Journal of Theoretical and Applied Information Technology
30th November 2011. Vol. 33 No.2

ISSN: **1992-8645** www.jatit.org E-ISSN: **1817-3195**

COUNTER HACKING MECHANISM IN CLUSTERED ROUTING TO PROVIDE QUALITY OF SERVICE IN MOBILE AD HOC NETWORKS

[1]B.SREEDEVI, [2] Y.VENKATRAMANI, [3]T.R.SIVARAMAKRISHNAN

[1] Assistant Professor, Department of Computer Science & Engineering, Srinivasa Ramanujan Centre, SASTRA University, Kumbakonam, Tamil Nadu, India.

[2]. Director (Academics), Saranathan College of Engineering, Trichy, Tamil Nadu, India.

[3]. Senior Professor, School of ECE, SASTRA University, Thanjavur, Tamil Nadu, India.

Email: sreedevi@src.sastra.edu,diracads@saranathan.ac.in, , deantrs@sastra.edu

ABSTRACT

In ad hoc networks, each node is connected instantaneously, wireless without a central control. Its challenge lies with dynamic topology and limited battery energy. Its instant infrastructure poses a greater dispute in routing. Since the medium is wireless and no central control, there are lots of chances of attack by intruders. The impact of hackers attack and the process to overcome from those attacks have been discussed. The consequence made by the hackers is analyzed in terms of packet loss, throughput and delay. At the same time, the performance is also measured after overcoming from the attack process. The analysis and performance are done using ns2 tool.

Keywords: *Intruder, Attack, Packet Loss, Throughput, Delay.*

1. INTRODUCTION

An ad-hoc network is a set of nodes that has the ability to communicate wireless without the existence of any fixed infrastructure. Nodes in an ad-hoc network use other nodes as intermediate relays to transmit packets to their destinations. Since nodes are usually battery operated, energy conservation is an important issue. Moreover, because of the broadcast nature of the wireless medium, ad hoc networks are also limited by interference/capacity considerations.

Performing routing in ad hoc network is somewhat a challenging task. Node disjoint virtual circuit approach is one of the methods where performance seems to increase [1]. Ad hoc networks find useful applications in military surveillance rescue operations, ubiquitous computing and disaster recovery. In many realistic ad hoc networks, nodes are actually heterogeneous. For example, in a battle field network, portable wireless devices are carried by soldiers and powerful reliable communication devices are carried in vehicles, tanks, aircraft and satellites; these devices/ nodes have different communication characteristics in terms of transmission power, data rate, processing capability, reliability, etc.

Creating and maintaining distributed network structures like dominating sets, clusters, spanning graph, etc have been the commonly agreed upon solution for organizing wireless networks in a large scale topology. A cluster is formed by associating a cluster head with some of its neighbours (i.e., nodes within the cluster head's transmission range) that become the ordinary nodes or member nodes of the cluster [2] [3]. In cluster based topology, there are two types of flows. They are inter-cluster and intra-cluster flows. The intra-cluster flows originate and terminate in the same cluster, whereas, the inter-cluster flows are meant for communication between clusters. The cluster structure imposes many important restrictions and difficulties in the estimation, exchange and updates of link state

Journal of Theoretical and Applied Information Technology
30th November 2011. Vol. 33 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

information which are inevitable for QOS implementations [2] [3] [4] [5].

In ad hoc networks, there are a lot of possibilities for the intruder (hacker) to attack. To overcome this situation, an implementation of end-to-end reliability and energy conservation routing is provided for quality of service in mobile ad hoc networks as a security measure but without clustering [6].

There are many possible attacks which may happen in mobile ad hoc networks, as they do not have a centralized control and the medium is wireless. When the hackers intrude, the data or the message may be interpreted in a different way and the content may pose a different meaning. This would be dangerous when secret message is being communicated e.g. ATM Pin number. So, this should be avoided. In this work, the damage made by the hackers is analyzed in terms of packet loss, throughput and delay. At the same time, the performance is also measured after overcoming the attack process. The analysis and performance are done using ns2 tool.

2. INITIALIZATION

This is the first phase consist of clustering and Certificate distribution. The Clustering phase is to elect the Cluster Head (CH) among the nodes in a cluster.

2.1 Clustering

Initially all the nodes are arranged randomly according to their radio coverage range. Each node will have its own IP address and MAC address. Each node will be provided with a maximum (100%) energy. As soon as all the nodes are arranged, each node will send a Hello packet among its neighbours and then a routing table is formed for each node.

The nodes with certain geographical coverage will form a group called cluster. All the nodes in the cluster will broadcast its residual energy within the cluster. A residual energy is the energy which retain after packet transmission. The node which has the maximum residual energy would declare itself as a Cluster Head (CH). This process is called as an Election process. Since there are many groups i.e. cluster, there would be many cluster heads. A node which acts like a watch dog and monitors all the cluster heads, clusters and other nodes is said to be a Base Station (BS) or gateway. Its work is simply to monitor the entire topology and to keep the information about all CH. This can be shown in the figure 1.

