International Journal of Soft Computing 8 (4): 247-251, 2013
ISSN: 1816-9503

Performance Evaluation of Multimedia Data in Hetrogeneous Network Using Multicasting with Kerberos Protocol

[1]R. Pugalenthi and [2]T.V. Gopal
[1]Department of Computer Science and Engineering,
St. Joseph's College of Engineering, Chennai-600119, Tamilnadu, India
[2]Department of Computer Science and Engineering, College of Engineering,
Anna University Chennai, Chennai-600025, Tamilnadu, India

Abstract: With the ever increasing demand in multimedia transmissions such as video, audio, image and text, researchers are in need to check the scalability, reliability and the quality of service in heterogeneous networks using multicasting protocols. Researchers have used the Kerberos authentication protocol to enhance the security of the network as the nodes in the network are increased. Three algorithms, Dvmrp, Ant Colony algorithm and Link State algorithm were analyzed for different multimedia with increase in nodes. Different metrics were used and calculated. The heuristic approach for different multimedia algorithms has a significant improvement in performance over earlier approach.

Key words: Multicasting, scalability, reliability, Qos, heterogeneous networks, Kerberos protocol and multimedia

INTRODUCTION

The demand for multimedia services has been increasing a lot in the last few years (Ge *et al*., 2004). Typical multimedia applications are online learning, conferences, gaming, audio, etc. These applications need data to reach the end user or receivers efficiently and with quality. With the increase in demand of these applications, the need to deliver such media through multicast rather than unicast has increased. Unicast protocols involve high costs which makes it unreliable for mass distribution. Hence, multicasting is the best solution for servicing multimedia applications. It has known to device maximum benefit from many applications such as video conferencing, real time multimedia applications and distributed interactive simulations. These applications are focused on utilizing certain inherited characters of a multicast protocol to maintain scalability as the number of end users increase and in turn increase the reliability and Qos (Shaha *et al*., 2001).

The performance of a multicast protocol in terms of scalability and security is a relatively complex job. For this, researchers have defined some metrics which will help determine the efficiency and performance in terms of scalability (Farrugia and Cutajar, 2011), reliability and Qos. The metrics for a multicast traffic can be developed from multiple perspectives for the three algorithms. One is the network provider who is interested in network resource usage. Another is the end user perspective who is concerned with quality and availability of services. The three algorithms coming under multicast protocols are described and evaluated and the best algorithm is found. Distance Vector Multicast Routing Protocols (DVMRP), Link state routing protocol and ant-colony based routing protocol are the three algorithms analyzed. With increase in devices supporting multicast protocols, performance evaluation model can help to determine which protocol has to be used in any given network condition/state.

Since, the number of members in a multicast protocol is highly dynamic and increase in number of receivers increases the complexity of maintaining the scalability. Scalability is one of the most important factors governing the efficiency of multicast networks (Ge *et al*., 2004). Scalability can be defined as the ability of a network to adjust or maintain its performance as the size of the n/w increases and the demands upon it become greater and greater. Since, homogeneous network is vulnerable to malicious attacks, the study will focus on heterogeneous networks in which each critical functionality is provided by a diverse set of protocols and implementation attacks. The computers available on a network may be made by different sellers or have different compilers. When a programmer wants to develop a collection of networked computers, he may have to compete with different types of heterogeneity like architecture, data format, computational speed, machine load and network load. The study also focuses on Kerberos whose primary purpose is to provide a secure network authentication service.

Corresponding Author: R. Pugalenthi, Department of Computer Science and Engineering, St. Joseph's College of Engineering, Chennai-600119, Tamilnadu, India

Single user sign in and protection of authentication information is done so that masquerading is far more difficult.

LITERATURE REVIEW

The foremost multicast routing protocols is the DVMRP (Sahasrabuddhe and Mukherjee, 2000) that employs RPM to send multicast packets. The metrics and threshold are used to specify the cost of routing and for constructing the RPST. The threshold is the minimum Time to Live (TTL) a multicast packet needs to be forwarded on to a given link. The threshold is used to limit the geographical scope of a multicast transmission. The other algorithm commonly known is the OLSR (Optimized Link State Protocol) (Munaretto *et al*., 2002). It is a proactive routing protocol for mobile Ad Hoc Networks. Such protocol is adopted for the reason that it reduces the size of the control messages and minimizes the overhead from flooding of control traffic. The protocol inherits stability of a link state algorithm and had the advantage of having routes immune available when needed due to its proactive nature OLSR is an optimization over the classical link state protocol, tailored for mobile Ad Hoc Network. The final algorithm studied is the ant colony algorithm (Lijuan *et al*., 2010). The basic idea of this algorithm is based on how ants release certain phenomena's along the path they passed when finding food according to the intensity of the pheromone, the follow up ants choose the path. The path with more intense phenomenon is more likely to be chosen forming a kind of positive feedback mechanism. Ultimately ants will choose the path which has the most intensive pheromone. The algorithm provides new idea to solve the problem of combinatorial optimization and currently has a wide range of applications in WSN as well. In the wireless transmission, the sent power decays exponentially as the distance increases. In this study, researchers use the Free Space Model. When the source has packets to mail to the sink node, the following equations should be followed Eq. 1:

$$P_r = P_t\left(\frac{\lambda}{G\pi d}\right)^2 \frac{G_r G_t}{L} \quad (1)$$

Where:

