Your name
Tutor's name
Course
Date

Wireless Sensor Network Security

Wireless sensor network can be often attacked within the modern information system field. Such vulnerability can be caused by devices with low battery power, minimal memory, and low energy. Communication between sensor nodes are initiated and executed through wireless links. Security is one of the most important issues when talking about wireless networking systems. This is evidence that sensor networks are vulnerable to various threats and attacks. One of the factors that may influence the wireless network security is the presence of environmental conditions (Singh & Verma).

The sensor nodes operate within the sensor field in a scattered manner. The scattered nodes can collect data and transmit it back to the sink and end users. The sink usually communicates to the task manager through the Internet or satellite. The task manager represents the centralized area of the control within the network. This point of control has a crucial role in obtaining information from the network and disseminates or transmits the information back into the network. The task manager also operates as the gateway to other networks. In addition, it functions as the data processing and storage centre and access point to human interface (Singh & Verma).

Wireless sensor networks are a common in today's society. A such, it serves as an economic solution to numerous problems that organizations face. Typical applications of the wireless sensor networks include:

- **Military applications** that are applicable in the use of military cases to monitor statuses such as position, quantity, and availability of the troops, equipment, and surveillance of the battlefield. The systems also provide accurate information with reference to detection of biological and chemical attacks.
- **Environmental Applications** are used to evaluate the conditions of the environment:

humidity, temperature, and pressure. It also helps detect disasters in reference to forest fires, flood, volcanoes, and other relevant activities as they occur.

- **Health Applications** are used to indicate attacks or conditions such hypertension, high blood pressure, and to monitor heart rates.
- **Commercial Applications** are also applicable in the detection of vehicles, warehouses, and buildings.
- **Scientific Application or Exploration** uses wireless sensor networks to operate under water and in other fields with the aim of delivering scientific explorations.
- **Area Monitoring** involves operations in the monitoring of phenomena within the area. Such phenomena include intrusion by enemies, heat, and pressure evaluation (Singh & Verma).

Security requirements include four areas of focus: authenticity, confidentiality, integrity, and scalability. Authentication is a crucial aspect of wireless or sensor networking systems. It enables the sender node and the receiver to communicate effectively. Confidentiality ensures that an external party, other than the communicating nodes, will not read the data transmitted correctly. This ensures that the message transmission is conveyed through encryption. Integrity indicates that the data should follow modifications by the adversary receiver. This ensures the validity of data between the sender and the receiver. Scalability requirement indicates that the key management scheme must be scalable in the sense that, in growth of the network in relation to size, there should be no increase in the compromising of the nodes, thus, it involves constant cost of operation (Singh & Verma).

Works Cited

Singh, S., & Verma, H. “Security for Wireless Sensor Network.” *International Journal on Computer Science & Engineering*, 3.6 (2011): 2393-2399. Print.