Adaptive security and privacy for mHealth sensing

Shrirang Mare\textsuperscript{1}, Jacob Sorber\textsuperscript{1}, Minho Shin\textsuperscript{2}, Cory Cornelius\textsuperscript{1}, and David Kotz\textsuperscript{1}

\textsuperscript{1}Dartmouth College, USA
\textsuperscript{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,
Secure, private, and efficient protocol

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

Mobile Node

Sensor Node

Fixed address a1:70:c3

0xa170c3

Encrypted Data

0xa21b3d
Wireless protocols

Mobile Node

Sensor Node

Fixed address a1:70:c3

0xa170c3  Encrypted Data  0xa21b3d

0xa170c3  Encrypted Data  0x001e72
Privacy preserving wireless protocols
Privacy preserving wireless protocols

Mobile Node

Address pool:
- 7a:0d:1e
- 47:c2:23
- 17:dc:b2

Sensor Node

<table>
<thead>
<tr>
<th>Header</th>
<th>Payload</th>
<th>MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x7a0d1e</td>
<td>Encrypted Data</td>
<td>0xa21b3d</td>
</tr>
<tr>
<td>0x17dc2b</td>
<td>Encrypted Data</td>
<td>0x001e72</td>
</tr>
</tbody>
</table>
# Packet overhead

In Wi-Fi networks

<table>
<thead>
<tr>
<th>Header</th>
<th>Payload</th>
<th>MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-16 bytes</td>
<td>1000+ bytes</td>
<td>16 bytes</td>
</tr>
</tbody>
</table>
Packet overhead

In Wi-Fi networks

<table>
<thead>
<tr>
<th>Header</th>
<th>Payload</th>
<th>MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-16 bytes</td>
<td>1000+ bytes</td>
<td>16 bytes</td>
</tr>
</tbody>
</table>

In medical sensor networks

Payload

~10-50 bytes
Packet overhead

In Wi-Fi networks

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

In medical sensor networks

- **Header**: ~10-50 bytes
- **Payload**: ~10-50 bytes
- **MAC**: ~10-50 bytes
Packet overhead

In Wi-Fi networks

```
<table>
<thead>
<tr>
<th>Header</th>
<th>Payload</th>
<th>MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-16 bytes</td>
<td>1000+ bytes</td>
<td>16 bytes</td>
</tr>
</tbody>
</table>
```

In medical sensor networks

```
<table>
<thead>
<tr>
<th>Header</th>
<th>Payload</th>
<th>MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>~10-50 bytes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Non-adaptive protocol

Adversary
Overhead

Non-adaptive protocol

Adversary
Overhead

Non-adaptive protocol

Adversary

Adaptive protocol
Overhead

Non-adaptive protocol

Adversary

Adaptive protocol
Adaptive packet overhead

Payload

Header       MAC
Adaptive packet overhead

- Payload
- Header
- MAC
Packet filtering logic

0x7a0da1  Encrypted Data  0xa21b3d

Header  MAC
Packet filtering logic
Packet filtering logic

0x7a0da1  Encrypted Data  0xa21b3d

Header  MAC

Accept Packet
Packet filtering logic

- Header: 0x7a0da1
- Encrypted Data: 0xa21b3d
- MAC: 0xda96b2
- Encrypted Data: 0xd7c012

Accept Packet
Packet filtering logic

- **Accept Packet**
  - Header: 0x7a0da1
  - Encrypted Data: 0xa21b3d
  - MAC

- **Ignore Packet**
  - Header: 0xa962b2
  - Encrypted Data: 0xd7c012
  - MAC
Packet filtering logic

Accept Packet

Ignore Packet

Header

MAC

0x7a0da1

Encrypted Data

0xa21b3d

0xa962b2

Encrypted Data

0xd7c012

0xa962c3

Encrypted Data

0xd7c012
Packet filtering logic

- Accept Packet
  - 0x7a0da1
  - Encrypted Data
  - 0xa21b3d
  - Header
  - MAC

- Ignore Packet
  - 0xa962b2
  - Encrypted Data
  - 0xd7c012

- Accept Packet
  - 0xa962c3
  - Encrypted Data
  - 0xd7c012

- Ignore Packet
Packet filtering logic

- Accept Packet
  - Header: 0x7a0da1
  - Encrypted Data: 0xa21b3d
  - MAC: 0xa962b2

- Ignore Packet
  - Header: 0xa962b2
  - Encrypted Data: 0xd7c012

- Forgery attempt
  - Header: 0xa962c3
  - Encrypted Data: 0xd7c012
When to adapt?

- Security guarantee: During a time period $T$
  \[
  \Pr(\text{successful forgery}) < 2^{-\delta}
  \]
- Successful forgery

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

\[ = 1 - \left(1 - \frac{1}{2^l}\right)^x < 2^{-\delta} \]
When to adapt?

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

Pr(successful forgery) in \( x \) forgery attempts

\[ = 1 - \left(1 - \frac{1}{2^l}\right)^x < 2^{-\delta} \]

\[ x < \frac{\log(1-2^{-\delta})}{\log(1-\frac{1}{2^l})} \]
Security throughout the sensor’s lifetime

\[ \Pr(\text{succ. forgery}) < 2^{-\delta} \]
Adaptive security plot

Bit-level security of protocol vs. Work done by an adversary (lg scale)
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\textsuperscript{1}, Jacob Sorber\textsuperscript{1}, Minho Shin\textsuperscript{2}, Cory Cornelius\textsuperscript{1}, and David Kotz\textsuperscript{1}

\textsuperscript{1}Dartmouth College, USA
\textsuperscript{2}Myongi University, South Korea