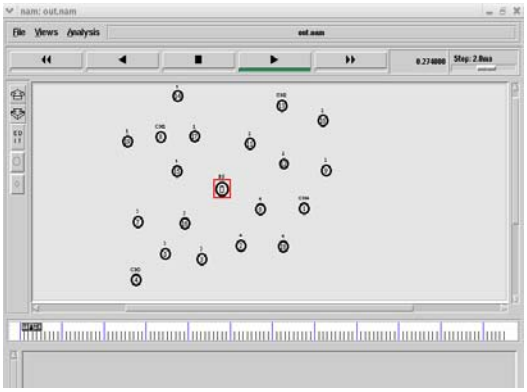


Figure1.Cluster Arrangement in Ad hoc Networks

2.2. Certificate Distribution

In this Phase, each node will broadcast its certificate and a message. The respective cluster head will check the certificate and verify. By the end of this phase all the cluster heads will come to know about the limited information about all the members and complete information about its own members. If the verification is found to be illegal then, that particular node is discarded from the entire topology, as that node may become a hacker. This can be seen from the figure 2.

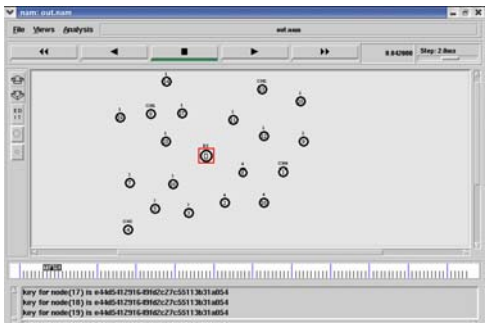


Figure 2. Certificate distribution among nodes

3. ROUTING

The Second phase is the route discovery phase, where routing table is formed and communication among the nodes takes place.

3.1 Routing Table

As soon as the nodes communicate with Hello packets, a routing table is built and updates, when

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the nodes come to stable state. This is to avoid an unnecessary looping and delay. A routing table contains the MAC address, source IP address, source sequence number, destination IP address, destination sequence number, TTL (time to live) and hop count.

3.2 Communication

The node which wants to send a packet becomes a source node (S) and a node which receives the packet becomes the destination (D). If S and D are within the same cluster then, intra-clustering is performed. If S and D belong to different clusters then, inter-clustering is performed.

```
Algorithm Init ( )
{
// D stands for destination node
// S stands for Source node
// MN stands for member node
// CH stands for cluster head
// BS stands for Base station or Gateway
// MN_s member node of source cluster
// CH_s denotes Cluster head of Source cluster
// MN_d denotes member node of destination cluster
// CH_d denotes cluster head of destination cluster

 If (D is within cluster S)
    Intra_cluster( )
   Else
    Inter_cluster( )

}

Algorithm Intra_cluster( )
{
      s_intra( )
      d_intra( )
}
Algorithm Inter_cluster( )
 {
    s_inter( )
     inter( )
    d_inter( )
}
Algorithm s_inter( )
{
    If (S = MN_s)
      {Send data packets to CH_s}
}
Algorithm inter( )
{
 // now the packets have reached at CH_s
   Send packets to BS;
   Receive the packets from BS to CH_d;
 }
Algorithm d_inter( )
{

    If (D = MN_d)
      {Receive data packets from CH_d & forward them to MN_d}
}

Algorithm s_intra( )
{
        if (S = MN)
          {Send the packets to CH}

}

Algorithm d_intra( )
{
        if (D = MN)
          {Receive the packets from CH}
}
```

The pseudo code given above is self explanatory. The packets will reach its destination until there is no intruder or hacker intercepts the packet. If the TTL reaches zero, and if no acknowledgement from the destination, then the source concludes that the packet has been intercepted by the intruder or it might have been lost. Under these circumstances, the intruder detection phase is essential. In addition to this, it is also necessary to safeguard the packets as the next phase i.e. attack phase may occur.

4. ATTACK PHASE

4.1 Misbehavior Nodes

A source node intends to send a packet to the destination. So, it finds the shortest path and initiates its transmission. The source node forwards the packet to the next hop neighbour. The node keeps on forwarding the packet till it reaches the destination. So the source node trusts each node as if it will deliver the packet safely. But sometimes, some of the nodes may misbehave and starts to malfunction. These nodes may either divert the path or it may block the path thereby not allowing the packets in reaching the destination (figure .3). These misbehaving nodes interrupt and gain all the

Journal of Theoretical and Applied Information Technology
30th November 2011. Vol. 33 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

packets from the intended neighbour till its buffer gets overflow.

