About project of national standard «Protocol of IoT for the interchanging data in narrowband spectrum (NB-Fi)» (brief cryptanalysis)

Nozdrunov Vladislav

TC 26

28 May 2018
17 April, 2018 TC 194 announced the first version of national standard «Protocol of IoT for the interchanging data in narrowband spectrum (NB-Fi)».

What is that?

It is technology which is designed for the low-power, wide-area, machine-to-machine communication, with the using the narrow band approach.
### Structure of package

<table>
<thead>
<tr>
<th>Preamble (Предамбула)</th>
<th>Node ID, присвоенный устройству</th>
<th>Data (Данные)</th>
<th>Error detection and correction (Определение ошибки и коррекция)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Head (Заголовок)</td>
<td>Payload (Полезные данные)</td>
</tr>
<tr>
<td>0x97</td>
<td>0x15</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>0x93</td>
<td>0x7a</td>
<td>SYS</td>
<td>ACK</td>
</tr>
<tr>
<td>0x96</td>
<td>0x61</td>
<td>Zigzag source (16 байт)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID2</th>
<th>ID1</th>
<th>ID0</th>
<th>7</th>
<th>6</th>
<th>5</th>
<th>4 – 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYS</td>
<td>ACK</td>
<td>MULTI</td>
<td>ITER</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 5 – Structure of the transport layer field of DOWNLINK packet

<table>
<thead>
<tr>
<th>Идентификатор, присвоенный устройству (Node ID)</th>
<th>Данные (Data)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Заголовок (Header)</td>
</tr>
<tr>
<td>ID2</td>
<td>ID1</td>
</tr>
<tr>
<td>SYS</td>
<td>ACK</td>
</tr>
</tbody>
</table>

от 8 до 128 байт
Security

Payload is encrypted by XTEA-2 in ECB mode; XTEA-2 is used twice with key $K = K_1 \parallel K_2$, $K_1, K_2 \in V_{128}$; Key $K \in V_{256}$ is generated once for each ID (pair server-modem); Authentication is provided by CRC-8 in Uplink package (Downlink... hmm...); Length of Payload is 8 byte, but length of the block in XTEA-2 is 16 byte...
1 Payload is encrypted by XTEA-2 in ECB mode;
Security

1. Payload is encrypted by XTEA-2 in ECB mode;
2. XTEA-2 is used twice with key $K = K_1 \parallel K_2$, $K_1, K_2 \in V_{128}$;
Payload is encrypted by XTEA-2 in ECB mode;

XTEA-2 is used twice with key $K = K_1 \| K_2$, $K_1, K_2 \in V_{128}$;

Key $K \in V_{256}$ is generated once for each ID (pair server-modem);
Security

1. Payload is encrypted by XTEA-2 in ECB mode;
2. XTEA-2 is used twice with key $K = K_1 \| K_2$, $K_1, K_2 \in V_{128}$;
3. Key $K \in V_{256}$ is generated once for each ID (pair server-modem);
4. Authentication is provided by CRC-8 in Uplink package (Downlink.. hmm...);
**Security**

1. Payload is encrypted by XTEA-2 in ECB mode;
2. XTEA-2 is used twice with key $K = K_1 \| K_2$, $K_1, K_2 \in V_{128}$;
3. Key $K \in V_{256}$ is generated once for each ID (pair server-modem);
4. Authentication is provided by CRC-8 in Uplink package (Downlink.. hmm...);
5. Length of Payload is 8 byte, but length of the block in XTEA-2 is 16 byte...
Old-school meet-in-the-middle

Let $F_K = E_{K_2}(E_{K_1}(P))$, where $E_k$ - block cipher, $K = K_1 || K_2$, $K_1, K_2 \in V_{128}$. 
Old-school meet-in-the-middle

