www.ioirp.com

International Journal of Innovative Research in Technology, Science & Engineering (IJIRTSE)
ISSN: 2395-5619, Volume – 2, Issue – 5. May 2016

DEDACTION AND PREVENTIONOF GRAYHOLE ATTACKS USING PACKET BASED CBDS

R.RAGAPRIYA
PG Scholar, Department of Electronics and
Communication Engineering,
Priyadarshini Engineering College,
Vaniyambadi – 6005,Vellore, INDIA

ABSTRACT
In MANET the primary requirement is co-operative communication among nodes. The malicious nodes may cause security problems like gray hole and collaborative attacks. To resolve these attack issue designing Dynamic source routing mechanism, which is referred as cooperative bait detection scheme (CBDS) that integrate the advantage of both proactive and reactive defense architecture.In black hole attacks, a node transmits a malicious broadcast informing that it has the shortest path to the destination, with the goal of intercepting messages.In this case, a malicious node (so-called black hole node) can attract all packets by using forged Route Reply (RREP) packet to falsely claim that "fake" shortest route to the destination and then discard these packets without forwarding them to the destination. In gray hole attacks, the malicious node is not initially recognized as such since it turns malicious only at a later time, preventing a trust-based security solution from detecting its presence in the network. It then selectively discards/forwards the data packets when packets go through it. In this we focus is on detecting gray hole/collaborative black hole attacks using a dynamic source routing (DSR)-based routing technique.

Index Terms:
Cooperative Bait Detection Scheme(CBDS), collaborative bait detection,collaborative blackhole attacks,detection mechanism,dynamic source routing(DSR),mobile ad hoc network(MANET).

INTRODUCTION

NEED OF COMMUNICATION

Communication is the process by which two or more people exchange ideas, facts, feelings, or impressions in ways that each gains a common understanding of the meaning, intent, and use of messages.

The term "communication" stems from the Latin word "communism" - meaning common. Thus, communication is a conscious attempt to share information, ideas, attitudes, and the like with others.

In short, it is the act of getting a sender of the message and a receiver of the message tuned together for a particular message, or a series of messages. For two or more people to engage in a common, co-operative effort, they must be able to communicate with each other. Thus, good communication consists of creating understanding of the message. In computerized technology, we need to transfer the data from one another without any problem like security and quality. To improve the communication in mobile adhoc network we need to test our proposed method is working well or not by using system modeling. System modeling refers to an act of representing an actual system in a simply way.System modeling is extremely important in system design and development, since it gives an idea of how the system would perform if actually implemented.

What does security mean?
Ability for [two] nodes to effectively communicate even in the presence of active adversaries in the network

- Ability to find routes
- Availability of service
- If an "honest" path exists

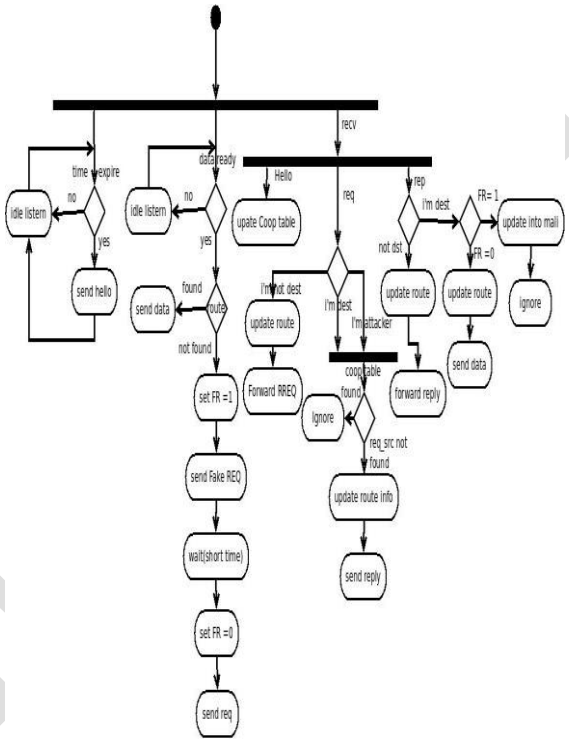
Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. The networks are computer networks, both public and private, that are used every day to conduct transactions and communications among