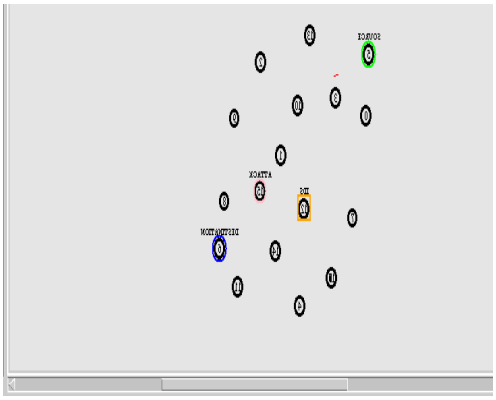


Figure 3. Misbehaving node becomes attacker

In due course of time, the sender used to have a counter equal to the turn around time. As soon as the sender has initiated transmission, the counter also gets started with the value equal to its turn around time. It keeps on decrementing for each transmission. When the counter value reaches zero, and the sender has not received any acknowledgement from the receiver, the sender comes to the conclusion that, its packet has been lost somewhere or it may be due to some intruder attacks i.e. by misbehaving nodes. So the sender chooses an alternate path by triggering.

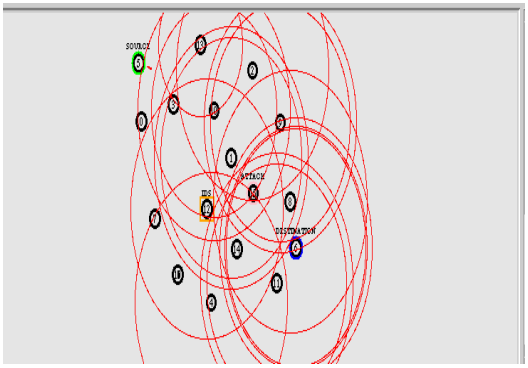


Figure 4. Source node tries to find the alternate path by triggering.

The source node tries for its alternate path by triggering (figure.4). Sometimes, it gets failed in its attempt and so the packets will get dropped (figure. 5). Figure 6 shows the failure attempt by source node and the dropping of packets.

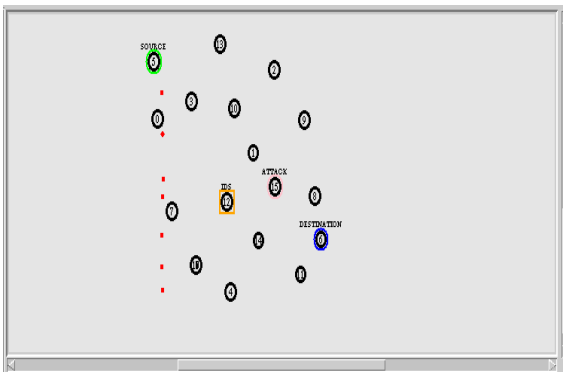


Figure 5. Source node fails in finding alternate path

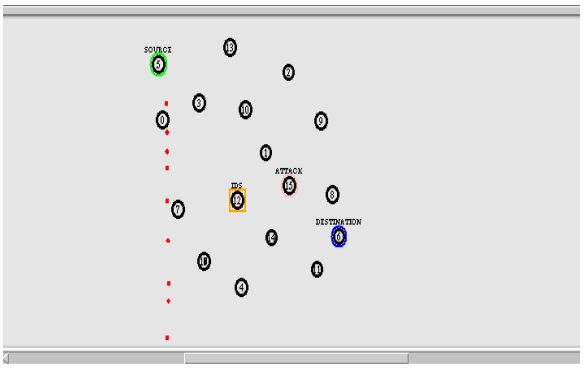


Figure 6. Source node drops its entire packets due to malfunctioning node.

4.2 Node Replication

There is also another type of attack called node replica or cloning. A malfunctioning node gets the IP address of its nearest neighbour and it replicates (clones) the neighboring node into multiple replica. The multiple replica nodes behave like original node and choose all possible shortest paths and get settled in those paths. The major task of multiple replications is to prevent the packets in reaching the destination.

Figure 7 shows the entry of a new attacker inside the network. Figure 8 shows the cloning (of node 4) by node 10 as it gets IP address of node 4.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

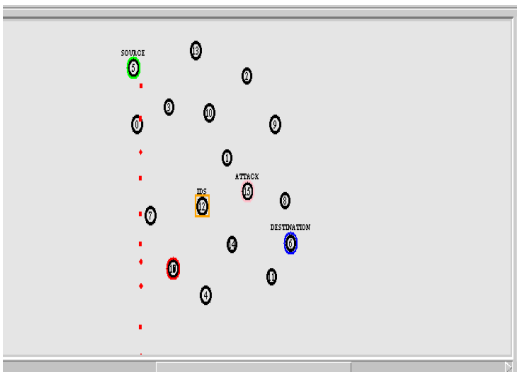


Figure 7. Another new attacker is rising.

