ISSN No. 0976-5697

Volume 2, No. 5, Sept-Oct 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Analyzing the Effect of Denial of Service Attacks on Packet Delivery Ratio in Mobile Ad-hoc Networks Carrying Packet Telephony

P.K.Suri
Professor& Head,
Department of Computer Sc&Appln
Kurukshtra University,
Kurukshtra, India
pksuritf25@yahoo.com

Sandeep Maan*
Assistant Professor,
Government Post Graduate College,
Gurgaon, India
sandeep.mann23@gmail.com

Abstract:Successful implementation of Packet Telephony over a mobile ad-hoc network has been a topic of research interest for some time now. One major deterrent to success of any viable solution are various 'Denial of Service', DoS, attacks launched by the malicious node(s). Successful implementation of packet telephony is subject to restriction imposed by various 'Quality-of-Service', QoS, parameters including packet delivery ratio (PDR). In this work authors have analysed the adverse effect that denial of service attacks can have on Packet Delivery Ratio. This analysis should prove to be helpful in real time implementation of Packet Telephony over Mobile Ad-hoc Networks.

Keywords:Mobile Ad-hoc Networks;Packet Telephony;Packet Delivery Ratio;Malicious Node;Denial of Service Attacks; Quality of Service.

I. INTRODUCTION

A mobile ad-hoc network is a collection of autonomous and mobile nodes where routing is done through cooperative effort. In other words each participant node in a mobile ad-hoc network is a potential router and forwards the packets routed though it towards next node in the route. Mobile ad-hoc networks can be highly beneficial in situations where setup time in hand is limited. The cost involved in their setup is also limited. Some major areas of their application include warfronts, natural calamities and emergency like situation triggered by some event.

One major application over mobile ad-hoc networks gaining interest of research fraternity is packet telephony or VoIP [1]. In packet telephony telephonic calls are transported over the mobile ad-hoc network in form of IP packets. The successful implementation of packet telephony over mobile ad-hoc network has proved to be difficult to realize. This can be attributed to the strict QoS requirements of packet telephony which are difficult to realize in mobile ad-hoc networks. In mobile ad-hoc networks the nodes are moving all the times and hence the routes keeps on changing making it really difficult to realize acceptable QoS constrained performance. Various important QoS parameters for packet telephony over mobile ad-hoc networks include packet delivery ratio, end to end delay, throughput, jitter, packet drop rate, packet loss rate, channel utilization, number of calls dropped, number of calls blocked etc. Overall various QoS parameters may be divided into two categories viz.

A. **Call level QoS parameters** including number of dropped calls and number of blocked calls
B. **Packet level QoS parameters** including Packet Delivery Ratio, Packet Drop Rate, jitter, End to End Delay.

International Telecommunication Union (ITU) has suggested reference values for various QoS parameters (Table 1) for ascertaining the successful implementation of packet telephony. Successful implementation of packet telephony can be highly beneficial in providing solutions for problem of wireless intercom and fixed to mobile convergence [2] meant for extending the reach of fixed telephony. Moreover by using medium in License free ISM band all the solution can come for free.

TABLE I. QOS PARAMETERS

QoS Parameter	Expected Range
End to End Delay	<= 120 ms
Jitter	<= 40 ms
Packet Delivery Rate	>= 95%
Packet Drop Rate	< = 5%
Packet Loss Rate	<= 5%

As described earlier it is really difficult to realize the packet telephony over the mobile ad-hoc network. Even if the packet telephony was successfully implemented over the mobile ad-hoc network then it will be vulnerable to open threats as is the case with other wireless solutions. The threats can come from outside as well as inside. Threats from inside the networks can be more dangerous as they tend to disrupt the working of network. One such attack is denial of service attack where one or more malicious node(s) from within the network try to disrupt the working of mobile ad-hoc network. The attacker may exhibit selfish or malicious intention. A selfish node in light of saving own resources do not actively participate in the network chores whereas a malicious nodes takes active part in the networking chores but tries to disrupt the working of the network. So it is of utmost importance to identify and segregate such nodes.

Packet Delivery Ratio represents fraction of packets that are successfully transported from source to destination and a PDR of more than 95% is must to successfully realize packet telephony over the mobile ad-hoc network. A denial of service attack can lead to lowering of packet delivery ratio and hence making network to perform in unacceptable manner. The authors felt a need to study the effect of differentdenial-of-service attacks caused by various nodes

within the network on the performance of mobile ad-hoc network carrying packet telephony. For the purpose authors decided to select an architecture that may lead to successful implementation of packet telephony over mobile ad-hoc networks. This architecture would be simulated using ns2. Then various DoS attacks would be imposed on this architecture and their effect on packet delivery ratio would be studied. The rest of paper is organized as:

First of all a survey of related work is performed to outline the network structure to be used. Then the network is simulated and various denial-of-service attacks are identified and imposed. The results of simulation would be plotted next to study the effect of attacks on PDR.

