ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 8(23), DOI: 10.17485/ijst/2015/v8i23/79224, September 2015* ISSN (Online) : 0974-5645

Evaluation of Quality of Service Metrics for Hacking and Counter Hacking Mechanism in Mobile Ad Hoc Networks

B. Sreedevi*

Department of Computer Science and Engineering, Srinivasa Ramanujan Centre, SASTRA University, Kumbakonam - 612001, Tamil Nadu, India; sreedevi@src.sastra.edu

Abstract

Objectives: The work is to identify the Quality of Service metrics for mobile ad hoc networks during hacking and counter hacking mechanism. **Methods:** The various quality metrics such as end to end delay, throughput and packet delivery ratio is determined. The implementation is done using ns2 simulator with the nodes at random waypoint mobility model. The performance is measured during intruder attack and counter attack for 20 nodes with 1000 packets of 512 bytes size. **Findings:** The simulation results showed a significant increase in packet delivery ratio for counter attack mechanism (98) when compared with intruder attack, which gave least value (40.6). This work is also compared with Anti Black Hole Mechanism and is found to be efficient in terms of packet delivery ratio. **Improvements:** In this work, all the nodes are assumed to be of maximum energy in terms of its battery power. While routing the energy drops and this is a major issue in ad hoc nodes. The future work will focus on energy efficiency during routing process.

Keywords: Anti-Black Hole Mechanism, Counter Attack, Intruder Attack, Packet Delivery Ratio, Quality of Service, Through put

1. Introduction

When the hackers poke in, the data or the message may get misinterpreted to a different meaning. This would be dangerous when a confidential is being communicated e.g. ATM Pin number. Ad hoc networks are more vulnerable for the intruder (hacker) to attack[1,2]. This paper discusses that, while routing in mobile ad hoc networks (MANET), hackers may intercept the message by any form[3] and deteriorate the quality of service metrics. To overcome this, preventive measures (i.e. counter attack mechanism) are taken. This work is also being compared with[1,2]. 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 routing out the attack.

2. Initialization

It consists of clustering and Certificate distribution.

2.1 Clustering

Initially all the nodes are arranged according to their radio coverage range. Each node will have an IP address and MAC address. They will be provided with maximum (100%) energy[4,5]. Then, each node contacts its neighbors and a routing table is formed for each node.

The nodes in a geographical coverage form a cluster[6]. All nodes in the cluster broadcast their residual energy within the cluster. A residual energy is the energy which retained after transmission. The node with maximum residual energy proclaims itself as Cluster Head (CH)[7].

* *Author for correspondence*

This process is called Election process. A Base Station (BS) or gateway node does the watch dog role, monitoring all nodes. It monitors the entire topology keeping the information about all CH (Figure 1).

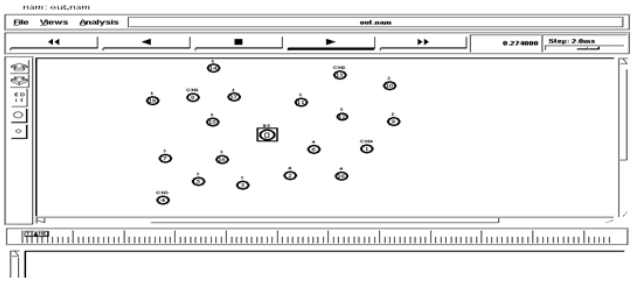

Figure 1. Cluster arrangement in Ad Hoc networks.

2.2 Certificate Distribution

In this Phase, each node broadcasts its certificate and a message. The cluster head verifies the genuineness of the node. By the end of this phase all the cluster heads will be wary of the information about the members. If on verification the node is found to be an illegal node then, it is discarded (Figure 2).

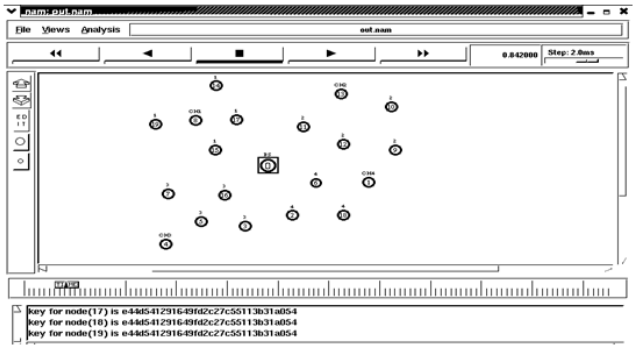

Figure 2. Certificate distribution among nodes.

2.3 Routing

The Second phase is the route discovery phase, where routing table is formed and communication among the nodes takes place[8].

