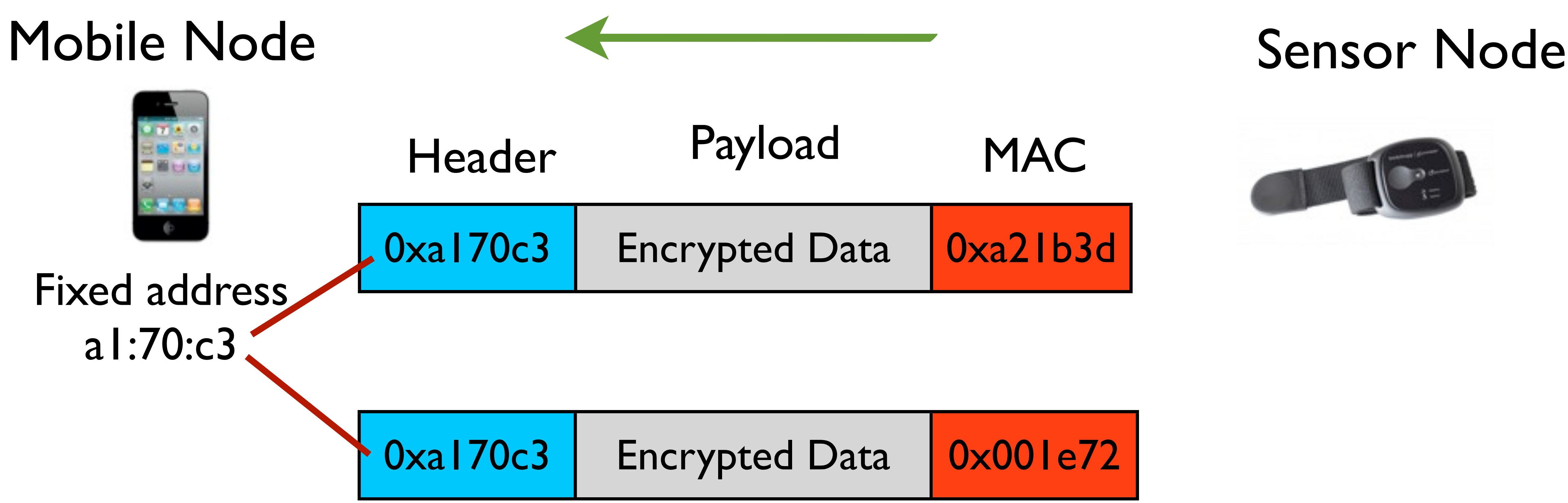
Mobile Node

Fixed address
a1:70:c3

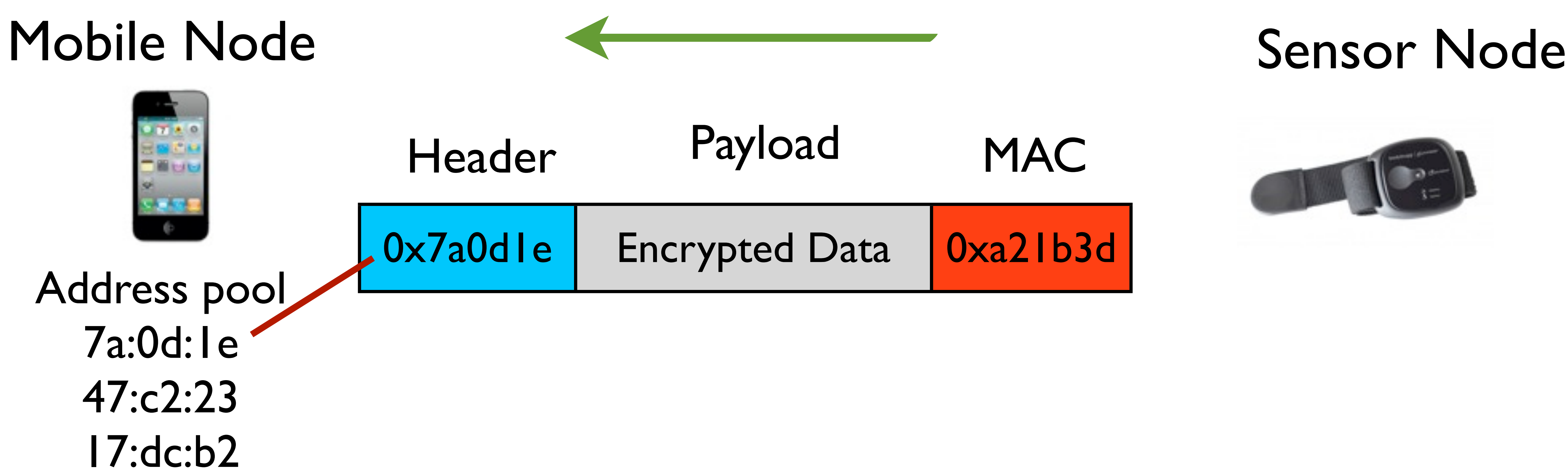
| Header | Payload | MAC |
|---|---|---|
| 0xa170c3 | Encrypted Data | 0xa21b3d |

