



RESEARCH ARTICLE

Rule-Based and Cluster-Based Intrusion Detection Technique for Wireless Sensor Network

Ms. Rachana Deshmukh¹, Ms. Rashmi Deshmukh², Prof. Manoj Sharma³

¹IT Department, NRI-Institute of Information Sciences & Technology, Bhopal, Madhya Pradesh, India

²CSE Department, Dr. Babasaheb Ambedkar College of Engineering & Research, Nagpur, Maharashtra, India

³IT Department, NRI-Institute of Information Sciences & Technology, Bhopal, Madhya Pradesh, India

¹ rachana_deshmukh@yahoo.com; ² rashmi_deshmukh86@yahoo.co.in; ³ manojsharma042@gmail.com

Abstract— Wireless Sensor Networks (WSNs) are playing a fundamental role in emerging pervasive platforms that have potential to host a wide range of next generation civil and military applications. Since WSNs are made up of numerous low-cost and small devices and usually deploy to an open, unprotected and hostile environments, it is vulnerable to security threats and susceptible to physical capture. Thus, it is necessary to use effective mechanisms to protect the network. Intrusion detection system is one of the major and efficient defensive methods against attacks on wireless sensor network. Sensor networks have different characteristics and hence security solutions have to be designed with limited usage of computation and resources. In this paper, the architecture of hybrid intrusion detection system (HIDS) is proposed for wireless sensor networks. In order to get hybrid scheme, the combined version of Cluster-based and Rule-based intrusion detection techniques is used and eventually evaluated the performance of this scheme by simulating the network. A prevention mechanism is used to counteract well-known attacks. The simulation result shows that the scheme performs intrusion detection using hybrid technique and detection graph shows ratings like attack rating, data rating and detection net rating with the attack name and performs better in terms of energy efficiency and detection rate.

Key Terms: - Wireless Sensor Network; Rule-based & cluster-based intrusion detection; Hybrid; Anomaly detection; Misuse detection

Full Text: <http://www.ijcsmc.com/docs/papers/June2013/V2I6201343.pdf>