ABSTRACT

Wireless Sensor Network (WSN) is an emerging technology that can be applied for various futuristic applications like commercial and military. The WSN nodes are tiny nodes which are used to sense the environmental surroundings like temperature, humidity etc. It has a tiny operating system that is capable of processing the data and routing the packets. The features of nodes make it more lucrative and provide wide opportunity to develop plenty of applications in future. Due to wireless communication, various types of security threats such as availability, confidentiality, integrity and authenticity are incurred while routing the packets in the network. In order to protect the network from routing attacks, malicious node detection schemes have been proposed in this study.

Security issues play a vital role in protecting the network from the malicious nodes. The detection schemes for malicious nodes must be smart enough to find out the root cause of the attack. The primary objective of this study is to provide malicious node detection schemes for WSN. Hence, network layer attacks and its counter measures are addressed to a limited extent. Software and hardware detection schemes have been proposed and simulated. The performance of the proposed detection schemes are analyzed based on the metrics such as throughput, packet delivery ratio, energy
wormhole link and thus increases the throughput of the network. Two normal nodes. It is proved that the proposed scheme detect the exact transmission time between the two wormhole nodes is higher than the detection (THD) scheme has been proposed. Wormhole nodes are detected by this attack is a challenging task. To address this issue, time and hop based cryptographic countermeasures cannot defeat this attack and hence defining which has low latency link and replaces the other parts of the network. In the wormhole attack, the malicious node creates the initial improves the performance of the network provides a secure routing in the forward routing path of the network and with lower energy is suspected as malicious node. The proposed scheme with lower energy is suspected as malicious node. The node energy, in THD scheme, node energy is distributed for detection. The node compromised node is detected and is confirmed by node identification and a compromised packet is detected and is confirmed by node identification. A cumulative acknowledgement packets of nodes then lie in the forward routing path are provided by the check points. Based on the cumulative acknowledgement (EFD) schemes are proposed in CHED scheme the cumulative acknowledgement based detection (CHED) and Energy Based Detection in the network. In order to detect this attack, CHED and cumulative acknowledgement detects the packet or refuses to forward the packet. Selective Forwaring Attack (SF-A), wormhole attack, sinkhole attack and this thesis begins with the literature survey on network layer, overheard, detection accuracy and detection complexity, consumption, communication overheard, memory overheard, consumption.
considerably improved because the routing scheme consumes less energy and the performance of the network is considerably improved. The proposed scheme consumes less energy for various mobility packet delivery ratio and throughput and are analyzed for various mobility packet delivery ratio and throughput and are analyzed for various mobility. Further, it is confirmed by the Euclidean distance between the nodes. The symbol node is detected if the energy value is less than the threshold value and symbol node is detected if the symbol node is detected by the base station. A node is detected by the other nodes if the identifier (ID) numbers of schemes are proposed. In NI Scheme, the Identification (ID) and Energy (E) schemes are proposed. In TH Scheme, the Identification (ID) and Energy (E) schemes are proposed. Additionally, the denial of service to legitimate nodes. In order to overcome the symbol is affected with symbol attack, malicious node sends incorrect data and data and causes hardware to check the feasibility of the algorithm. determine the exact malicious node. The proposed scheme is implemented in the proposed scheme causes many malicious nodes in the current and which helps in
network performance.

Further, the research should focus on security issues are simulated using Verilog Hardware Description Language (VHDL) of detection schemes for sinkhole attack, secure AODV, and modeled DSSS. The detection implementation simulated using the Network Simulator-Ns2. The hardware implementation increased.

hardware which consumes less energy and hence the life time of the node is transmitter and receiver is perfect. The proposed scheme is implemented in the radio of the proposed scheme is better when the synchronization between the Specimen (XIDSS) using robust cipher has been proposed. The efficiency in order to achieve signal level security: Modified Direct Spread.

The security threats such as data integrity and confidentiality are achieved. The proposed architecture is compatible with the wireless sensor node. The proposed data transmitted at the transmitting end, then the node is said to be malicious. The decrypted data at the receiving end is different from the original encrypted