Sensor Node

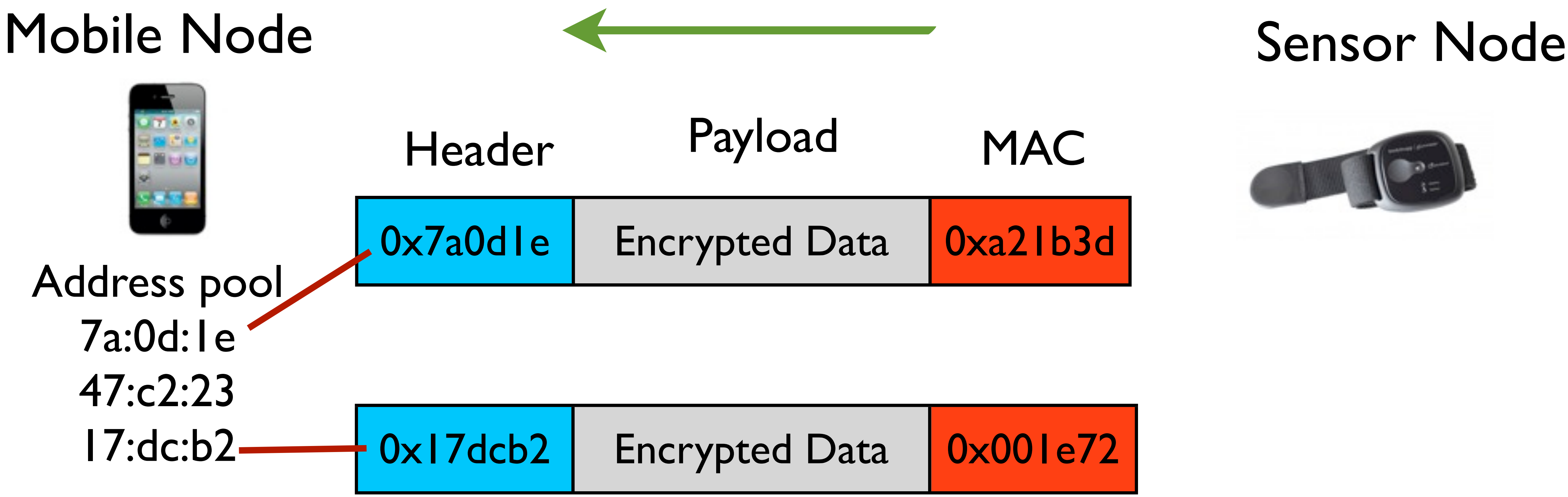
# Wireless protocols



# Privacy preserving wireless protocols

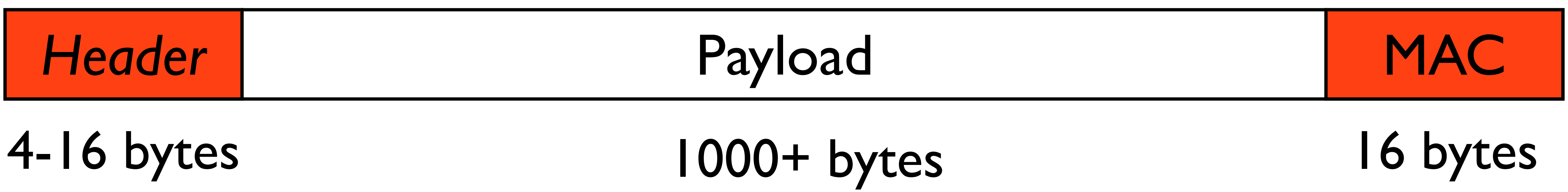


# Privacy preserving wireless protocols



# Packet overhead

In Wi-Fi networks



# Packet overhead

In Wi-Fi networks

*Header* Payload MAC

4-16 bytes 1000+ bytes 16 bytes

In medical sensor networks

Payload

~10-50 bytes

# Packet overhead

In Wi-Fi networks

| *Header* | Payload | MAC |
|---|---|---|
| 4-16 bytes | 1000+ bytes | 16 bytes |

