ISSN No. 0976-5697

Volume 3, No. 4, July- August 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Implementation of Protected Routing to Defend Byzantine Attacks for MANET's

Sathisha M S*
Asst. Professor, Dept. of CSE,
Canara Engineering College
Mangalore, Karnataka, India
sathishams1983@gmail.com

Suresha D
Asst. Professor, Dept. of CSE,
Canara Engineering College,
Mangalore, Karnataka, India
sureshasss@gmail.com

Alok Ranjan
Asst. Professor, Dept. of CSE
Canara Engineering College
Mangalore, Karnataka, India
mibalok07@gmail.com

Prasanna Kumara
Asst. Professor, Dept. of MCA
Cambridge Institute of Technology
Bangalore, Karnataka, India
prasanna.s_kumara@yahoo.com

Abstract: Mobile ad-hoc networks are being extensively deployed currently since they provide some features which are difficult or impossible to be emulated by conventional networks. The applications ranges from the defense sector (sensor nodes in hostile territory) to general transportation (gadgets used to communicate traffic congestion while traveling) for providing useful infrastructure during disaster recovery. Due to the significance attached to the applications of MANET, security in ad-hoc networks is an important aspect. This paper is focused on byzantine attacks in MANET's. Byzantine attacks can be defined as attacks against routing protocols, in which two or more routers collude to drop, fabricate, modify, or misroute packets in an attempt to disrupt the routing services. In this paper a Protected Routing (PR) algorithm is designed and implemented to overcome the problem of Byzantine attacks in mobile ad-hoc network.

Key words: AODV- Ad- hoc On Demand Distance Vector, DOS-denial of service, MANET-Mobile ad-hoc network, PR-Protected Routing

I. INTRODUCTION

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. MANETs are self-organizing and self-configuring multi hop 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 multi hop 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 MANETs where there is no infrastructure support as is the case with wireless networks[1], 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.

MANETs are becoming ever more popular due to their flexibility, low cost, and ease of deployment. However, to achieve these benefits the network must employ a sophisticated routing protocol[2].

There is an increasing need to develop and deploy highly secure mobile ad- hoc networks, particularly for military tactical and other security-sensitive operations in adversarial environments. Since a MANET does not rely on a fixed infrastructure, and network elements are wireless mobile nodes, they can rapidly be deployed with relatively low cost.

The main challenges in assuring MANET networks are due to the fact that a mobile link is susceptible to attacks, and node mobility renders the networks to having a highly dynamic topology. The attacks against routing protocols can be categorized into external and internal attacks. An external attack originates from a router that does not participate in the routing process but masquerades as a trusted router. They can either advertise false routing information or generate floods of spurious service requests, such as a DOS attack. An internal attack originates from a compromised, misconfigured, faulty, or even malicious router inside a network domain.

A. *Problem Statement:*

Among the internal attacks, Byzantine attacks can be defined as attacks against routing protocols, in which two or more routers collude to drop, fabricate, modify, or misroute packets in an attempt to disrupt the routing services. Here developed algorithm detects internal attacks by using both message and route redundancy during route discovery.

B. *Protected Routing:*

The route-discovery messages are protected by secret key between a source and destination and some intermediate nodes along a route established by using cryptographic mechanisms. This algorithm can be integrated into ad-hoc on-demand distance vector routing. Such an integrated protocol called Protected Routing, in which a node makes a routing decision based on its trust of its neighboring nodes and the performance provided by them.

II. RELATED WORK

A MANET is a self-configuring network of mobile routers (and associated hosts) connected by wireless links[3]

—the union of which form an arbitrary topology. The routers are free to move randomly and organize themselves arbitrarily. Thus, the network's wireless topology may change rapidly and unpredictably. MANET's are usually set up in situations of emergency for temporary operations or simply if there are no resources to set up elaborate networks.

These types of networks operate in the absence of any fixed infrastructure, which makes them easy to deploy, at the same time however, due to the absence of any fixed infrastructure, it becomes difficult to make use of the existing routing techniques for network services and this poses a number of challenges in ensuring the security of the communication, something that is not easily done as many of the demands of network security conflict with the demands of mobile networks, mainly due to the nature of the mobile devices (e.g. low power consumption, low processing load).

