ABSTRACT

Recent years have seen the adoption of wireless sensor networks (WSNs) as communication infrastructure for distributed real-time applications such as industrial process monitoring and control, structural health monitoring, and patient monitoring. These applications require real-time communication over multi-hop WSNs. While significant advances towards this goal have been made, existing solutions usually falls short in one (or more of) the following aspects:

Existing results are often derived for simplified communication workloads such as converge-cast or query services where data is routed from sensors to a single base station. While this leads to elegant solutions, it also limits the applicability of these protocols. For example, in contrast to current centralized architectures in which all communication goes through one or a few gateways, to achieve higher scalability, the next generation of industrial process monitoring and control will require multiple control loops to be established between arbitrary sensors and actuators using real-time flows.

Existing solutions often adopt unrealistic interference models or ignore interference. For example, WirelessHART – a standard for sensor-actuator networks – prohibits concurrent packet transmissions within the same channel. As a result, the scale of existing WirelessHART networks is limited.

Effective real-time solutions must also ensure reliable data delivery to end-points under variable workloads and network
dynamics. This is difficult since packet retransmissions must be integrated effectively during scheduling and real-time analysis.

The computation of transmissions schedules is often performed in a centralized fashion. This approach limits both system scalability as well as the capability of a system to adapt to workload and network dynamics.

Interference in Wireless Sensor Network (WSN) is of practical interest in many applications such as detecting an intruder in a battlefield. The interference detection is defined as a mechanism for a WSN to detect the existence of inappropriate, incorrect, or anomalous moving attackers. In the present study, we consider this issue according to heterogeneous WSN models. Furthermore, we consider two sensing detection models: single-sensing detection and multiple-sensing detection. Our simulation results show the advantage of multiple sensor heterogeneous WSNs.

**Existing System**

1. In single-sensing detection, at a time only one intruder detected by the WSN.

2. Our Previous work was according to homogeneous and heterogeneous single sensor in wireless sensor network.

3. It is because individual sensors can only sense a portion of the intruder.
The disadvantages with the existing system are

1. The sensed information provided by a single sensor might be inadequate for recognizing the intruder.
2. So that there is no guarantee for our information has been sent securely.
3. Data will not rout if primary detector fails.

**Proposed System**

Interference detection in heterogeneous WSNs by characterizing interference detection with respect to the network parameters.

1. In Heterogeneous wireless sensor, Intruder detected anywhere in the network.
2. We are detecting the intruder both single sensor and multiple sensor heterogeneous wireless sensor networks.

The advantages with the proposed system are

1. If primary detector fails another detector detect the intruder.
2. By finding the intruders we can send our information in a secured manner.