ABSTRACT

Title: SECURE ROUTING STRATEGIES FOR WIRELESS SENSOR NETWORKS USING TRUST AND ANONYMITY

Emerging of Wireless sensor networks has increased in recent times, therefore the need for effective security mechanisms is essential. Because sensor networks may interact with sensitive data and operate in hostile unattended environments, it is imperative that these security concerns be addressed from the beginning of the system design.Based on energy, power consumption, and response time of the nodes, this research work provides a novel framework to detect the behavioural defect of wireless sensor network nodes. The association of the detection model with the attack response knowledge base helps in order to produce prompt suggestions to prevent the attacks is another innovative result of this work. The goal of this work is to develop a responsive system for limiting the harms brought on by any attack on wireless sensor networks and thereby, increase the reliability of wireless communication.

The data transmission in WSNs are managed by routing protocols and the new node registration policy . Therefore, across the whole life cycle of wireless sensor networks, these two circumstances are the most vulnerable. Thus, this paper examines two distinct solutions which are mutually exclusive. In this research work routing with randomize channel is used to prevent the majority of network attacks, and the node registration process is implemented using multi order key. Separating the header and content portions of data packets is done to reduce the computing power across communication channel is another result of this research work.

One of the most important issues affecting the channel performance is the security issues. Therefore, to overcome this security issues in WSN, an intelligent crypto mechanism is required. Hence, a novel Recurrent-based Public Crypto System (RbPCS) is proposed. Here, the recurrent function in the public cryptosystem identifies the malicious users and neglects them. Moreover, the proposed technique helps in hiding the data from third parties. Also, it reduces energy consumption by ignoring the high-power consumption nodes. Furthermore, the robustness of the proposed technique is determined by launching security attacks in the WSN communication channel. Moreover, the performances of the designed model are estimated in terms of communication delay, energy consumption, packet drop, packet delivery, and throughput ratio. Finally, the outcomes of the developed model are compared with other existing techniques.

Mohammed Abdul Azeem