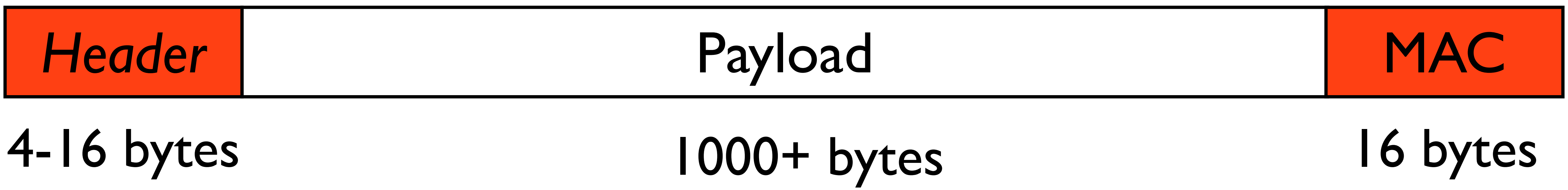
In medical sensor networks

| Header | Payload | MAC |
|---|---|---|

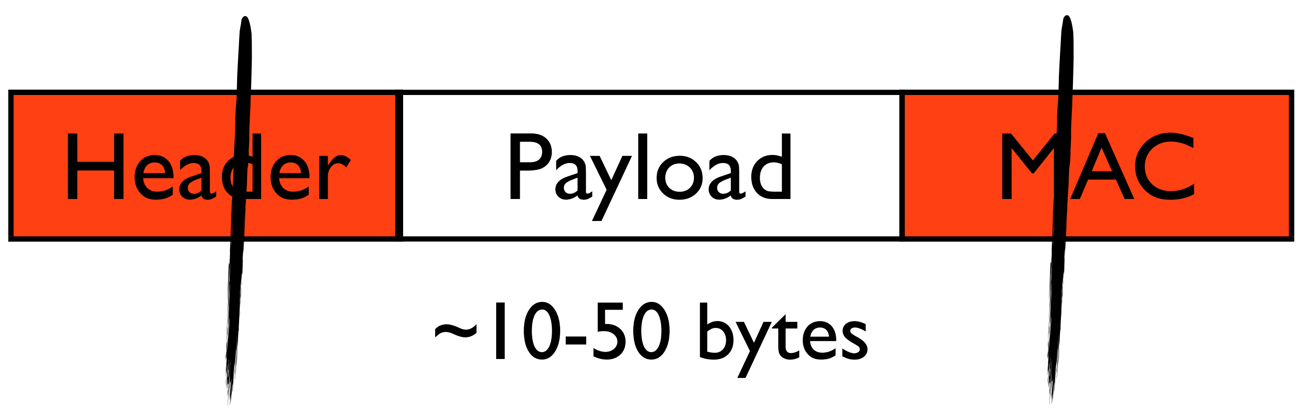
~10-50 bytes

# Packet overhead

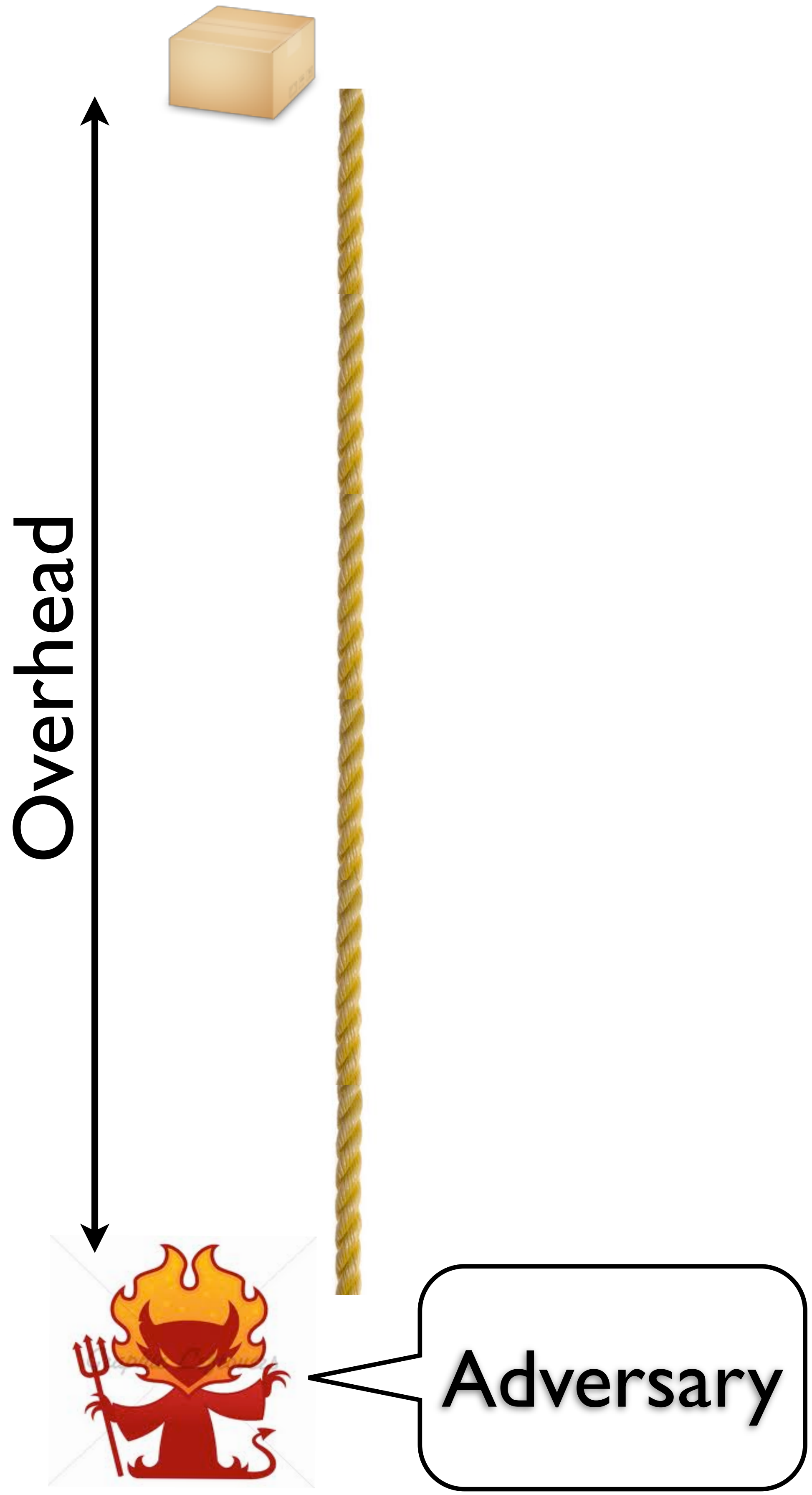
In Wi-Fi networks



