International Conference on Computer and Communication Engineering (ICCCE 2010), 11-13 May 2010, Kuala Lumpur, Malaysia

Network Security for QoS Routing Metrics

I.A. Almerhag
Computer Engineering Department
Naser Nations University
Trhoona, Libya
almerhag@yahoo.com

A.M. Goweder
Computer Department
Institute of Comprehensive professions
Surman, Libya

A.A. Almarimi
IT Department
Higher Institute of Electronics
Baniwalid, Libya

A.A. Elbekai
IT Department
Higher Institute of Technology
Tripoli, Libya

Abstract— **Data security is an essential requirement, especially when sending information over a network. Network security has three goals called confidentiality, integrity and availability (or Access). Encryption is the most common technique used to achieve this goal. However, the computer society has not yet agreed on a standard method to measure data security.**

The ultimate goal of this study is to define security metrics based on different aspects of network security, and then demonstrate how these metrics could be used in Quality of Service (QoS) routing to find the most secure path connecting two distant nodes (source and destination) across an internetwork.

Three security metrics are proposed in this document, these metrics have been derived from three important issues of network security, namely: authentication, encryption and traffic filtration techniques (firewalls and intrusion detection systems). The metrics follow different composition rules in that the first is binary, the second is either concave or additive and the last is multiplicative.

Routing algorithms that make use of such metrics have been implemented in the C# programming language to test the viability of the proposed solution. Computational effort and blocking probability are the most commonly used performance measures were used to assess the behavior and the performance of these routing algorithms.

Results obtained show that the algorithms were able to find feasible paths between communicating parties and helped in making reasonable savings in the computational effort needed to find an acceptable path. Consequently, higher blocking probabilities were encountered, which is thus the price to be paid for the savings.

Keywords- QoS routing; routing metrics; security metrics.

I. INTRODUCTION

Quality of Service (QoS) routing is a well known problem and much research has been done in the area. It is concerned with finding a path across a network for a message to follow starting at a source node till it reaches its final destination. Moreover, that path has to satisfy a set of requirements specified by the application. This process relies on a routing algorithm that uses topological data collected, also called metrics or weights, in the first phase.

The available routing algorithms use conventional metrics like delay, bandwidth, cost and, packet loss. This study is motivated by the fact that network security has not been used as a QoS routing criterion. In addition, researchers in the fields of computer communication and data security have not agreed on a definition of a security metric(s) that could be used for finding the most secure path across an interconnected network.

A. *QoS Routing*

There is no common or formal definition of quality of service routing. However, there is a number of definitions at the communication level [1, 2, 3, 4]. The main goal of QoS is to provide different services to different network traffic over various technologies. Emerging networks, such as Asynchronous Transfer Mode (ATM), can provide QoS guarantees on bandwidth and delay for the transfer of continuous media data [3]. Basically, QoS is a collection of technologies that allow applications to request and receive predictable service levels in terms of data throughput capacity (bandwidth), latency variations (jitter), cost, reliability and delay [1].

In the case of routing, each forwarding decision is associated with a particular service response, so that a "best-effort" path to a particular destination address may differ from a "low-latency" path, which in turn may differ from a "high-bandwidth" path, and so on.

B. *Routing Metrics*

A routing metric is a number associated with a route indicating the goodness of that route. If more than one route to a destination are available then the route with the lowest metric is considered the best [5]. Using bandwidth is the simplest way to describe QoS. However, it is not good enough to define QoS using a single metric only. Practically, a number of metrics are used to express the concept of QoS. Examples of typical metrics are packet loss rate, delay and jitter (or variation in delay) [6]. The computation of path metric value depends on

978-1-4244-6235-3/10/$26.00 ©2010 IEEE

the individual metric performance. Three main types of metrics are defined; these are: additive, concave and multiplicative. Typical examples of these metrics are delay, bandwidth and packet loss respectively [7]. But, what makes a good metric? Jelen claimed that good metrics are those known to be Specific, Measurable, Attainable, Repeatable, and Time-dependent (SMART) [8].