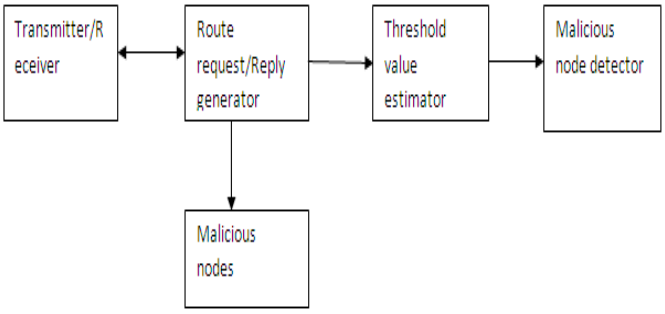
businesses, government agencies and individuals. The networks are comprised of "nodes", which are "client" terminals (individual user PCs), and one or more "servers" and/or "host" computers. They are linked by communication systems, some of which might be private, such as within a company and others which might be open to public access. The obvious example of a network system that is open to public access is the Internet, but many private networks also utilize publicly-accessible communications. Today, most companies' host computers can be accessed by their employees whether in their offices over a private communications network, or from their homes or hotel rooms while on the road through normal telephone lines.

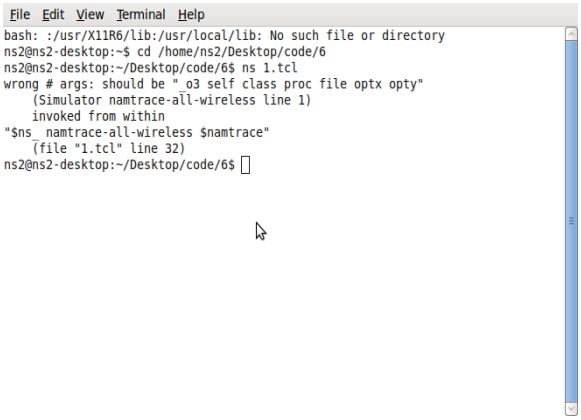
Mobile Ad-hoc Networks:

An ad-hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any stand-alone infrastructure or centralized administration. Mobile Ad-hoc networks are self-organizing and self re-configuring multihop wireless networks where, the structure of the network changes dynamically. This is mainly due to the mobility of the nodes. Nodes in these networks utilize the same random access wireless channel, cooperating in a friendly manner to engaging themselves in multihop forwarding. The nodes in the network not only act as hosts but also as routers that route data to/from other nodes in network.

BLOCK DIAGRAM







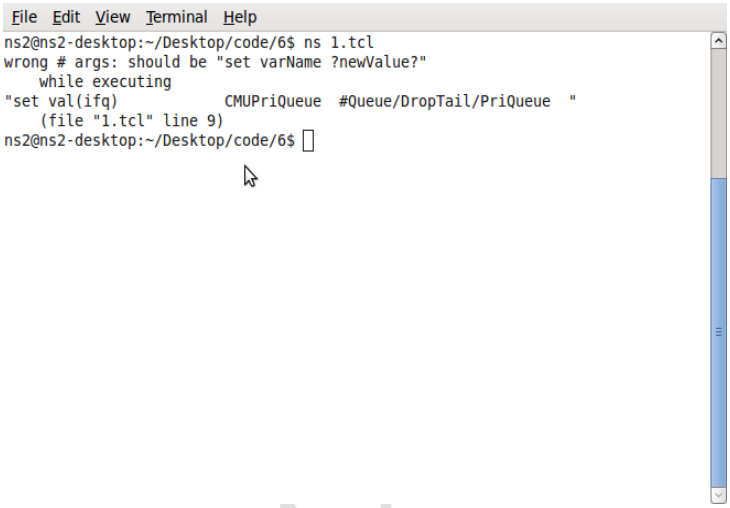
In AODV, the network is silent until a connection is needed. At that point the network node that needs a connection broadcasts a request for connection. Other AODV nodes forward this message, and record the node that they heard it from, creating an explosion of temporary routes back to the needy node. When a node receives such a message and already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node. The needy node then begins using the route that has the least number of hops through other nodes. Unused entries in the routing tables are recycled after a time.When a link fails, a routing error is passed back to a transmitting node, and the process repeats.Much of the complexity of the protocol is to lower the number of messages to conserve the capacity of the network. For example, each request for a route has a sequence number. Nodes use this sequence number so that they do not repeat route requests that they have already passed on. Another such feature is that the route requests have a "time to live" number that limits how many times they can be retransmitted. Another such feature is that if a route request fails, another route request may not be sent until twice as much time has passed as the timeout of the previous route request.The advantage of AODV is that it creates no extra traffic for communication along existing links. Also, distance vector routing is simple, and doesn't require much memory or calculation. However AODV requires more time to establish a connection, and the initial communication to establish a route is heavier than some other approaches.