Let $F_K = E_{K_2}(E_{K_1}(P))$, where $E_k$ - block cipher, $K = K_1||K_2$, $K_1, K_2 \in V_{128}$.
And let we have pairs $(P_i, C_i)$ such that $F_K(P_i) = C_i, i = 1, 2$. Then we initiate the following algorithm:
Let $F_K = E_{K_2}(E_{K_1}(P))$, where $E_k$ - block cipher, $K = K_1 || K_2$, $K_1, K_2 \in V_{128}$.
And let we have pairs $(P_i, C_i)$ such that $F_K(P_i) = C_i$, $i = 1, 2$.
Then we initiate the following algorithm:

1. for each $K_1 \in V_{128}$ compute $E_{K_1}(P_1) = x$, then put $K_1$ in the memory cell with address $x$. 
Old-school meet-in-the-middle

Let $F_K = E_{K_2}(E_{K_1}(P))$, where $E_k$ - block cipher, $K = K_1 || K_2$, $K_1, K_2 \in V_{128}$.

And let we have pairs $(P_i, C_i)$ such that $F_K(P_i) = C_i$, $i = 1, 2$.

Then we initiate the following algorithm:

1. for each $K_1 \in V_{128}$ compute $E_{K_1}(P_1) = x$, then put $K_1$ in the memory cell with address $x$.

2. for each $K_2 \in V_{128}$ compute $E_{K_2}^{-1}(C_1) = \bar{x}$, then put $K_2$ in the memory cell with address $\bar{x}$.
Old-school meet-in-the-middle

Let $F_K = E_{K_2}(E_{K_1}(P))$, where $E_k$ - block cipher, $K = K_1 || K_2$, $K_1, K_2 \in V_{128}$.
And let we have pairs $(P_i, C_i)$ such that $F_K(P_i) = C_i$, $i = 1, 2$. Then we initiate the following algorithm:

1. for each $K_1 \in V_{128}$ compute $E_{K_1}(P_1) = x$, then put $K_1$ in the memory cell with address $x$.
2. for each $K_2 \in V_{128}$ compute $E^{-1}_{K_2}(C_1) = \overline{x}$, then put $K_2$ in in the memory cell with address $\overline{x}$.
3. for each pair $(K_1, K_2)$ verify equation $F_{(K_1,K_2)}(P_2) = C_2$.

Totaly we have $3 \cdot 2^{128}$. 

Nozdrunov Vladislav CTCrypt 2018

Brief cryptanalysis

CTCrypt 2018
We have Magma

<table>
<thead>
<tr>
<th>Block cipher</th>
<th>block</th>
<th>Key</th>
<th>Security</th>
<th>GE</th>
<th>Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Magma</td>
<td>64</td>
<td>256</td>
<td>$2^{192} - 2^{224}$</td>
<td>1.017</td>
<td>200</td>
</tr>
<tr>
<td>XTEA-2</td>
<td>128</td>
<td>128</td>
<td>$3 \cdot 2^{129}$</td>
<td>6.980</td>
<td>28.2</td>
</tr>
</tbody>
</table>
Attacks on authentication

1. Easy forging
   - Since there is no CRC in Downlink, any package will be accepted.

2. Replay Attack
   - Since uses ECB, an adversary could repeat any package, which will be accepted.

3. Bruteforce attack
   - For forging new Uplink, it is enough 256 attempts.
Attacks on authentication

1. Easy forging
   - there is no CRC in Downlink, therefore any package will be accepted.
Attacks on authentication

1 Easy forging
   - there is no CRC in Downlink, therefore any package will be accepted.

2 Replay Attack
   - since uses ECB then adversary could repeat any package, that will be accepted.
Attacks on authentication

1. Easy forging
   - there is no CRC in Downlink, therefore any package will be accepted.

2. Replay Attack
   - since uses ECB then adversary could repeat any package, that will be accepted.

3. Bruteforce attack
   - for forging new Uplink it is enough 256 attempts.
There is no crypto without thinking.

Thank you for your attention!