DYMO is advance version of AODV routing protocol develop to improve the network performance. Here, a mitigation algorithm to avoid and prevent genuine nodes from malicious attack can be developed.
A novel strategy to reduce single and collaborative black hole attacks, with decreased routing, storage and computational overhead can be described. The method will incorporate fake route request, destination sequence number and next hop information to alleviate the limitations of available schemes.
In this topic, a trusted AODV routing protocol in which trust value will be calculated by using tangent hyperbolic function can be introduced.
Bulwark-AODV which prevents single or cooperative Black hole attacks by identifying malicious route replies at source and intermediate nodes can be proposed and will also find a shortest valid path. It will also work in case of single adjacent node to the source and when there are multiple Black holes in the network.
A technique for detecting a cooperative black hole attack using crosschecking with True-Link concept can be designed by using modified-AODV routing protocol.
In this topic, a new method RTMAODV (Real Time Monitoring AODV) can be proposed. It will not introduce any overhead. This method will be effective for multiple sessions. The concept of broadcasting can be used in the method.
In this topic, to detect malicious nodes effectively, a Permutation based Acknowledgement for most widely used reactive protocol ad-hoc on demand distance vector routing AODV can be proposed.
In this topic, black hole attack can be detected and eliminated through implementing Digital Signature with Two-fish Algorithm. On-demand routing protocol Temporally Ordered Routing Algorithm (TORA) can be modified and named it as STORA.
Here, a solution can be proposed, which will enhance the security of the Ad-hoc On-demand Distance Vector (AODV) routing protocol to encounter the black hole attacks.
To avoid single black hole attack in MANET, a mechanism can be considered that will use Further Route Request packets. For detecting and avoiding cooperative black hole attack, a new technique can be proposed which will use Cooperative Cluster Agents. In this approach, DRI and SRT-RRT table as an input to Cooperative Security Agents can be passed.
In this topic, wormhole attack launched by exploiting AODV protocol in MANET, can be detected and eliminated in two phases. The preliminary phase in the process of identifying wormhole attack can be performed, based on timing analysis and hop count. After suspecting the attack, a Clustering based approach can be used to confirm the presence of attack, and also to identify the attacker nodes.
A Hybrid Approach For Preventing Black And Gray Hole Attacks In MANET

Here, a hybrid approach for preventing black/gray hole attacks can be presented by selecting second shortest route for secure route selection and hash function and time stamp base solution for consisting data transmission.
In this topic, a scheme can be proposed to detect the new identities of Sybil attackers without using centralized trusted third party or any extra hardware, such as directional antennae or a geographical positioning system.
Here, by using QABR (Q-Learning Based ABR) protocol, it can be shown that an honest node in the network along with the Local Server (LS) can detect the Sybil attacker, using the concept of a PKI secured unique key called the SESSION KEY (SESS_KEY).
Malicious and Irrelevant Packet Detection Algorithm (MIPDA) can be proposed which will be used to analyze and detect the Denial-of Service (DoS) attack.
Here, a strategy can be made to prevent the DOS and Man in the middle attacks on ALERT by using Hash function with SHA-1 algorithm.
In this topic, a method can be known as Merging Using MRDR (MUMRDR) will be used to merge two MANETs based on the Monitoring, Detection, and Rehabilitation (MRDR) method to mitigate such attacks. By using this method, it will be possible to detect DOS attacks when merging two MANETs.
Mitigation Of Dos Attacks By Using Multiple Encryptions In MANETs

A hybrid security approach can be proposed by using AES (Advance Encryption Standard) with Blowfish Algorithm for enhancing security.
Here, the design, implementation, and evaluation of Cap-Man, a capability-based security mechanism can be presented that will prevent denial-of-service (DOS) attacks against mobile ad-hoc networks (MANETs).
In this topic, a statistical approach to defense against RREQ flooding attacks in MANETs can be proposed. Then mechanism can be applied on AODV-based ad hoc networks.
A new Mobile Agent Based Intrusion Detection System (IDS) can be proposed. The approach will use a set of Mobile Agent (MA) that can move from one node to another node within a network. This as a whole will reduce network bandwidth consumption by moving the computation for data analysis to the location of the intrusion detection of Denial Of Service Attack Due To Selfish Node In MANET By Mobile Agent.
Improvement In AODV Performance In DOS And Black Hole Attack Environment

An algorithm can be proposed which will introduce a mechanism of DOS and Black hole attacks prevention and check network performance in malicious environment on the analysis of throughput and end to end delay.
In this topic, a new technique can be proposed to prevent the flooding attack targeting the DOS. This technique can be applicable to all the three phases, that are 'route discovery', 'route maintenance' and 'data transfer'.
THANK YOU...

Contact us at queries@thesisscientist.com