RESEARCH ARTICLE OPEN ACCESS

Performance Analysis of AODV and MAODV Routing Protocols in MANET

Aanchal Joshi
M.Tech, Department of Computer Science
Seth Jai Prakash Mukand Lal Institute of Engineering and Technology (JMIT)
Kurukshetra University
India

ABSTRACT

A mobile ad hoc network made up of mobile nodes which are wireless. Mobile Ad- Hoc Network is self organized and self configurable. In MANET mobile nodes move randomly. Like a router, the mobile nodes in MANET can forward and receive packets. Routing is a critical issue in MANET. A recent trend in Ad Hoc network routing is the reactive on-demand philosophy where routes are established only when they are required. Most of the protocols in on-demand category are not associating with proper security features. The ad hoc environment can be accessed by both legitimate network users and attackers. It has been monitored that different protocols need different security strategies. Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network.

The scope of this review paper is to study the effect of Black hole in Manet using the very famous on demand routing protocol i.e. AODV protocol. A new protocol namely MAODV i.e. Modifying AODV is proposed which is malicious and suffering from black hole attack. A comparative analysis of black hole attack for both protocols is taken into account to show how the attack will decrease the performance of MANET. The metrics used for simulation are Packet Delivery Ratio, Average End-to-End Delay and Throughput. Simulation is done using Network Simulator 2 (version 2.34).

Keywords:- MANET, Black hole Attack, AODV, MAODV

I. INTRODUCTION

A Mobile Adhoc Network is a collection of various independent and individual mobile nodes that can communicate to each other through radio waves. That nodes which are in the radio range of one another can directly communicate with each other, whereas others needs the aid of intermediate nodes for routing their own packets. Each of that node has a wireless interfacing medium to communicate with each other. Mobile ad-hoc networks are fully distributed, and it will worked at any place without the help of any fixed infrastructure like access points or base stations. Figure 1 shows very simple ad-hoc network with 3 nodes. Node 1 and node 3 are not within range of one another, however the node 2 use to forward packets between node 1and node 2. The node 2 will act as a router and these three nodes combined to form an ad-hoc network.[1]In this paper we are discussed about two routing protocols and compare their performances.One of the important research areas in MANET is establishing and maintaining the ad hoc network through the use of routing protocols. Though there are so many routing protocols available, this paper considers AODV and MAODV for performance comparisons due to pause time. These protocols are analyzed based on the important metrics such as throughput, packet delivery ratio and average end-to-end delay.

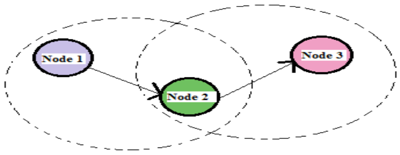

Fig 1. Example of mobile ad-hoc network

II. LITERATURE SURVEY

MANET has no centralized control and the communication is carried out with blind mutual trust amongst the nodes on each other[2].Various kinds of MANET are discussed below:

1. Types of Mobile Ad-Hoc Network:

1. Vehicular Ad-Hoc Networks (VANET's)
2. Intelligent Vehicular Ad-Hoc Networks (InVANET's)
3. Internet Based Mobile Ad-Hoc Networks (iMANET's)

1.1 Vehicular Ad-Hoc Networks (VANET's)

VANET is one of the type of Mobile Ad-Hoc network where vehicles are equipped with wireless network and form a network without help of any infrastructure. The equipment is equipped inside vehicles [2] as well as on the road sides for providing access to other vehicles in order to form a network and communication.

1.2 Intelligent Vehicular Ad-Hoc Networks (InVANET's)

Vehicles that form MANET for communication using WiMax IEEE 802.16 and Wi-Fi 802.11. The main aim of designing In VANET's is to avoid vehicle to vehicle collision so as to keep safe distance as possible between passengers. This also help drivers to keep secure distance [2] between the vehicles as well as assist them that how much speed and distance other vehicles are approaching. InVANET's applications are also employed for military purposes to communicate with each other.

1.3 Internet Based Mobile Ad-Hoc Networks (iMANET's)

These networks are used for linked up the mobile nodes and fixed internet gateways. In these kinds networks the normal routing algorithms will not apply.