These cloned nodes take its shortest path and gets settled in the network and is shown in the figure 9. Figure 10 shows the settlement of replicated node. The replicated nodes will do all sort of malfunctioning by not making them reaching the destination.

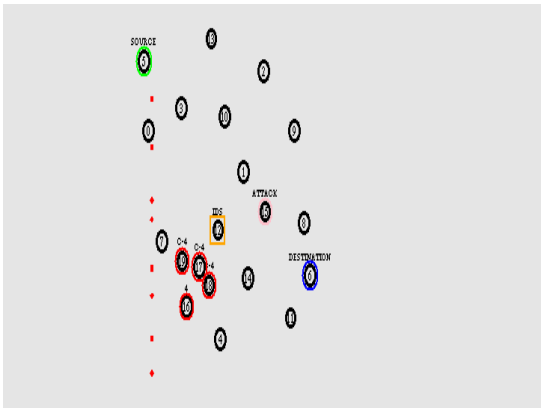


Figure 8. Node replication or cloning

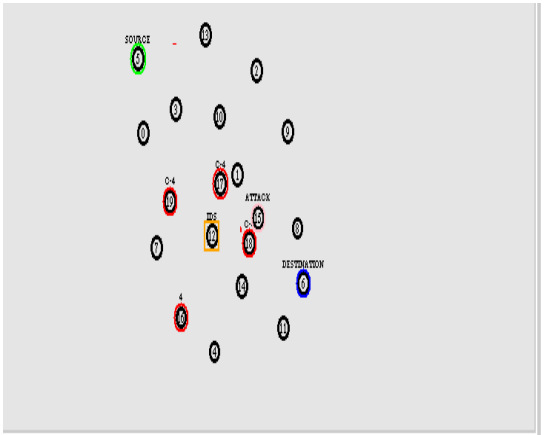


Figure 9. Replicated node takes its shortest paths

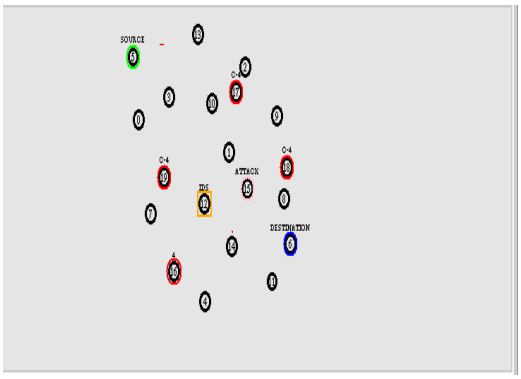


Figure 10. Settlement of replicated nodes in various paths

The replicated nodes capture all the packets by blocking its path. So source node tries to find an alternative path and in most of the cases, its attempt gets failed and thereby the packets get dropped and are shown in figure11.

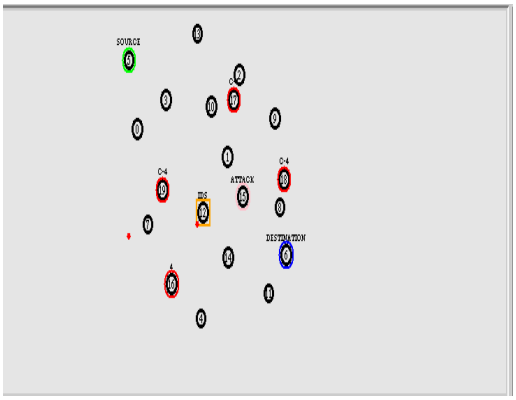


Figure 11. Packet dropping by source node.

4.3 A Non Member Node Enters a Cluster

When a node (a member node of previous cluster) enters into a cluster, it makes a request to the current CH. After certificate verification, the CH accepts the new node by giving its ID and certificate and converts it as its own member node. Now a new arrival node may become a hacker and it may act as a CH as it has obtained the certificate form the CH. This is similar to node replication. But in this case a new arrival makes CH replication and performs blocking.

5. CHECK & COUNTER ATTACK

This is an important and essential phase for secured routing. At first, each node has to check whether an intruder has made an attack. Then,

Journal of Theoretical and Applied Information Technology
30th November 2011. Vol. 33 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

some attack prevention methods are undergone for security.

5.1 Checking for a Malicious Intruder

If a node detects a same certificate during routing process from more than one node, then it marks that node as suspicious and simply discards that node (or path) and prefers an alternate path. This happens till the packet reaches the destination. Figure 12 shows the entry of malicious intruder.

