One design goal of Constrained Application Protocol (CoAP): “keep message overhead small, thus limiting the need for fragmentation.”

Where does the energy go? … Communication!

6LoWPAN L2 packets are limited to 127 bytes including various overheads
Examples

› Integrity Protection only
  - MAC → HMAC-SHA256
  - Signature only → ECDSA with 64 bytes signature

› Integrity Protection and Encryption
  - AEAD → AES-CCM
  - Symmetric Encryption Asymmetric Signature (SEAS) → AES-CTR + ECDSA
## Information Elements

<table>
<thead>
<tr>
<th>Integrity Protection Only</th>
<th>Encryption &amp; Integrity Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>› Sequence Number</td>
<td></td>
</tr>
<tr>
<td>› Context Identifier</td>
<td></td>
</tr>
<tr>
<td>› CoAP Payload</td>
<td>› Ciphertext</td>
</tr>
<tr>
<td>› Signature / MAC</td>
<td></td>
</tr>
</tbody>
</table>
## COSE Profile: MAC

<table>
<thead>
<tr>
<th>Sequence Number</th>
<th>Context Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>CoAP Payload</td>
<td>Ciphertext</td>
</tr>
<tr>
<td>Signature / MAC</td>
<td></td>
</tr>
</tbody>
</table>

```json
[
  msg_type,
  protected: alg, seq,
  unprotected: -
]
```

```json
payload
```

```json
MAC,
```

```json
[
  #recipients:
  [
    #recipient:
      protected: -
      unprotected: alg:dir, cid
ciphertext: -
  ]
]
```

```json
]}
```
Suggested Modification for COSE

1. “Flattened out” structure: no recipients, no multiple signatures
2. Security context defines uniquely the cipher suite: no alg parameter
3. All parameters should be protected when possible: no “unprotected” field
4. Define key/label values for the introduced parameters and algorithms
COSE modified profile: MAC

- Sequence Number
- Context Identifier
- CoAP Payload
- Ciphertext
- Signature / MAC

```
[ msg_type,
  protected: cid, seq,
  payload,
  MAC
]
```
### Message Overhead Example

<table>
<thead>
<tr>
<th>Scheme</th>
<th>seq+cid</th>
<th>MAC</th>
<th>Total Size</th>
<th>Overhead</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HMAC-SHA256</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COSE</td>
<td>11 B</td>
<td>16 B</td>
<td>53 bytes</td>
<td>26 bytes</td>
</tr>
<tr>
<td>mod-COSE</td>
<td>11 B</td>
<td>16 B</td>
<td>37 bytes</td>
<td>10 bytes</td>
</tr>
<tr>
<td><strong>ECDSA with 64 bytes signature</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COSE</td>
<td>11 B</td>
<td>64 B</td>
<td>100 bytes</td>
<td>25 bytes</td>
</tr>
<tr>
<td>mod-COSE</td>
<td>11 B</td>
<td>64 B</td>
<td>86 bytes</td>
<td>11 bytes</td>
</tr>
<tr>
<td>bound</td>
<td>11 B</td>
<td>64 B</td>
<td>81 bytes</td>
<td>6 bytes</td>
</tr>
</tbody>
</table>

The message size is calculated without payload.
## Message Overhead Example

### AES-CCM

<table>
<thead>
<tr>
<th>Scheme</th>
<th>seq+cid</th>
<th>TAG</th>
<th>Total Size</th>
<th>Overhead</th>
</tr>
</thead>
<tbody>
<tr>
<td>COSE</td>
<td>11 B</td>
<td>8 B</td>
<td>44 bytes</td>
<td>25 bytes</td>
</tr>
<tr>
<td>mod-COSE</td>
<td>11 B</td>
<td>8 B</td>
<td>29 bytes</td>
<td>10 bytes</td>
</tr>
<tr>
<td>bound</td>
<td>11 B</td>
<td>8 B</td>
<td>24 bytes</td>
<td>5 bytes</td>
</tr>
</tbody>
</table>

### AES-CTR-ECDSA

<table>
<thead>
<tr>
<th>Scheme</th>
<th>seq+cid</th>
<th>SIG</th>
<th>Total Size</th>
<th>Overhead</th>
</tr>
</thead>
<tbody>
<tr>
<td>COSE</td>
<td>11 B</td>
<td>64 B</td>
<td>134 bytes</td>
<td>59 bytes</td>
</tr>
<tr>
<td>mod-COSE</td>
<td>11 B</td>
<td>64 B</td>
<td>86 bytes</td>
<td>11 bytes</td>
</tr>
<tr>
<td>bound</td>
<td>11 B</td>
<td>64 B</td>
<td>81 bytes</td>
<td>6 bytes</td>
</tr>
</tbody>
</table>

The message size is calculated without payload.
Thank you!

Comments/questions?
COSE profile: Sig

- Sequence Number
- Context Identifier
- CoAP Payload
  - Ciphertext
- Signature / MAC

```
[  
  msg_type,
  protected: seq,
  unprotected: -
  payload
  [  
    #signatures:
    [  
      #signature:
        protected: alg, cid
        unprotected: -
        SIG
      ]
    ]
  ]
]`
COSE profile: Sig

- Sequence Number
- Context Identifier
- CoAP Payload
- Ciphertext
- Signature / MAC

```
[ msg_type,
  protected: cid, seq
  payload,
  SIG
]
```
COSE profile: AEAD

- Sequence Number
- Context Identifier
- CoAP Payload
- Ciphertext
- Signature / MAC

[ ]
  msg_type,
  protected: alg, seq,
  unprotected: -
  TAG: -
[ ]
  #recipients:
  [ ]
    #recipient:
      protected: -
      unprotected: alg:dir, cid,
      ciphertext
    ]
  ]
COSE profile: AEAD

- Sequence Number
- Context Identifier
- CoAP Payload
- Ciphertext
- Signature / MAC

```
[ msg_type,
  protected: cid, seq,
  ciphertext,
]
```
COSE profile: SEAS

- Sequence Number
- Context Identifier
- CoAP Payload
- Ciphertext
- Signature / MAC

msg_type, protected: seq, unprotected: -
payload: COSE_encryptData

#signatures:
[  
  #signature:
  protected: -
  unprotected: alg:dir, cidSIG
]

[  
  #recipients:
    
]

[  
  msg_type, protected: -
  unprotected: -
  TAG: -
]

[  
  ciphertext
]

COSE profile: SEAS

- Sequence Number
- Context Identifier
- CoAP Payload
- Ciphertext
- Signature / MAC

```
[ msg_type,
  protected: cid, seq,
  ciphertext,
  SIG
]```