2. Manets Characteristics:

1) ***Distributed operation***:

   There is no any background network for the central control of the network operations, the control of the networks are distributed among the nodes. The nodes involved in a MANET should cooperate with one another and will communicate among themselves and each node acts as a relay as needed, to implement specific functions such as security and routing.

2) ***Multi hop routing:***

   When any node tries to send data and information to different nodes which is out of its communication range, the packets must be forwarded through one or more intermediate nodes.

3) ***Autonomous terminal:***

   In MANET, each and every mobile node is an independent node, which could function as both as a host and as a router.

4) ***Dynamic topology:***

   Nodes are free to move where the want with different speeds; thus, the network topologies may change randomly and at unpredictable time periods. The nodes in the MANET dynamically establish routing among themselves as they travelled around, establishing their own mobile network.

5) ***Light-weight terminals:***

   commonly, the nodes at MANET are mobile with less power storage, less CPU capability and little memory size.

6) ***Shared Physical Medium:***

   The medium of wireless communication is accessible by any entity with the adequate resources and appropriate equipment. Accordingly, access to the channels are not restricted.

III. MANETs APPLICATIONS

Some of the typical applications include:

1)Military battlefield: Ad-Hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information head quarter.

2) Collaborative work: For some business environments, the need for collaborative computing might be more important outside office environments than inside and where people do need to have outside meetings to cooperate and exchange information on a given project.

3) Local level: Ad-Hoc networks can autonomously link an instant and temporary multimedia network using notebook computers to spread and share information among participants at a e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information.

4) Personal area network and bluetooth : A personal area network is a short range, localized network where nodes are usually associated with a given person. Short-range MANET such as Bluetooth can simplify the inter communication between various mobile devices such as a laptop, and a mobile phone.

5) Commercial Sector**:** Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed.

III. PROBLEM FORMULATION

Security is very major and important issue in MANET. Existing AODV defines no special security mechanisms [6]. So an impersonation attack can easily be done. A node is said to be malicious if it is an attacker that cannot authenticate itself as a legitimate node because due to lacking of valid cryptographic information. A node is compromised if it is an inside attacker who behaved maliciously but can be authenticated by the network as a legitimate node and is being trusted by other nodes.

Several attacks [3, 12] can be launched against the AODV routing protocol:-

Message tampering attack: An attacker can be able to alter the content of routing messages and forward them with falsified information. For example, by decresing the hop-count field in either an RREQ or RREP packet, an attacker can increase its chance to be [7] an intermediate node of the route. A selfish node can relieve the burden of forwarding messages for others by setting the hop-count field of the RREQ to infinity.

Message dropping attack: Attackers and selfish nodes both can intentionally drop some (or all) routing and data messages. Since within a MANET all the mobile nodes function as both end hosts and routers, this attack can paralyze the network completely [7] as the number of message dropping increases.

Wormhole Attack (Message replay) attack: Attackers can retransmit eavesdropped messages again later in a different place. One kind of replay attacks is the wormhole attack. A wormhole attacker can tunnel an RREQ directly to a destination node. Since a wormhole attacker may not increase [8] the hop-count field value, it prevents any other routes from being discovered. The wormhole attack can be combined [8] with the message dropping attack to prevent the destination node from receiving packets.

Black hole Attack: The black hole attack [3] is an active insider attack, it has two properties: first, the attacker [9] consumes the intercepted packets without any forwarding. Second, the node exploits the mobile ad hoc [9] routing protocol, to advertise itself as having a valid route [4] to a destination node, even though the route is spurious, with the intention of intercepting packets [4].In other words the routing protocol are used by malicious node to advertise as having the shortest path to nodes whose packets it wants to intercept. In the AODV protocol case, the attacker [10] listens to requests for routes. When the attacker receives a request [9] for a route to the target node, the attacker creates a reply where an extremely short route is advertised, if the reply from various malicious node reaches [9] to the requesting node before the reply from the actual node,their has been created a fake route. Once the malicious device has been able [9] to insert itself between the communicating nodes, it is able to do anything with all packets [5] passing between them. It can choose to drop the packets to form a denial-of-service attack.