II. RELATED WORK

In [3] authors have worked on the issue of feasibility of fixed to mobile convergence using a mobile ad-hoc network. The authors have proposed complete system architecture for their implementation. The proposed architecture was then evaluated by the authors in terms of various quality-of-service (QoS) parameters like Call Drop Rate, MOS etc.

In [4] authors have proposed a possible architecture for successful implementation of Packet Telephony. In this work authors have proposed a network architecture involving RTP/UDP/IP protocol stack. The G.729 codec was employed for encoding and compression of telephonic data. The legacy IEEE 802.11 based MAC and Physical layers were employed by the authors.

In [5] authors have classified various denial-of-service attacks in terms of motive behind the attacks, nature of attacks, location of attacker node, stage of attack and number of nodes colluding to launch the attack. Various possible attacks launched to disrupt the routing process have been identified like Overflow attack (overflow the victim node with fake route requests), Cache poising attack (propagate wrong routing information), packet misrouting attack, black hole attack (attract route request but drop data packet), Warm hole (tunnel the route request for early discovery of route, then drop data packets), Jelly Fish attack (drop packets smartly) etc.

III. NETWORK ARCHITECTURE

The proposed system will be composed of five layers as outlined in figure 1. The structure of the network architecture employed is:

- ***A. Application Layer:*** The voice conversations were digitized and compressed as per G .729 codec [6]. The telephonic calls were made in accordance with the recommendations of ITU-T in terms of single/double talk times, silence period and inter-call arrival times [7].
- ***B. Transport Layer:***The de-facto transport layer for any VoIP application i.e.RTP[8]/UDP was employed.
- ***C. Network Layer:*** The network layer was based on DSR algorithm[9][10].
- ***D. Physical and MAC Layer:*** The IEEE 802.11g [11] based Physical and MAC layer were employed.

The system was simulated using network simulator [12] (version ns2.34) running on Fedora Core 14 based machine.

The simulation scenario was generated as per random waypoint model where to start with each node moves in a random direction with random speed constrained by a specified maximum speed. At the destination it pauses and then again moves in random direction as earlier.

G .729 Codec working at 8kbps (Application Layer)
RTP over UDP (Transport Layer)
IP with DSR Routing algorithm (Network Layer)
LLC & IEEE 802.11 based MAC (Data Link Layer)
(IEEE 802.11 PHY working at 2.4 GHz) (Physical Layer)

Figure 1: Network System Architecture for MANET carrying Packet Telephony

IV. SIMULATION

A close study of various denial of service attacks reveals that each attack is launched using one or more basic mechanism. These mechanisms include:

- ***a. Dropping the route request:*** A number of DoS attacks are based on dropping the route request maliciously thereby depriving the source of a possible optimum route to the destination.
- ***b. Dropping Route Replies:*** Malicious node may drop the route reply thereby again depriving the network of fruitful routes; this attack when followed by propagating wrong routing information may lead to attacks like cache poisoning attack.
- ***c. Dropping route requests as well as replies:*** Malicious nodes may drop both route request and replies so that it is never in any legitimate route and thereby extending selfish behavior.
- ***d. Dropping Data packets:*** Most of the attacks are based on dropping data packets. Malicious nodes may drop all the packets or may opt for selective dropping of packets.
- ***e. Dropping control packets:*** Apart from route request/reply and data packets,other important control information flows through the network. Malicious node may drop control packets in order to disrupt the working of network

It can be easily demonstrated that almost every identifieddenial-of-service attack can be launched using one or more of the above basic mechanisms. So, authors decided to study the effect of these malicious activities on the performance of network individually.

A. Packet Delivery Ratio

Packet Delivery ratio may be defined as the fraction of data packet that are successfully delivered at destination. It is very much established that in case of real time voice transportation TCP cannot of much help and it is better to use UDP helped by Real Time Protocol, RTP. The RTP/UDP/IP protocol stack does not guarantee any delivery rather tries to improve on delay and provides some sort of synchronization. Hence any packet loss virtually means loss of conversation. For packet telephony a packet delivery ratio above 95% is must as it represents amount of conversation transported from source to destination. The PDR was plotted under normal circumstance and under various malicious attacks as discussed in earlier sections. The observations are summarized next:

B. Effect of maliciously dropping route request

The network was simulated with 75 users (nodes) moving with a maximum speed of 20KMPH in a square area of 4 KM2. A total of 7 telephonic calls were simulated. The PDR is plotted with respect of number of malicious nodes (figure 2).

