ABSTRACT

A Wireless Sensor Networks consists of small, inexpensive, battery-powered wireless sensors, which self configure and collaborate with each other to support cost effective sensing in situations where human observation or wired systems deployment can be inefficient, expensive, dangerous, or otherwise untenable. Unfortunately, the desirable nature of a WSN introduces many security challenges. Wireless Sensor Networks are often deployed in an open environment in specific applications such as battlefield. Overall in a typical WSN, sensor nodes with severe energy and other resources constraints are responsible for data collection, data processing, localization, time synchronization, data forwarding upstream and downstream, while facing numerous security threats.

The broadcast nature of wireless communication introduces various attacks in WSN. In which, the attackers can capture the sensor nodes to extract secret data or reprogram them to execute malicious code which affects the other uncompromised sensors significantly. In the worst case, the entire WSN can fall in the attacker’s hand. An adversary may use higher energy signals to jam radio communication between sensors. Relatively little work have been done to address physical attacks in WSNs.

This research work mainly focus on lack of issues regarding achievement of security for certain attacks like jamming attack, denial of sleep attack, tampering and cheating attack in IEEE802.15.4 based wireless
sensor networks. Initially, the research has been started by the problem of identifying jamming attack in IEEE802.15.4 based wireless sensor network. A defense technique based on swarm intelligence has been proposed to identify the pulse jamming attack. Swarm intelligence algorithm is proficient enough to adapt change in network topology and traffic.

Using the swarm intelligence technique, the forward ants either unicast or broadcast at each node depending on the availability of the channel information for end of the channel. If the channel information is available, the ants randomly choose the next hop. The source on receiving the channel information from the backward ant verifies the prevalence of the attacker for long time and avoids the particular channel for transmission in order to improve the performance of wireless sensor network. Simulation results assessing the performance of the proposed Swarm Based Defense Technique based on rate, time and number of attackers proves the efficiency of the proposed scheme compared to the existing techniques.

The next step towards the detection scheme is to introduce a resistant countermeasure for defending against specific attack like denial of sleep attack in wireless sensor networks. More specifically, SBDT model has been extended to detect denial of sleep attack. Time series S-ARMA (Swarm intelligence Auto Regressive Moving Average) model is proposed to predict the network traffic in future using Swarm intelligence and Auto Regressive Moving Average.
This model estimates the difference in actual and predicted traffic. If the difference is above a threshold value, the current traffic is abnormal and the node requests for frequency hopping. The number of nodes requesting for the frequency hopping is identified and if it is below a threshold value, then the frequency hopping is not initiated. In S-ARMA model, the administrator node sends its communication frequency and the frequency hopping time through the forward ants during the route discovery. The forward ants collect the information from all the nodes and when it reaches the destination, the collected frequency hopping time is verified. The node having a frequency hopping time greater than the threshold value is identified as a node with fault channel. This information is sent to the administrator node through the backward ants. Administrator node obtains the information and omits the node with fault channel from the network and transmits the data through remaining channels. This technique proves to be efficient in detecting the faulty channel with less overhead compared to the existing scheme.

A Defense technique based on swarm intelligence has been expanded to identify the tampering and cheating attacks. Swarm Based Trusted Node model for Tampering and Cheating Attack (SBTN-TC) has three main phases namely Trusted node selection phase, Route establishment phase and Processing phase. Initially, Trusted Node (TN) is selected based on highest trust value using swarm intelligence. When the TN receives a session receipt using Cryptographic Puzzle Hiding Scheme (CPHS), it first verifies
whether the receipt is processed before, using session identifier. The TN classifies each session into fair or cheating and fair sessions are further classified into complete or broken based on session receipt formats to reduce cheating attacks. The CPHS used for communication between TN and a node improves the security has been modeled using Petri Nets. Thus the proposed SBTN-TC model reduces tampering attack and also restricts the cheating attacks in wireless sensor networks. The security analysis of the proposed method proves to be effective compared to an existing scheme from the simulation results. It has been believed that the detection algorithm proposed will have practical use in real world deployment and provides a platform for further investigation of more attractive solution against tampering and cheating attacks for IEEE802.15.4 based wireless sensor networks. The performance is evaluated for dropping of Route Reply Packet, Data Packet and Acknowledgement Packet.

The general framework to overcome these vulnerabilities in wireless sensor networks is based on Swarm intelligence incorporated with frequency hopping, ARMA model and cryptographic puzzle hiding scheme is a powerful security mechanism to identify various attacks like jamming attack, denial of sleep attack, tampering and cheating attack without degrading the performance of the network. The effectiveness of these security mechanisms has been proved from the simulation results.