ISSN 2047-3338

A Comprehensive Study of Adverse Effect of Malicious Attacks on End-to-End Delay in Mobile Ad-hoc Networks Carrying Packet Telephony

Sandeep Maan[1] and Dr. P. K. Suri[2]

[1]Department of Computer Science and Applications, Kurukshetra University, Kuruskhetra, India
[2]Govt. P.G. College, Sec-14, Gurgaon-India

***Abstract*– Like any other wireless network, mobile ad-hoc networks are highly vulnerable to security threats coming from various intruders. Attacks launched by nodes that are part of the network, have attracted attention of research fraternity. A malicious node may work in a manner to increase the transfer delay and hence disrupt the working of network. Successful implementation of packet telephony is subject to constraints imposed by various QoS parameters including end-to-end delay. In this work authors have tried to gauze the adverse effect on end-to-end delay caused by the presence of various nodes with malicious intention in the network.**

***Index Terms*– Mobile Ad-hoc Networks, End-to-End Delay, Packet Telephony, Quality-of-Service, Voice over Internet Protocol, Malicious Nodes and Denial of Service Attacks**

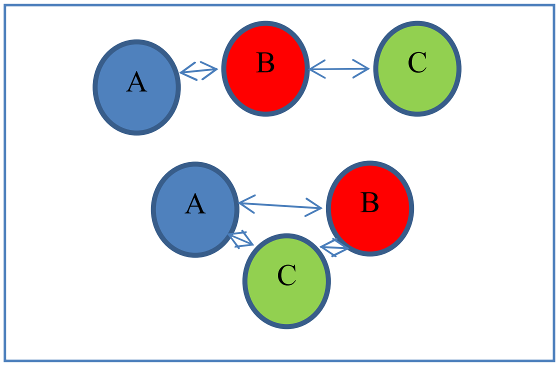

Fig. 1: Dynamic Nature of MANETs

I. INTRODUCTION

UNDERLYING presumption while defining or creating a mobile ad-hoc network is the cooperation among various participating nodes. Every node must work towards the common goal setting aside its own interests. If some node gets selfish then it can have some lasting effect on the performance of the network.

To define informally, mobile ad-hoc network represents a collection of autonomous and mobile nodes where routing is done through cooperative effort. Every participating node is supposed to forward data received from adjoining nodes to some other neighbour as per underlying routing protocol. Mobile ad-hoc network have some unique characteristics that distinguishes them from other wireless networks. These includes dynamic nature (Fig. 1), low node power, small setup time, small range, distributed routing, no centralised control etc.

Dynamic nature of mobile ad-hoc networks, MANET, is illustrated in figure 1 where in first scenario node ‘A’ and node ‘C’ have to depend on node ‘B’ for communication whereas in second case they become neighbour.

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.

In packet telephony or VoIP [1] 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 is 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 node 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.

International Telecommunication Union 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 wireless intercom, fixed to mobile convergence [2] for extending the reach of fixed telephony. Moreover by using medium in License free ISM band all the solution can come for free.

Any viable solution to the problem of packet telephony over mobile ad-hoc network is subject to the threats from various malicious nodes. The threat may 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.

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%

A participating node(s) from within the network may try to disrupt the working of mobile ad-hoc networks due to its malicious or selfish nature. 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 important to identify and segregate such nodes.

End-to-End (E2E) delay represent time elapsed between entry of sound in caller mouthpiece and the exit of sound at receiver's earpiece. End to End delay comprises of a number of sub-types of delays. These include:

a) *Codec Delay:* It is delay occurred during the digitization and compression of voice conversations.
b) *Algorithmic Delay:* For actual reproduction of sound a compression algorithm need to know about next block of voice, this leads to a delay which is of the order 5ms in case of G.729 codec.
c) *Packetization Delay:* This type of delay occurs due to collection of the encoded samples into a packet for transmission.
d) *Network Delay:* This factor contributes maximum to the delay and represents delay during journey from source to destination.

It is observed that a delay of more than 150 ms is undesirable and there after any increase in delay leads to more or less half-duplex communication rather than a full duplex one. Hence, in packet telephony any proposed solution must ensure that end-to-end delay is kept less than 150ms.

A malicious node may involve itself in an activity leading to increase of E2E delay and hence making network to perform in unacceptable manner. The authors felt to study the effect of presence of malicious nodes within the network on the performance of mobile ad-hoc network carrying packet telephony. 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 then various possible attacks are identified and imposed. The results of simulation would be plotted next to study the effect of attacks on E2E delay.

II. Related Work

Study of packet telephony over mobile ad-hoc network has been explained in details by the authors in [3]. The authors have proposed complete system architecture for their implementation. The authors evaluated the proposed architecture 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.