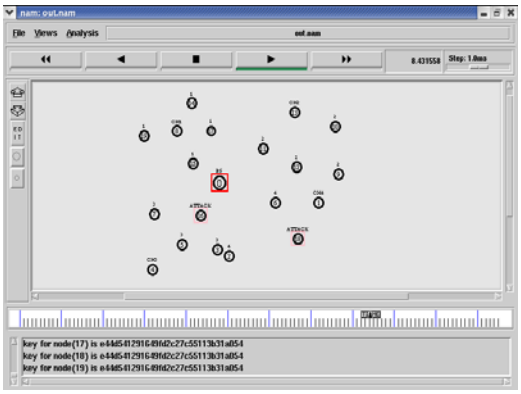


Figure 12. A malicious intruder

5.2 Intruder Detection System Implementation

The Intruder Detection System (IDS) can be implemented under three conditions: i) When a node misbehaves in a network ii) a non-member node enters a cluster iii) a node may replicate into multiple replicas.

5.2.1 A node misbehaves in a network

Whenever a misbehaving node tries to divert the path or it blocks the path, thereby not allowing the packets further to reach destination, the current source node chooses an alternate path and proceeds.

5.2.2 A non-member node enters into a cluster

When a node (a member node of previous cluster) enters into a cluster, it makes a request to the current CH. After certificate verification, the CH accepts the new node by giving its ID and certificate and converts it as its own member node. Then the current CH updates its certificate and intimates this information to BS and other CH's. Now, the current CH is having an updated new certificate with itself. This is to prevent a new arrival member node of being a hacker (an intruder) or a malicious node or the new member might pretend to act as a CH (instead of current CH) as it has recently obtained current CH's certificate. This is only a preventive measure. Figure 13 shows the entry of non member node into a cluster. Figure 14 shows the update of CH's certification.

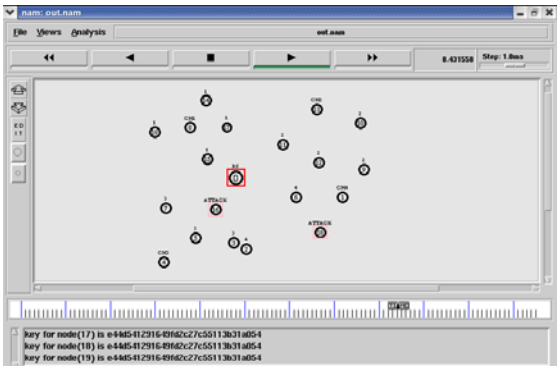


Figure 13. Entry of a non-member node

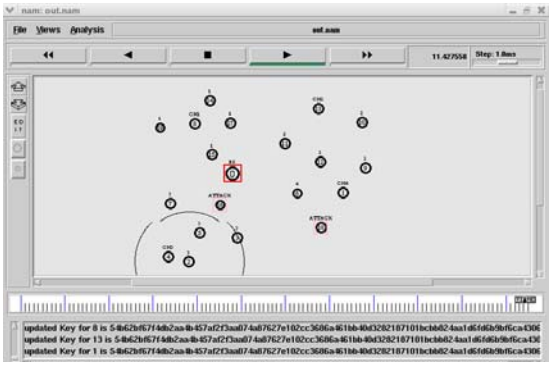


Figure 14. Updating of CH certificate

5.2.3 Node Replication

A malfunctioning node gets the certificate of its nearest neighbour and it replicates (clones) the neighboring node into multiple replicas. The multiple replicated nodes acts as an original node and chooses all possible shortest paths and gets settled in those paths. The major task of these multiple replicated nodes is to prevent the packets being reaching the destination. If many nodes issue a same copy of the certificate, the checking criteria become false and the current source chooses the alternate path

.

Journal of Theoretical and Applied Information Technology
30th November 2011. Vol. 33 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

6. FLOW DIAGRAM

The entire process can be presented with a flow diagram, which may give a brief overview and is shown in figure 15.

7. SIMULATION SCENARIO

We use a detailed simulation model base on ns2 [7] [8]. The other parameters are shown in the table 1.

Table 1. Simulation Parameters

Parameter description	Value
MAC Protocol	802.11 [9]
Mobility Model	Random waypoint mobility model
Simulation Area	600 X 400 m
Traffic pattern	CBR / UDP
Transmission range	64 m
Packet Size	512 bytes
Data rate	1 Mbps
Maximum packets	1000
No. of nodes	20
Queue length	10
Routing protocol	AODV [10]
Node initial energy	Infinite

8. SIMULATION RESULTS

8.1 Intruder Attack

The impact of intruder (hacker) has decreased the overall performance of the network i.e. in terms of delay, packet loss and throughput. These have been analyzed using ns2 tool with x-graph.

8.1.1 Throughput

Initially all the nodes does their work as usual without any disturbance. So there is a hike in throughput. As the intruder malfunctions severely, the throughput significantly reduces and this can be seen from the figure 16.

