Verification of Time Telegrams in Long Wave Radio systems

Matthias Schneider[1], Christoph Ruland[1]

[1]Institute for Data Communication Systems, University of Siegen, 57068 Siegen, Germany

Email: matthias.schneider@uni-siegen.de

Long Wave Radio systems are widely used to distribute the actual date and time information, because wireless transmission guarantees timeliness. The provision of timeliness and reliability of time information is very important for many devices, which are controlled by time stamped telematic telegrams or time triggered events, and play an essential role for public and private safety. The correct behavior of the devices of any system is only possible, if a synchronized and correct system time is available in all devices.

The distribution of time telegrams is used to synchronize the system clocks of the receivers and their real time clocks. These received time messages, which contain the actual system time, cannot be securely verified by the Long Wave Radio Receiver, because there is no backchannel. No receipt or confirmation can be requested by the transmitting station without the existence of a back channel.

Time telegrams can be manipulated or generated by "man-in-the-middle" attacks. Therefore it is possible to manipulate the system clocks of groups of devices or individual devices depending on the location of the attacker. By manipulating the receiver´s system clock the control behavior of the device can be completely changed. Even the application of digital signatures and encryption to time telegrams doesn´t protect against man-in-the-middle attacks, for example by delaying the time telegrams.

Possible attack scenarios on broadcast data services have been published [1].

This paper describes a method to verify received time telegrams distributed by Long Wave Radio systems on the example of the radio ripple control technology.

By this approach, the time between two time telegrams is continuously measured and compared with the time difference calculated by the time information contained in the time telegrams. In other words, physical and logical information is compared. The physical time difference is directly calculated using the carrier frequency of the transmission system (for example: DCF49 transmission system uses a carrier frequency of 129,1 kHz with FSK modulation ± 170 Hz). A counter is clocked by the received carrier frequency of the system. The physical time difference between the transmission of two time telegrams can be derived by the number of oscillations. The logical time difference is given by the content of the time telegrams.

The comparison of physical and logical time differences is continuously verified to detect time jumps, which may appear during the transmission of time telegrams. Manipulated or delayed time telegrams can be accurately identified. This method can be applied without changing the time distribution protocol and can applied to other time distribution services.

The paper closes with an analysis of remaining risks, a summary and an outlook.

REFERENCES

[1] M. Schneider; Ch. Ruland: Sicherheit von Broadcast-Datendiensten im Smart Grid am Beispiel der Rundsteuertechnik. Tagungsband des 13. BSI-Kongresses. S. 483–496.