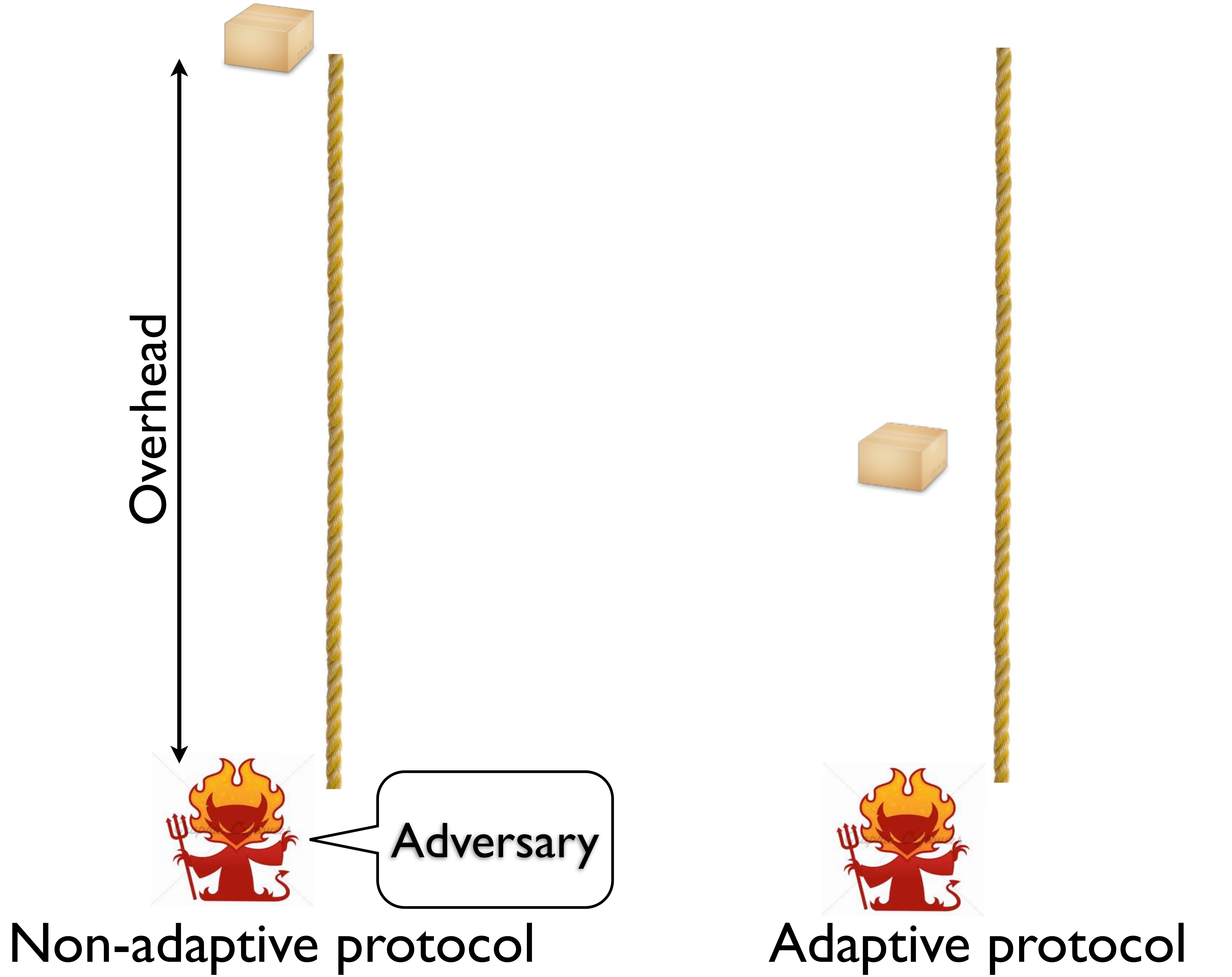

In medical sensor networks



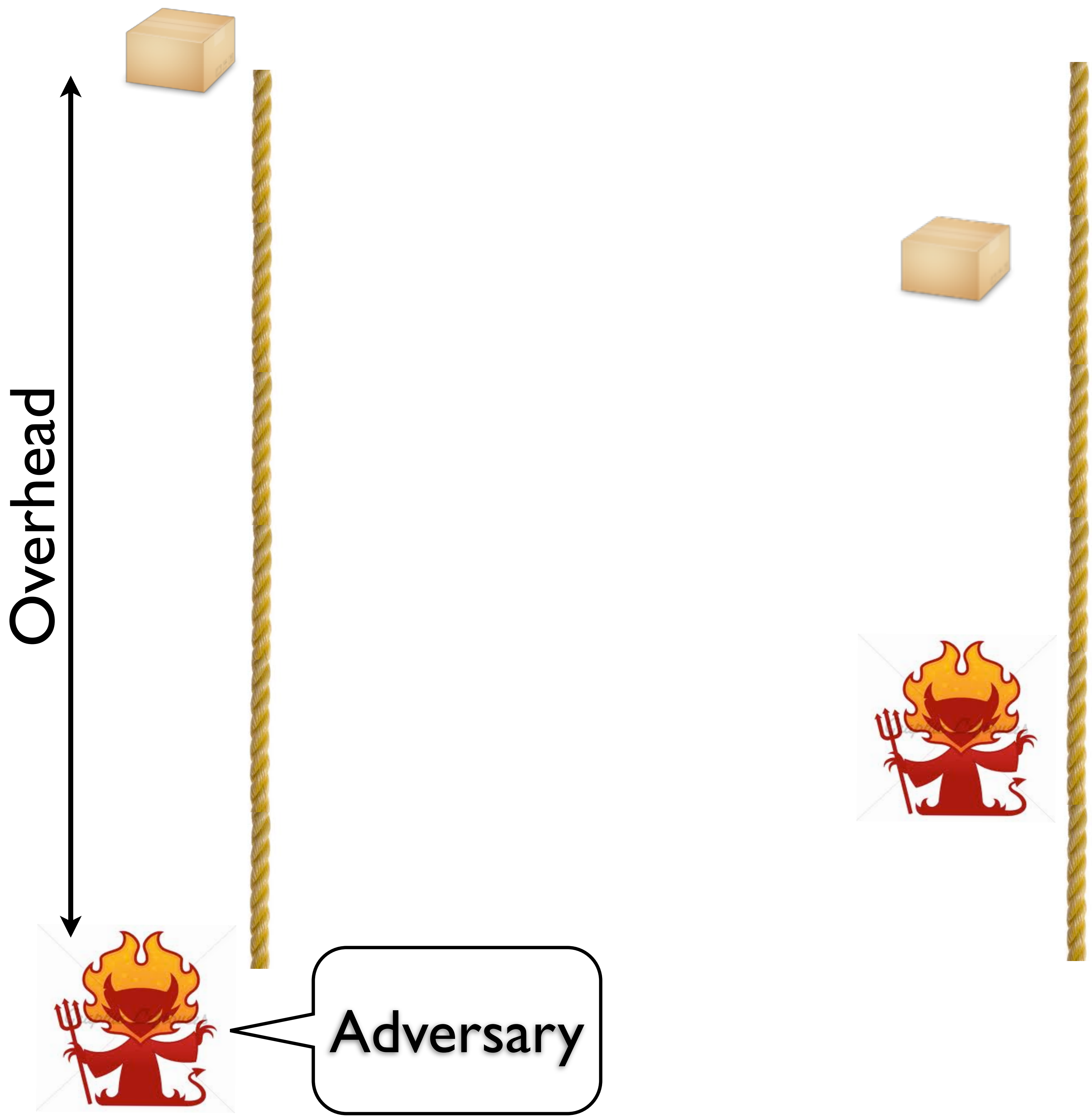

Non-adaptive protocol




Non-adaptive protocol



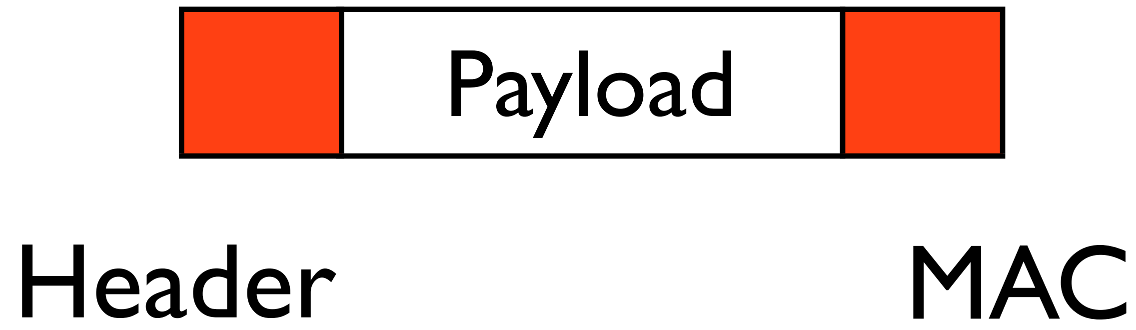
Overhead
Adversary
Non-adaptive protocol
Adaptive protocol