III. Network Architecture

The proposed system will be composed of five layers as outlined in Fig. 2.

The outlines of the architecture are given below:

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

Fig. 2: Employed System Architecture

a) *Application Layer:* The voice conversations were digitized and compressed as per G .729 codec [5]. The telephonic calls were made as per recommendations of ITU-T in terms of single/double talk times, silence period and inter-call arrival times [6].
b) *Transport Layer:* There are two obvious transport layer solutions in TCP and UDP. TCP would offer connection oriented reliable end-to-end transport service while UDP lacks connection and reliability. On other side TCP involves a number of control information that may lead to congestion and hence delays. For real time voice service like packet telephony it has been recommended to use UDP. Real Time Protocol [7] may be used to extend UDP for controlling delays, providing sequencing and synchronization. So, RTP/UDP was employed.
c) *Network Layer:* The network layer based on DSR [8][9] algorithm was employed.
d) *Physical and MAC Layer:* The IEEE 802.11g [10] based Physical and MAC layer were employed.
e) *Scenario Generation:* The 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.
f) *Simulation:* The system was simulated using network simulator (version ns2.34) running on Fedora Core 14 based machine [11].

IV. Simulation

A malicious node may involve itself in one or more basic mal-mechanism [12]. These mechanisms include:

a) *Dropping the Route Request:* It might drop the route request maliciously thereby depriving the source of a possible better route to the destination.
b) *Dropping Route Replies:* Malicious node may drop the route reply thereby again depriving the network of fruitful routes.
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:* Malicious nodes may drop all the packets or may opt for selective dropping of packets.

e) *Dropping Control Packets:* Malicious node may drop control packets in order to disrupt the working of network

The E2E delay was plotted under normal circumstance and under various malicious attacks as discussed in earlier sections. The observations are summarized next:

Case 1: Maliciously dropping route request

The E2E Delay is plotted with respect of number of malicious nodes (Fig. 3). It was observed that with increase in number of malicious nodes E2E Delay increases exponentially and remains acceptable, in terms of QoS requirements for successful implementation of packet telephony. This unexpected behaviour can be explained in terms of basic nature of DSR where more than one simultaneous route are maintained and if one good route is not discovered due to the malicious node there may be other sub-optimal routes that would help to maintain performance in acceptable range. One important thing to mention is that we are considering only voice data to be present in the network.

Case 2: 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 upto 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. The E2E Delay is plotted with respect of number of malicious nodes (figure 4). It was observed that with increase in number of malicious nodes E2E Delay increases but remains in the acceptable range even for quite a good proportion of malicious nodes.

Case 3: Maliciously dropping route request as well as route reply

The E2E Delay is plotted with respect of number of malicious nodes (figure 5).The behaviour of the curve depicts that with increase in number of malicious nodes E2E delay increases but remain in acceptable range as was the case in earlier two.

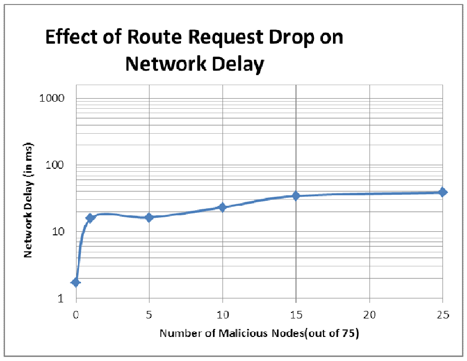

Fig. 3: Study of End to End Delay with number of malicious nodes in a network with DSR routing algorithm while keeping other parameters constant as Number of Nodes =75, Speed = 20 KMPH , Network Size= 04 KM^2 (square area) and Number of Active Calls= 07.

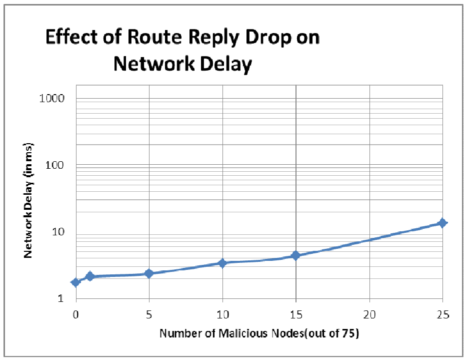

Fig. 4: Study of End to End Delay with number of malicious nodes in a network with DSR routing algorithm while keeping other parameters constant as Number of Nodes =75, Speed = 20 KMPH, Network Size= 04 KM^2 (square area) and Number of Active Calls= 07.

Case 4: Maliciously dropping data packets

The transport layer in the network architecture is modelled 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 E2E Delay. The E2E Delay is plotted with respect of number of malicious nodes (Fig. 6).

