Network. normal flow of messages creating a virtual

network. While passive attacks aremainly due to lack of cooperation with the purpose of saving energy selfishly. Nodes that perform active attacks with the aim of damaging other nodes by causingnetwork outage are considered as malicious while nodes that make passiveattacks with the aim of saving battery life for their own communications are consideredto be selfish.

4. 1 WormholeAttacksWormhole attack is also called astunnelling attack. A tunnelling attack is where two or more nodes may collaborateto encapsulate and exchange messages between them along existing data routes.

This exploitation gives the opportunity to a node or nodes to short-circuit thenormal flow of messages creating a virtual vertex cut in the network that iscontrolled by the two colluding attackers. 4. 2 AttacksUsing ImpersonationAs there is no authentication ofdata packets in current ad hoc network, a malicious node can launch manyattacks in a network by masquerading as another node i. e. spoofing.

Due to amalicious node misrepresents its identity in the network (such as altering itsMAC or IP address in outgoing packets) and alter the target of the networktopology. 4. 3 Lack ofCooperationMobile Ad Hoc Networks (MANETs)rely on the cooperation of all the participating nodes. The more powerful aMANET gets as the more nodes cooperate to transfer traffic. But one of thedifferent kinds of misbehaviour a node may exhibit is selfishness. Aselfishness node uses the resources of other nodes while preserving ownresources. This can endanger the correct network operation by simply notparticipating to the operation or by not executing the packet forwarding.

Thisattack is also known as the black hole attack. 4. 4 Attacksthrough FabricationIn Fabrication an unauthorized partynot only gains the access but also inserts counterfeit objects into the system. In MANET, fabrication is used to refer the attacks performed by generatingfalse routing messages. Such kind of attacks can be difficult to verify as theycome as valid constructs, especially in the case of fabricated error messagesthat claim a neighbour cannot be contacted. Security Attacks on each layer inMANETTable1Layer AttacksApplication layer Repudiation, data corruptionTransport layer Session hijacking, SYN floodingNetwork layer Wormhole, black hole, Byzantine, flooding, resourceconsumption location disclosure attacksData link layer Traffic analysis, monitoring, disruption MAC (802. 11), WEP weaknessPhysical layer Jamming, interceptions, eavesdroppingTable – 2Security Issues for MANETLayer SecurityIssuesApplication layer Detecting and preventingviruses, worms, malicious codes and application abusesTransport layer Authentication and securingend to-end or point-to-point communicationthrough data encryptionNetwork layer Protecting the ad hoc forwarding protocolsData link layer Protecting the wireless MAC protocoland providing link layersecurity supportPhysical layer Preventing signal jamming denial-of-serviceattacks 5.

CountermeasuresSecure communication between twocommunicating devices is one of the primary concerns in MANET. It is necessary for basic

networkfunctions like routing and packet forwarding. If countermeasures are not embeddedinto basic network functions at the early stages of their design, the networkoperation can easily be jeopardized. To handle the malicious attacks, a number of mechanisms have been proposed. Following two mechanisms widelyused to protect the MANET from the attackers. Preventive mechanism: Theconventional approaches such as access control, authentication, encryption anddigital signature are used to provide first line of defence. Some security modules, such astokens or smart card that is accessible through PIN, passphrases or biometricsverification are also used in addition.

Reactive mechanism: Intrusion detection system (IDS)and cooperation enforcement mechanisms schemes etc are used in MANET to detectmisuse and anomalies. Cooperationenforcement such as Nuglets, Confidant, CORE and Token-based reduce selfish nodebehaviour. 5. 1 Countermeasures on Physical LayerAttacks