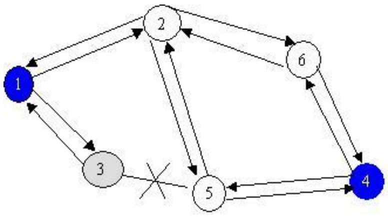

Fig 2: Black Hole Attack

Working of Black Hole: - On the bases of original AODV protocol, any intermediate node may respond to the [11] RREQ message if it has fresh enough route, which is checked by the destination sequence [11] number contained in the RREQ packet. In Figure 2: node 1 is source node and node 4 is destination node. Source node broadcasts route request packet to find a route to destination node. Node 3 acts as black hole. Node 3 [11] also sends a route reply packet to the source node. But a route reply from node 3 reaches to [11] source node before any other intermediate node. In this case source node sends the data [11] packet to destination node through node 3. But as the property of black hole node [11] that this node does not forward data packets further and dropped it. But source node is not aware of it and continues [11] to send packet to the node 3. In this way the data, which has to be reached to the destination, fails to reach there. There is no way [11] to find out such kind of attack. These nodes can be in large number [11] in a single MANET, which makes the situation more critical.

In this work, effort has been made to detect the Black hole Attack in existing AODV and to show that how this attack will decrease the performance of AODV.

IV. PROPOSED PLAN

A New protocol has been proposed called MAODV modifying AODV protocol. In this protocol a malicious node is present at a random location.

Then using NS-2 simulator a comparative study of two protocols AODV and MAODV has been done for 10, 25 and 50 nodes. By using TCL scripts the simulation has been done. Three metrics Packet delivery ratio, End to End Delay and Throughput have been used to show the simulation results. The results of AODV & MAODV are represented in the form of Graph. Using these graphs MAODV & AODV performance comparison has been made. To carry out the analysis a malicious node has been introduced in the script. When this node communicates directly with the routing nodes, the result becomes hacker attack. This causes fall of packets. Broad simulations with varying scripts have been used to study this performance

Algorithm: Proposed plan has been built on AODV protocol, but its principal will be applicable to other routing protocol as well. In this scheme we modified the famous AODV routing protocol and add a new field, next_hop, in the routing messages, so that a node accordingly can correlate the overheard packets.In this propose plan three important algorithms are implemented.

In algorithm Section 1: describes modified route request procedure, Section 2: describes route reply procedure and Section 3: discusses the packet forwarding procedure respectively.

Each and every node in order to take part in any network activity, says Route Request (RREQ), has to declared its token as described in Algorithm Section 1. If the node bit htype is "1" indicating that the node is malicious, protocol do not allow the node to participate in any network activity. Otherwise, the htype bit is "0" indicating the node is Non malicious, which confers it the freedom to participate in all network activity. Where htype is node type, Mi is monitor node identity & Idi is identity of node.

Algorithm section 1: RREQ packet's working

```
Step 1:  for each RREQ  packet (P)
             if each node htype = "0" then broadcast RREQ
Step 2:  prevhop ← currenthop [node ID]
               neighhop1←prevhop[node ID]
               neighhop2←nexthop[node ID]
Step 3:  repeat the steps from step 2 to step 6 until it reaches
         the destination node else drop Monitor RREQ packet
         (P) sent
```

In this system, three monitoring nodes are used to convict the malicious node. In this scheme the nodes have dual roles – packet forwarding and monitoring. For node Idi, Idi-1, Mi and Mi+1 will be monitoring in the packet forwarding operation and Mi+1, mi and Mi+1 will be monitoring in the route reply operation. Route reply process (RREP) as given in Algorithm Section 2.

Algorithm 2: RREP packet's working

```
Step 1:   For each RREP  packet (P) sent do
              if node htype="0" then
 Step 2:  Set designated monitors
           neighhop1←prevhop[node ID]
           neighhop2←nexthop[node ID]
           nexthop ← prevhop [node ID]
Step 3:   unicast RREP  to previous node
Step 4:   repeat the steps from step 2 to step 7 until it reaches
          the source node
Step 5:   If currenthopcount and neighhop1 and neighhop2 is
          equal to nexthopcount then process this RREP as
          specified in the standard protocol
```

Whenever a node is found to be misbehaving – say dropping data packets, the corresponding monitors immediately send ERROR message to the source node and the status bit of guilty node is set to "1". In order to correlate correctly the overheard messages an additional field next_hop. Though there are several tpes of misbehavior that could be captured by promiscuous hearing we are focusing only on malicious actions: dropping packets.