Technical description

The AODV Routing protocol uses an on-demand approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packets. It employs destination sequence numbers to identify the most recent path. The major difference between AODV and Dynamic Source Routing (DSR) stems out from the fact that DSR uses source routing in which a data packet carries the complete path to be traversed. However, in AODV, the source node and the intermediate nodes store the next-hop information corresponding to each flow for data packet transmission. In an on-demand routing protocol, the source node floods the RouteRequest packet in the network when a route is not available for the desired destination. It may obtain multiple routes to different destinations from a single RouteRequest. The major difference between AODV and other on-demand routing protocols is that it uses a destination sequence number (DestSeqNum) to determine an up-to-date path to the destination. A node updates its path information only if the DestSeqNum of the current packet received is greater than the last DestSeqNum stored at the node.

A RouteRequest carries the source identifier (SrcID), the destination identifier (DestID), the source sequence number (SrcSeqNum), the destination sequence number (DestSeqNum), the broadcast identifier (BcastID), and the time to live (TTL) field. DestSeqNum indicates the freshness of the route that is accepted by the source. When an intermediate node receives a RouteRequest, it either forwards it or prepares a RouteReply if it has a valid route to the destination. The validity of a route at the intermediate node is determined by comparing the sequence number at the intermediate node with the destination sequence number in the RouteRequest packet. If a RouteRequest is received multiple times, which is indicated by the BcastID-SrcID pair, the duplicate copies are discarded. All intermediate nodes having valid routes to the destination, or the destination node itself, are allowed to send RouteReply packets to the source. Every intermediate node, while forwarding a RouteRequest, enters the previous node address and it's BcastID. A timer is used to delete this entry in case a RouteReply is not received before the timer expires. This helps in storing an active path at the intermediate node as AODV does not employ source routing of data packets. When a node receives a RouteReply packet, information about the previous node from which the packet was received is also stored in order to forward the data packet to this next node as the next hop toward the destination.

DSR includes source routes in packet headers. Resulting large headers can sometimes degrade performance-particularly when data contents of a packet are small, AODV attempts to improve on DSR by maintaining routing tables at the nodes, so that data packets do not have to contain routes. AODV retains the desirable feature of DSR that routes are maintained only between nodes which need to communicate. Route Requests (RREQ) are forwarded in a manner similar to DSR. When a node re-broadcasts a Route Request, it sets up a reverse path pointing towards the source-AODV assumes symmetric (bi-directional) links. When the intended destination receives a Route Request, it replies by sending a Route Reply (RREP).Route Reply travels along the reverse path set-up when Route Request is forwarded.Route Request (RREQ) includes the last known sequence number for the destination. An intermediate node may also send a Route Reply (RREP) provided that it knows a more recent path than the one previously known to sender. Intermediate nodes that forward the RREP, also record the next hop to destination. A routing table entry maintaining a reverse path is purged after a timeout interval. A routing table entry maintaining a forward path is purged if not used for an active_route_timeout interval.



RESULT AND DISCUSSION

BLACK BOX TESTING

Black box testing also called behavioral testing focuses on the functional requirements of the software. That is black box testing enables the software engineer to derive sets of input conditions that will fully exercise all functional requirements for a program. Black box testing attempts to find errors in the following categories. Incorrect or missing functions or interface errors or Errors in data structures or external data base access Behavior or performance errors. Initialization and termination errors

Black box Testing.

Mobile Ad hoc Networks

An ad hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any stand-alone infrastructure or centralized administration. Mobile Ad-hoc networks are self-organizing and self-configuring multihop wireless networks where, the structure of the network changes dynamically. This is mainly due to the mobility of the nodes. Nodes in these networks utilize the same random access wireless channel, cooperating in a friendly manner to engaging themselves in multihop forwarding. The nodes in the network not only act as hosts but also as routers that route data to/from other nodes in network.

