Mobile ad hoc network security

A Research Paper Writing Proposal

Submitted by

Subedar singh chauhan (11408580)

Harpreet singh (11411958)

TO

School of Computer Applications

In partial fulfillment of the Requirement for the

Award of the Degree of

Master of Computer Applications

Under the guidance of

Mr. Guravtar Singh

April 2015

CERTIFICATE

This is to certify that Subedar Singh Chauhan(11408580),Harpreet Singh(11411958) have completed their MCA Research Paper Writing Proposal titled "Mobile ad hoc network security" under my guidance and supervision. To the best of my knowledge, the present work is the result of their original investigation and study. No part of the dissertation proposal has ever been submitted to any other degree or diploma.

The proposal is fit for the submission and the partial fulfilment of the conditions for the award of the degree of Master in Computer Applications.

Date: ----------

Signature of the Advisor

Name:

DECLARATION

We hereby declare that the research paper writing proposal entitled, "Mobile ad hoc network security", submitted for the MCA Degree is entirely our original work and all ideas and references have been duly acknowledged.

It does not contain any work for the award of any other degree or diploma**.**

Date: ----------

Investigator1 Name:

Registration Number:

Investigator2 Name:

Registration Number

Introduction:

A mobile ad hoc network is fastest growing research field in wireless system. Which consist of laptops, mobile telephone, personal gadgets and handheld digital devices these can revolutionary change in computer world. In the all over computing environment character users use at the same time some electronic platforms through which they can access all the required information whenever and everywhere they may be. In the mobile ad hoc network nodes can nonstop communicate with all the other nodes within their radio ranges whereas nodes that not in the direct communication range use middle node to communicate with each other.

Some mobile ad hoc are restricted to a local area of wireless devices such as a group of laptop computers while others may be connected to the Internet.

For example a vehicular ad hoc network is a type of MANET that allows vehicles to communicate with roadside tools. While the vehicles may not have a direct Internet connection the wireless roadside tools may be connected to the Internet allowing data from the vehicles to be sent over the Internet.

Wireless Ad hoc network are mainly characterized in following three types:

1) Wireless sensor network-

The wireless sensor network is built of nodes from a few to several hundreds or even thousands ,where each nodes is connected to one or sometimes a number of sensor this network is development was encouraged by military application such as battlefield examination. But today it is second-hand in number of industrialized and consumer application.

2) Mobile ad hoc network (MANET)-

Mobile ad hoc network is a type of ad hoc network that can change locations and configure itself. Because mobile ad hoc network are mobile, they use wireless connections to connect to

Different Networks. This can be a model Wi-Fi connection or another medium such as a cellular or satellite broadcast.

Wireless Mesh network-

Wireless mesh networks extend the connectivity area of mobile devices within the limited range of a single access point. Mesh networks can be easily setup inside a shop, university and in a large environmental area or at a adversity site without requiring every access point to be physically associated to the Internet. it is design in which each node on the network connects to one or more nodes.

Attacks at network layer

The fundamental idea behind network layer attacks is to add itself in the active path from source to destination node.

1) Wormhole Attack:

In wormhole attack, malicious node receive data packet at one point in the network and tunnels them to another **Malicious Node. Malicious nodes are known to as a Wormhole** when tunnel exist between two nodes.

For example, the nodes “x” and “y” are malicious node that forms the tunnel in network. The source node “s” when starts the route request message to find the route to node “d” destination nodes. In the immediate neighbour node of source node “s”, namely “a” and “c” forwards the route request message to their respective neighbours h and x. The node x when receive the route request it immediately share with it “y” and later it initiate route request to its neighbour node b, through which the Route request is delivered to the **Destination nodes d. due to high speed Connection, it forces** the source node to select route <s-a-b-d> for destination. It results in “d” ignore route request that reach your destination at later on on time.

(s < c < h < e < f < d.)

2) Rushing Attack:

In rushing attacks when malicious node receives a route request packet from the source node, it floods the packet quickly all over the network earlier than other nodes, which also receive the same route request packet For example, the node "4" represents the **Rushing Attack node, Where S and d' refers to source and destination** nodes.

The compromise node of Rushing Attack "4" quickly broadcasts the route request messages to ensure that the RREQ message from itself arrive earlier than those from other nodes.

This result in when neighbouring node of "d" i.e. "7" and "8" when receive the actual route request from source, they simply discard requests. So such attacks "s" fail to find out any useable safe route without the participation of attacker.