II. Security Metrics

Generally, the need for information security and trust in computer systems is described in terms of three fundamental goals: Confidentiality, Integrity and Access/Availability (CIA) [9, 10, 11].

Lowans in [12] talked about a network security cycle where he suggested ten metrics; few of them are: number of unsuccessful logons, number of guessed passwords, number of security policy violations. In the light of the definition of network security and the three goals of network security; most if not all of these metrics are designed for management purposes with risk assessment in mind. They are applicable at application level only and they do not reflect on the state of network security at a lower level like: the level of security of a communication link and do not show how secure a certain node could be.

From the point of view of a routing algorithm, a good metric should represent the value of a network security parameter; this is analogous to a typical routing metric which corresponds to a physical network parameter like bandwidth, delay or packet loss. Therefore, three metrics are proposed in the following sections to show to what extent the goals of network security have been maintained by the system under consideration, followed by a detailed explanation of how these metric could be used in QoS routing.

III. The Proposed Security Metrics

In previous studies [13, 14, 15, 16, 17], the notion of security metrics was mentioned for the sake of developing multi-metric routing algorithms. Since it was beyond the scope of their work and because the problem was poorly researched, the metrics they used were oversimplified and imprecisely defined. It had been represented using a single valued metric; while [14, 15] proposed a value between 0 and 1; in [13] a binary value was used. Moreover, different authors apply different composition rules to the proposed security metric; the authors of [15] claimed that security is an additive metric but [13] treated it as a binary metric and [14] as a bottleneck (concave) metric.

Since the status of network security is quite complicated, it cannot be verified using a single feature. So, any effective security metric should integrate a number of important aspects of security to form either: a single compound metric or a collection of metrics each measuring a specific aspect of network security. In this study, the second approach has been adapted for the proposed security metrics; since a compound metric tends to lose the details as a result of the aggregation whereas the multi-metric approach will preserve the detailed state of the network as measured by each metric.

Three important issues of network security, among different security aspects, the router authentication protocol, encryption (precisely the key size) and access control systems have been used to define the security metrics [18, 19]. The selected features are those which can demonstrate to what extent the three goals of data security (CIA) have been maintained by a specific information system.

The three metrics are defined based on three important aspects of security; as encryption guarantees the confidentiality of data during transmission, neighbor router authentication ensures and validates the identity of the communicating party and traffic filtration and control techniques maintain the availability of information or service.

A. Traffic Filtration Systems

This includes the use of access control lists (ACL), Intrusion Detection/Prevention systems (IDS/IPS) and firewalls to enhance the overall level of network security. This is achieved by examining every single packet of the incoming and outgoing traffic against a predefined criteria that will result in either forwarding that packet or dropping it [20]. Firewalls can protect the network from routing based attacks [21] on the other hand; IDSs detect with high accuracy those attacks with known patterns only, like Denial of Service (DoS) attacks [22].

Basically, each node along the path may enclose a firewall and/or an IDS. So, the metric value (W_i) of all links leaving that node is given by equation (1); where P_{fw} and P_{ids} respectively are the probability that the firewall will prevent an attack and the IDS will detect an attack and react accordingly.

$$W_i = 1 - \lfloor P_{fw} + P_{ids} - (P_{fw} \times P_{ids}) \rfloor \cdots\cdots\cdots (1)$$

For example, assume that a properly configured firewall router will eliminate 84% of common breaches and an IDS will protect the system from 79% of known attacks. Clearly, there will be a significant number of attacks that are preventable by both techniques; this leads to the conclusion that this node is vulnerable to 3% only of the total number of known attacks.