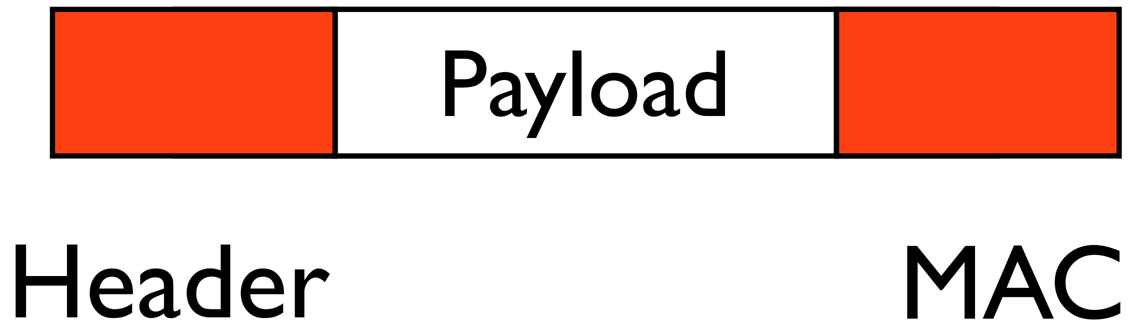

Non-adaptive protocol

Adaptive protocol

# Adaptive packet overhead

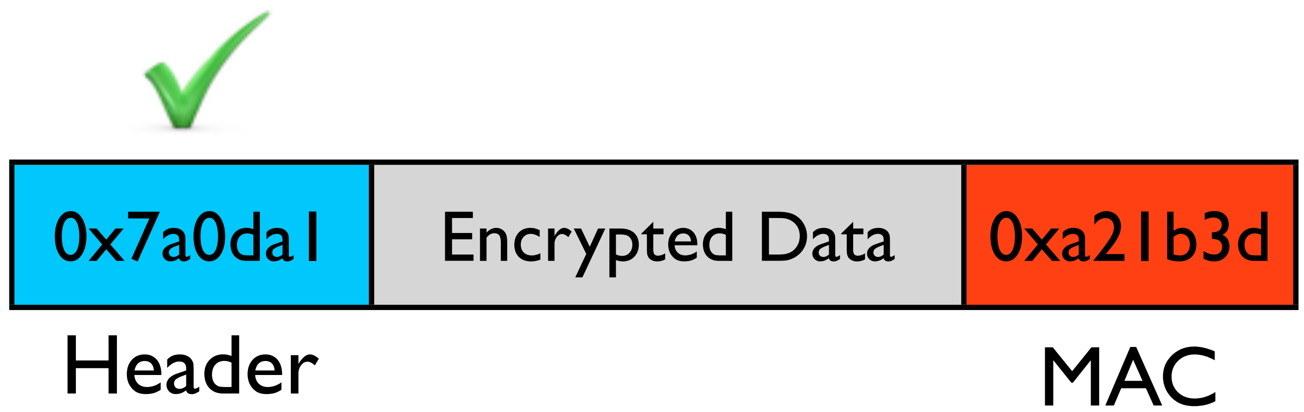


# Adaptive packet overhead



# Packet filtering logic

# Packet filtering logic



# Packet filtering logic


Accept Packet

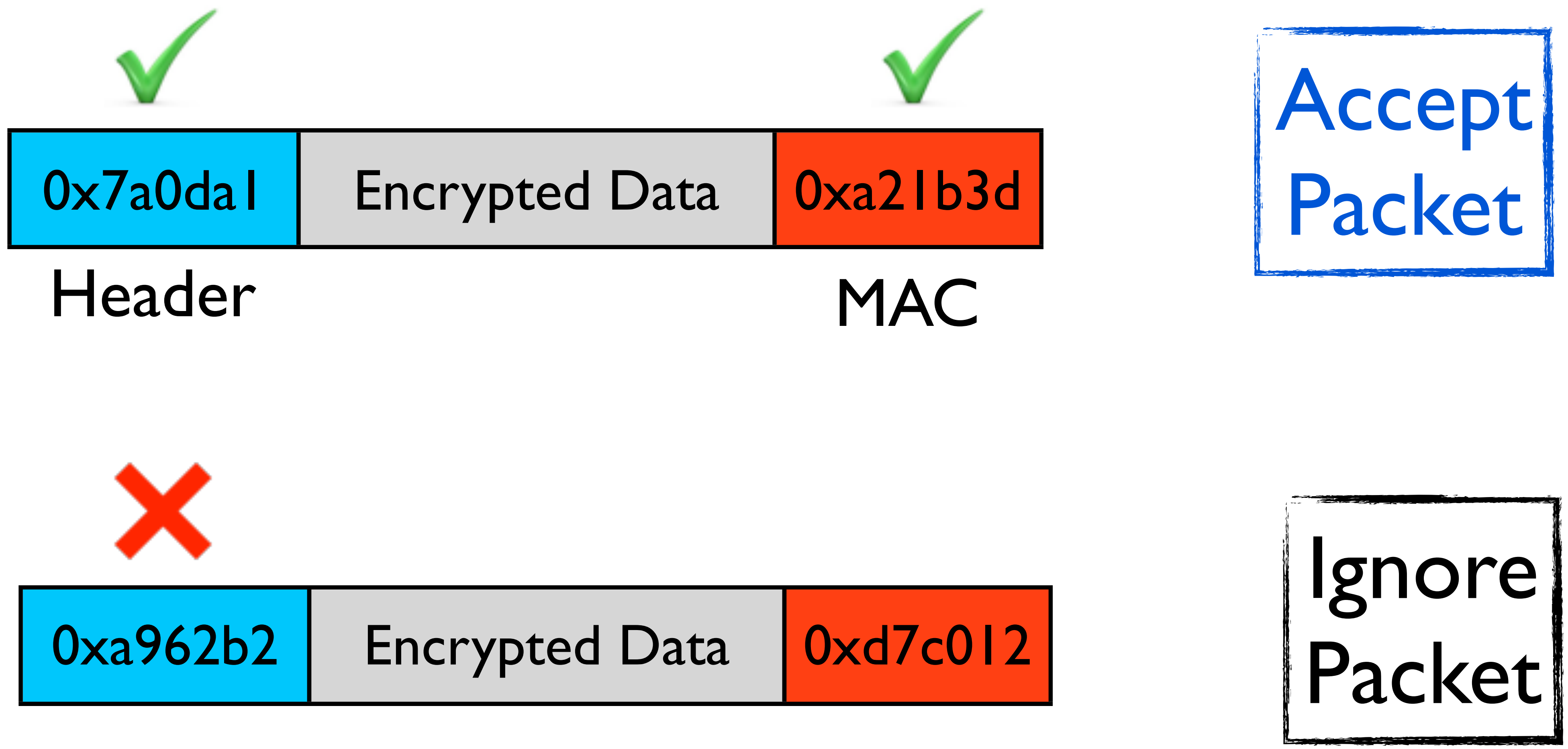
# Packet filtering logic

| 0x7a0da1 | Encrypted Data | 0xa21b3d |
|---|---|---|
| Header | | MAC |