3) Grey whole attack:

In this type of attacks, malicious node claims having an optimum route to the node whose packets it wants **To Intercept. It is related to black hole Attack but it** drop data packet of a particular node.

Work done over the Black hole Problems

Problems in Black hole

Black hole problem in MANETS is a serious security problem to be solved.

In this malicious node uses the routing protocol to promote itself as having the short path to reach the destination node whose packets it wants to intercept.

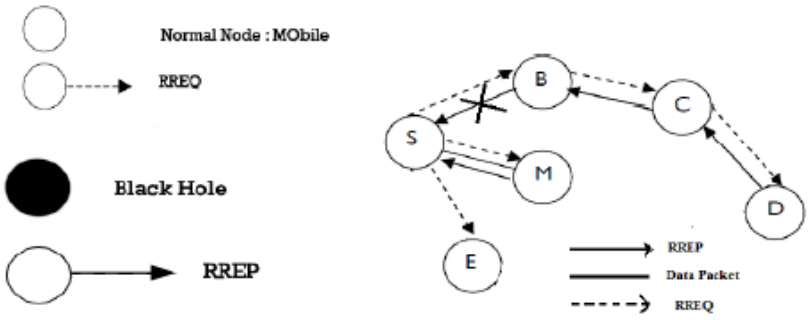
If the malicious replies reach the requesting node before the reply from the actual node, a malicious route has been created.

Malicious node then can choose whether to crash the packets to perform a denial-of-service attack or to access the data. For example, when node "S" wants to send data to destination node 'd' it starts the route discovery process.

The malicious node "M" when receives the route request it without delay sends response to source. If reply from node M reaches first to the source than the source node "S" ignore all other reply messages and start to send packet route node "M".

As a result, all data packets are consumed lost at malicious node.

Diagram of Black hole problem in MANETS

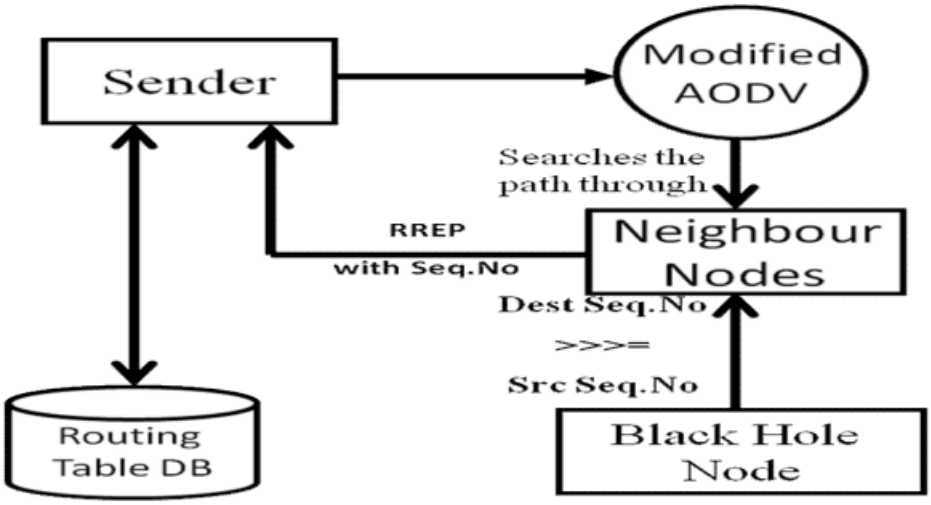


RREQ - Route Request packet

RREP – Route Response packet

Black Hole Attack Implementation

In this Black Hole node sends the Destination Sequence Number much greater than the Source Sequence number to the source node which initiates the route discovery. The sender then sorts the Routing table entries according to the sequence number and starts sending the packets towards the Black Hole node. The Black hole node then start drops or alters packets which come from the Source or neighbour nodes. The Fixed path or single path has been chosen by the source to send the packets towards the Black hole node using modified AODV.



Proposed Solutions for Black Hole

First Solution:-

In this solution the dispatcher node needs to verify the legitimacy of the node that initiate the RREP packet by utilize the network redundancy.

Since any packet can be inside to the goal through many redundant paths the idea of this solution is t wait for the RREP packet to arrive from more than two nodes.

During this time the sender nodes will buffer its Packet until a safe route are identified.