B. Key Length

Any cryptographic system consists of an encryption algorithm and a secret (or secret and public) key(s). These elements determine the strength of that system also. However, for the sake of this study the algorithm is assumed not to have any built-in weaknesses. This makes the key size as the only factor that influences the strength of any cryptographic system. As a result of the rapid technological advancement in electronics, especially in information technology; more and more sophisticated tools have become available to hackers and crackers, like powerful computers at affordable price, even parallel computing facilities and electronic devices specially designed to break codes.

According to Moor's law, the computing power is doubled every 18 months [23]. And clearly adding an extra bit to the key-size doubles the number of possible keys. Therefore, to maintain today's data security levels, the key size used for encryption should also grow in response to that achievement.

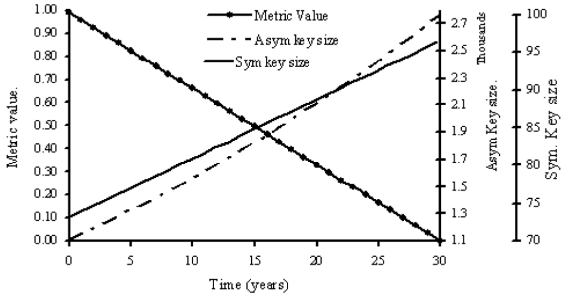

Figure 1. The metric value over the next thirty years.

So, the key length must be increased by a single bit at-least every doubling period. All links leaving a node are assigned a metric value that falls in the range between zero and one, inclusive. Where zero denotes a secure link and vice versa. At one extreme, a node is considered to be secure if it uses a key that can maintain the required security level for the next thirty years. At the other extreme, it is vulnerable when the key used is below the recommended key size. Between the two margins, there exists a linear relationship between the metric value and time in years that a key could maintain an acceptable level of security, as shown in Figure(1).

Such a value could be calculated using equation (2) [24].

$$W_i = \begin{cases} 1 & \textit{if the size of key used} > \textit{the recommended size} \\ 0.99 - 0.033\,y & \textit{otherwise} \end{cases} \qquad (2)$$

Figure (1) demonstrates also the growth of key size over the next thirty years for symmetrical and asymmetrical key systems; it also shows the relationship between time and the metric value. The idea behind assigning a metric value of zero to a secure node or value of one to a vulnerable one, is to be able to use the shortest path algorithm to find the least vulnerable (clearly the most secure) path across a network.

C. Device Authentication

It is an important issue in network security because routers exchange routing updates regularly. Therefore, device authentication is used to guarantee that routers receive reliable routing information. Otherwise, the security of the whole network could be compromised. If for example, an unauthorized or deliberately malicious data fabricated by an unfriendly party were used to update the routing tables. The network traffic then could be diverted to a cruel destination, where confidential information may be revealed or simply the updates are used to prevent the network from functioning effectively.

This metric will have a binary value, that is the metric value is true (or 1) if the authentication protocol is using MD5 to exchange information between neighbor routers and the metric value is false (or 0) otherwise, as described in equation(3).

$$W_i = \begin{cases} 1\, \textit{if MD5 is used} \\ 0 \qquad \textit{therwise} \end{cases} \qquad (3)$$

The proposed metrics have implemented and sustained the five features (SMART) that a good metric should have.

IV. Use of The Metrics

Wang and Crowcroft have defined three types of metrics and associated with them a set of composition rules. Typically, each metric obeys a single composition rule; for example delay is additive, bandwidth is concave and probability of packet loss is multiplicative [7].

Two approaches are possible to deal with the three security metrics that have been defined earlier; either by combining them into a single compound metric or leave them as separate metrics. While the compound metric represents the whole situation using a single value, which eases the process of path computation. The latter choice is preferable since this preserves the details of every measured network characteristic.

The three sections below explain the different composition rules which each metric follows; where W_p is the metric value of the entire path and W_i is the weight of link i.