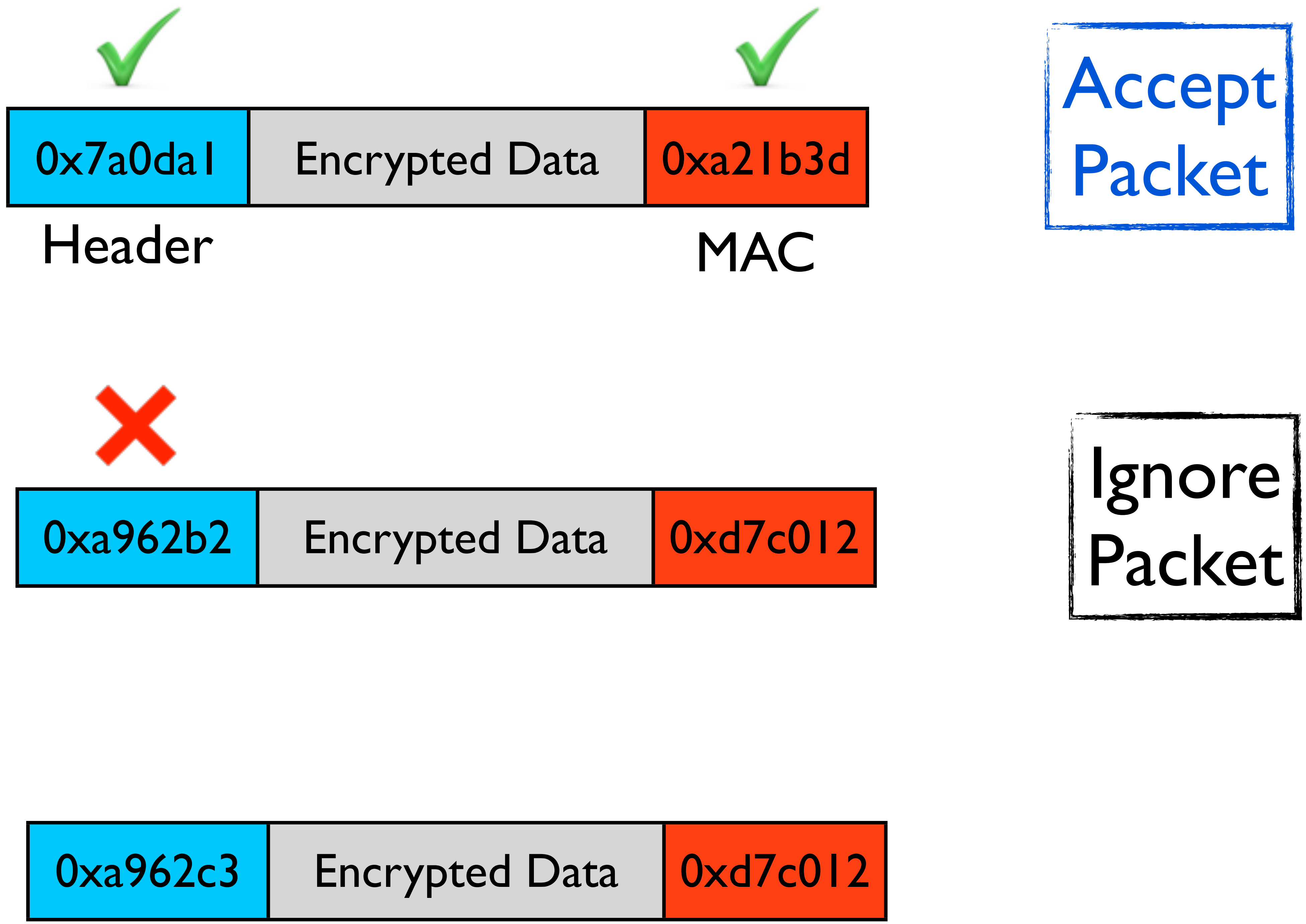
Accept Packet

| 0xa962b2 | Encrypted Data | 0xd7c012 |
|---|---|---|

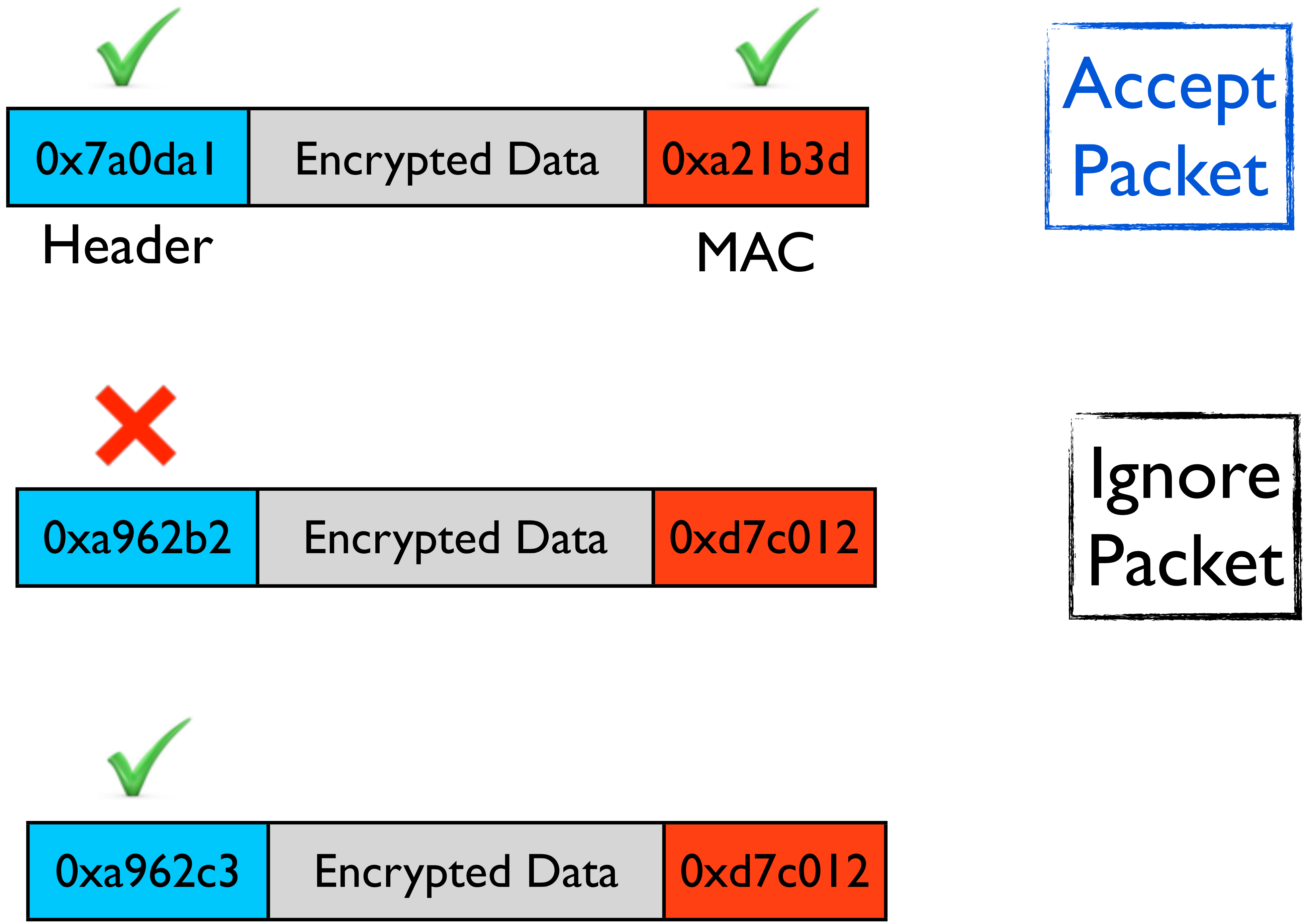
# Packet filtering logic



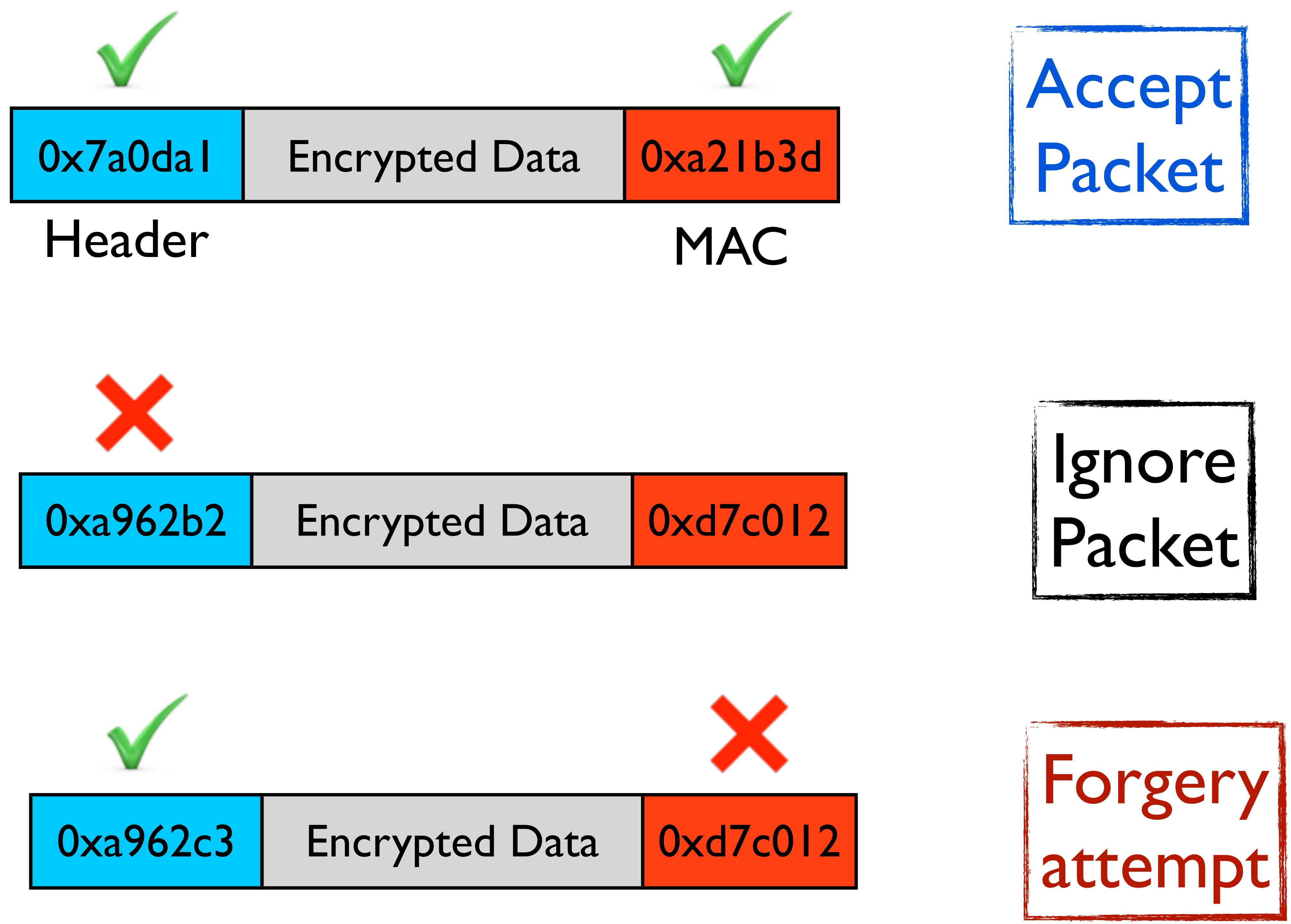
# Packet filtering logic



# Packet filtering logic



# Packet filtering logic



# When to adapt?

- Security guarantee: During a time period T

$$\Pr(\text{successful forgery}) < 2^{-\delta}$$

- Successful forgery


