# Exploring Security Algorithms and Protocols for Wireless Sensor Networks: A Comprehensive Survey and Analysis

ECE 543 Technical Paper

## Abstract:

This technical report aims to investigate security algorithms and protocols for wireless sensor networks. In today's digital world, network security has become increasingly important due to the rising frequency, sophistication, and harm of cyber-attacks. Network security protocols are critical in safeguarding wireless sensor networks and data against various types of attacks, including eavesdropping, tampering, impersonation, and denial of service. To achieve the objectives of this report, we will focus on a specific area of study, namely security techniques for wireless sensor networks. We will begin by conducting a thorough literature survey of recent academic research in this field, with a particular emphasis on the references listed in this report. We will then formulate the problem to be studied, summarize and classify existing solutions to the problem, and identify open issues that require further investigation. Finally, we will explore possible solutions to these open issues. This technical report aims to contribute to the development of more secure and resilient wireless sensor networks by providing insights into key security challenges and potential solutions.

## References:

1. Moudni, H., Er-rouidi, M., Mouncif, H., & El Hadadi, B. (2016). Secure Routing Protocols for Mobile Ad Hoc Networks. In 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM) (pp. 1-6). IEEE. DOI: 10.1109/WINCOM.2016.7777395
2. Yufei Wang, Weimin Lin, and Tao Zhang. "Study on Security of Wireless Sensor Networks in Smart Grid." 2010 IEEE International Conference on Wireless Communications, Networking and Information Security. IEEE, 2010. DOI: 10.1109/WCINS.2010.5542937.

3. Tao Chen, Haiping Huang, Zhengyu Chen, Yiming Wu, and Hao Jiang. "A Secure Routing Mechanism Against Wormhole Attack in IPv6-based Wireless Sensor Networks." Proceedings of the 2015 IEEE 4th International Conference on Progress in Applied Mathematics in Science and Engineering (PIAMSE). IEEE, 2015. DOI: 10.1109/PAAP.2015.30.
4. Priya, N., & Asswini, M. (2015). A survey on vulnerable attacks in online social networks. 2015 International Conference on Communications and Signal Processing (ICCSP), 978-1-4799-8788-7/15/$31.00/45.
5. Mahmoud, M.M.E.A., Lin, X., & Shen, X. (2015). Secure and Reliable Routing Protocols for Heterogeneous Multihop Wireless Networks. IEEE Transactions on Parallel and Distributed Systems, 26(4), 1140. DOI: 10.1109/TPDS.2013.138.
6. Wang, H., Wang, Y., & Han, J. (2009). A Security Architecture for Tactical Mobile Ad hoc Networks. Proceedings of the 2nd International Conference on Knowledge Discovery and Data Mining (WKDD'09), 154-157. DOI: 10.1109/WKDD.2009.154.
7. Buttyan, L., & Csik, L. (2010). Security Analysis of Reliable Transport Layer Protocols for Wireless Sensor Networks. In Proceedings of the 2010 7th IEEE Consumer Communications and Networking Conference (CCNC) (pp. 1-5). IEEE. DOI: 10.1109/ccnc.2010.5421665.
8. Xiao, D., Wei, M., & Zhou, Y. (2006). Secure-SPIN: Secure Sensor Protocol for Information via Negotiation for Wireless Sensor Networks. Proceedings of the 2006 5th International Conference on Information Processing in Sensor Networks (IPSN '06), 417-424. DOI: 10.1109/IPSN.2006.243784.
9. Sirohi, P., & Agarwal, A. (2015). Cloud Computing Data Storage Security framework relating to Data Integrity, Privacy and Trust. In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT) (pp. 1214-1219). IEEE. DOI: 10.1109/ICGCIoT.2015.7380755.
10. Yang, W., & Fung, C. (2016). A Survey on Security in Network Functions Virtualization. In IEEE International Conference on Communications (ICC) (pp. 1-7). IEEE. DOI: 10.1109/ICC.2016.7510906.