A. Traffic Filtration Systems

Access control follows a multiplicative composition rule and the path's metric value is given by equation (4).

$$W_p = 1 - [W_1 \times W_2 \times W_3 \times \cdots\cdots \times W_n] \qquad (4)$$

B. Key Length

Encryption can be treated either as an additive metric or as a bottleneck characteristic. So, the additive or the concave composition rule could be applied to this metric. If a path is considered to be as secure as the weakest link amongst those links forming that path then the concave composition rule is applicable, so the path will have a metric value given by equation(5).

$$W_p = Min\,[W_1, W_2, W_3, \cdots\cdots, W_n] \qquad (5)$$

Clearly when comparing different paths, the path with the smallest number of hops is preferable to others if all links have equal metric values, because the smaller the number of hops is the lower is the chance that a breach could take place. This implies that the metric value of a path could be calculated using equation (6).

$$W_p = \sum_{i=1}^{n} W_i \qquad (6)$$

C. Device Authentication

Neighbor router authentication is a binary metric. So, if the application/user requires a path that uses a secure router authentication protocol, then this metric value should be true for all links forming that path. In other words, the path metric value could be computed using the logical AND operation given by equation (7).

$$W_p = W_1 \otimes W_2 \otimes W_3 \otimes \cdots\cdots \otimes W_n \qquad (7)$$

V. The Routing Algorithms

Most available routing protocols use the shortest path algorithm like Dijkstra or Bellman-Ford to solve the routing problem. These algorithms need to know about the complete structure of the network to be able to find the best path [25, 26]. To the best of the author's knowledge, the problem of QoS routing based on network security has not been studied in this context yet. Therefore, three different solutions have been proposed and implemented based on the metrics defined earlier in a specific order to minimize the complexity of the path computation phase.

These solutions facilitate the process of testing, comparing and benchmarking the solutions and ultimately draw conclusions.

Depending on the way the key size security metric is treated, three versions of this algorithm have been designed. While the first considers key size as a bottleneck parameter the other two consider it as an additive metric. All versions of this algorithm consist of three steps; in the first phase, all links that do not use MD5 to exchange routing updates are removed if the application specifically requires that. The subsequent phases depend on the way the key size metric is treated and the way the other two metrics have been ordered.

A. Binary-Concave-Multiplicative (BCM) Algorithm

When the key size metric is dealt with as a bottleneck characteristic, all the links that do not satisfy the application's requirement (having key size smaller than the required value) are also removed. Finally, Dijkstra's algorithm is applied to the simplified network to compute the shortest path between the source and the destination nodes within the remaining network based on the third multiplicative metric (traffic filtration technique).

B. Binary-Additive-Multiplicative (BAM) Algorithm

Here the key size is treated as an additive metric. Therefore, if a path metric value exceeds the QoS metric value specified by an application that path is dropped. Otherwise, the path's third metric value is checked for the satisfaction of the QoS requirements as before. If that is the case, then a suitable path has been found, if not this process should start over again.

C. Binary-Multiplicative-Additive (BMA) Algorithm

This version works the same way as the previous one with the exception that the second and third metrics are evaluated in the reverse order. So if a path that satisfies the multiplicative metric has been found the algorithm examines the value of the additive metric to ensure that that value fulfils the application's needs.

VI. THE SIMULATION

Selecting a model for a particular study depends basically on several factors including the nature of the study to be performed, the size of the required generated topology, the weight certain characteristics of the generated topologies may have [27].

To represent real interconnected networks, the simulation was designed to generate networks having a number of nodes ranging from 10 to 100. These nodes are randomly distributed on a plane. Then the process of assigning a link between each pair of nodes is governed by Doar's model [28]. The goal is to generate a network that is very close to a real wide area network. The simulation operates only on connected networks that have at least a single path between any pair of nodes and that network should have an average node degree of 4, which equals the node degree of the Internet [29-31]. Then the routing algorithm is applied to the generated random network, and statistics about computational effort and blocking probability are collected.

This process, network generation and data collection, is repeated 100,000 times for each network size and for each algorithm. Specifically, each run is divided into ten samples where a hundred random networks are generated per sample.