2.3.1 Routing Table

As soon as the nodes communicate, a routing table is built and updated, when the nodes come to stable state. This is to avoid unnecessary 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.

2.3.2 Communication

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

The packets will reach its destination if no hacker intercepts it. If no acknowledgement is received from the destination, conclusion is made that the packet has been intercepted or it might have been lost. Under these circumstances, the intruder detection phase is essential[9].

3. Attack Phase

3.1 Misbehavior Nodes

A source node intends to send a packet to the destination. So, it finds the shortest path and initiates transmission. The source node forwards the packet to the next hop neighbor. The intermediate nodes keep forwarding till it reaches the destination. So the source node trusts each node to deliver the packet safely. But some nodes may misbehave and start to malfunction. These misbehaving nodes interrupt and gain all the packets from the neighbor till its buffer overflow (Figure 3).

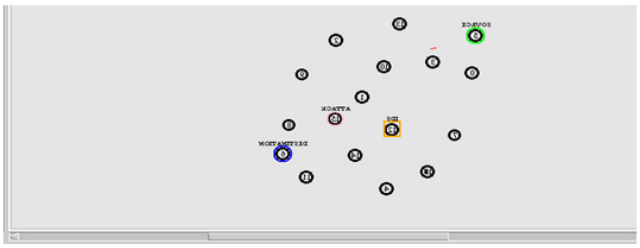

Figure 3. Misbehaving node becomes an attacker.

In course of time, the sender's counter equals to the turnaround time. As soon as the sender has initiated transmission, the counter also gets started with the value equal to its turnaround 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 lost due to some intruder attacks[10]. So, the source node tries for an alternate path by triggering (Figure 4). Sometimes, it fails in attempt and so the packets will get dropped (Figure 5).

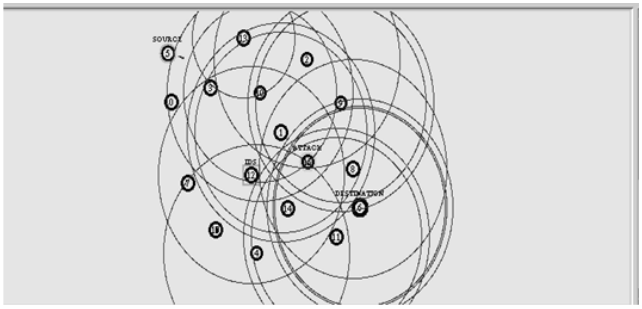

Figure 4. Source node tries to find the alternate path by triggering.

Figure 5. Source node fails in finding alternate path.

3.2 Node Replication

There is also another type of attack called node replication or cloning. A malfunctioning node gets the IP address of its nearest neighbor and replicates the neighboring node. The replicated ones behave like original node and choose all possible shortest paths (Figure 6).

The replicated nodes will perform all sorts of illegal functions preventing the packets from reaching the destination (Figure 7).

The replicated nodes capture all the packets by blocking their path. So source node tries to find an alternative path and in most of the cases, its attempt fails and thereby the packets get dropped (Figure 8 and 9).

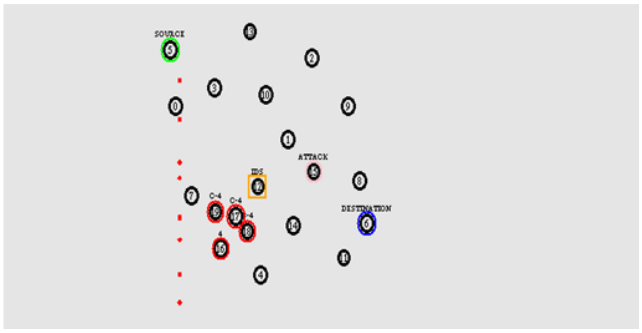

Figure 6. Node replication or cloning.

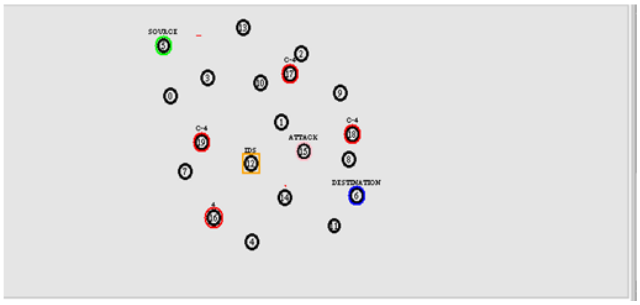

Figure 7. Settlement of replicated nodes in various paths.

Figure 8. Packet dropping by source node.

