Errata

In the OSEMA (Open Sensor Manager) software, the HMAC used to ensure the integrity and authenticity of the messages is calculated with a too short key that is 128-bit-long. The recommended key length for the SHA-256 algorithm is 256-bits [1]. The key length was changed to 256 bits in the code, and this change was also committed to the GitHub code available from [2]. In the dissertation, the key length is stated in p. 40 as follows:

“HMAC (keyed-Hash Message Authentication Code) with a 128-bit key is used to provide authenticity and integrity”,

whereas it should read:

“HMAC (keyed-Hash Message Authentication Code) with a 256-bit key is used to provide authenticity and integrity”.

In Publication III, the key length is stated in p. 8 as follows:

“a keyed-Hash Message Authentication Code (HMAC) is calculated with SHA-256 (Secure Hash Algorithm) and a 128 bit key”,

whereas it should read:

“a keyed-Hash Message Authentication Code (HMAC) is calculated with SHA-256 (Secure Hash Algorithm) and a 256 bit key”.

References:
