ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 2 Issue Special 1 Jan-March 2014
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)

Secure Route Discovery in Mobile Ad-Hoc Network Using MAC Based Group Key Management Protocol

[I]K.Pazhanisamy, [II]Dr. Lathaparthiban
[I]Dept. of CSE, University college of Engineering Villupuram, Tamilnadu, India
[II]Dept. of CS, Pondicherry University Community College, Pondicherry, India

Abstract
Security in MANET is the most vital concern for the basic functionality of network. One of the most important challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks. Different type of mechanisms has been proposed using different cryptographic techniques to countermeasure the routing attacks against MANET. We have taken VBOR as the base protocol. The VBOR protocol consists of two phases namely, Route maintenance and Route discovery with the use of variable bit rate. In this paper proposed the message authentication code is generated during route discovery phase then these data are exchanged between the nodes. In VBOR and MAC algorithm is to provide more security in route discovery and data are exchanged to the MANETs.

Keywords
MANET Security, Secure Routing, Attacks, MAC, VBOR, Key Management Protocol.

I. Introduction For Routing Protocols

There are different type of routing protocols [10] are used to discover routes and locate the MAC addresses between Ad- hoc wireless nodes. The main goal of ad-hoc network routing protocol is to make optimum and best route establishment between mobile nodes so that message reached to the destination in time. The best route in Ad-hoc wireless communication is that in which bandwidth spending and overhead is less. In ad-hoc networks, there is lack of topology information so that nodes have to discover the topology by transfer hello messages within the network. When new node enters the topology it announces its presence within the network and listens to broadcast announcements from its neighbors. Routing algorithms have to:

- Maintain routing table reasonably small.
- Select best route for given destination includes fastest, reliable, highest throughput.
- Keep table up-to-date when nodes leave, join or move.
- Little amount of messages/time is required to converge.

II. Overview of Manets Routing Protocols

Mobile Ad-Hoc Network [2] is the rapid increasing technology from the past twenty years. The growth in their popularity is because of the easily deployment, infrastructure less and their dynamic nature. Mobile Ad-Hoc Networks created a new set of demands to be implemented and to provide proficient better end-to-end communication. Mobile Ad-Hoc Networks works on TCP/IP structure to provide the means of communication between communicating work stations. The work stations are mobile and they have limited resources, therefore the traditional TCP/IP model requests to be refurbished or modified, in order to compensate the MANETs mobility to give efficient functionality. Therefore the key research part for the researchers is routing in several network. Routing protocols in MANETs are complicated and attractive tasks, researchers are giving great amount of attention to this key area. The most important features of MANET are listed some as below:

- MANET can be created without any preexisting infrastructure.
- It follows dynamic topology where nodes may join and leave the network at any time and the multi-hop routing may keep changing as nodes join and depart from the network. It does have mostly limited physical security, and thus increasing security is a main concern.
- Every node in the MANET can support in routing of packets in the network.
- Limited Power and Limited Bandwidth.

Routing protocols can be divided into reactive, proactive and hybrid protocols depending on the routing topology (Papadimitratos and Haas, 2002). Proactive protocols are either distance vector protocols or table-driven. In such protocols, the nodes periodically refresh the existing routing information so that every node can immediately operate with consistent and up-to-date routing tables Papadimitratos and Haas, 2002. On the contrast, source-initiated or reactive on demand protocols do not periodically update the routing information (Hubaux et al., 2001). Thus, they create a big overhead when the route is being determined, since the routes are not automatically up-to-date when required. The Hybrid protocols make use of both proactive and reactive approaches. They typically offer the means to switch dynamically between the reactive and modes of the protocol (Hubauxetal. 2001). The hierarchy of these protocols is give bellow Fig 1.

III. Routing Attacks In MANET

The malicious node(s) can attacks in Mobile Ad-Hoc Network using different ways, such as transfer fake messages many times, fake routing information, and advertising fake links to disrupt routing operations. In the following paragraph, current routing attacks and its countermeasures against Mobile Ad-Hoc Network protocols are discussed in detail below Fig. 2.