Ad-hoc networks are a new paradigm of wireless communication for mobile hosts. There is no fixed infrastructure such as base stations for mobile switching. Nodes within each other's radio range communicate directly via wireless links while those which are far apart rely on other nodes to relay messages. Node mobility causes frequent changes in topology. The wireless nature of communication and lack of any security infrastructure raises several security problems. The following flowchart depicts the working of any general ad-hoc network.

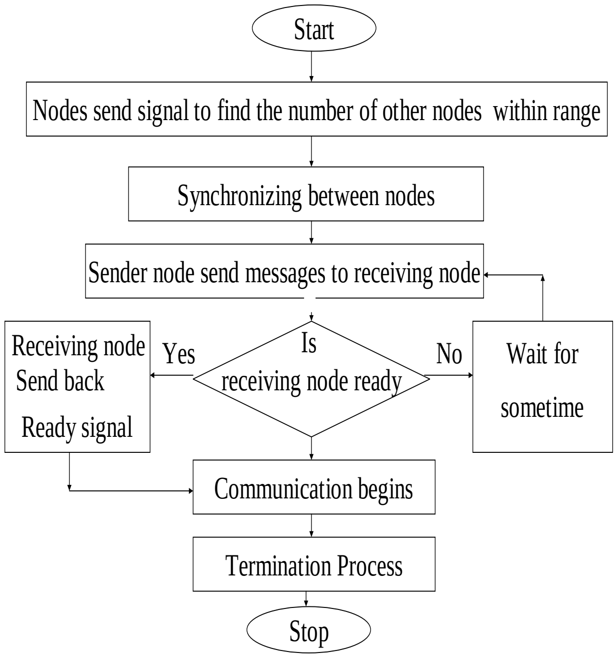
Start
Nodes send signal to find the number of other nodes within range
Synchronizing between nodes
Sender node send messages to receiving node
Receiving node Send back Ready signal
Yes
Is receiving node ready
No
Wait for sometime
Communication begins
Termination Process
Stop

Figure 1: Working of a Ad-Hoc Network

There are two different types of wireless networks:

a. The easiest network topology is where each node is able to reach all the other nodes with a traditional radio relay system with a big range. There is no use of routing protocols with this kind of network because all nodes "can see" the others.
b. The second kind uses also the radio relay system but each node has a smaller range, therefore one node has to use neighboring nodes to reach another node that is not within its transmission range. Then, the intermediate nodes are the routers.

This paper concentrates on the security aspect of the ad-hoc network. Main focus is regarding the security of the currently implemented routing algorithms. The focus is mainly on the security of the routing protocols used in the ad-hoc network.

Any routing protocol must encapsulate an essential set of security mechanisms. These are mechanisms that help prevent, detect, and respond to security attacks. Broadly there are two major categories of attacks when considering any network attacks [4] from external sources and attacks from within the network.

MANETs are being extensively deployed currently since they provide some features which are difficult or impossible to be emulated by conventional networks. The applications range from the defense sector (sensor nodes in hostile territory) to general transportation (gadgets used to communicate traffic congestion while traveling) to providing useful infrastructure during disaster recovery. Due to the significance attached to the applications of MANET, security in ad-hoc networks is crucial.

Use of wireless links renders an ad-hoc network susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion. Nodes roaming freely in a hostile environment with relatively poor physical protection have non-negligible probability of being compromised. Hence, it is required to consider malicious attacks not only from outside but also from within the network from compromised nodes.

Here presented security framework is integrated into the routing protocols in the design phase itself as a viable solution to satiate the security needs of the ad-hoc networks.

The contemporary routing protocols for ad-hoc networks cope well with dynamically changing topology but are not designed to accommodate defense against malicious attackers. Today's routing algorithms are not able to thwart common security threats. Most of the existing ad-hoc routing protocols do not accommodate any security and are highly vulnerable to attacks. A wireless ad-hoc network is a decentralized type of wireless network. The network is ad-hoc because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. In addition to the classic routing, ad-hoc networks can use flooding for forwarding the data.

A. MANET's:

A MANET is a self-configuring infrastructure less network of mobile devices connected by wireless links. Ad-hoc is Latin and means "for this purpose".

