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

About

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

Таблица 4 – Структура формата UPLINK-пакета

Preamble (Преамбула)				Node ID (Идентификатор, присвоенный устройству)			Data (Данные)					Error detection and correction (Определение ошибки и коррекция)				
							Header (Заголовок)				Payload (Полезные данные)	Payload CRC (Контрольная сумма полезных данных)	Packet CRC (Контрольная сумма пакета данных)			Zigzag code
0x97	0x15	0x7a	0x6f	ID2	ID1	ID0	7	6	5	4 – 0	8 байт	CRC-8	CRC-32	CRC-32	CRC-32	16 байт
							SYS	ACK	MULTI	ITER						
				Zigzag source (16 байт)												

Таблица 5 – Структура поля данных транспортного уровня DOWNLINK-пакета

Идентификатор, присвоенный устройству (Node ID)			Данные (Data)				
			Заголовок (Header)				Полезные данные (Payload)
ID2	ID1	ID0	7	6	5	4 – 0	от 8 до 128 байт
			SYS	ACK	MULTI	ITER	

Security

Security

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 $K = K_1 \| K_2$, $K_1, K_2 \in V_{128}$;

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);

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:

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.

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 $\overline{x}$.

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 $3 \cdot 2^{128}$.

We have Magma

Block cipher	block	Key	Security	GE	Speed
Magma	64	256	$2^{192} - 2^{224}$	1.017	200
XTEA-2	128	128	$3 \cdot 2^{129}$	6.980	28.2

Attacks on authentication

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.

The End

There is no crypto without thinking.

Thank you for your attention!