{tag} {/tag}International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 155
-
Number 4

Year of Publication: 2016

Authors:

Koriata P. Tuyaa, W. Okelo-Odongo

10.5120/ijca2016912298

{bibtex}2016912298.bib{/bibtex}

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

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

1. K. Sohraby, D. Minoli And T. Znati, Wireless Sensor Networks: Technology, Protocols, And Applications, Hoboken, New Jersey.: John Wiley & Sons, Inc., 2007.
2. K. Chelli, Security Issues In Wireless Sensor Networks:Attacks And Countermeasures, Proceedings of The World Congress on Engineering 2015, Vol. 1, pp. 1-6, 2015.
3. A. B. Karuppiah and S. Rajaram, False Misbehavior Elimination of Packet Dropping Attackers during Military Surveillance using WSN, Advances in Military Technology, vol. 9, no. 1, 2014.
4. D. S. Alam And Debashis, Analysis Of Security Threats In Wireless Sensor Network, International Journal of Wireless & Mobile Networks (IJWMN), Vol. 6, 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 Technologies, vol. 5, pp. 7720-7722, 2014.
6. R. Sharma and N. Tripathi, Comprehensive Review on Wireless Sensor Networks, Oriental Journal of Computer Science & Technology, Vol. 8, No. 1, pp. 59-64, April 2015.
7. D. G. Padmavathi and M. D. Shanmugapriya, A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks, International Journal of Computer Science and Information Security,, vol. 4, 2009.
8. I. M. Atakli, H. Hu, Y. Chen, W. S. Ku and Z. Su, Malicious Node Detection in Wireless Sensor Networks, The Symposium on Simulation of Systems Security (SSSS'08), Ottawa, Canada, p. 838, 2008.
9. S. A. Soomro, A. G. Memon and . A. Baqi, Denial of Service Attacks in Wireless Ad-hoc Networks, Journal of Information & Communication Technology, vol. 04, pp. 01-10, 2008.
10. D. Virmani, A. Soni, S. Chandel and M. Hemrajani, Routing Attacks in Wireless Sensor Networks: A Survey, Bhagwan Parshuram Institute of Technology, India, 2014.
11. H. Y-C and A. Perrig, A Survey of Secure Wireless Ad Hoc Routing, IEEE Security and Privacy, 2004.
12. Y.-C. Hu, A. Perrig and D. B. Johnson, Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks, in Twenty-Second Annual Joint Conference of the IEEE Computer and Communication Societies, 2003.
13. Y. L. Sung and Y.-H. Choi, Malicious Node Detection Using a Dual Threshold in Wireless Sensor Networks, Journal of Sensor and Actuator Networks, 2013.
14. D. I. Curiac, O. Banias, F. Dragan, C. Volosencu and O. Dranga, Malicious Node Detection in Wireless Sensor Networks Using an Autoregression Technique, in the 3rd International Conference on Networking and Services , Athens, Greece, 2007.
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

Distributed Systems , Pennsylvania, 2007.

16. F. Bao, I.-R. Chen, M. Chang and J.-H. Cho, Trust-Based Intrusion Detection in Wireless Sensor Networks, in International Conference on Communications,, Kyoto, Japan, 2011.

17. T. Nidharshini and V. Janani, Detection of Duplicate Nodes in Wireless Sensor Networks Using Sequential Probability Ratio Testing, International Journal of Advanced Research in Computer and Communication Engineering, vol. 1, no. 10, December 2012..

18. S. Zhao, K. Tepe, I. Seskar and D. Raychaudhuri, Routing Protocols for Self-Organizing Hierarchical Ad-Hoc Wireless Networks, Proceedings of the IEEE Sarnoff Symposium, Trenton, NJ,, March 2013.

19. H. Hu, Y. Chen, W.-S. Ku, Z. Su and C.-H. J. Chen, Weighted trust evaluation-based malicious node detection for wireless sensor networks, Int. J. Information and Computer Security, vol. 3, no. 2, p. 148, 2009.

20. D. M. Venkatesan and K. Sumathi, A Survey on Detecting Compromised Nodes in Wireless Sensor Networks," (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 5, pp. 7720-7722, 2014.

21. I. F. Akykildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, A Survey on Sensor Networks, IEEE Communication Magazine, 2002.

22. R. Das, D. B. S. Purkayastha and D. P. Das, Security Measures for Black Hole Attack in MANET: An Approach, Proceedings of Communications and Computer, 2002.

23. T. Sathyamoorthi, D. Vijayachakaravarthy, R. Divya And M. Nandhini, A Simple And Effective Scheme To Find Malicious Node In Wireless Sensor Network, International Journal of Research In Engineering And Technology, Vol. 03, No. 02, 2014.

Index Terms

Computer Science Wireless

Keywords

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