$$\text{Number of forgery attempts required to succeed} = 2^{l}$$

# When to adapt?

Pr(successful forgery) in 1 forgery attempt $= \frac{1}{2^l}$

Pr(successful forgery) in x forgery attempts $= 1 - (1 - \frac{1}{2^l})^x$

# When to adapt?

Pr(successful forgery) in 1 forgery attempt $= \frac{1}{2^l}$

Pr(successful forgery) in x forgery attempts $= 1 - (1 - \frac{1}{2^l})^x < 2^{-\delta}$

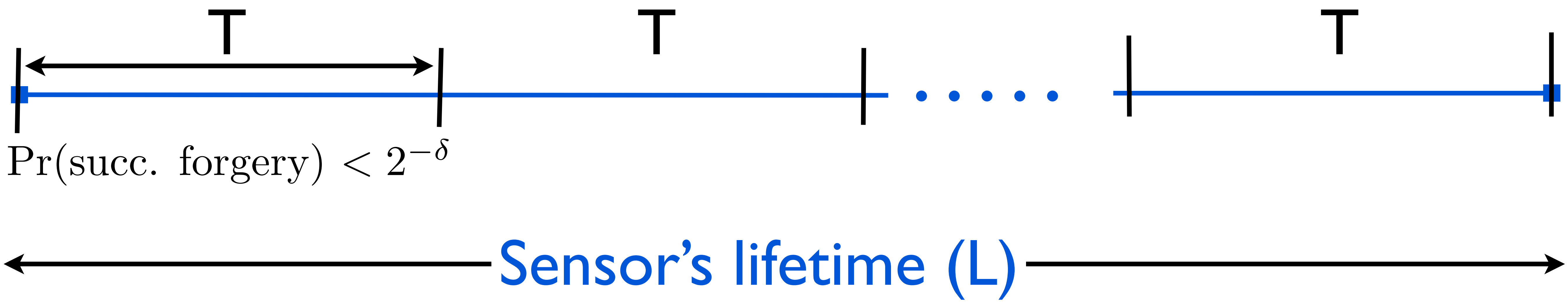
# When to adapt?