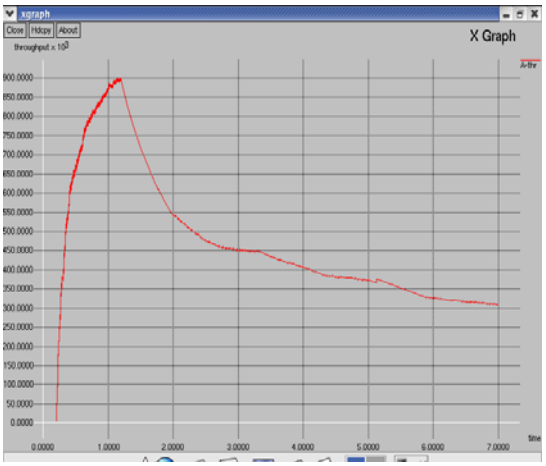


Figure 16. Throughput

8.1.2 Delay

The routing is very much affected by the hackers and so the source node search for its destination and so it incurs much delay. This can be seen from the figure 17.

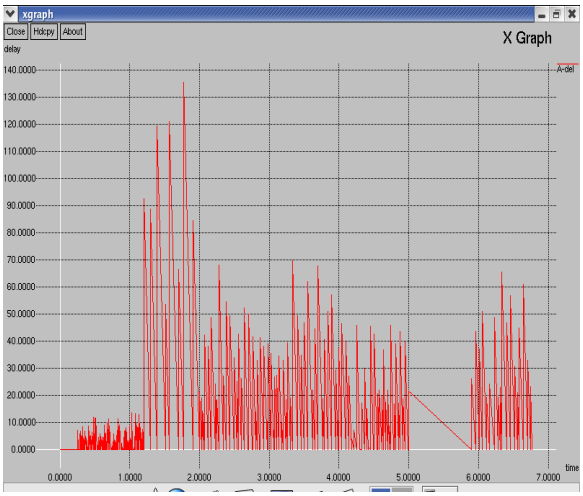


Figure 17. Delay

8.1.3 Packet Loss

As the intruders capture the packets, the packets reaching the destination are almost nullified and this can be depicted from the figure 18.

Journal of Theoretical and Applied Information Technology
30th November 2011. Vol. 33 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

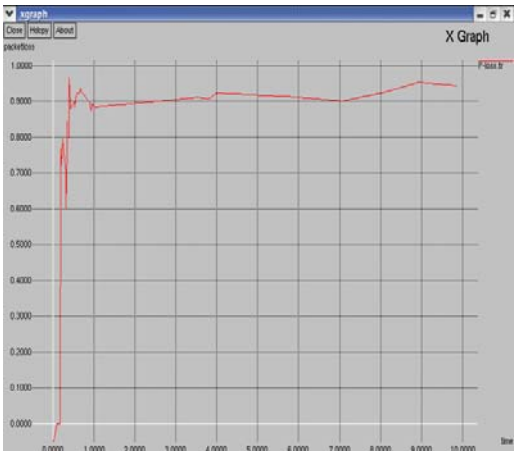


Figure 18. Packet Loss

8.2 Counter Attacks

Intruder (Hacker) prevention method routing uses AODV protocol to measure its performance in terms of throughput, delay, packet delivery ratio, packet loss and residual energy.

8.2.1 Delay

During initial stages, the nodes arrange themselves in clusters. Then it spends much time in certificate distribution, certificate verification and intruder detection. So it incurs a delay in routing the packets to destination and that can be depicted in figure 19.

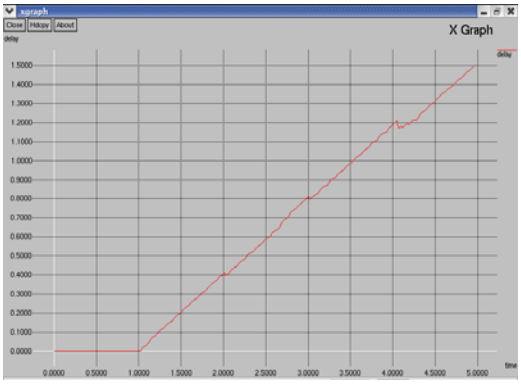


Figure 19. Delay

8.2.2 Throughput

Throughput is initially less, followed by some fluctuations and finally it gets hike. As it undergoes three phases for routing it finds such fluctuations: but later on it succeeds in routing the packets to destination, its throughput goes hike and can be seen from the figure 20.