Then ten different source/destination combinations are selected per topology and the weights are also changed ten times for each network. Finally, the average values of the computational effort and the blocking probabilities that have been collected throughout the running period of the simulation are calculated and then saved in a data file.

VII. THE RESULTS

Two of the mostly used performance measures are employed in this work; namely, computational effort and blocking probability; these measures were used to evaluate the performance of the proposed algorithms. During the simulation, the values of the previously mentioned performance measures are collected and then the average values of the computational effort and the blocking probability are computed for that run. Finally, the 95% confidence levels for those measures, per network size, have been calculated using the ten different samples.

A. The Computational Effort

The results obtained from both BAM and BMA algorithms are quite close to each other (see Figure 3), since the effort needed to find a path in both cases is almost the same as the only difference between them is the order in which the metrics are satisfied. However, BCM has better performance in terms of the computational effort needed to find a feasible path which is because the latter algorithm takes advantage of the concave metric to reduce the size of network before it starts looking for a satisfactory path within a simplified network. The other two algorithms have to search the full network before any feasible path could be found.

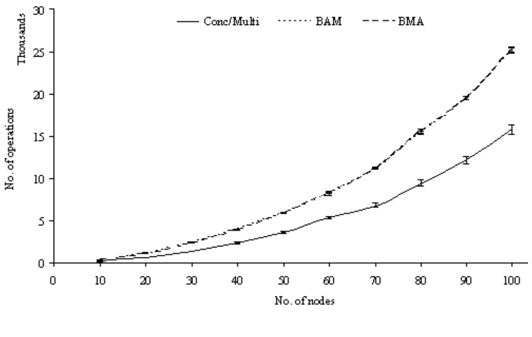

Figure 2. Computational effort of the three algorithms.

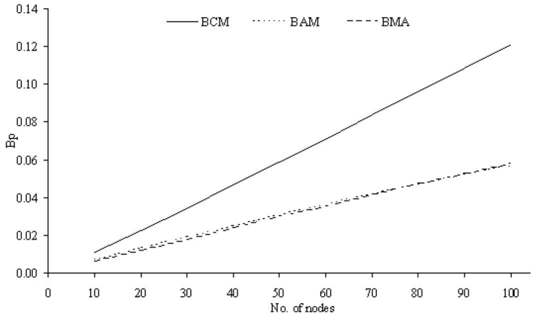

Figure 3. Blocking probability of the three algorithms.

B. *The Blocking Probability*

The value of the blocking probability for a given network is expected to increase as a result of reducing the size of the network. Because the total number of routes available for choosing by the routing algorithm decreases, hence the probability of finding an acceptable path decreases too.

The three figures (5-7) below show the behavior of each algorithm as the criteria for satisfying the key-size and traffic filtration techniques requirements become tighter. In both cases (loose, tight), the simulation randomly generates the QoS requirement values. In the first case ”loose”, the values generated are not restricted at all under these conditions each metric value can be between zero and one. However, under the ”tight” arrangement the metrics values assigned can have a random value within the range (0, 0.5). Results show that by tightening the QoS requirements the blocking probability increases as this would limit the choices available to the routing algorithm because all the links that do not satisfy the requirements are eliminated by the path computation process. Because satisfying the concave metric has an effect on the network topology. The BCM algorithm has been outperformed by the other two algorithms in terms of this performance measure that could be considered as the price been paid for having reduced the computational effort. Consequently, a balance between the number of failed connection attempts and the computational effort gained should be maintained**.**