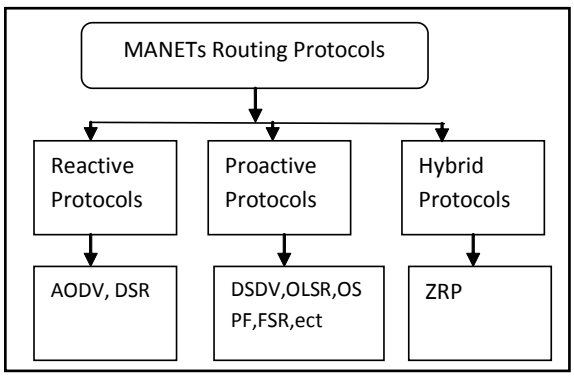

Fig. 1: MANETs Routing Protocols

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

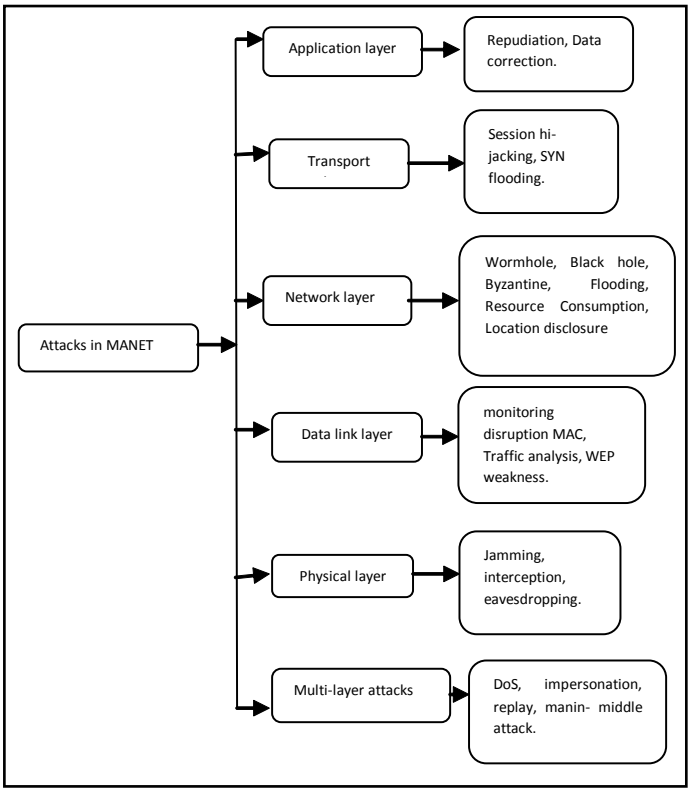

Fig. 2: Classification of attacks on MANET

A. Rushing Attack

It is an unfamiliar attack [1], in which the attacker attempts to be part of routing path to cause the denial of service attack. The attack is directed to reactive protocol only. This attack exploits the property that each node processes just the route request packet for specified identity once.

When rushing attack launched during the route discovery, only a route not longer than two hops is found. As shown in Fig. 3 the source A starts by forward packet to the destination B. The malicious node P when received the route request to B it quickly broadcasts the request to one of the destination neighbour Q without any checking for request demand. Finally, the destination received the request from Q. So this route request is selected and other discards since each node must process one route request.

