Neighbour-based intrusion detection in wireless sensor networks

Lukáš Folkman
Masarykova univerzita, Fakulta informatiky

Sensor nodes situated spatially close to each other tend to have similar behaviour. The neighbour-based detection technique is based on this principle and should provide means for anomaly intrusion detection in wireless sensor networks without prior training. Recently, this technique has been successfully applied to detect the fabricated information attack in wireless sensor networks.

This work provides the analysis of the symptoms of jamming, hello flood, selective forwarding, sinkhole, sybil, packet alteration and fabricated information attacks for the applicability of the neighbour-based technique. Furthermore, a neighbour-based intrusion detection system is designed and implemented for the operating system TinyOS. The intrusion detection system comes in two modifications – one with local knowledge of immediate neighbours only and one involving information exchanged among 1-hop or 2-hop neighbours. Collaboration is employed in order to refine information about the activity of neighbouring nodes. The accuracy of the technique was evaluated in detection of jamming, hello flood and selective forwarding attacks. Results of the simulations, namely the number of false negatives, false positives and correct warnings, are involved in this work as well.

The results presented in this SVOČ were submitted as the author's master thesis in January 2010. The topic was further researched and a publication involving the results from this work will be submitted to a conference in May 2010. Furthermore, a comprehensive technical report will be published in May 2010.