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.

MANET's are a kind of wireless ad-hoc networks that usually has a routable networking environment on top of a Link Layer ad-hoc network.

The growth of laptops and 802.11/Wi-Fi wireless networking has made MANET's a popular research topic since the mid 1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measure such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc.

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. MANETs are self-organizing and self-configuring multi hop 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 multi hop 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 MANETs 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.

B. *Types of MANET:*

a. ***Vehicular Ad-Hoc Networks (VANET's):*** are used for communication among vehicles and between vehicles and roadside equipment.

b. ***Intelligent vehicular ad-hoc networks (InVANET's):*** are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents, drunken driving etc.

c. ***Internet Based Mobile Ad-hoc Networks (iMANET):*** are ad-hoc networks that link mobile nodes and fixed Internet-gateway nodes. In such type of networks normal ad-hoc routing algorithms don't apply directly.

C. *List of ad-hoc Routing Protocols:*

An ad-hoc routing protocol is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a MANET.

In ad-hoc networks, nodes do not start out familiar with the topology of their networks; instead, they have to discover it. The basic idea is that a new node may announce its presence and should listen for announcements broadcast by its neighbors. Each node learns about nodes nearby and how to reach them, and may announce that it, too, can reach them.

The following is a list of some ad-hoc network routing protocols:

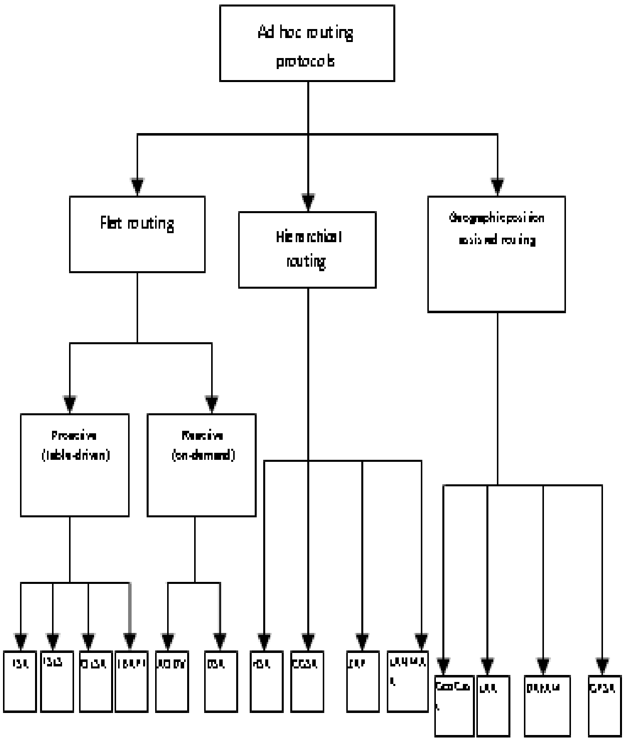

Figure 2: Ad-hoc network routing protocols

D. *Pro-active (table-driven) routing:*

This type of protocols maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. The main disadvantages of such algorithms are:

a. Respective amount of data for maintenance.

b. Slow reaction on restructuring and failures.

These protocols are also called as proactive protocols since they maintain the routing information even before it is needed[5]**.** Each and every node in the network maintains routing information to every other node in the network. Routes information is generally kept in the routing tables and is periodically updated as the network topology changes.

Many of these routing protocols come from the link-state routing. There exist some differences between the protocols that come under this category depending on the routing information being updated in each routing table. Furthermore, these routing protocols maintain different number of tables.

The proactive protocols are not suitable for larger networks, as they need to maintain node entries for each and every node in the routing table of every node. This causes more overhead in the routing table leading to consumption of more bandwidth.

E. *Reactive (on-demand) routing:*

This type of protocols finds a route on demand by flooding the network with Route Request packets [6]. The main disadvantages of such algorithms are:

a. High latency time in route finding.

b. Excessive flooding can lead to network clogging.

These protocols are also called reactive protocols since they don't maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. The route discovery usually occurs by flooding the route request packets throughout the network.

F. Ad-hoc On-Demand Distance Vector Protocol:

Ad-hoc On-Demand Distance Vector (AODV) Routing is a routing protocol for MANETs (MANET's) and other wireless ad-hoc networks.