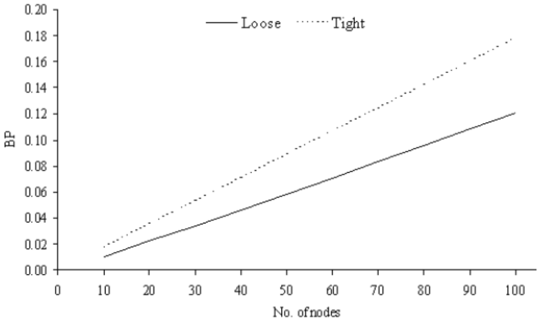

Figure 4. BCM tight versus loose QoS requirements

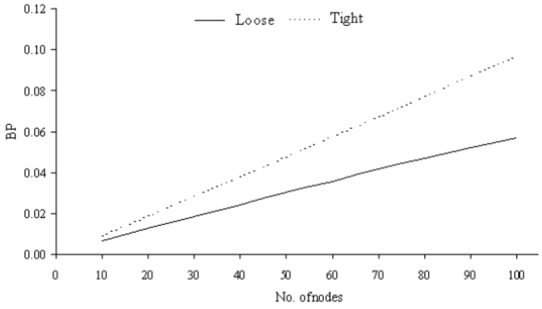

Figure 5. BAM tight versus loose QoS requirements.

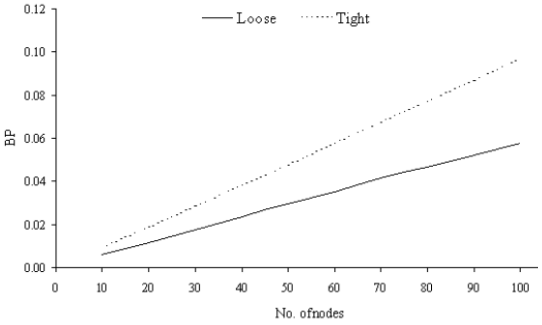

Figure 6. Figure 1. BMA tight versus loose QoS requirements.

VIII. CONCLUSIONS

Security is a complicated feature of computer networks; it cannot be characterized using a single metric. A set of three security metrics has been defined based on selected network security features, so that they can be used to find a secure path between source and destination across a network and that path satisfies the QoS constraints specified by the application.

Results show that BCM has out-performed BAM and BMA in terms of computational effort but at the price of higher blocking probabilities. That is because of the nature of the concave metric. Furthermore, the results show that the performance of BAM and BMA are almost the same since they only differ in the order of satisfying the last two metrics.

REFERENCES

[1] Cisco Systems Inc, “Network security: An executive overview," 2001. http://www.managednetworks.com/docs/networksecurityoverview.pdf.

[2] M. Hendry, Practical Computer Network Security. Norwood, MA.: Artech house, 1995

[3] B. Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C. NY.: John Wiley & Sons, 1994.

[4] A. T. Velte and T. J. Velte, Cisco: a beginner's guide. California, USA: Mc Graw Hil, Osborne, 3rd ed., 2004.

[5] B. Parkhurst, Routing first-step. Indianapolis, USA: Cisco Press, 2005.

[6] Sun Microsystems Inc, Enterprise quality of service (QoS): Part I - Internals, Mar 2005. http://www.informit.com/articles/printerfriendly.asp?p=26023.

[7] Z. Wang and J. Crowroft, “Quality-of-service (QoS) routing for supporting multimedia applications," IEEE Journal on selected areas in communication, vol. 14, pp. 1228-1234, Sept. 1996. TY-JOUR.

[8] G. Jelen, SSE-CMM Security Metrics, The National Institute of Standards and Technology (NIST) and Computer System Security and Privacy Advisory Board (CSSPAB) Workshop, Washington, D.C., June 13-14, 2000.

[9] ISO, “ISO/IEC 17799 code of practice for information security management.," 2000.

[10] The Information Security Glossary, “Confidentiality, integrity and availability." http://www.yourwindow.to/information-security/gl_confidentialityintegrityandavailabili.htm.

[11] US Congress, “Protecting privacy in computerized medical information," tech. rep., Office of Technology Assessment, 1993.

[12] P. Lowans, “Implementing a network security metrics program," 2000. http://www.giac.org/practical/Paul Lowans GSEC.doc.