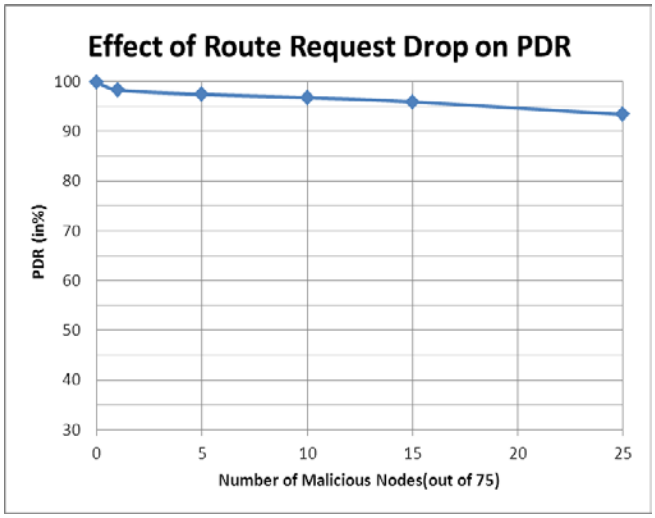

Figure 2: Study of Packet Delivery Ratio with number of malicious nodes in a network with DSR routing algorithm while keeping other parameters constant as Number of Nodes =75, Speed = 20 KMPH , Network Size= 04 KM2 (square area) and Number of Active Calls= 07.

It was observed that with increase in number of malicious nodes PDR drops almost linearly and becomes unacceptable, in terms of QoS requirements for successful implementation of packet telephony, when around 25% of nodes start misbehaving. It was observed that increasing the number of malicious nodes do affect the PDR but it still remains in acceptable range if proportion of maliciously behaving nodes is small.

C. Effect of maliciously dropping route reply

The network architecture used for this study makes use of DSR algorithm, in this discovered route are piggybacked on the route reply packets. The route reply packets may be forwarded by simply reversing the route they followed to the destination or another route discovery with route reply piggybacked may be initiated to source. In ns2 route replies are treated as data packets from destination to source with discovered route as data. Again, the network was simulated with 75 users (nodes) moving with a maximum speed of 20KMPH in a square area of 4 KM2. A total of 7 telephonic calls were simulated. The PDR is plotted with respect of number of malicious nodes (figure 3). It was observed that with increase in number of malicious nodes PDR do not drop that significantly. It is observed that DoS attacks depending upon destroying route replies may not be that much effective in this environment. One important point worth mentioning here is that we are considering network with telephonic conversation only and no other data was simulated in the network. It might be interesting to study the effect after adding some data transfers in addition to telephonic conversations.

D. Effect of maliciously dropping route request as well as route reply

Again, the network was simulated with 75 users (nodes) moving with a maximum speed of 20KMPH in a square area of 4 KM2. A total of 7 telephonic calls were simulated. The PDR is plotted with respect of number of malicious nodes (figure 4). It was observed that with increase in number of malicious nodes PDR drops almost linearly and becomes unacceptable (in terms of QoS requirements for successful implementation of packet telephony) when around 20% of nodes start misbehaving. It was observed that increasing the number of malicious nodes do affect the PDR but it still remains in acceptable range if proportion of maliciously behaving nodes is small.

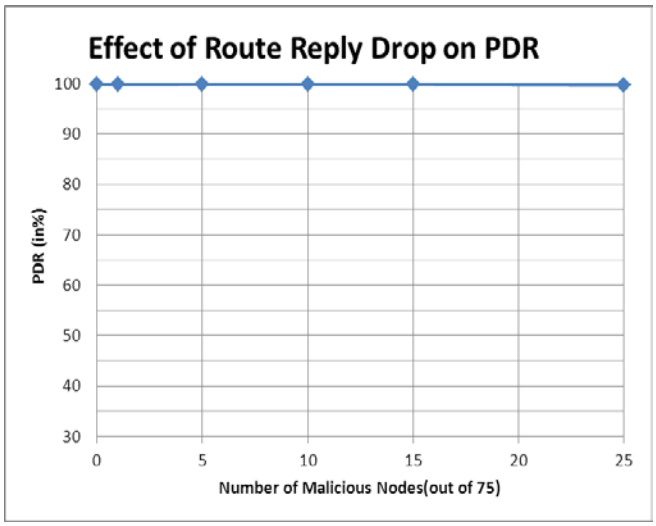

Figure 3: Study of Packet Delivery Ratio with number of malicious nodes in a network with DSR routing algorithm while keeping other parameters constant as Number of Nodes =75, Speed = 20 KMPH , Network Size= 04 KM2 (square area) and Number of Active Calls= 07.