It was observed that with increase in number of malicious nodes E2E Delay increases but remains in acceptable range. One important point worth mentioning would be that we are employing RTP/UDP transport layer. UDP is an unreliable protocol which do not ensure and hence acknowledges successfully delivery. The RTP is used to induce some sort of reliability but the system still is not as reliable as with TCP. But the problem is TCP cannot be employed in bandwidth constrained systems and hence we have to depend on UDP. Overall a packet loss almost means a permanent loss and end-to-end delay is modelled for those packets which are successfully delivered and hence dropping of data packets does not show that much of effect on E2E delay curve.

Case 5: Maliciously dropping control packets

The E2E Delay is plotted with respect of number of malicious nodes (Fig. 7). It was observed that effect of increasing number of malicious nodes is not that prominent

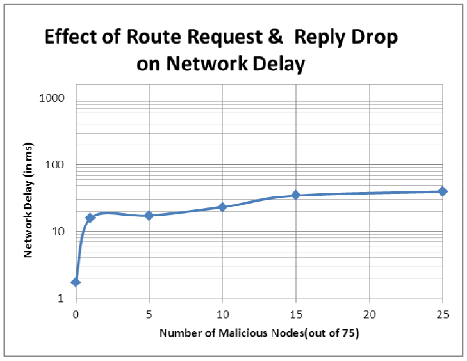

Fig. 5: Study of End to End Delay with number of malicious nodes in a network with DSR routing algorithm while keeping other parameters constant as Number of Nodes =75, Speed = 20 KMPH, Network Size= 04 KM^2 (square area) and Number of Active Calls= 07.

on E2E Delay still it causes network performance to deteriorate in terms of E2E Delay and it keeps on attaining acceptable values even with 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.

Different mechanisms employed by various types of malicious nodes 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 route request packets hurts most in terms of E2E Delay. But the malicious nodes do not affect the overall value of E2E delay so that it becomes unacceptable. This fact can be explained by the very definition of E2E delay in which delay for those packets which are successfully delivered is only considered. The packets that were never delivered do not contribute to overall delay and hence such a study would not reveal the true picture of the system and one must try and model both E2E delay and Packet delivery ratio to study the actual effect of malicious nodes on the performance a mobile ad-hoc network carrying packet telephony. Though it was observed that every 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.

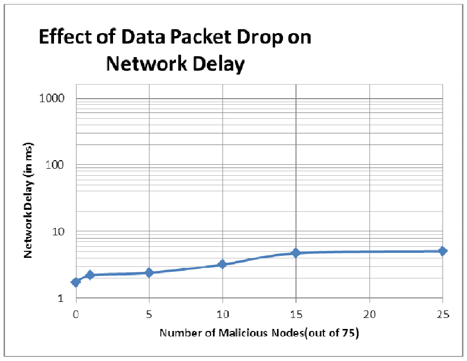

Fig. 6: Study of End to End Delay with number of malicious nodes in a network with DSR routing algorithm while keeping other parameters constant as Number of Nodes =75, Speed = 20 KMPH , Network Size= 04 KM^2 (square area) and Number of Active Calls= 07.

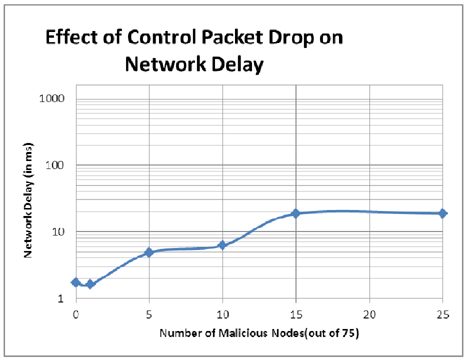

Fig. 7: Study of End to End Delay with number of malicious nodes in a network with DSR routing algorithm while keeping other parameters constant as Number of Nodes =75, Speed = 20 KMPH , Network Size= 04 KM^2 (square area) and Number of Active Calls= 07.

VI. References

[1] Jori Liesenborgs, “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] 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.

[6] 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.

[7] Juhana Mattila, “Real-Time Transport Protocol”, Oct 2003.

[8] 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.

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

[10] “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

[11] 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.

[12] 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.

Sandeep Maan (sandeep.mann23@gmail.com) is presently working as Assistant Professor in the Subject of Computer Science at Govt. P.G. College, Sec-14, Gurgaon. He is pursuing PhD in the subject of computer science in the area of mobile ad-hoc networks.

Dr. P.K. Suri is working as Chairman, Department of Computer Science & Applications at Kurukshetra University, Kurukhetra. He is also dean of faculties of Science & Engineering. He has decades of research experience.