In this networking multi-hopping communication can be occurred. In mobile ad-hoc networks where there is no infrastructure support as is the case with wireless networks, and since a destination node might be out of range of a source node transmitting packets. A routing procedure is always needed to find a path so as to forward the packets appropriately between the source and the destination. Within a cell, a base station can reach all mobile nodes without routing via broadcast in common wireless networks. In the case of ad-hoc networks, each node must be able to forward data for other nodes. This creates additional problems along with the problems of dynamic topology which is unpredictable connectivity changes.

WHITE BOX TESTING

White box testing sometimes called glass box testing is a test case design method that uses the control structure of the procedural design to derive test cases. Using white box testing methods, the software engineer can derive test cases that guarantee that all independent paths within a module have been exercised at least once. Exercise all logical decisions on their true and false sides. Execute all loops at their boundaries and within their operational bounds. Exercise internal data structures to ensure their validity

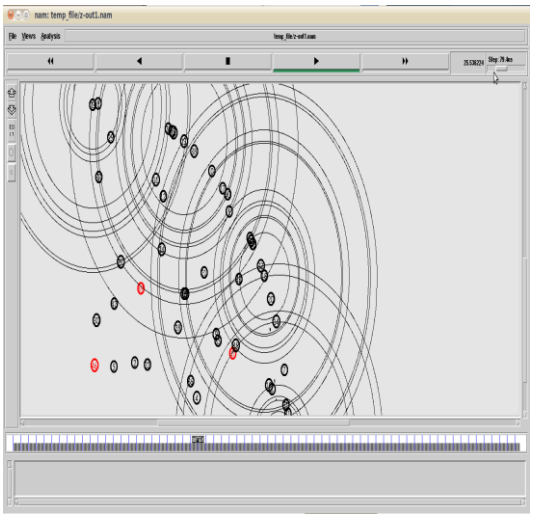
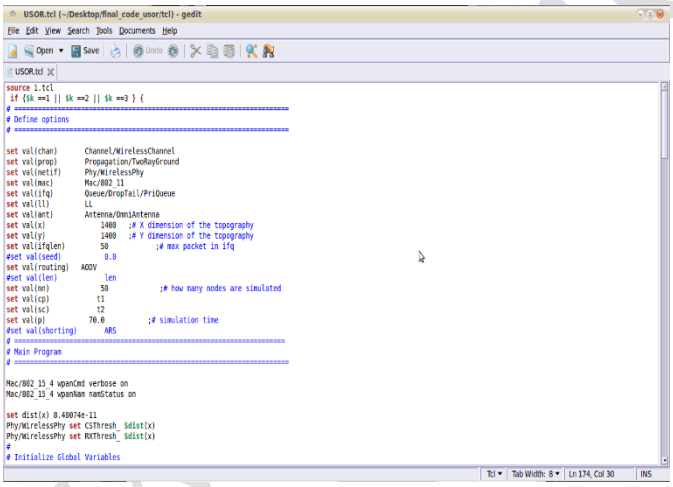


Figure6.2 White Box Testing

UNIT TESTING

The most 'micro' scale of testing to test particular functions or code modules. Typically, it is done by the programmer and not by tester, as it requires detailed knowledge of the internal program design and code. Not always easily done unless the application has a well designed architecture with tight code; may require developing test modules or test harnesses.



REFERENCE

[1] S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, "Mobile ad hoc networking", Wiley, 2004.

[2] D. Djenouri, L. Khelladi, and N. Badache, "A survey of security issues in mobile ad hoc networks", IEEE communications surveys, Vol. 7, No. 4, pp. 2-28, 2005.

[3] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks", Journal of Wireless communications, IEEE,Vol. 14, No. 5, pp. 85-91, 2007.

[4] N. Badache, D. Djenouri, and A. Derhab, "Mobility impact on mobile ad hoc routing protocols", ACS/IEEE International Conference on AICCSA, Vol. 3, 2003.

[5] D. Cerri, and A. Ghioni, "Securing AODV: the A-SAODV secure routing prototype", Communications Magazine, IEEE, Vol. 46, No. 2, pp. 120-125, 2008.

[6] The Network Simulator ns-2, http://www.isi.edu/nsnam/ns/.