P_r = Power of destination node
P_t = Sending power of source antenna
λ = Length of carrier wave
d = Distance between source and the sink node
G_r = Gain of source antenna
G_t = Gain of sink antenna
L = Factor of software consumption, $L \geq 1$

Researchers mentioned the use of Kerberos authentication protocol same modifications related to this protocol is also discussed. The principles secret key will be independent of the user password to overcome the weak passwords chosen by the network principal that are susceptible to password guessing attacks, the main drawbacks of the Kerberos protocol. Instead the Kerberos distribution centre saves a profile for every instance in its realm to generate the principles secret key by hashing the profile and encrypting the output digest. The Kerberos authentication protocol allows a client to repeatedly be authenticated to multiple servers assuming that there is a long-term secret key shared between the Kerberos in fracture and the client. The client's password is used to generate the client long-term secret key.

In the first phase, the client sends a request to the Authentication Server (AS) requesting a ticket generating ticket TGS to be used in the second phase with the TGS. The AS is expected to reply with a message consisting of a ticket granting ticket (tgs) of lifetime and an encrypted component containing a fresh session key K_C, tgs to be shared between the client and the TGS. In the second phase, the client forwards the ticket granting ticket along with the authenticator, encrypted with the session key K_C, tgs obtained in the first phase to the TGS, requesting a service ticket to be used in the third phase with the application server. The third phase, the client forwards the application server ticket, along with a new authenticator $\text{Authenticator}_{C2}$ encrypted with the session key obtained in the second phase $K_{C,V}$ to the application server ticket plus the secret session key are the client's credentials to be authenticated to a specific application server. It is concluded from the performance analysis of the Kerberos protocol (El-Hadidi *et al*., 1997) in a distributed environment that improved throughput and delay characteristic can be achieved by using efficient implementations of the Kerberos protocol, together with multiple sessions for each access of the Kerberos server.

The focus of these researches is towards quantizing the protocol's performance for cost estimation and billing. Two important factors analyze is how certain inherited characteristics of a multicast protocol can be helpful in providing the desired Qos (Mohammad and Woodward, 2009) to multimedia application and to provide scalability as the no. of users in an heterogeneous network increases. For a more accurate analysis of multicast protocol both the network load and the quality of service that a multimedia.

IMPLEMENTATION AND OPERATION OVERVIEW

The network consists of a huge number of end-users. Different users transmit different forms of multimedia data in different ways using multicasting protocol. There is no fixed time for this transmission; it can happen anytime.

Therefore, researchers have risks of traffic overloading which can lead to poor Qos and less scalability thus reducing the reliability. Also, as there are many users accessing the network at the same time, there is the problem of security. Users should not be able to break into anonymous network easily. Thus, the study mainly focuses on maintaining the scalability and in turn, reliability and Qos when using these multicast protocols even when the number of end users is increased. By using Kerberos protocol in the network, researchers ensure security and unwanted break in by other users in the network. Researchers propose a model and define the metrics depending on the algorithms, researchers study in this study to get a clear idea which multicast protocol is the best for which multimedia transmissions.

METRICS

Researchers have proposed a routing model that evaluates the protocols performance and efficiency. This model was developed from the network providers perspective and as well as to the end users perspectives. The model acts as the representative for both network cost and the Qos outlay by the end user. The ambiguity is prevented by denoting the efficiency of a multicast protocol as:

$$\varepsilon(m) = W_n \cdot X(m) + W_q \cdot Y(m) \quad (2)$$

Where:

ϵ = Efficiency of a multicast protocol m
X(m) = Network load cost of a multicast protocol m
Y(m) = Qos experienced by the user while protocol m is serving

$$W_n + W_q = 1 \quad (3)$$

W_n, W_q the weights assigned to each component.