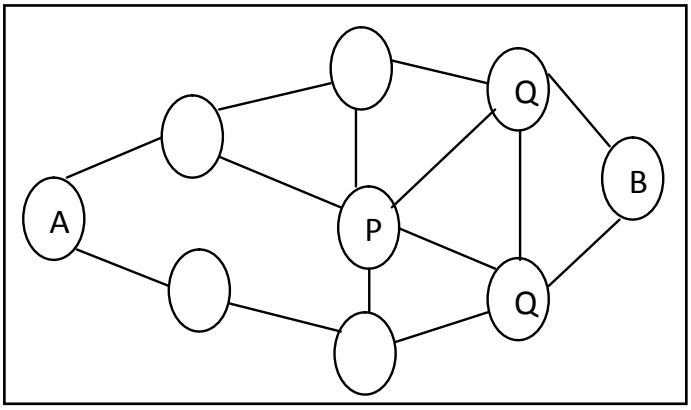

Fig. 3: Rushing Attack

B. Blackhole Attack

Black hole attack is an attacked node cooperated well in the route discovery, but it is dropped the packet while forwarding it. Within route discovery the black hole node all the time gives the correct responds to route request and route reply. On the other hand, it does not have a path to the destination node. When the source node forwards the data packet, this node discarded the data packet and makes a hole in the path that denied any packets transmit. There are 2 types of black hole: Single Back Hole (Deng et al., 2002) and Multiple Black Hole (Ramaswamy et al., 2003). The Single Black Hole attack, one node pretended had the shortest path to the destination. The black hole node when engage in the routing, it performs denial of service or drops the forward packets. In Multiple Black Hole attack two nodes or more cooperate to misrepresent the existence of a path to the destination. There are two solutions for Single black hole attack is suggested in Al-Shurman et al. (2004). One solution is done by receiving repeated reply at the source. The source selects a route path that has repeated portion with another route path. In the second solution, each node constructs two tables to keep sequence numbers of the packets. The first table consists of sequence numbers of the last packet sent to other nodes. While the second table is comprised of sequence numbers received from other nodes. In reply phase, each node required to match the sequence number of the packet received with a sequence number in the table to verify the correctness of the reply packet. Ramaswamy et al. (2003) proposed a solution for Multiple Black Hole attack by using an additional table Data Routing Information (DRI) to provide nodes reliability to and cross checking algorithms to check node reliability and find the cooperative black hole nodes.

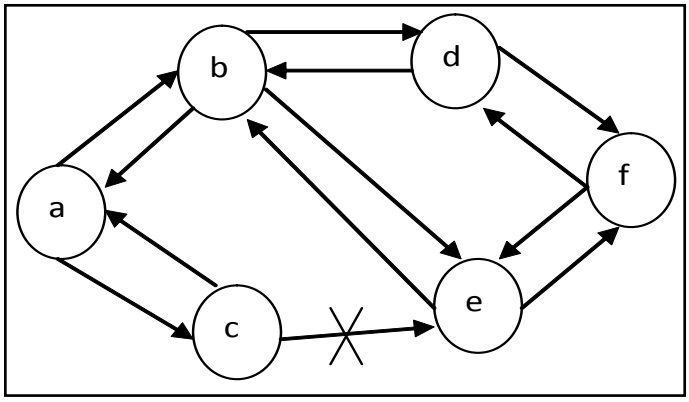

Fig. 4: Black hole attack

Example of the black hole attack [9] a malicious node injects false route replies to the route requests it receives advertising itself as having the shortest path to a destination. These fake replies can be made-up to divert network traffic through the malicious node for eavesdropping, or just to attract all traffic to it in order to perform a denial of service attack by dropping the received packets.

C. Jellyfish Attack

In jellyfish attack [2], the attacker attacks in the network and introduce unwanted delays in the network [7]. In this type of attack, the attacker node first get access to the network, once it get into the network & became a division of the network. The attacker then proposed the delays in the network by delaying all the packets that it receives, once late are propagated then packets are released in the network. This enables the attacker to produce highly end-to-end delay, high delay jitter and considerably affect the performance of the network.

D. Wormhole Attack

Wormhole attack is a severe attack in which two attackers placed themselves strategically in the network. The attackers then maintain

on hearing the network, record the wireless data. Shows the two attackers placed themselves in a strong strategic location in the network.