It is a reactive routing protocol, meaning that it establishes a route to a destination only on demand. In contrast, the most common routing protocols of the Internet are proactive, meaning they find routing paths independently of the usage of the paths.

AODV is, as the name indicates, a distance-vector routing protocol. AODV avoids the counting-to-infinity problem of other distance-vector protocols by using sequence numbers on route updates, a technique pioneered by DSDV. AODV is capable of both unicast and multicast routing.

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 AODV Routing protocol[7] 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[8], 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.

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

G. Challenges in Ad-hoc On-Demand Distance Vector (AODV) Protocol:

a. AODV defines no special security mechanisms for data protection.
b. Impersonation attack can easily be done**.**

H. Cryptography:

The art of protecting information by transforming it (*encrypting* it) into an unreadable format, called cipher text. Only those who possess a secret *key* can decipher (or *decrypt*) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called *codebreaking*, although modern cryptography techniques are virtually unbreakable.

I. Rijndael Algorithm:

Rijndael (pronounced rain-dahl) algorithm[9] is a new generation symmetric block cipher that supports key sizes of 128, 192 and 256 bits, with data handled in 128-bit blocks - however, in excess of AES design criteria; the block sizes can mirror those of the keys. Rijndael uses a variable number of rounds, depending on key/block sizes, as follows:

9 rounds if the key/block size is 128 bits
11 rounds if the key/block size is 192 bits
13 rounds if the key/block size is 256 bits

Rijndael is a substitution linear transformation cipher, not requiring a Feistel network. It uses triple discreet invertible uniform transformations (layers). Specifically, these are: Linear Mix Transform; Non-linear Transform and Key Addition Transform. Even before the first round, a simple key addition layer is performed, which adds to security.

Thereafter, there are N_r-1 rounds and then the final round. The transformations form a State when started but before completion of the entire process.

III. ANALYSIS

A significant number of research efforts have been devoted to investigate MANETs over the past few years. Interest in MANET's is due to their promising ubiquitous connectivity beyond that is currently being provided by the Internet.

Firstly, MANET's are easily deployed allowing a plug-and-communicate method of networking. Secondly, MANET's need no infrastructure. Eliminating the need for an infrastructure reduces the cost for establishing the network. Moreover, such networks can be useful in disaster recovery where there is not enough time or resources to install and configure an infrastructure. Thirdly, MANET's also do not need central management. Hence, they are used in military operations where units are moving around the battle field and a central unit cannot be used for synchronization.

Nodes forming and Ad–hoc network are required to have the ability to double up as a client, a server, and a router simultaneously. Moreover, these nodes should also have the ability to connect to and automatically configure to start transmitting data over the network. It is impractical to expect a MANET to be fully connected, where a node can directly communicate with every other node in the network. Typically, nodes are obliged to use a multi hop path for transmission, and a packet may pass through multiple nodes before being delivered to its intended destination.

A number of MANET routing protocols were proposed in the last decade. These protocols can be classified according to the "routing strategy" that they follow to find a path "route" to the destination.

Routing in a MANET is challenging because of the dynamic topology and the lack of an existing fixed infrastructure. In such a scenario a mobile host can act as both a host and a router forwarding packets for other mobile nodes in the network. Routing protocols used in MANETs (MANET) must adapt to frequent or continual changes of topology, while simultaneously limiting the impact of tracking these changes on wireless resources.

There is an increasing need to develop and deploy highly secure mobile ad- hoc networks (MANET's), particularly for military tactical and other security-sensitive operations in adversarial environments. Since a MANET does not rely on a fixed infrastructure, and network elements are wireless mobile nodes, they can rapidly be deployed with relatively low cost.

The main challenges in assuring MANET networks are due to the fact that a mobile link is susceptible to attacks, and node mobility renders the networks to having a highly dynamic topology. The attacks against routing protocols can be categorized into external and internal attacks. An external attack originates from a router that does not participate in the routing process but masquerades as a trusted router. They can either advertise false routing information or generate floods of spurious service requests, such as a denial of service (DOS) attack. An internal attack originates from a compromised, misconfigured, faulty, or even malicious router inside a network domain.