Network load and cost: The measure of network resource utilization by a multicast protocol and the cost of resources (Shaukt *et al*., 2009) utilize within a given network scenario. Mathematically, it can represented as follows:

$$X(m) = N_r(m) + S_c(m) + C_t(m) \quad (4)$$

Where:

X(m) = Network load cost
$N_r(m)$ = Link traversed
$S_c(m)$ = Storage cost of the multicast states maintained by the router
$C_t(m)$ = Percentage of overhead traffic generated as control messages

Traffic overhead: Unicast routing generates infrequently overhead traffic or control messaging. This is not the possible in case of multicast. In multicast some type of control messaging has been provided for creating, managing and updating the multicast tree. The overhead traffic has been calculated using the equation which is given (Shaukt *et al*., 2009):

$$C_t = \left(\frac{\alpha}{\alpha + \text{user data}}\right) \times 100 \quad (5)$$

Jitter: If streams of packets, i.e., audio or video files are communicated in a network each packet may incident different delay, this variation in delay is called as a jitter or delay jitter. The audio and video transmission requires synchronizations to the received data (Shaukt *et al*., 2009). The jitter can be measured by the ration between the jitter incidents in the unicast to that of multicast:

$$J(m) = \frac{\text{Avg. jitter in unicast stream}}{\text{Avg. jitter for multicast protocol}} \times 100 \quad (6)$$

Latency: Latency is calculated the no. of hops and the hop delay. Latency should be directly proportional to the number of hops. The latency shows how many times a message has to be relayed which is a resource utilization issue:

$$\text{Latency} = \frac{1000 \times \text{Distance}}{299792.458\ (\text{msec})} \quad (7)$$

Packet loss: Packet loss is said to have occurred when one or more packet travelling across a network fail to reach the destination from source. TCP protocol provides a reliable mode of transmission. It requests for the retransmission of data or the sender retransmits the data when the packets acknowledgement is not received for a certain fixed time of periods. The only drawback is that when the packets are retransmitted again, it also sends all the packets sent after that packet. This can cause a decrease in throughput to drop. In state x, the intensity of loss traffic is equal to x×c-C if x×c>C and to 0 otherwise; the estimate for packet loss rate is:

$$L = \frac{\sum_{x:x\times c>C} (x\times c - C)\, \pi(x)}{\sum_x (x\times c)\, \pi(x)} \quad (8)$$

NETWORK AND SIMULATION CHARACTERISTICS

Latency: Table 1 gives the variation in latency for different protocols as the nodes are increased. Keeping a packet size and bandwidth, researchers find that the latency is constant for all the protocols as the nodes are increased. Figure 1 show this latency change in graph

Table 1: Latency

No. of receiver	DVMRP	Ant colony	Link state
10	0.27	0.47	0.25
20	0.27	0.47	0.25
30	0.27	0.47	0.25
40	0.27	0.47	0.25
50	0.27	0.47	0.25
60	0.27	0.47	0.25

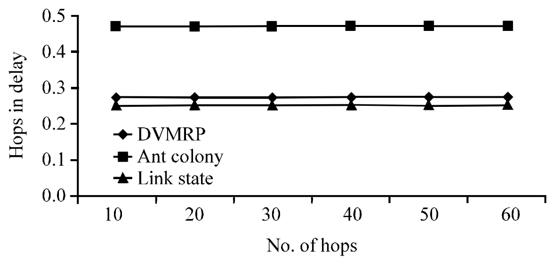

Fig. 1: Latency

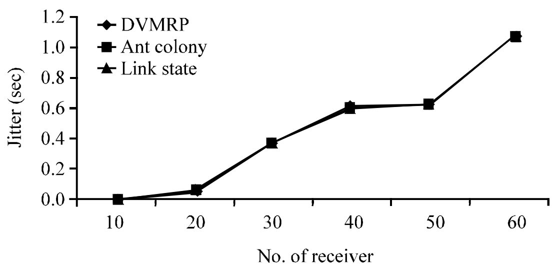

Fig. 2: Delay jitter

form and researchers conclude that link state protocol has the least latency and it remains constant even as the nodes are increased.

Jitter: Table 2 gives the variation in jitter for different multicast protocols as the node is increased, researchers keep the packet size and bandwidth constant. At first, with 10 nodes, there is no jitter. But as the nodes increases, jitter also varies. Figure 2 shows the variation for jitter change and ant colony algorithm has the least variation and it is the best suited for multimedia transmission.

Packet loss: Table 3 shows the packet loss in multimedia transmission using three different protocols. Yet again, researchers maintain the packet size. As the nodes increase, there is no variation in the packet loss. Figure 3 plots the graph for this variation and researchers find that there are two protocols, DVMRP and the link state protocol that offers less packet loss in multicasting network.