Algorithm Section 3: Data Packet Forwarding

```
Step 1:   For each DATA packet (P) sent do
          if node htype="0" then send a packet to the next
          forwarded node
Step 2:   If tampered with the payload or header of the
          currently sent packet
          nodenexthop ← nodecurrentpacketheader
          neighhop1←nodecurrentpacketheader
          neighhop2←nodecurrentpacketheader
          it keeps this header information until next packet is
          forwarded to the node else nextnode has dropped the
          packet, thus, the malicious node
          prevnode, neighhop1 and neighhop2 is umpire node
          for next immediate  forwarded node
Step 4:   if nexthop←currentpacketheader and
          neighhop1←nodecurrentpacketheader and
          neighhop2←nodecurrentpacketheader is not equal to
          prevhop←currentpacketheader
          Mark as malicious  node it broadcast ERR  packet to
          1-hop or 2-hop node distance
         nextnode htype = "1"
Step 5:   Monitors node sent link error message to the source
          node process this RERR message as specified in the
          standard protocol
```

V. COMPARATIVE SIMULATION RESULTS BETWEEN AODV AND MAODV

The working of routing greatly depends upon successful transmission of packets to the destination. This requires appropriate selection of Routing path and algorithm. AODV and MAODV have been used for routing solutions. All the simulations have been done using Network Simulator Ns-2.34 on the platform Fedora 13. CBR (continuous bit–rate) are the traffic sources. The pairs of source-destination are spread randomly over the network. During the simulation, each and every node starts its journey from a random spot to a destination which is randomly chosen. Once the node reaches destination, it takes a rest period of time in seconds and another destination is chosen randomly after that pause time. Throughout the simulation this process repeats, which causes continuous changes in the underlying network topology. Different network scenario for various numbers of nodes and different node transmission range are generated. The parameters that have been used in the whole experiment are summarized in Table 1.

- **Metrics Used:**

There are many qualitative and quantitative metrics that are used to compare reactive routing protocols. Most of the existing routing protocols ensure the qualitative metrics. For analysis the following metrics have been used. These performance metrics determines the correctness and completeness of the routing protocol.

a) **Packet Delivery Ratio:** PDR is defined as a percentage of data packets delivered at receiver end compared to that of number of data packets sent for that nodes. It is used to measure the efficiency and effectiveness, reliability of routing protocols. Generally the reliability, effectiveness and efficiency of routing protocols can be improved by improving the PDR.

b) **Throughput:** It is one of the networked dimensional parameters which gives the fraction of the channel capacity used for useful transmission selects a destination at the beginning of the simulation i.e., information whether the data packets correctly delivered to the destinations or not.

c) **Average end to end delay:** The average end-to-end delay of data packets is the interval between the data packet generation time and the time when the last bit arrives at the destination.

Simulation Parameters	Parameter Value
Simulator	NS-2.34
Simulation Area	750m × 750m
Mobile Nodes	10,25, 50
Hacker Nodes	1,2,3
Pause Time	100,200,300,400,500
Speed	1,2,3,4,5
Packet Size	512 Bytes
Routing Protocols	AODV & Modi_AODV
Traffic Sources	CBR(TCP)
Simulation Time	700 Sec.
Performance Metrics	Packet Delivery Ratio, Throughput, Average end to end delay

Table 1: Evaluation Parameters

VI. RESULTS AND DISCUSSION

A comparative analysis of the performance metrics generated from all simulation, over AODV and MAODV routing protocols has been shown in graphs. An Attempt has been made to compare the two protocols under the same simulation environment.

ANALYSIS

Screenshots for protocols AODV and MAODV has been taken using the NAM animator. These screenshots are showing how the nodes are communicating with each other. Number of nodes are 50 and the connection used is TCP. For both protocols screenshots have been taken with variation in speed and pause time.