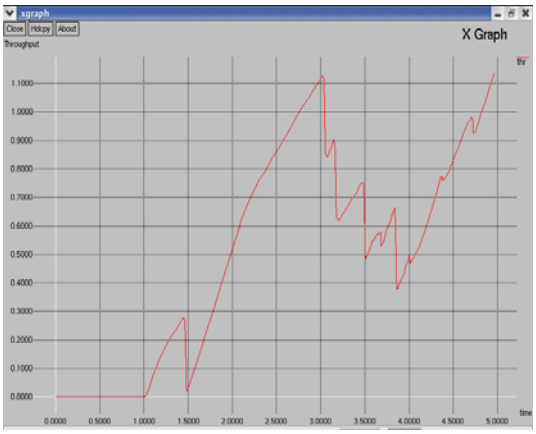


Figure 20. Throughput

8.2.3 Residual Energy

Residual energy is the energy retained by a node after transmitting the packets. These selection criteria for cluster heads (CH) which is said to be an election process. Each node spends its energy for certificate distribution, checking and forwarding packets. So, its energy has been spent and this can be seen from figure 21.

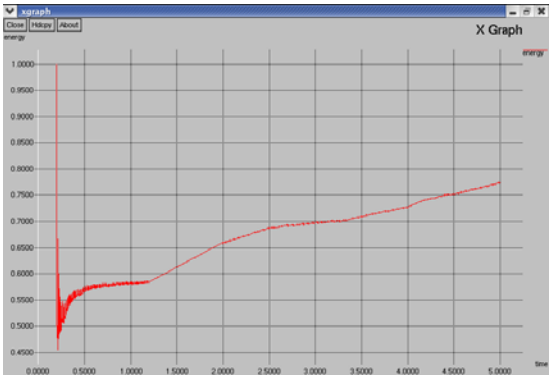


Figure 21. Residual Energy

8.2.4 Packet Loss

Routing takes in three phases and hackers have been prevented from malfunctioning. So there is no chance of packets being lost. This can be seen from the graph (figure 22) as the packet loss is almost negligible.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

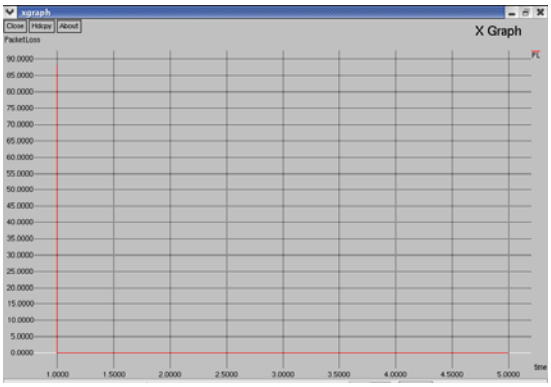


Figure 22. Packet loss after routing

9. CONCLUSION

This work shows the impact of hacker on packet loss to be tremendously high and after counter attack the packet loss to be insignificant. So, this methodology has greater reliability over transmission and thus provides a quality of service with secured routing. But this method has its own limitations. There is no metric proposed for selecting cluster head as far as this paper is concerned. In our future work this would be important criteria for selecting such nodes. The QoS parameters are delay, throughput, residual energy and packet loss are taken into account for the present paper. In future, some more parameters like transmission power, Connection resilience and priority of packets could be taken for consideration.

REFERENCES:

[1] Sreedevi. B, Venkataramani .Y, Sivaramakrishnan T.R., "Node Disjoint-Virtual Circuit Approach in Ad Hoc On-Demand Multipath Distance Vector Routing to offer Quality of Service in Ad Hoc Networks" ,International Journal of Engineering Science and Technology (IJEST), ISSN : 0975-5462, April 2011, Vol. 3 issue 4 , pp.3045 – 3050.

[2] J.Y.Yu and P.H.J Chong, "A Survey of Clustering Schemes for Mobile Ad hoc Networks", IEEE Commun, Surveys and Tutorials, vol.7, No.1.pp 32-48, Ql, 2005.

[3] Puneet Sethi, Gautam Barua, "CRESQ: Providing QoS and Security in Ad hoc Networks", Proceedings of 11th Euromicro Conference on Parallel, Distributed and Network-Based Processing (Euro-PDP'03), IEEE, 2003.

[4] Sreedevi. B, Venkataramani .Y, SivaramakrishnanT.R., "Implementation of Zone Routing Protocol for Heterogeneous Hybrid Cluster Routing to Support QoS in Mobile Ad hoc Networks" , International Journal of Computer Applications (IJCA), ISSN 0975-8887, Vol.25 issue 10. July 2011, pp.1-6.

[5] Sreedevi. B, Venkataramani .Y, Sivaramakrishnan T.R.," Performance Comparison using AODV and AOMDV Protocols in Heterogeneous Hybrid Cluster Routing using Partial Authority Nodes in Mobile Ad hoc Networks" European Journal of Scientific Research (EJSR), ISSN 1450-216X, Vol.58 No.4 (2011), pp.542-549.