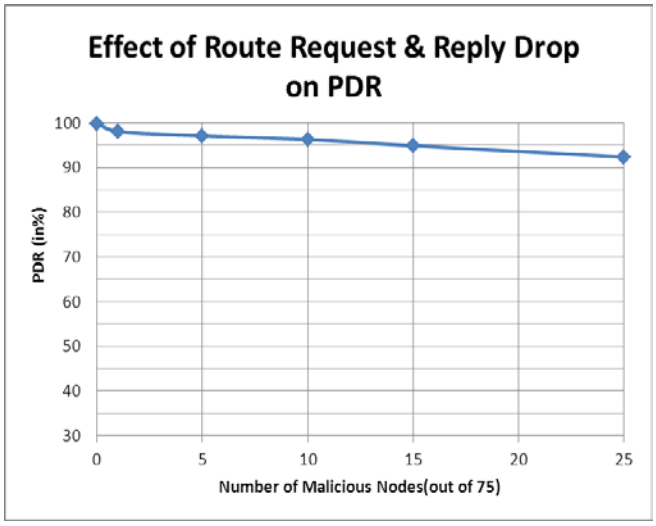

Figure 4: Study of Packet Delivery Ratio with number of malicious nodes in a network with DSR routing algorithm while keeping other parameters constant as Number of Nodes =75, Speed = 20 KMPH,Network Size= 04 KM2 (square area) and Number of Active Calls= 07.

One interesting observation made was that the nature of curve is similar to that obtained for 'maliciously dropping route requests' but here the deterioration in network performance is much faster.

E. Effect of maliciously dropping data packets

The transport layer in the network architecture is modeled as RTP/UDP and dropping a data packet would more or less mean loss of conversation due to the underlying unreliable nature of UDP and hence it is very important to study the

effect of malicious data packet drop on PDR. The network was simulated with 75 users (nodes) moving with a maximum speed of 20KMPH in a square area of 4 KM2. A total of 7 telephonic calls were simulated. The PDR is plotted with respect of number of malicious nodes (figure 5).

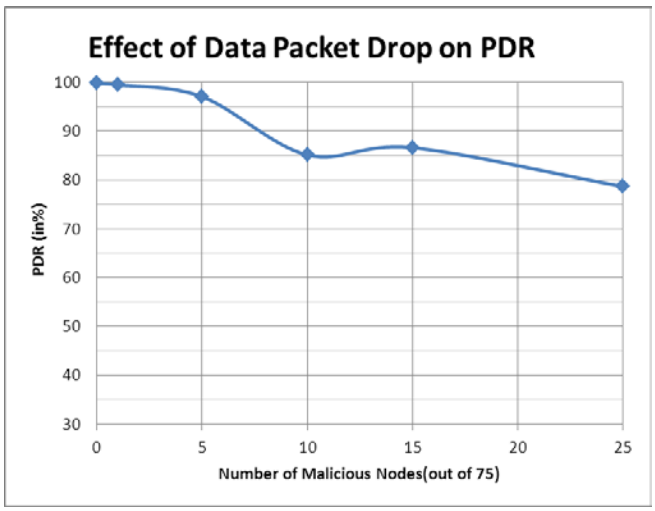

Figure 5: Study of Packet Delivery Ratio with number of malicious nodes in a network with DSR routing algorithm while keeping other parameters constant as Number of Nodes =75, Speed = 20 KMPH, Network Size= 04 KM2 (square area) and Number of Active Calls= 07.

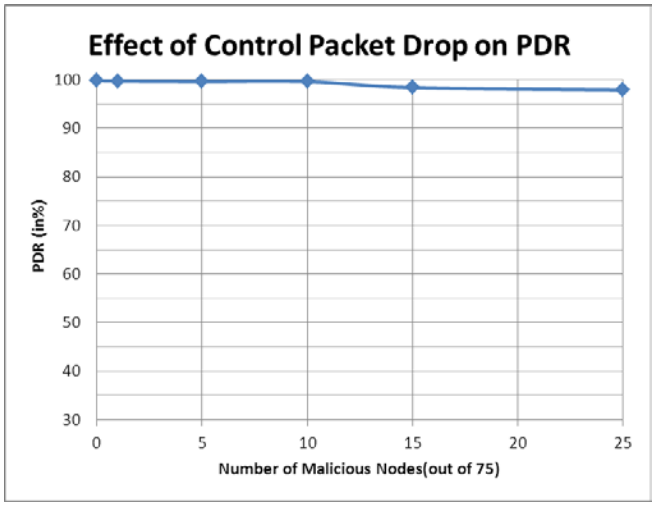

Figure 6: Study of Packet Delivery Ratio with number of malicious nodes in a network with DSR routing algorithm while keeping other parameters constant as Number of Nodes =75, Speed = 20 KMPH, Network Size= 04 KM2 (square area) and Number of Active Calls= 07.