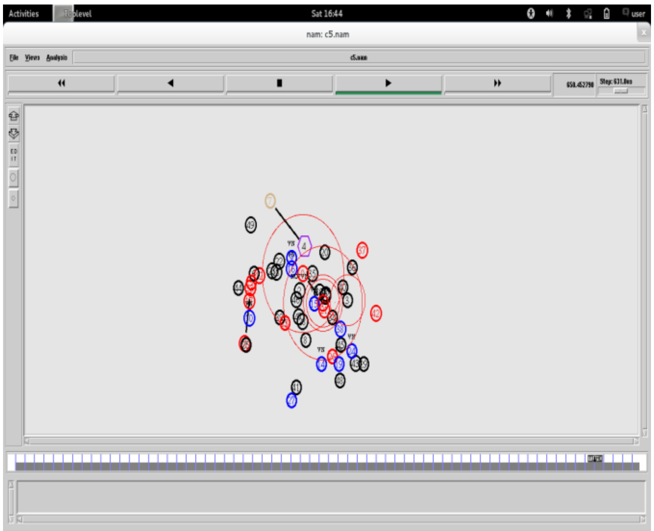

Fig 3: Screenshot of AODV for 50 nodes varying speed using TCP connection

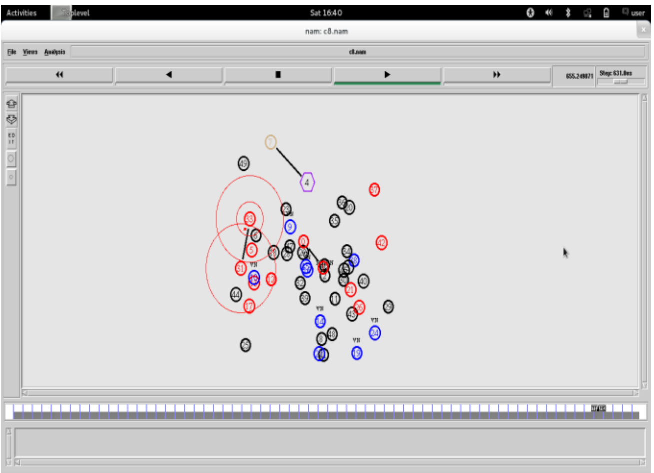

Fig 4: Screenshot of AODV for 50 nodes varying pause time using TCP connection

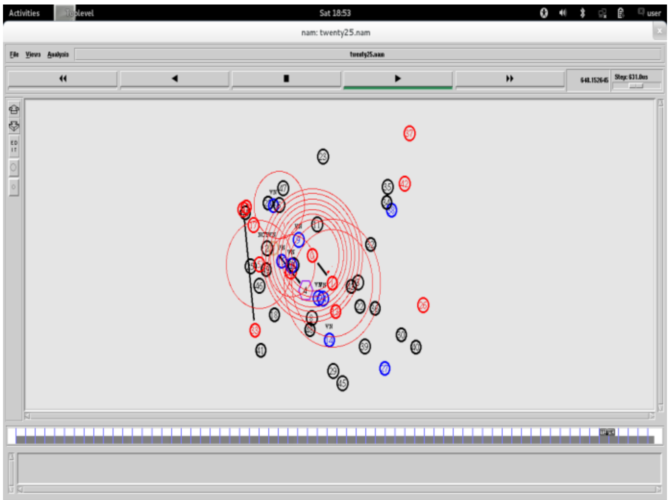

Fig 5: Screenshot of MAODV for 50 nodes varying speed using TCP connection

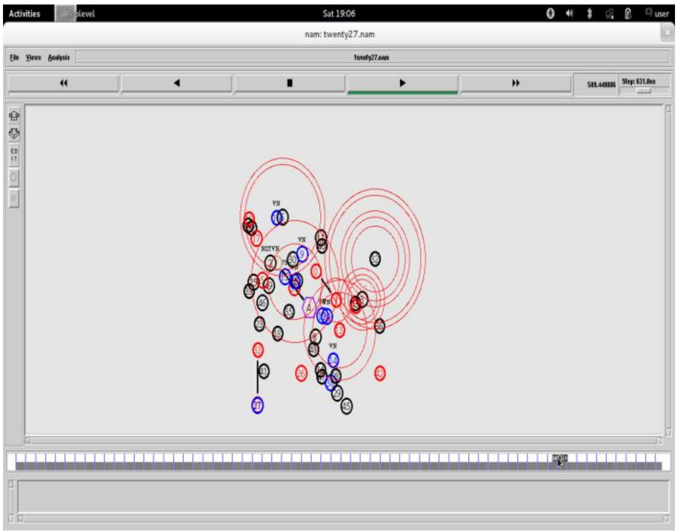

Fig 6: Screenshot of MAODV for 50 nodes varying pause time using TCP connection

VII. CONCLUSION

The field of ad-hoc networking has been receiving attention increasing among researchers in recent years, as the available wireless networking and mobile computing hardware bases are now able to support the promise of this technology. Over the past few years, variety of new routing protocols targeted specifically at the ad-hoc networking environment have been proposed. Here, a performance comparison of protocols for ad-hoc network routing protocol AODV, MAODV using a network simulator NS-2 with scenario consisting of different speed and pause time. AODV results are much more better when nodes are less but as the nodes increased to 25 & 50 the difference in the performance of AODV & MAODV also increased. The routing Throughput of the two protocols is increased as pause time increases. The routing delay of the two protocols is increased as pause time decreases.

In future this study can be increased for more than 100 nodes. Present study works only with single hacker, this study can be extended using more hackers. In Ad-hoc networks any node can enter in the network at any time but it is very difficult to detect which node is malicious. A new protocol can be also designed for detecting the hackers' nodes and providing security to the network. The proposed algorithm is capable of detecting only the Black hole attack in MANET.

There is lot of work required to be done in the field of ………….

- More denser and sparse real life scenarios are needed for the protocol to be robust in nature
- More comparisons are required with other schemes like DSR, TORA
- May be Power feature can also influence the study further

REFERENCES

