ABSTRACT

The evolution of Wireless Network (WN) has dominated the field of communication across the globe as compared to wired network through its advantages such as the absence of physical media, concept of mobility and ease of installation. The current splurge in the attractiveness of wireless services can be attributed to the sharp decrease in the cost of wireless hardware equipment’s and subsequent reduction in the set-up price of wireless infrastructure. Furthermore, the ease of availability of wireless services at anytime and anywhere makes it the most popular mode of communication now-a-days.

Based on the architecture, wireless networks are broadly classified as follows: *Infrastructure mode* in which the coordination of WN is done through central device namely Access Point (AP) deployed for connecting the devices in the WN. Wireless APs are further connected to broadband modem and provide a link for the nodes with the outside world. *Adhoc mode* is a peer to peer communication methodology followed for communication between nodes. Moreover, ad hoc mode does not require the deployment of AP’s. In setting up of ad hoc mode, there is need of manual configuration of all wireless adapters.

Ad hoc network (AN) belongs to a class of peer to peer wireless communication network in which direct communication takes place between wireless devices without the assistance of any AP’s. As and when the need of communication arises the WN is established spontaneously subject to the condition that the participating nodes should be in close proximity of each other. The self-supporting nature of AN’s is quite handy in dealing with the situations such as natural calamity, emergency situations, military operations and other scenarios where a prompt response for data communication is...
required. The typical characteristics of AN include infrastructure less, dynamic topology, limited storage capacity, limited battery and limited bandwidth and lack of centralized management. Nevertheless, in spite of being easy to deploy and quick response, there are few practical limitations of AN’s especially in terms of security and reliability.

ANs are broadly categorized as Mobile Adhoc Network (MANET), Wireless Sensor Network (WSN) and Wireless Mesh Network (WMN). MANET is a dynamically reconfigurable, self-organizing and can be deployed rapidly. In spite of numerous advantages like easy deployment with reduced cost MANETs are susceptible to various security concerns. The main culprits for the security breach in MANETs are missing of central coordinator and the use of wireless communication media. Moreover, no well-defined boundaries, decentralized administration and issues of scalability also contribute towards security vulnerability of MANET’s. Routing is one of the most important attribute of MANET and is often explored and misused by the attackers for infiltration in to the network. The routing protocols designed for MANET’s are mostly optimized for reduction of computational overheads as almost every node of MANET is involved in the routing process. Thus, security concerns usually take the backseat eventually leading to security breach. Reactive protocols are considered better than proactive protocols in terms of performance because of low bandwidth consumption. Whereas proactive protocols consume lots of network resources to maintain up-to-date status of network routes. In recent times there have been numerous innovations in the field of routing protocols for MANET’s but still Adhoc On Demand Distance Vector (AODV) protocol remains the most widely deployed routing protocol and the credit goes to its loop-free routing behavior. Further, AODV routing protocol consumes minimum power, memory and network resources. In spite of possessing so many
advantages one of major flaw of AODV routing protocols is that it is prone to various security breaches as during the design of AODV protocol the security aspect has not been taken care off. AODV falls under reactive routing category of protocols in which a route is established by activating route discovery process only when a node needs to transfer data. Stale routes are not maintained to reduce the extra overhead. A sequence number is used for loop prevention and keep freshness of routes. In spite of various advantages, AODV is designed to work within trusted environment and unable to address malicious activities of adversary. Thus, in order to utilize the proper services of AODV, it is imperative to inculcate the security aspects so that the security attacks can be avoided.

Wireless Sensor Network is another type of adhoc network that comprises number of sensor nodes deployed in a specific region to track the real world physical or environmental conditions remotely viz: pressure, temperature, humidity, pollution etc. Sensor nodes are small in size with limited processing capacity, storage capability, and communication ability. Sensor node transmits the readings of the physical phenomenon to the base station which has larger memory and power for processing the data than the sensor nodes. In WSNs, the energy is dispersed while sensing, processing, transmitting or receiving data. WSN is dynamically adaptable to any environment at reduced installation cost. Despite possessing the attribute of ease of deployment, WSNs suffers from a major drawback of being prone to various security threats. Moreover, due to their adhoc nature and energy constraint the existing security model being deployed in wireless and wired networks cannot be applied for WSN’s Hence, power aware security protocols become a necessity for proper working of WSN’s. Energy consumption of sensor nodes is another big challenge in order to improve the performance of WSN.
Various routing strategies in terms of energy efficiency and security have been proposed in literature.

WSNs based on network architecture are categorized in flat networks, Hierarchical networks and location based networks. Accuracy of location information is main issue in location based networks whereas flat network routing protocols suffer from scalability issue as they are only feasible with small area networks. Hierarchical routing removes problem of scalability. In Hierarchical protocols, whole network is divided into clusters in which few nodes become cluster head (CH). These cluster head nodes process and send the data to base station (BS), rest of nodes collect data from environment and send it to CH nodes. Secure and energy efficient routing protocol is a challenge for data communication between clusters and base station. Low Energy Adaptive Clustering Protocol (LEACH) and its variants are a good solution for energy efficiency. However, the security issues concerns are missing in LEACH.

In proposed research work two algorithms namely: Two Step Protection Method (TSPM) to prevent flooding attack in MANETs and a Secured Energy Efficient Technique (SEET) to address blackhole attack in WSN are proposed to improve routing and energy efficiency of MANET and WSN respectively. TSPM has been subjected to extensive testing and simulation and the obtained results establish that TSPM improves the route discovery process of AODV by adding security features which subsequently leads to a secured performance of MANET. Moreover, TSPM is designed to improve security flaws of AODV by keeping update information about its neighbors and by checking the legality of standard routing parameters. Performance evaluation of the scheme has been carried out through simulation experiments, to test the effectiveness of our approach in terms of throughput, packet delivery ratio and average end to end delay.
SEET has been specifically designed for embedding the security features in the working of LEACH. It inculcates the feature of attack prevention and improves the energy efficiency of LEACH by refining the cluster formation and data communication process of LEACH. In SEET a new concept of associate clusterhead (ACH) is introduced. ACH is one of a legal member node of a cluster that keeps track of malicious activity of clusterhead (CH) and helps to process data collected from member nodes of corresponding cluster. ACH prevents the loss of data that may occur because of blackhole attack in WSN. The effectiveness of SEET is comprehensively evaluated in terms of energy consumed, number of alive nodes and throughput of WSN.

The computational experiments depict that proposed methods TSPM and SEET are superior to the existing protocols and successfully detect and prevent the network from malicious nodes under attack. TSPM shows consistent performance under different number of attackers and with different node mobility as compare to existing protocols. SEET proves to elongate network life time because ACHs reduces the work load of CHs and conserves the energy consumption even in the case of an attack.