PROPOSED TITLE:

VAMPIRE ATTACK DETECTION AND SECURE ROUTING IN WIRELESS AD HOC SENSOR NETWORK

OBJECTIVES:

- Detect Vampire attack
- Provides Security against vampire attacks.
- Ensure Quality of Service.
    - ✓ Minimum delay in data delivery
    - ✓ High packet delivery ratio
    - ✓ High malicious detection rate
    - ✓ High network lifetime

SCOPE OF THE RESEARCH WORK

1. Trust based secure transmission routing
    - Detect vampire attack using KID-SASR
2. Secure routing scheme to mitigate the attack
    - Detect anti-nodes from safe nodes.
    - Provide security in routing using BSCSRP

PREVIOUS WORK:

- Focused on denial of communication at the routing or medium access control level
- Previous studied Dos attacks are Reduction of Quality (ROQ) and Routing Infrastructure Attacks.
- Previous work are confined to MAC or application layer(not in Routing Protocol Layer)
- In the existing methods low throughput and the packet delay happens during communication.
- Some protocol doesn't offer secure routing and high in energy consumption.
- Existing scheme protects against only in hostile attacks.
- No other techniques presented with security, trustworthiness against vampire attacks and low energy consumption.
- The main aim of the introduced method is to provide good quality of service and security in WSN

RESEARCH PROBLEM

- Various experts have published their report on identifying vampire attacks in WSN.
- Attackers aim to broadcast little data, making long source paths to reach the destination.
- Results in waste of energy by consuming its battery power e.t.c.

PROPOSED WORK

1. SASR Algorithm for Optimal Route Selection
   I. Problem formulation for secure routing.
   II. Routing design using SASR
2. A secure routing scheme to mitigate the attack in WASN