[1] Aarti et al., Dr. S. S. Tyagi "Study of MANET: Characteristics, Challenges, Application and Security Attacks" international journal of Advanced Research in Computer Science and software Engineering May-2013, pp.252-257.

[2] Irshad Ullah and Shoaib ur Rehman (2010), "Analysis of black hole attack in Manet Using different MANET routing protocols (master's thesis)" Blekinge Institute of Technology, Sweden.

[3] D. P. Agrawal and Qing-An Zeng, "Introduction to wireless and Mobile Systems," Brooks/Cole, 2005.

[4] Nitya Jain and Aparajita Naiwal, "SURVEY ON SECURE ROUTING PROTOCOLS FOR AODV", International Journal of Computing and Business Research (IJCBR), Volume 4 Issue 2 May 2013. ISSN (Online): 2229-6166

[5] Available at: *cs.engr.uky.edu/~singhal/term-papers/Fourth-paper.doc.*

[6] Vladimir. A. Navarro H, Juan Manuel Rojas P., Kadian A, “Special Issues on Ad-Hoc Networks”, International journal of Computer Science and Management Research, Volume 1 Issue 3 October 2012: Sl. No. 60. ISSN: 2278- 733 X.

[7] Available at: http://www.ece.ubc.ca/~vincentw/C/LRWSc05.pdf.

[8] Suman Bala (2009), Secure Routing in Wireless Sensor Networks (master’s degree). Thapar University, Patiala.

[9] Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre, “Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET”, International Journal of Computer Science, Engineering and Applications (IJCSEA), Vol.2, No.1, February 2012. DOI: 10.5121/ijcsea. 2012.2105.

[10] Kusum Nara, Aman Dureja, “A New Approach for Improving Performance of Intrusion Detection System over MANET”, IOSR Journal of Computer Engineering (IOSR-JCE), Volume 11, Issue 2(May. - Jun. 2013), PP 01-09. e-ISSN: 2278-0661, p-ISSN: 2278-8727.

[11] Rajni Tripathi and Shraddha Tripathi, “Preventive Aspect of Black Hole Attack in Mobile Ad Hoc Network”, International Journal of Advances in Engineering & Technology, Vol. 4, Issue 1, pp. 304-313, July 2012. ISSN: 2231-1963.

[12] R. G. T. Anderson, B. Bershad, and D. Wetherall, “A System Architecture for Pervasive Computing,” In Proc. 9th ACM SIGOPS European Workshop, pp. 177–182, Kolding, Denmark, September 2000.