

We recently found out a security flaw in “Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks” published in IEEE JSAC, which, however, is very easy to fix.

In Section V-B of the original version, the same $(t - 1)$ -degree polynomial $\mathcal{F}(x)$ is used for generating secret shares of all the area keys. This may introduce room for the following attack: the attacker first compromises at least t nodes in a certain area to obtain all the polynomial coefficients; then the attacker can obtain the area key of another area by compromising a single node in that area. The simple solution is to use a unique polynomial for secret-sharing of each area key. Accordingly, we made changes to the first paragraph of Section V-B.1 and Equation (4). All the other portions of this paper remain unaffected.