Network cost: Table 4 gives the cost for each transmission as the No. of nodes is increased. By maintaining packet size and bandwidth, researchers wish to achieve least cost for transmission. Figure 4 plots the graph for the values in Table 4 and researchers conclude that DVMRP offers the least cost and very little variation compared to other algorithms as the nodes are increased.

Table 2: Delay jitter

No. of receiver	DVMRP	Ant colony	Link state
10	0	0	0
20	0.0625	0.0623	0.0627
30	0.3711	0.3716	0.3709
40	0.5979	0.5945	0.5934
50	0.6230	0.6236	0.6238
60	1.0841	1.0844	1.0845

Table 3: Packet loss in kB

No. of receiver	DVMRP	Ant colony	Link state
10	0.047712	0.047812	0.047712
20	0.047712	0.047812	0.047712
30	0.047712	0.047812	0.047712
40	0.047712	0.047812	0.047712
50	0.047712	0.047812	0.047712
60	0.047712	0.047812	0.047712

Table 4: Overall cost network performance

No. of receiver	DVMRP	Ant colony	Link state
10	1	3	4
20	3	5	5
30	1	7	7
40	3	8	6
50	2	4	8
60	1	6	5

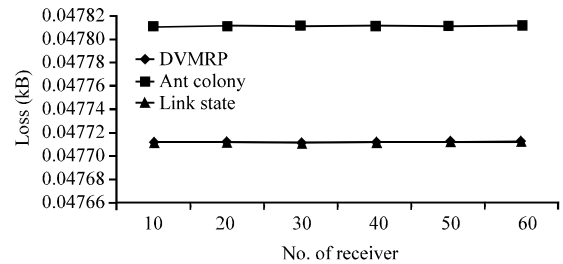

Fig. 3: Packet loss

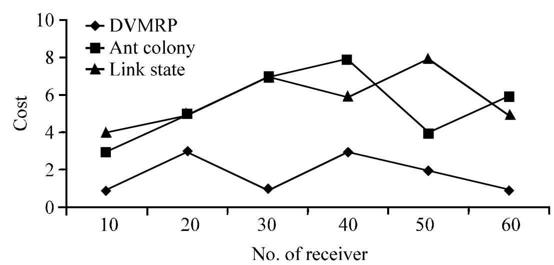

Fig. 4: Overall cost network

CONCLUSION

In this study, researchers have defined a model to evaluate multicast protocols performance in all spheres of multimedia transmissions, i.e., audio, video, text, image. Researchers have concluded that there is no fixed algorithm for multimedia data transmission. As the number of end users increase, different algorithms based on the metrics calculations are found. The model was developed around the concept of comparing the cost of delivering multimedia data through multicast traffic and how bandwidth, latency, jitters, loss in KB and efficiency effect transmission. In future research, researchers use rekeying to enable the increase in security. Also, as researchers analyze how the increase in nodes, say 500, researchers can achieve scalability, reliability and the Qos.

REFERENCES

El-Hadidi, M.T., N.H. Hegazi and H.K. Aslan, 1997. Performance analysis of the Kerberos protocol in a distributed environment. Proceedings of the 2nd IEEE Symposium Computers and Communications, July 1-3, 1997, Alexandria, pp: 235-239.

Farrugia, R.A. and L. Cutajar, 2011. Scalable video coding transmission over heterogeneous networks. Proceedings of the 3rd International Conferences on Advanced in Multimedia, April 17, 2011, Iaria, pp: 124-129.

Ge, Y., L. Lamont and L. Villasenor, 2004. Improving scalability of heterogeneous wireless networks with heirarchical OLSR. Proc. WIMOB, 5: 1-4.

Mohammad, A.H. and M.E. Woodward, 2009. Localized QoS routing and admission control: Performance evaluation. Proceedings of the 6th International Conference on Innovations in Information Technology, December 15-17, 2009, Al Ain, pp: 75-79.

Munaretto, A., H. Badis, K. Al Agha and G. Pujolle, 2002. A link-state Qos routing protocol for Ad Hoc networks. Proceedings of the 4th International Workshop on Mobile and Wireless Communications Network, September 9-11, 2002, Washington, USA., pp: 222-226.

Sahasrabuddhe, L.H. and B. Mukherjee, 2000. Multicast routing algorithms and protocols: A tutorial. Network IEEE, 14: 90-102.

Shaha, N., A. Desai and M. Parashar, 2001. Multimedia content adaptation for QoS management over heterogeneous networks. Proceedings of the 3rd International conference on Internet computing, June 2001, CSREA Press, USA., pp: 642-648.

Shaukt, U., A. Qayyum and S. Hussain, 2009. Performance evaluation of multicast protocols for multimedia traffic. Proceedings of the International Conference on Emerging Technologies, October 19-20, 2009, Islamabad, Pakistan, pp: 383-388.