A. *Existing system:*

AODV Routing Protocol[10].

a. Is an on demand routing protocol with small delay
b. AODV supports Unicast, Broadcast and Multicast without any further protocols.
c. AODV uses IP in a special way. It treats an IP address just as a unique identifier.
d. AODV defines no special security mechanisms for data protection.
e. Impersonation attack can easily be done.

B. *Proposed System:*

Protected Routing(PR)

The route-discovery messages are protected by secret key between a source and destination and some intermediate nodes along a route established by using cryptographic mechanisms. This algorithm can be integrated into ad-hoc on-demand distance vector routing (AODV). As an example, We present such an integrated protocol called Protected Routing(PR), in which a node makes a routing decision based on its trust of its neighboring nodes and the performance provided by them.

IV. REQUIREMENT SPECIFICATION

A. *Functional Requirements:*

The proposed system PR has the following functions to be implemented to avoid the Byzantine attack and automatically generate the shortest path to be routed among the systems in the Ad-hoc network to transfer the file.

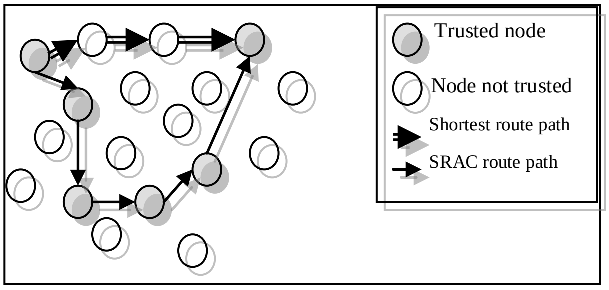

Figure 3: Variation of shortest path route selection between PR and other routing algorithms

The functional requirements are;

a. First the ECHO packet has to be created.
b. The created ECHO packet has to be encrypted using secrete key.
c. The encrypted ECHO packet has to broadcast to the neighboring nodes.
d. The neighboring node has to decrypts the ECHO packet.
e. In the decrypted ECHO packet the neighboring node has to replaces the sender IP address with its IP address.
f. The neighboring node has to encrypt the ECHO packet and sends back to the sender.
g. Then the sender on receiving the ECHO packet has to decrypt the packet and checks whether node is trustworthy, if so calculate the time required reach its neighboring nodes.
h. The routing table is to be created with the calculated delay and stored in XML format.
i. The new routing table has to be encrypted and exchanged with its neighboring nodes.
j. The new routing table with shortest path has to be updated in every node.

B. *Nonfunctional Requirements:*

a. Stringent energy requirements - the nodes have very limited energy availability with sources like battery, etc so energy utilization should be less.
b. The Time stamp field associated with each packet reflects on how fast that node is reachable from the source.
c. The source IP field associated with each packet reflects the trustworthiness of the neighboring node
d. The shared secrete key should be distributed to only trustworthy nodes.

V. SYSTEM DESIGN AND IMPLEMENTATION

This paper has been implemented by creating the functions listed below in order to avoid Byzantine attack and find the shortest path in Ad-hoc network using XML services to exchange the data.

a. Create EchoPacket ()
b. Encrypt EchoPacket using key ()

c. Send Echopacket()
d. Receive EchoPacket()
e. Decypt EchoPacket using key()
b. 6.Calculate distance()
a. Create XML File()
b. Send XMl file()
c. 9.Recieve XML file()
d. 10.Update XML files()