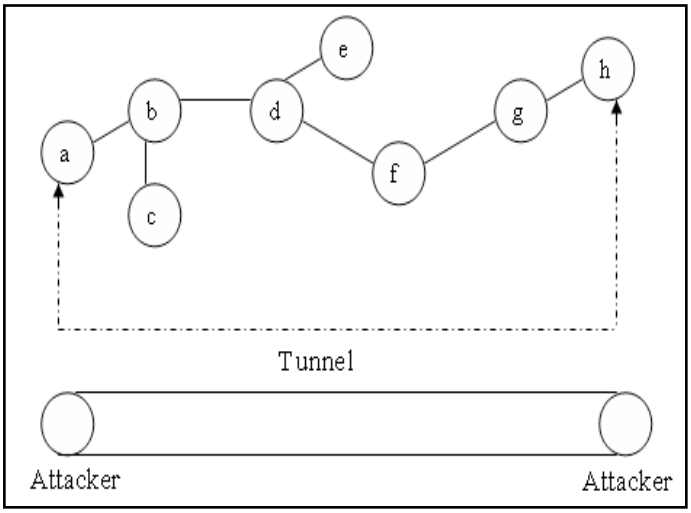

Fig. 5: Wormhole attack

In wormhole attack [2], the attacker gets themselves in strong strategic location in the network. They make the use of the position i.e. they have shortest path between the nodes as shown in the Fig. 5 above. They advertise their path letting the other nodes in the network to know they have the shortest path for pass on their data. The wormhole attacker creates a tunnel in order to records the ongoing communication and traffic at one network position and channels them to another position in the network [6].When the attacker nodes create a direct link between each other note in the network, wormhole attacker then receives packets at one end and transmits the packets to the other end of the network. When the attackers are in such location the attack is known as out of band wormhole [7].

The other type of wormhole attack is identified as in band wormhole attack [7]. In this type of attack the attacker builds an overlay tunnel over the existing wireless medium. Band wormhole attack is potentially very much harmful and is the most preferred choice for the attacker.

E. Sybil attack:

If a malicious node impersonates some nonexistent nodes, it'll seem as many malicious nodes conspiring along, that is termed a Sybil attack. A Sybil attack is one within which associate aggressor subverts the name system of a peer-to-peer network by making an outsized variety of onymous entities, exploitation them to realize a disproportionately giant influence. A name system's vulnerability to a Sybil attack depends on however cheaply identities are often generated, the degree to that the name system accepts inputs from entities that don't have a sequence of trust linking them to a sure entity, and whether or not the name system treats all entities identically. This attacks aims at network services once cooperation is important, and affects all the machine configuration schemes and secure allocation schemes supported trust model further. However, there's no effective thanks to defeat Sybil attacks. Validation techniques are often wont to stop Sybil attacks and dismiss masquerading hostile entities. An area entity could settle for a distant identity supported a central authority that ensures a matched correspondence between associate identities associated an entity and will even offer a reverse search. Sybil bar techniques supported the property characteristics of social graphs also can limit the extent of harm which will be caused by a given sybil aggressor whereas conserving namelessness, tho' these techniques cannot stop sybil attacks entirely, and will be prone to widespread small-scale sybil attacks.

So avoided the above attacks we have taken MAC as the security constraint. This security procedure includes the previous work of variable bit rate on-demand routing protocol (VBOR). In VBOR, the MAC algorithm is implemented to provide more security. We have study has following modules:

- Grouping and Gateway member selection
- Secure key generation for VBOR
- Secure data transmission

IV. Proposed Work

In mobile ad-hoc networks, the safety is main concern in achieving the economical and deployable network for military and rescuer areas. In security, there are three mechanisms to be maintained: Confidentiality, Authentication and Non-repudiation. Confidentiality maintains that the actual message is to be received by the licensed receiver. Authentication assures that the actual message is being sent by a certified sender. Non-Repudiation assures that any sender or receiver couldn't ready to deny the previous transactions (Sender cannot deny that the previous Message had not been sent by me or receiver cannot deny that the previous message had been received by me). If any security algorithmic rule provides these three security mechanisms, it'll be an honest and deployable security algorithmic rule. However providing these mechanisms in ad-hoc networks is tough since there aren't any such infrastructures of these mechanisms want a central authority to store the key pairs of the mobile nodes. As an example, in military setting anyone mobile node may be selected as a central node to that all alternative mobile nodes send their key pairs. In these networks, the nodes apart from central node have restricted power and low stability.

We are proposed in MAC based Group Key Management Protocol, A source node 'K' maintains a Query Sequence number (Q_{SEQ}) for every destination it securely communicates with. This 32 bit sequence number increases for every route request generated by K and allows D to detect outdated route request. For every of the outgoing Route Request, K generates a 32bit random Query Identifier (Q_{ID}), which is used by midway nodes as a means to identify the request. Both Q_{ID} and Q_{SEQ} are input to the MAC (Message Authentication Code) along with route request message, security association number, source address and destination address. Then the all information is encrypted using the shared secret key Ki,j of that group. The Message Authentication Code M is calculated as Equation 1[16]:

$$M = \square C\ (K_{i,j}\{RREQ, SA_{num}, Q_{id}, Q_{seq}, SA, DA\}),\ SA,\ DA \quad (1)$$

