Presentation slide

Attack names	Attribute name
Grayhole	Who_CH , JOIN_R ,DATA_R,DIST_CH_TO_BS,is_CH, Time, ADV_R
Blackhole	Who_CH, JOIN_R , DATA_R, is_CH, Time, ADV_R
Flooding	Who_CH, DATA_SEND_TO_BS, DIST_CH_TO_BS, is_CH, ADV_S, ADV_R , Comsumed_energy
TDMA	SCH_S , JOIN_R , DATA_SEND_TO_BS, is_CH, Time,
Normal	Id, Dist_to_CH, JOIN_S, SCH_R, RANK, DATA_S, SEND_CODE

- **Attack type when and why occurs:**
- **Scheduling attack:** Scheduling attack occurs during the setup phase of LEACH protocol, when CHs set up TDMA schedules for the data transmission time slots. The attacker which acts as a CH will assign all nodes the same time slot to send data. This change will cause packets collision and leads to data loss.
- **Flooding attack:** Flooding attack occurs during the setup phase of LEACH protocol. A large number of advertising CH message with high transmission power is received by sensor leads to consume sensors energy and waste more time to determine which CH to join.
- **Blackhole attack: B**lackhole attack occurs during the setup phase and steady-state phase of LEACH protocol. Advertising itself as a CH at the beginning of the round. any node that has joined this CH during this round will send the data packets to it in order to be forwarded to the BS. any node that has joined this CH during this round will send the data packets to it in order to be forwarded to the BS.
- **Grayhole attack: G**rayhole attack occurs during the setup phase and steady-state phase of LEACH protocol. It advertising itself as a CH for other nodes. the forged CH receives data packets from other nodes, it drops some packets (randomly or selectively) and prevents them from reaching the BS.