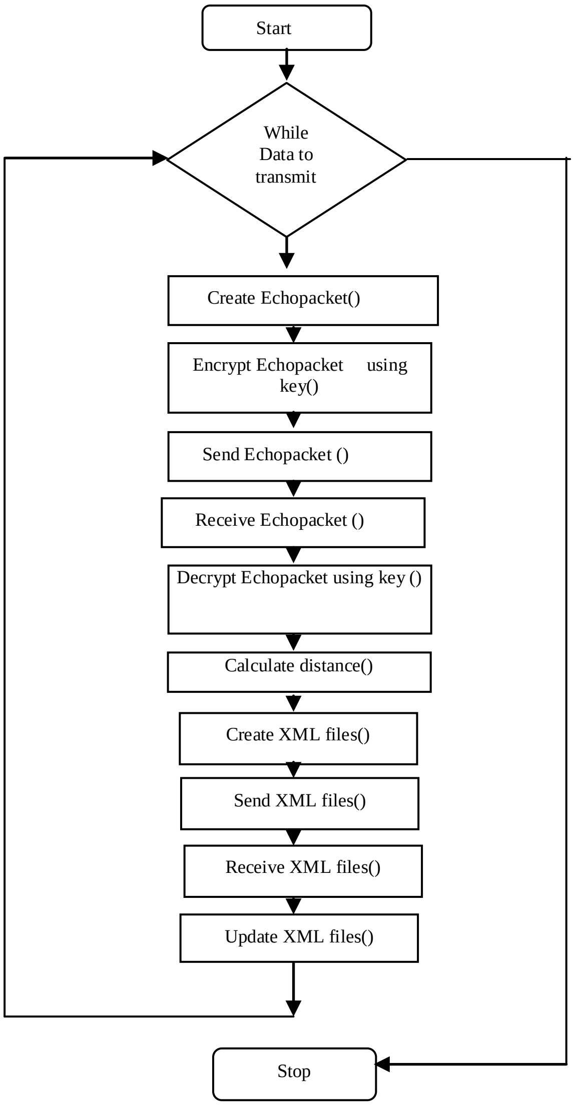

Figure 5: Flow Chart

A. *Packet Structure:*

Table: 1 Sender ECHO packet format

Session ID	Header text	Sent time	Address list
CHAR	SECHO	10:40:40	Sender IP address

Table: 2 Receiver ECHO packet format

Session ID	Header text	Sent time	Address list
CHAR	RECHO	10:40:40	Sender IP address

VI. CONCLUSION

Here in this paper an efficient algorithm is developed that detects internal attacks by using both message and route redundancy during route discovery. These route discovery messages are protected by secret key between a source and destination and intermediate nodes along a route established by using shared-key cryptographic mechanisms.

This Paper develops PR Routing aims in finding the shortest path in the Ad-hoc Network using the XML services so that packets navigate to destination system by avoiding the network traffic.

This paper overcomes the problem of Byzantine attacks.

VII. FUTURE ENHANCEMENT

a. Intermediate Node Route Rebuilding
b. Elimination of ECHO Messages
c. Locality of Association and QoS

VIII. REFERENCES

[1]. Andreas Tønnesen,”Mobile Ad-Hoc Networks”. [Courtesy of http://www.olsr.org/docs/wos3-olsr.pdf]

[2]. Introduction to Mobile Ad hoc Networks (MANETs). [Courtesy of http://user.it.uu.se/~erikn/files/DK2-adhoc.pdf]

[3]. Andrew S .Tanenbaum “Computer Networks “, 4th edition, Pearson Education, 2003.

[4]. A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments. [Courtesy of http://ieeexplore.ieee.org/xpl/ freeabs_all.jsp?arnumber=4490171]

[5]. Narendra Singh Yadav, R.P.Yadav, “Performance Comparison and Analysis of Table- Driven and On-Demand Routing Protocols for Mobile Ad-hoc Networks”. [Courtesy of www.waset.org/journals/waset/v48/v48-98.pdf]

[6]. V. P. Patil, K.T.Patil, A. R. Kharade & D. D.Gote, “Performance Enhancement of Reactive on Demand Routing Protocol in Wireless Ad Hoc Network” [Courtesy of http://interscience.in/IJSSAN_Vol1Iss4/ paper13.pdf**]**

[7]. P. Yi et al., “A New Routing Attack in Mobile Ad-hoc Networks,” Int’l. J. Info. Tech., vol. 11, no. 2, 2005.

[8]. Krishna Ramachandran. Aodv. Technical report, University of California, Santa Barbara, USA. [Courtesy of http://moment.cs.ucsb.edu/AODV/ aodv.html]

[9]. Andrew Troelsen,”ASP.NET concepts”, 2nd edition, Apress, 2003.

[10]. A Quick Guide to AODV Routing by Luke Klein Berndt. [Courtesy of http://www.antd.nist.gov/wctg/aodv_kernel/ AQuick Guide to AODV Routing.pdf]