This is the message, the secure VBOR sends through intermediate nodes towards destination. This Message Authentication Code value will be sent through intermediate nodes towards destination. The security of this proposed work lies in calculating Message Authentication Code value. In Fig. 6, the intermediate nodes 1 and 2 cannot decrypt the MAC value because shared secret key of source and destination is only known to the source and destination but not to intermediate nodes. Thus it provides more security for the messages and it avoids message tampering attack. The procedure for Gateway Member Selection and key generation of proposed scheme are discussed in Table 1, 2 respectively.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

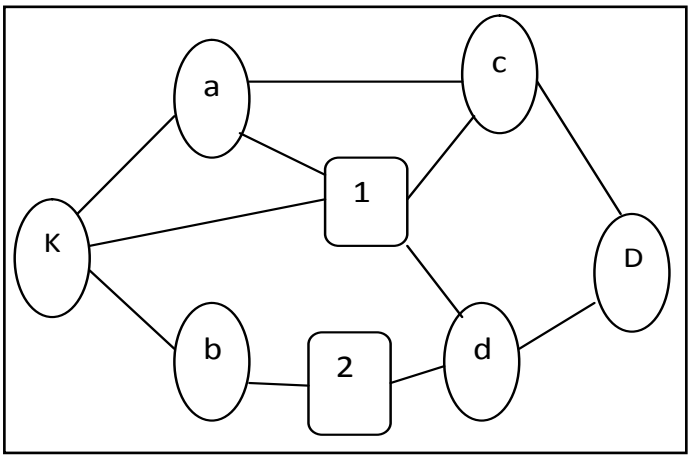

Fig 6: Data communication

K= Source node, D= Destination node
Node 1, 2= malicious nodes
ie Source k communicates with Destination d through malicious nodes 1 and 2

TABLE 1
GATEWAY MEMBER SELECTION

Network is separated into groups
Subgroups are generated with the total number of nodes as well as number of subgroups that are needed and it is restricted to 'n'.
That is, $K = N/N_k$ and $k \leq n$
Choose gateway member if the residual energy of the node is greater than the threshold residual energy
If ($E_R > R_{th}$)
Then $Gm = K[M_i]$
Where $K[M_i]$ is the member of the subgroup K
Find the public key and private key pair for each member $K[M_i]$
If a new node 'i' enters into the subgroup K, a new gateway member is selected.
Then follow step 3.

TABLE 2
KEY GENERATION

User x generates it's private key PR_x
User y generates it's private key PR_y
User x and y calculate their public key such as
$PU_x = PR_x * G$
$PU_y = PR_y * G$
ie. G is the generated point in public key cryptography
User x sends its public key to user y
User y computes group key such that
$K_y = PR_y * PU_x$
User y sends its public key to user x
User x computes group key such that
$K_x = PR_x * PU_y$
Check $K_y = K_x$
If they are same then the gateway member stores this key as $K_{x,y}$

5. Conclusion

This paper discusses common possible attacks on different type of protocols being used in MANETs. We have tried to evaluate them so as to prevent the attacker to intrude in wireless networks. There are many of techniques with which, one can easily detect most of the attacks. One can select them in accordance with the protocol being used in the network. However, no protocol is fully secure from attacks being encountered in the MANETs. Now introduced new technique gives security to the Variable Bit rate on demand Routing protocol (VBOR). In compared symmetric key cryptography, public key cryptography gives more security to the ad hoc networks because the nodes have to secure their keys with themselves. Here the malicious nodes cannot get the data since the message authentication code is computed within the group members. Thus the MAC value should be known to the group members. The nodes are authenticated and then the group members are decided also the gateway member is selected based on the residual energy of the nodes. The data is transmitted with confidentiality that is no malicious and selfish node cannot get the MAC value

Future research work should be focused not only on improving the effectiveness of the security schemes but also on minimizing the Traffic Load based Performance to make them suitable for a Mobile Ad-Hoc Network environment. Furthermore, each proposed solution can work only with a specific attack and is still vulnerable to unexpected attacks.