0nce a safe route has identified, these buffer packets will be transmitted. When a RREP arrive to the s0urce it will extract the full path to the destination and pass the time for another RREP.

Second Solution:-

Every packet in MANETs has a only one of its kind sequence number.

This number is a growing value.

The next packet must have upper value that the recent packet series number. Node

in normal routing protocols keep the last packet sequence number that it has received and uses it to check if the received packet was received previous two from the same originate source or not.

The node in this state needs to have two extra tables the first table consists of the sequence numbers of the final packet sent to the every node in the network, and the second table for the sequence number received from every dispatcher.

Through the RREP phase the in-between or the target node must contain the sequence number of last packet received from the source that initiates RREQ.

Once the source receive this RREP it will drag out the last succession figure and then compare it with the value save in its table.

If it match the spread will get place.

If not this replied node is a hateful node, so an alarm message will be transmitting to warn the network about this node.

Literature Review

In this paper[1] the authors Hongmei Deng, Wei Li, and Dharma P. Agrawal, discus routing security issues of MANETs, and analyze in specify one type of attack — the "black hole "quandary that can easily be operational against the MANETs.

In this paper[2] find the two possible solution. The first is to unearth more than one route to the destination. The second is to exploit the carton sequence number included in any packet header**"**Mohammad Al-Shurman and Seong-Moo Yo Electrical and Computer Engineering Department"

In this paper [3]In this paper Vishnu K B.tech V sem MNNIT Allahabad INDIA and Amos J Paul B.tech V sem MNNIT, Allahabad INDIA present a instrument to detect and remove the above two types of malevolent nodes. Our proposed technique works as follows. Initially a vertebral column network of trusted nodes is established over the ad hoc network

In this paper [4] authors ram ramanathan and Jason redi, converse ad hoc networks planned for the military scalability is one of the most important open problems. Scalability is ad hoc networks can be normally defined as whether the network is able to provide a fitting
Level of service in the direction of packet even. in the company the large number of nodes in the network. In the wired networks this ability is intimately connected as to how quickly network protocol control overhead increases as a function of an increase in the number of nodes and connection changes.

In this paper [5] authors Franck Legendre, Theus Hossmann, Felix Sutton, Bernhard Plattner In this paper we start by review communication solutions Stemming from 30 years of research on ad hoc mesh and wait open-minded Networks able to maintain communications during disasters when the communication transportation is damaged weighed down or not existing in the first place. here how these solutions can be apply and review the advantages and disadvantages of every exclusive approach. In a second part we present Twilight a Twitter application relying on delay-tolerant opportunistic communications to increase tweets and sensor data in an outbreak fashion.

Objectives

The major objectives of our topic of research are as follows

- Find the solution algorithm of black hole problem.
- Find the Complete protocol for detection & removal of networking Black Holes.

References

- Black hole attack prevention using Random dispersive routing for mobile Ad hoc network**S**kamatchiv@gmail.com1, rajimukesh95@yahoo.co.in2, rajamce@yahoo.com3

- Detection and Removal of Cooperative Black/Gray hole Attack in Mobile ADHOC Networks Vishnu K B.tech V SEM Amos J Paul B.tech V SEM

- Black Hole Attack in Mobile Ad Hoc Networks Mohammad Al-Shurman and Seong-Moo Yoo Electrical and Computer Engineering Department The University of Alabama in Huntsville Huntsville, Alabama 35899 E-mail: {al-shum,yoos}@eng.uah.edu

- Imrich Chlamtaca, Marco Conti b,*, Jennifer J.-N. Liu c a School of Engineering, University of Texas at Dallas, Dallas, TX, USA b Istituto IIT, Consiglio Nazionale delle Ricerche, Pisa, Italy c Department of Computer Science, University of Texas at Dallas, Dallas, TX, USA "Mobile ad hoc networking: imperatives and challenges"

- Sarvesh Tanwar, Prema K.V. International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013

"Threats & Security Issues in Ad hoc network: A Survey Report"

- David A. Maltz May 2001 CMU-CS-01-130 "On-Demand Routing in Multi-hop Wireless Mobile Ad Hoc Networks"

- Franck Legendre, Theus Hossmann, Felix Sutton, Bernhard Plattner Communication Systems Group ETH Zurich, Switzerland lastname@tik.ee.ethz.ch and fsutton@student.ethz.ch "30 Years of Wireless Ad Hoc Networking Research: What about Humanitarian and Disaster Relief Solutions? What are we still missing"