Pr(successful forgery) in 1 forgery attempt $= \frac{1}{2^l}$

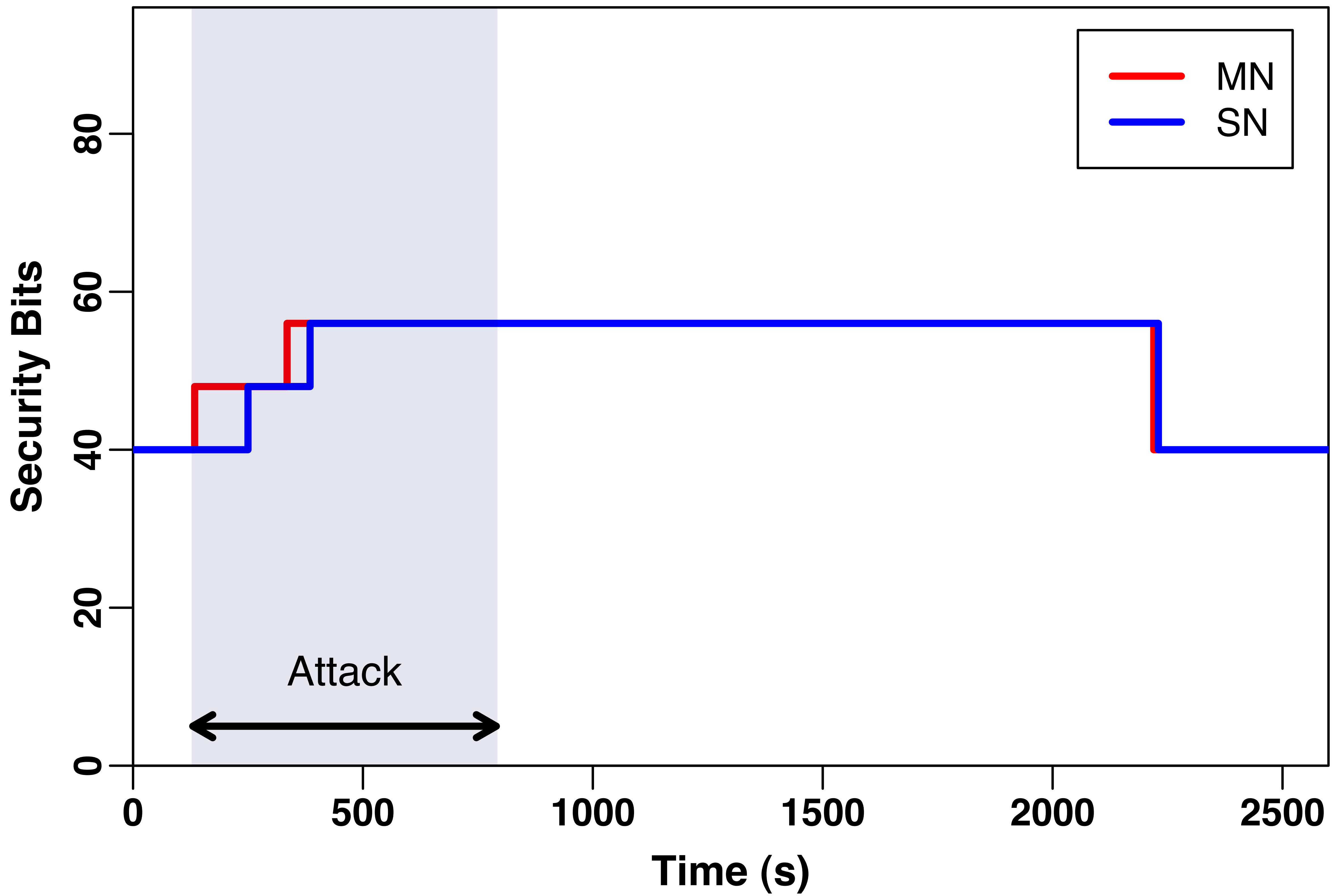
Pr(successful forgery) in x forgery attempts $= 1 - (1 - \frac{1}{2^l})^x < 2^{-\delta}$

$$x < \frac{\log(1-2^{-\delta})}{\log(1-\frac{1}{2^l})}$$

# Security throughout the sensor's lifetime

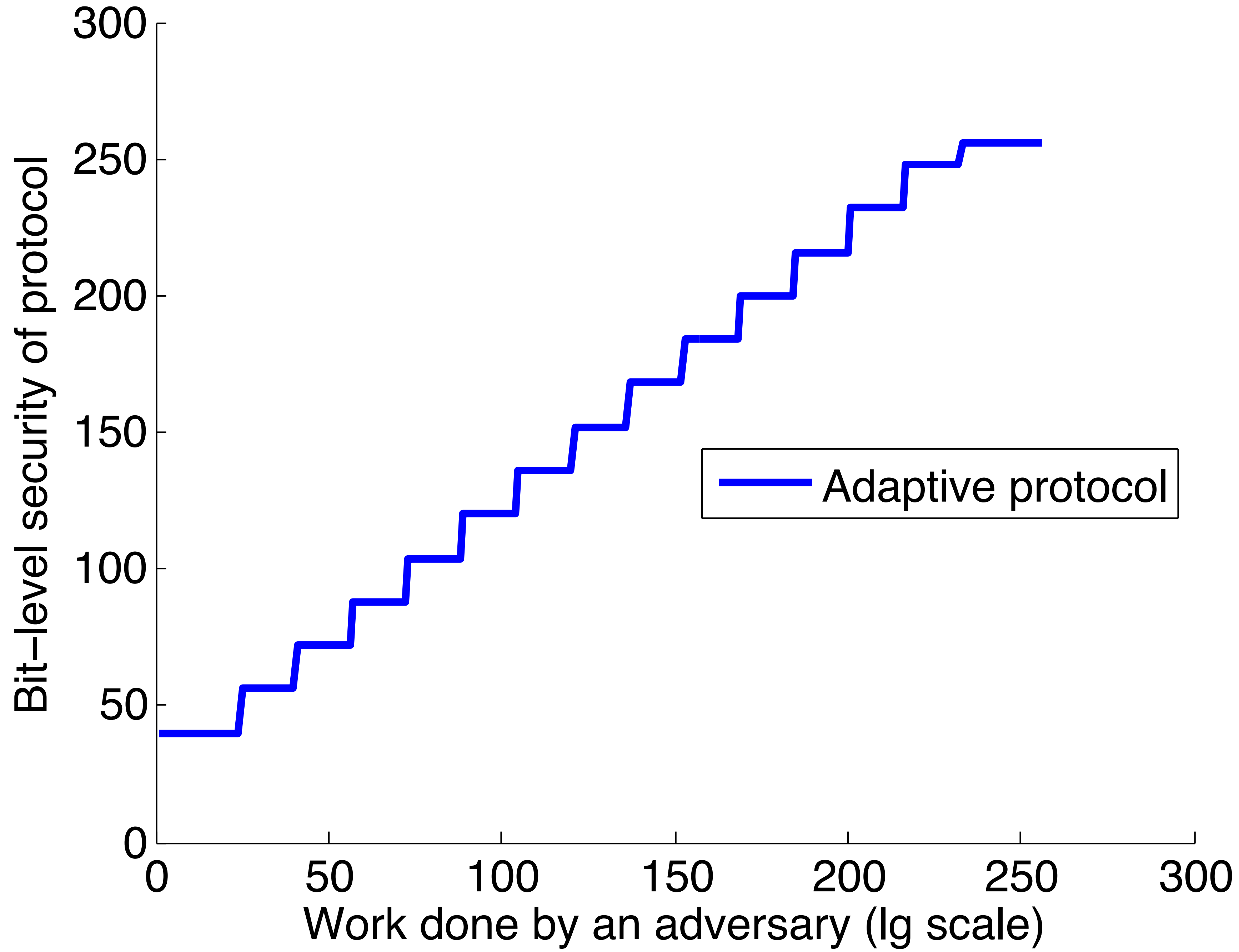


# Evaluation



MN
SN
Security Bits
0
20
40
60
80
Attack
0
500
1000
1500
2000
2500
Time (s)

# Adaptive security plot



# Conclusion

- Using fixed large packet overhead is inefficient for low-power sensor networks
  - because a network is not always in a hostile environment
- Adaptive protocol provides privacy and is efficient.
- Adaptive protocol provides reasonable security when required

# Adaptive security and privacy for mHealth sensing

**Shrirang Mare[1],** Jacob Sorber[1], Minho Shin[2], Cory Cornelius[1], and David Kotz[1]

[1] Dartmouth College, USA
[2] Myongi University, South Korea