References

[1] *Salwa Aqeel Mahdi, Mohamed Othman, Hamidah Ibrahim, Jalil Md. Desa and Jumat Sulaiman" Protocols For Secure Routing And Transmission In Mobile Ad Hoc Network: A Review" Journal of Computer Science 9 (5): 607-619, 2013.*

[2] *IRSHAD ULLAH, SHOAIB UR REHMAN" Analysis of Black Hole attack on MANETs Using different MANET routing protocols"sep 2010*

[3] *M.Nasir Iqbal, Junaid A.Khan, Farooq Umer, Nadeem Javaid, Izhar-ul-Haq, Mustafa Shakir" Security Enhancement of Pro-active Protocols in Mobile Ad-hoc Networks"2013*

[4] *Rashid Hafeez Khokhar, Md Asri Ngadi & Satria Mandala" A Review of Current Routing Attacks in Mobile Ad Hoc Networks" 2006*

[5] *Shekhar Saini, Rajesh Kumar" Comparison of layerwise attacks in MANETs" 2013*

[6] *H.L.Nguyen, U.T.Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks", International Conference on System and Networks and International Conference on Mobile Communications and Learning Technologies (ICN/ICONS/MCL 2006), pp.149-149, April, 2006.*

[7] *V.Mahajan, M.Natue and A.Sethi, "Analysis of Wormhole Intrusion attacks in MANETs", IEEE Military Communications Conference, pp. 1-7, Nov, 2008.*

[8] *F.Stanjano, R.Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing", Vol. 35, pp. 22-26, Apr, 2002*

[9] *Sarvesh Tanwar, Prema K.V. "Threats & Security Issues in Ad hoc network: A Survey Report"Jan2013*

[10] *M.Nasir Iqbal, Junaid A.Khan, Farooq Umer, Nadeem Javaid, Izhar-ul-Haq, Mustafa Shakir" Security Enhancement of Pro-active Protocols in Mobile Ad-hoc Networks"2013*

[11] *P.A.R Kumar, S.Selvakumar, "Distribute Denail-of-Service (DDoS) Threat in Collaborative Environment – A survey of DDoS Attack Tools and Traceback Mechanism" IEEE International Advance Computing Conference (IACC 2009), pp. 1275-1280, March, 2009.*

[12] *L.Zonglin, H.Guangming, Y.Xingmiao, "Spatial Correlation Detection of DDoS attack" International Conference on Communication, Circuits and System (ICCCAS 2009), pp. 304-308, July, 2009.*

[13] X.Y.Zhang, Y.Sekiya, Y.Wakahara, "Proposal of a method to detect black hole attack in MANET", international Syposium on Autonomous Decentralized System (ISADS 2009), pp. 1-6, March, 2009

[14] Jeremy J. Blum, Andrew Neiswender and Azim Eskandarian," Denial of Service Attacks on Inter-Vehicle Communication Networks" in 11th IEEE conference on Intelligent Transportation Systems, 2008, pp 797- 802

[15] Nikos Komninos, Dimitris Vergados, Christos Douligeris" Layered security design for mobile ad hoc networks" 2006

[16] T. Peer Meera Labbai and V. Rajamani" message authentication code Based secure group key management Protocol for mobile ad hoc networks" Journal of Computer Science, ISSN: 1549-3636,pp 1274-1282, 2013.

[17] Labbai, T.P.M. and V. Rajamani," A variable bitrate on-demand routing protocol for mobile ad hoc Networks" Int. J. Ad Hoc Sensor Ubiquit. Comput.,3: 31-40, 2012.

[18] Zhou, H., M. Zheng and T. Wang. A novel group key establishment scheme for MANETs. Proc. Eng., 15: 3388-3395. DOI: 10.1016/j.proeng.2011.08.635, 2011.

[19] Rasmussen, K.B. and S. Capkun, Location privacy of distance bounding protocols. Proceedings of the 15th ACM Conference on Computer and Communications Security, Oct. 27-31, ACM Press, New York, USA., pp: 149-160. DOI: 10.1145/1455770.1455791, 2008.

[20] Sanzgiri, K., B. Dahill, B.N. Levine, C. Shields and E.M. Belding-Royer, A secure routing protocol for ad hoc networks. Proceedings of the 10th IEEE International Conference on Network Protocols, Nov. 12-15, IEEE Xplore Press, pp: 78-87. DOI: 10.1109/ICNP.2002.1181388, 2002.