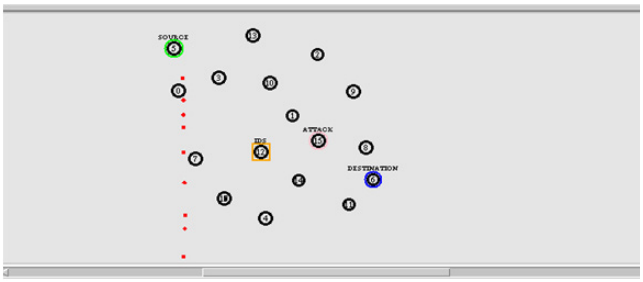

Figure 9. Source node drops its packets due to malfunctioning node.

4. Intruder Detection System Implementation

The Intruder Detection System can be implemented under three conditions: 1.When a node misbehaves in a network, 2.a non-member node enters a cluster, 3.a cloning node.

Whenever a misbehaving node tries to divert the path or it blocks the path, thereby not allowing the packets to reach the destination, the current source node chooses an alternate path and proceeds. When a node (a member node of previous cluster) enters, it makes request to the

current CH (Figure 10). After verification, the CH accepts the new node by giving an ID, a certificate. The current CH renews its certificate and intimates this info, to other nodes (Figure 11). This is only a preventive measure.

A malfunctioning node gets the certificate of its nearest neighbor and replicates the neighboring node into multiple replicas. If many nodes issue a same copy of the certificate, the checking criteria become false and the current source chooses the alternate path.

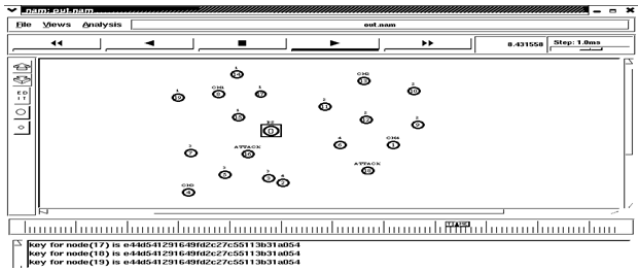

Figure 10. Entry of a non-member node.

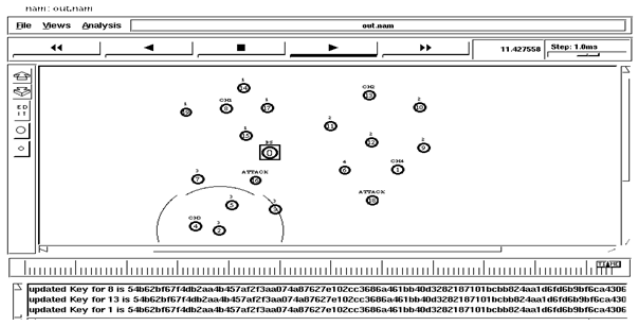

Figure 11. Updating of CH certificate.

5. Simulation scenario

The simulation parameters are taken as given in Table 1.

Table 1. Simulation parameters

Parameter description	Value
MAC Protocol	802.11
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[11]
Node initial energy	Infinite

5.1 Intruder Attack

The impact of intruder decreases 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. The values are given in the Table 2.

Table 2. Analysis results during intruder attack and counter attack

Description	Intruder Attack values	Counter attack values
End to End Delay	427.26 ms	14.85 ms
Throughput	314397.31 kbps	355072.31 kbps
PDR	40.63	98
CBR Traffic: Receive/ Send traffic	0.4063	0.98

5.2 Comparison

The counter hacking method is compared with ABM (Anti-Black Hole Mechanism)[1]. The performance is measured for its throughput, delay, and PDR as given in Table 3. It is apparent that the throughput is high for counter hacking method than ABM (Anti-Black Hole Mechanism). The PDR is high for counter hacking method (or counter attack) than ABM. The delay is lesser for counter attack than ABM. The results prove that counter hacking method shows the best performance in all aspects (Figure 12-14).

Table 3. Analysis results for ABM and Counter Hacking Mechanism

Description	ABM Values	Counter Hacking Mechanism values
End to End Delay	466.68 ms	14.85 ms
Throughput	105836.24 kbps	355072.31 kbps
PDR	56.42	98
CBR Traffic: Receive/ Send traffic	0.5642	0.98

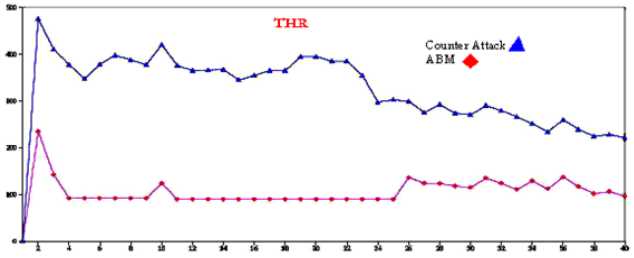

Figure 12. Comparison of throughput with simulation time.

