Abstract

Wireless Sensor Networks (WSNs) present myriad application opportunities for several applications areas such as precision agriculture, environmental monitoring, traffic control, industrial process monitoring and control, home automation and mission-critical applications such as military surveillance, healthcare applications, disaster relief and management, fire detection applications among others.

Since WSNs are used in mission-critical tasks, security is an essential requirement. An adversary can easily compromise sensor nodes due to unique constraints inherent in WSNs such as limited sensor node energy, limited computational and communication capabilities and the hostile deployment environments. These WSNs unique challenges render existing traditional security schemes used in traditional networks inadequate and inefficient. An adversary may take control of some sensor nodes and use them to inject false data with the aim of misleading the network’s operator (Byzantine attack). It is therefore critical and crucial to detect and isolate malicious nodes so as to prevent attacks that can be launched from these
Enhanced Weighted Trust Evaluation Scheme for Detection of Malicious Nodes in Wireless Sensor Networks

nodes and more importantly avoid being misled by incorrect falsified information introduced by
the adversary. This research explores and gives emphasis on improving Weighted Trust
Evaluation (WTE) as a technique for detecting and isolating these malevolent nodes. Extensive
simulation is performed using MATLAB in which the results show the proposed enhanced WTE
based algorithm has the ability to detect and isolate malicious nodes; both malicious sensor
nodes and malicious forwarding nodes in WSNs at a reasonable detection rate and short
response time whilst achieving good scalability.

References

2. K. Chelli, Security Issues In Wireless Sensor Networks: Attacks And Countermeasures,
3. A. B. Karuppiah and S. Rajaram, False Misbehavior Elimination of Packet Dropping
1, 2014.
5. K. Sumathi and D. M. Venkatesan, A Survey on Detecting Compromised Nodes in
Wireless Sensor Networks, (IJCSIT) International Journal of Computer Science and Information
6. R. Sharma and N. Tripathi, Comprehensive Review on Wireless Sensor Networks,
and Challenges in Wireless Sensor Networks, International Journal of Computer Science and
Sensor Networks, The Symposium on Simulation of Systems Security (SSSS’08), Ottawa,
9. S. A. Soomro, A. G. Memon and . A. Baqi, Denial of Service Attacks in Wireless Ad-hoc
Attacks in Wireless Networks, in Twenty-Second Annual Joint Conference of the IEEE
13. Y. L. Sung and Y.-H. Choi, Malicious Node Detection Using a Dual Threshold in
Detection in Wireless Sensor Networks Using an Autoregression Technique, in the 3rd
15. Y. Yang, X. Wang, S. Zhu and G. Cao, Distributed Software-based Attestation for Node
Compromise Detection in Sensor Networks, in 26th IEEE International Symposium on Reliable

Index Terms

Computer Science Wireless

Keywords

Weighted Trust Evaluation, Malicious nodes, Malicious Nodes Detection Techniques, Wireless Sensor Networks Security