[13] M. M. Al-Fawaz and M. E. Woodward, “QoS routing with multiple-constraints" in Delson Group Inc. World Wireles Congress, (San Francisco, USA.), 2002.

[14] A. Alghannam, M. E.Woodward, and J. Melor, “Security as a QoS routing issue," in Proceedings of the 2nd Annual Postgraduate Symposium (PGNet'01) (M. Merabti, ed.), The School of Computing & Mathematical Sciences, Liverpool John Moores University, 2001.

[15] A. M. Alkahtani, M. E. Woodward, and K. Al-Begain, “The analytic hierarchy process applied to best effort QoS routing with multiple metrics: a comparative evaluation," in Personal Mobile Communications Conference, 2003. 5th European (Conf. Publ. No. 492), pp. 539-544, 2003. TY-CONF.

[16] M. Baltatu, A. Lioy, F. Maino, and D. Mazzocchi, “Security issues in management, control and routing protocols," Computer Networks, vol. 34, pp. 881-894, 2000.

[17] B. R. Smith, and J. J. Garcia-Luna-Aceves, “Efficient security mechanisms for the border gateway routing protocol," Computer Communications, vol. 21, no. 3, pp. 203-210, 1998. TY - JOUR.

[18] I. A. Almerhag, and M. E. Woodward, “Quality of service routing metrics based on selected aspects of network security," in Fourth HET-NET's05 (D. Couvatsous, ed.), (Ilkley, UK), pp. P26/1-P26/7, July 2005

[19] I. A. Almerhag, and M. E. Woodward, “Security as a Quality of Service Routing Problem,” in CoNEXT’05: Proceedings of the 2005 ACM conference on Emerging network experiment and technology, (Toulouse - France), pp. 222–223, ACM Press, New York, NY, USA, 2005, http://doi.acm.org/10.1145/1095921.1095951 .

[20] Cisco Systems Inc, “Internetworking technologies handbook," 2002. http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito doc/.

[21] M. Goncalves, “Firewalls Complete.” http://www.secinf.net/firewalls_and_VPN/Firewalls Complete/ : McGraw-Hil, 2002.

[22] E. Biermann, E. Cloete, and L. M. Venter, “A comparison of intrusion detection systems," Computers & Security, vol. 20, no. 8, pp. 676-683, 2001. TY - JOUR.

[23] Wikipedia the free encyclopedia, “Moor's law," 2004. http://en.wikipedia.org/wiki/Moore's_Law.

[24] I. A. Almerhag, and M. E. Woodward, “Key length as a QoS routing metric," in Sixth informatics workshop (D. Rigas, ed.), (Bradford, West Yorkshire, UK), pp. 23-24, University of Bradford, March 2005.

[25] S. Chen and K. Nahrstedt, “On finding multi-constrained paths," in IEEE International Conference on Communications, ICC 98., vol. 2, pp. 874-879, 1998. TY - CONF.

[26] Y. Yang, L. Zhang, J. K. Muppala, and S. T. Chanson, “Bandwidth-delay constrained routing algorithms," Computer Networks, vol. 42, no. 4, pp. 503-520, 2003. TY - JOUR.

[27] E. Zegura, “Thoughts on router-level topology modelling.," 2001. http://www.postel.org/pipermail/end2end-interest/2001-January/000033.html.

[28] J.M. Doar, “A better model for generating test networks," in Proceedings of Globecom '96, 1996.

[29] D. S. Reeves and H. F. Salama, “A distributed algorithm for delay-constrained unicast routing," Networking, IEEE/ACM Transactions on, vol. 8, no. 2, pp. 239-250, 2000. TY - JOUR.

[30] H. F. Salama, D. S. Reeves, and Y. Viniotis, “A distributed algorithm for delay-constrained unicast routing," in INFOCOM '97. Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, vol. 1, pp. 84-91 vol.1, 1997. TY - CONF.

[31] Salama H., “Multicast Routing for Real Time Communication on High Speed Networks.” PhD thesis, Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC, USA, 1996.