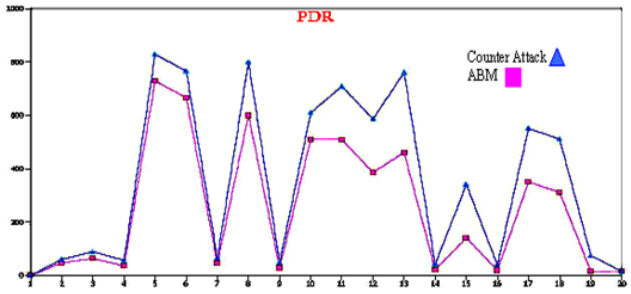

Figure 13. Comparison of Packet Delivery ratio.

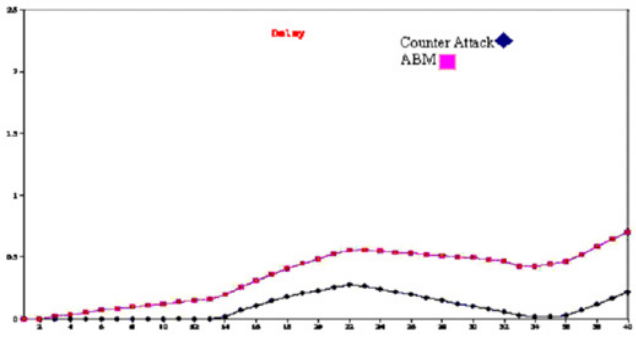

Figure 14. Comparison of delay with simulation time (ms).

6. Conclusion

The work has shown that the impact of hacker has made packet loss to be tremendously high and after counter hacking the loss is insignificant. This is also numerically been compared with Anti-Black Hole Mechanism. The future work would be based on energy efficiency.

7. References

1. Su MY. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. Journal of Computer Communications. 2011 Jan 15; 34(1):107–17.
2. Su MY, Chaing K-L, Liao W-C. Mitigation of black-hole nodes in Mobile Ad hoc networks. International Symposium on Parallel and Distributed Processing with Applications; 2010. p. 162–7.
3. Baddache A. Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks. Journal of Networks and Computer Applications. 2012 May; 35(3):1130–9.
4. Sreedevi B, Venkataramani Y, Sivaramakrishnan TR. Implementing end-to-end reliability and energy conservation routing to provide quality of service in mobile ad hoc networks. EJSR 2011; 55(1): 28–36. ISSN:1450-216X.
5. Reina D, Johnson P, Baarrero F, Toral S. Optimization of network lifetime through energy-efficient broadcast scheme using dynamic random walk. 2012, 15th International Power Electronics and Motion control conference (EPE/PEMC); 2012. p. LS4e.2-1–LS4e. 2-5.
6. Sreedevi B, Venkataramani Y, Sivaramakrishnan TR. Research challenges in heterogeneous hybrid routing in ad hoc networks to provide QOS. National Conference on Communications, Networking and cryptography (NCCNC2008). SASTRA University: Thanjavur; 2008. p. 34–7.
7. Sreedevi B, Venkataramani Y, Sivaramakrishnan TR. Partial authority node selection in heterogeneous hybrid cluster routing to support QoS in mobile ad hoc networks. 2011 IEEE International Conference on Computational Intelligence and Computing Research. IEEE Xplore 2011 Dec 14–18; p. 402–406.
8. Reina DG, Toral SL, Johnson P, Barrero FJ. Route duration improvement in Wireless Sensor and Actual networks based on mobility parameters and flooding control. EURASIP Journal on Wireless Communications and Networking. 2012; 147–72.
9. Sreedevi B, Venkataramani Y, Sivaramakrishnan TR. Implementation of intruder detection system for security in clustered routing for MANETs. 2011 IEEE International Conference on Computational Intelligence and Computing Research. IEEE Xplore 2011 Dec 14–18; 630–3.
10. Sreedevi B, Venkataramani Y, Sivaramakrishnan TR. Counter hacking mechanism in clustered routing to provide quality of service in mobile ad hoc networks. JATIT 2011 Nov 30; 33(2):239–49. ISSN:1992–8645.
11. Perkins CE, Belding-Royer EM, Dass SR. Ad Hoc On-demand Distance Vector (AODV) Routing. Internet draft. 2003 Feb. Available from: Draft-ietf-manet-aodv-13.txt