Attacks on Mobile Ad hoc networks: A Survey

Joshua Reginald Pullagura
Dept of ECE
VFSTR University Guntur, A.P, India

Perala.Srikanth
Dept of ECE
VFSTR University Guntur, A.P, India

D.Venkata Rao, PhD
Narasaraopet Institute of Technology,Narasaraopet, A.P,India

ABSTRACT
In recent years Wireless technology iswidely used with the advent of IEEE 802 standard. Lowrate Wireless personal area networks are widely usedbecause of low cost. A mobile ad-hoc network isinfrastructure less network which consist of mobile devices connected wirelesslyand usually move to other places from time totime, move around or join the network. Over the pastyears simulation work has been carried out to achievereliable routing protocol for IEEE 802 standard. The Wireless sensor and ad hoc networks are easily prone to security attacks, once deployed these networks are prone to be attacked and are unprotected. This paper mainly concentrates on various attacks that degrade the network performance. Attacks on the node degrade systemperformance, especially during the route discovery process by malicious entities which results in data loss and slower the network speed. In this paper various security threats will be discussed extensively.

Keywords
Ad hoc Networks, Attacks, Vampire, Black hole,Protocols.

1. INTRODUCTION
Wireless communication is one of the current emerging areas of research. It became so popular inthe last few years and became an integral part of the human life. Apart from the conventional wireless communications techniques like cellular phones, Wi-Fi and Blue tooth, there are emerging techniques for wireless communication coming into the picture which include Mobile ad hoc and Wireless sensor networks. Ad hoc networks consist of movable nodes, whichintercourse each other without wires and do not require any fixed infrastructural support. Embedded devices are known as sensors ormotes will transfer the data among themselves and cansense various physical and biological parameters form asensor network. The Wireless sensors are placedstrategically inside a physical medium so that they canmeasure various physical, biological and environmentalparameters from the surrounding selected area and givesthis information to the system. The network topologykeeps changing constantly because of the mobility of thenodes and hence they are prone to fail. These sensornodes or devices will have limited power, limitedmemory and low computational capabilities. The mainissues with Sensor nodes that should be considered arescalability feature, limited energy to supply the deviceand their connection strategy for communication definedby the physical layer.

2. RELATED WORK
The resourcesare very limited in Mobile ad hoc and sensor networks. They pose serious challenge forresearchers and developers. Routing protocols are developedfor sensor and ad hoc networks which considers parameters like bandwidth, memory andcomputational complexity. The development andmaintenance cost of these networks is high mainly due topower related issues. Energy efficiency is an importantissue here. Hence, most of the developers concentrate ondeveloping energy efficient networks. “Sleep deprivationattack” is the power enervation attack [1]. This attackprevents sensor nodes from getting into the sleep cycleand drains their batteries quickly. Current research workin this area concentrates on MAC layer which in turnwith LLC forms the Data link layer. Studies proved thatdenial of service attack on hardware or network is aserious one to note. These adverse nodes will preventroute setup, disrupt communication and creates routes by themselves so that they drop or manipulate. The securitybased route discovery approach in ad hoc sensornetworks cannot protect against vampire attacks. Thisis raised because vampire attacks does not return to wrong paths or to prevent communication. The vampireattack[2]creates confusion in some networks by increasing energy. Vampires will create packets and it covers a numberof nodes than actual nodes in the network, therefore more energy is drained even if the nodes use minimum energy to transmit packets [3]. Thus, in the presence of vampires it is relatively expensive to route the packets. One is when the new sequence number and destination sequence numbers are equal and secondly, when the existing sequence number is unknown. If the link to the next hop is broken, thenroute error packets (RERR packets) will send to neighbor nodes.Then RERR packets are forwarded by neighboring nodes to its unique list of activeneighbors, thus uses the disrupted list to invalidate routes[4]. The following table shows variousattacks on different layers.

Table 1. Attacks on each layer

Attacks	Layers affected
Overhead/Jamming	Physical layer
Monitoring disruption MAC (802.11), WEP Weakness	Data link Layer
Wormhole, Byzantine, Vampire,Black hole,locationdisclosure attacks.	Network Layer
Hijacking, Flooding	Transport layer
Datacorruption, Mismatch	Application layer

3. ATTACKS ON VARIOUS LAYERS
Almost six layers of the OSI Model are prone toattacks. The worst hit layers are Network and Data linklayers. Network layer deals with the Routing conceptwhich is the most essential phase in source to destination Packet delivery. If there is any attack on the routingprotocol, then they absorb network load and injectinto the route between the source anddestination nodes, and controls thenetwork traffic. They

will also drain the energy.The Byzantine,black hole,wormhole attacks are the few examples;those are described below.