[6] Sreedevi. B, Venkataramani.Y, Sivaramakrishnan T.R.," Implementing End-To-End Reliability and Energy Conservation Routing to Provide Quality of Service in Mobile Ad hoc Networks", European Journal of Scientific Research (EJSR), ISSN 1450-216X, Vol.55 No.1 (2011), pp.28-36.

[7] K.Fall and K.Varadhan (Eds.). "Ns notes and documentation", 1999. available from http://www.mash.cs.berkeley.edu/ns/

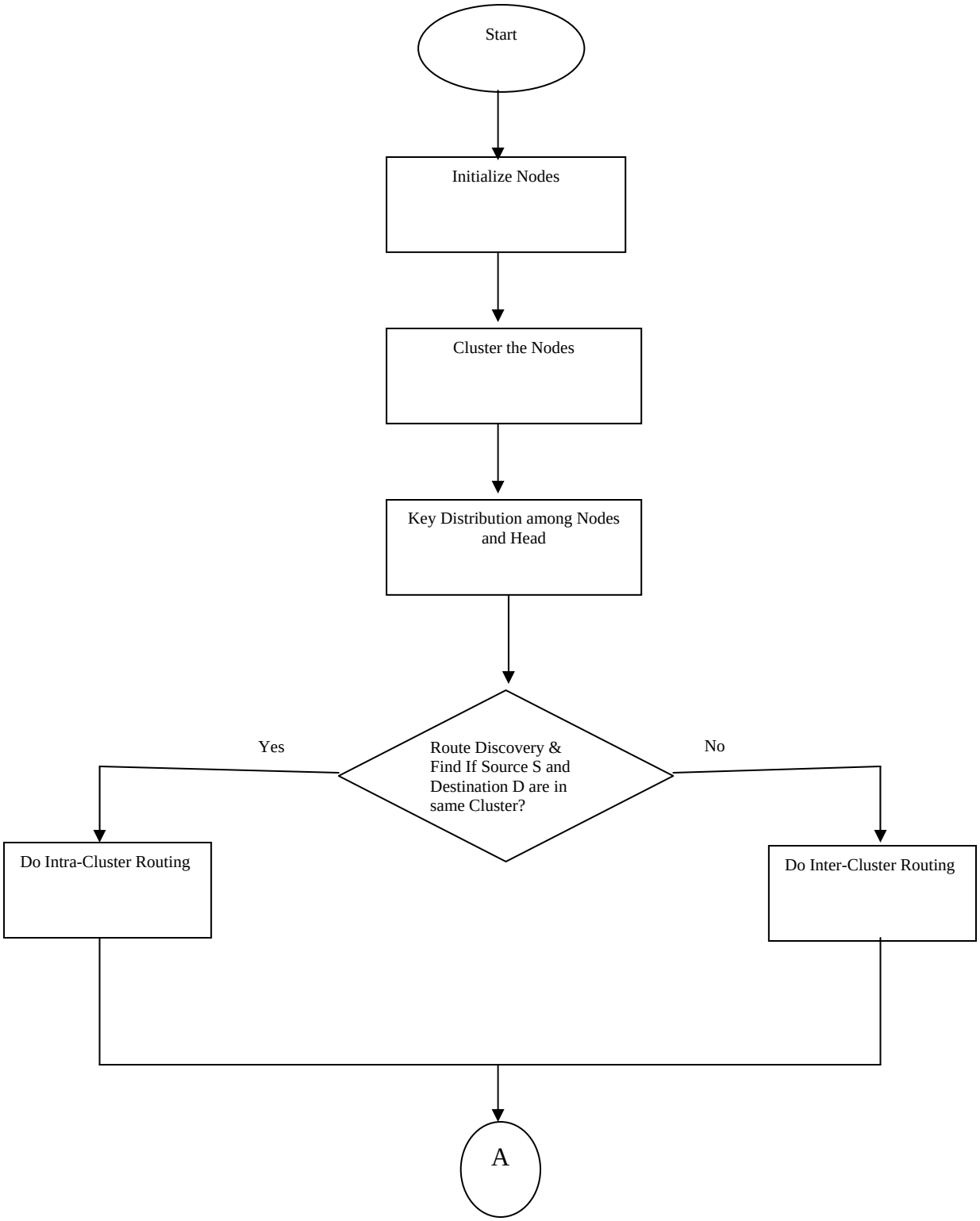
[8] Ns 2: Network Simulator: (http://www.isi.edu/nsnam/ns/.).

[9] IEEE Computer Society, "802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[10] C.E.Perkins, E.M.Royer, S.R.Das,"Ad hoc on-demand distance Vector (AODV) Routing [EB/OL],"RFC3561. http://www.faqs.org/rfes/rfe3561.html,2003-07-01.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Figure 15.The Flow diagram for entire process



ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195