Ban-Logic for Security-Packet-Transmission

BAN logical notation

BAN logical notation used in the paper as followed:
1. $P|^{\equiv}X$: *P* believes *X*;
2. $P|\Rightarrow X$: *P* controls *X*;
3. #(X): *X* is fresh;
4. $\{X\}_K$: the ciphertext of *X* encrypted by the key *K*;
5. $P \lhd X$: *P* sees *X* ;
6. $P|\backsim X$: *P* said *X*.

BAN logical postulates

We only need two rules for SPT:
1. Nonce-verification rule:

R4:
$\frac{P|^{\equiv}(\#X),P|^{\equiv}Q|\backsim X}{P|^{\equiv}Q|^{\equiv}X}$. States that if P believes that X could have been uttered only recently and that Q once said X, then P believes that Q believes X.
2. Jurisdiction rule:

R5:
$\frac{P|^{\equiv}Q|^{\Rightarrow}X,P|^{\equiv}Q|^{\equiv}X}{P|^{\equiv}X}$. States that if P believes that Q has jurisdiction over X and P trusts Q on the truth of X,then P believes X.

Verifying Authentication process for SPT with BAN logic:

Idealized protocol

We let E denote to a normal node; S denote to a LoRaWan server; X denote to the value to making xor operation; Njr denotes to *New Join Request*. According to the protocol proposed in the paper, The authentication can be idealized as follows:
1. $S \lhd\{Njr_1,Njr_2\}_X$.

Establishment of security goals

1. $S|\equiv X$.

Initiative premises

1. Premise P1: $S|\equiv E|\Rightarrow X$;
2. Premise P2:$S|\equiv E \backsim X$;

Protocol Analysis:

1. Using R4: $\frac{P|\equiv \#X, P|\equiv Q|\backsim X}{P|\equiv Q|\equiv X}$ and P2, we can obtain the following: $S|\equiv E|\equiv X$; 2.Using R5: $\frac{P|\equiv Q|\Rightarrow X, P|\equiv Q|\equiv X}{P|\equiv X}$ plus the last result and P1, we can get the security goal:$S|\equiv X$.

Conclusions of BAN Analysis

By analyzing the security of the authentication process for SPT, the results demonstrate that the protocol proposed can effectively achieve the security goal.