Wormhole attack: In this Mischievous noderecords packets at one place andtunnels them to another location in the network.If the messages which controls the routing are tunneled, then it disrupts the routing.The tunnel between the attackers collided istermed as wormhole. Thisis a severe attack on Wireless Sensor routing protocols. If this attack is detected on an On-demand routing protocol such as AODV, AOMDV andDSR, then itprevents the discovery of new routes otherthan through the wormhole way.

Black hole attack: Here black node uses therouting protocol to find the shortestpath to its destination, but it drops the routingpackets and these are not forwarded toneighbors inthe network. A single black hole attack is usuallyoccurs in the mobile ad hoc networks.

4. ENERGY DRAINING ATTACKS

4.1 VAMPIRE ATTACKS

Malicious node causes Vampire attack on network.Heremessage sent by node drains more energy and thuscauses a slow depletion of node's power source.This type of attack degrades the performance ofNetwork. At the network layer the source node insertsentire path in the packet header. The intermediate nodeswill not make any decision about the route but follow theroute given by source node in packet header. Hencesource node has to make sure that routed path is thecorrect one and each node is neighbor of the previoushop. Entire route can be made sender authenticated bydigital signature.

Attack on Stateful Protocols

In this case the nodes are aware of the topology and will forward packets based on stored data. The stateful protocols are of two types 1) link-state protocols 2) Distance vector protocols. In link-state, every node maintainsdetails of up or down state links in the network andthese are updated in the nodes cache every timewhen there is a change of link in the network [3].Distance-vector protocols method tracks the next hop tillit gets destination. Vampire attacks are classified as 1.Carousel Attacks2. Stretch attacks.

Carousel Attacks

In this attack packets are sent into the route composed of loops so that same node appears repeatedly, this increases the routing length, butnumber of allowable entries in the source node can limit it. It increases overall energy consumption by a factor of 3.96 per message.

Stretch attacks

This attack creates artificially longer routes so that the packet has to travel a longer path than the optimal path. Thus more nodes are used for transferring packets which leads to more energy consumption and battery drainage and it is not a healthy scenario asthe path is artificially established.This attack cause less damage than Carousel attack. The total hops per packet depends on the number of nodes in the network, there is a chance of a combined attack so that packet can be kept in the network for longer routes. This results in more energy consumption as stretched cycle is always in the loop. Thus, routeloops will be detected and removed to protect the network

Tantamount attacks

Here the malicious node will unnecessarily generate duplicate packets, thereby flooding the entire network, which in turn decreases the network lifetime by draining the battery of the nodes.

5. CONCLUSION AND FUTURE SCOPE

In this paper, various attacks which affect the network performance are discussed. These attacks use the routing protocols to permanently deactivate the ad hoc and sensor networks and Mobile networks by draining the battery of nodes. These attacks are independent of the protocols or implementation, but these shows the susceptibility in different protocol classes.

The future work is to develop efficient and securerouting protocols which are not endangered to these attacks and also the protocols need to consume less power.

6. REFERENCES

[1] Haowen Chan and Adrian Perrig, Security and privacy in sensor networks, Computer 36 , IEEE 2003.

[2] Eugene Y.Vasserman and Nicholas Hopper "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks"- IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL.12,NO.2, FEBRUARY. 2013.

[3] Denial of service attacks(Timothy J. Mc Nevin, Jung-Min Park), IEEE 2004 University of Texas at San Antonio, San Antonio, TX 782490667.

[4] J. Deng, R. Han, and S. Mishra,"Defending against Path-Based DoS Attacks in Wireless Sensor Networks," Proc. ACM Workshop Security of Ad Hoc and Sensor Networks, IEEE 2005.

[5] Aashima, Gagandeep, Pawan Kumar,Analysisof Different Security Attacks in MANETs on Protocol Stack A – Review,International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 –8958, Volume-1,Issue-5, June2012

[6] Frank Stajano and Ross Anderson, The resurrecting duckling: security issues for ad-hoc wireless networks, International workshop on Security protocols, IEEE 1999.

[7] Rashid Hafeez Khokhar, Md Asri Ngadi & Satria Mandala,A Review of Current Routing Attacks inMobile Ad Hoc Networks,International Journal of Computer Science andSecurity, volume (2) issue (3).