It was observed that with increase in number of malicious nodes PDR drops very quickly and attains unacceptable values even for very small number of malicious nodes. It may be concluded from this curve that attacks resorting on data packet drop would be more deterrent to the functioning of network carrying packet telephony than any other discussed above. This is the reason why most of the proposed DoS attacks make use of this mechanism.

F. Effect of maliciously dropping control packets:

Finally the system was modeled for malicious dropping of control packets with other system setting being similar to above cases i.e. with 75 users (nodes) moving with a maximum speed of 20KMPH in a square area of 4 KM2. A total of 7 telephonic calls were simulated. The PDR is plotted with respect of number of malicious nodes (figure 6).

It was observed that effect of increasing number ofmalicious nodes is not that prominent on PDR still it causes network performance to deteriorate in terms of PDR and finally it attains unacceptable values for large number of malicious nods.

V. CONCLUSION

In this work effect of DoS attacks on the performance of a mobile ad-hoc network carrying packet telephony was studied. The network architecture employed includes G .729 codes for digitization and compression of voice, RTP/UDP as transport layer with DSR as routing algorithm To increase the practicability of the system most popular IEEE 802.11g based MAC and physical layer working around ISM band at 2.4 GHz was employed.

Rather than studying individual DoS attack different mechanisms employed by various type of attacks were simulated including dropping route requests, dropping route replies, dropping control packets, dropping data packets etc.

It was observed that in the given network architecture dropping of data packets hurts most in terms of PDR and even a small number of maliciously behaving nodes can lead to unacceptable behavior of the network. While dropping of route replies hurts least. So those attacks that make use of data packet drop prove to be more threatening than others. Overall all type of malicious attacks leads to the deterioration of network performance and a proper check must be installed in the system to look for malicious nodes so that they are identified earlier even before causing any major effect on the performance of QoS based application like packet telephony over the mobile ad-hoc networks.

VI. REFERENCES

[1] JoriLiesenborgs, “Voice over IP in networked virtual Environments”, PhD Thesis, University of Maastricht, 1999-2000, pp. 30-40.

[2] P.K. Suri and Sandeep Maan, A Novel Approach to Implement Fixed to Mobile Convergence in Mobile Ad-hoc Networks”, International Journal of Advanced Computer Science and Applications(IJACSA), Vol 2, No 1 , January 2011, pp 93-99.

[3] Paolo Giacomazzi et al., “Quality of Service for Packet Telephony over Mobile Ad Hoc Network”, IEEE Network, Jan/Feb 2006.

[4] P.K. Suri and Sandeep Maan, “Towards Realizing Mobile Intercom Systems”, International Journal of Computer Engineering and Computer Applications (IJCECA), Vol 4, 2011, pp 33-42.

[5] P.K. Suri and Sandeep Maan, “A Survey of Denial of Service Attacks Against Routing Protocols of Mobile Ad-Hoc Networks”, International Journal of Computer Engineering and Computer Applications (IJCECA), Vol 5, 2011, pp 14-19.

[6] M. E. Perkins et al., “Characterizing the Subjective Performance of the ITU-T 8 kb/s Speech Coding Algorithm ITU-T G.729,” IEEE Commun. Mag., vol. 35, no. 9, Sep. 1997 pp. 74–81.

[7] P.K. Suri and Sandeep Maan, “Traffic Simulation for Packet Telephony in Mobile Ad-hoc Networks”, International Journal of Computer Science and Technology(IJCST), Vol 2, Issue 1 , March 2011, pp 123-127.

[8] JuhanaMattila, "Real-Time Transport Protocol", Oct 2003.

[9] E. M. Royer and C.-K. Toh. "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," IEEE Pers. Commun., vol. 6, no. 2, Apr. 1999.

[10] D.B. Johnson et al., "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, pp. 153–81.

[11] "Information Technology—Telecommunications and Information Exchange Between Systems — Local and Metropolitan Area Networks- Specific Requirements — Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11-1997

[12] P.K. Suri and Sandeep Maan, "Simulation of Packet Telephony in Mobile Ad-hoc Networks Using Network Simulator", International Journal of Advanced Computer Science and Applications(IJACSA), Vol 2, No 1 , January 2011, pp 87-92.