Grayhole Attack and Prevention in Mobile Adhoc Network

Megha Arya
SATI (vidisha)
SATI Sagar Road Vidisha
M.P,India

Yogendra Kumar Jain
SATI (vidisha)
SATI Sagar Road Vidisha
M.P,India

ABSTRACT
Mobile ad-hoc networks (MANETs) are composed of autonomous nodes that are self- managed, dynamically deployed without any pre-existing infrastructure. Gray hole attacks are an active type of attack, which leads to dropping of messages, attacking node first agrees to forward packets and then fails to do so. For this we are using an AODV routing protocol to discover route. Initially the Malicious node behaves correctly and a reply sends true Route Reply (RREP) messages to nodes that initiate Route request (RREQ) messages. We use an intrusion detection system (IDS) to monitors the network or system activities for malicious activities or policy violation and produces reports to a Management Station. It takes over the sending packets. Afterwards, the node just drops the packets to launch a (DoS) denial of service attack. If neighbors nodes that try to send packets over attacking nodes lose the connection to destination then they may want to discover a route again and broadcasting Route Request (RREQ) messages. In Network Simulation-2 (NS-2) scenario the simulation result has shown that the throughput packet delivery is improved rather than traditional Gray hole attack.

General Terms

- To develop intrusion Detection system for Gray Hole Attack for securing routing misbehavior.
- To Find out Misbehavior node in mobile ad-hoc environment.
- Through the IDS Module we enhance the performance of network in presence of Gray Hole attack node.

Keywords
Gray hole, Packet dropping, malicious node, Routing, MANET, AODV

1. INTRODUCTION
MANETs [1] are composed of autonomous nodes that are self-managed without any infrastructure. In this way, ad-hoc net works have a dynamic topology such that nodes can easily join or leave the network at any time. MANETs are suitable for areas where it is not possible to set up a fixed infrastructure. Since the nodes communicate with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves. To support this connectivity, nodes use some routing protocols [2] [3] such as AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing) and DSDV (Destination-Sequenced Distance-Vector). Each node also acts as a router to discover a path and forward packets to the correct node in the network. As MANETs lack an infrastructure, they are exposed to a lot of attacks. One of these attacks is the Gray Hole attack. In the Gray Hole attack [4], which lead to dropping of messages? Attacking node first agrees to forward packets and then fails to do so. Gray Hole attack [4] may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface we simulated the Gray Hole attack node which is deliberately misbehaving, as well as a damaged node interface we simulated the Gray Hole attack.

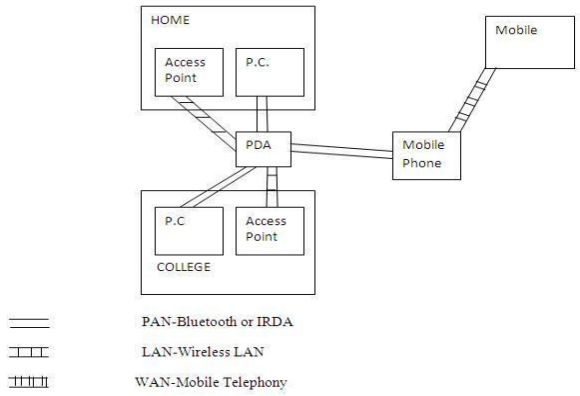


Figure 1 - Wireless uses in differing environments

in wireless ad-hoc networks and evaluated its damage in the network We made our simulations using Network Simulator version 2 (NS-2) [22] simulation program that consists of the collection of all network protocols to simulate many of the existing network topologies. Having implemented a new routing protocol which simulates the Gray hole we performed tests on different topologies to compare the network performance with and without Gray holes in the network. As expected, the throughput in the network was deteriorated considerably in the presence of a Gray hole. Afterwards, we proposed an IDS solution to eliminate the Gray Hole effects in the AODV network. We implemented the solution into the NS-2.And evaluated the results as we did in Gray Hole implementation.

2. LITERATURE REVIEW
Ad-hoc On-Demand Distance Vector:-
AODV [7] [9] is a very simple, efficient, and effective routing protocol for Mobile Ad-hoc Networks which do not have fixed

topology. This algorithm was motivated by the limited bandwidth that is available in the media that are used for wireless communications. The network layer is responsible for routing packets delivery including routing through intermediate router. Gray hole attack .networks using dedicated nodes to support basic functions like packet. Forwarding, routing, and network management, in ad hoc networks, those functions are carried out by all active nodes. The Network Layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination host via one or more networks while maintaining the quality of service function. Gray Hole attack [5], which lead to dropping of messages. Attacking node first agrees to forward packets and then fails to do so. Initially the node behaves correctly and replies true Route Reply (RREP) messages to nodes that initiate RREQ message. Gray Hole attack may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface. In any case, nodes in the network will constantly try to find a route for the destination, which makes the node consume its battery in addition to losing packets. In our study, we simulated the Gray Hole attack in wireless ad-hoc networks and evaluated its damage in the network. Each intrusion detection [5][8] agent runs independently and detects intrusion from local traces. Only one-hop information is maintained at each node for each route. If local evidence is inconclusive, the neighboring IDS agents cooperate to perform global intrusion detection.

3. Background theory

Intrusion Detection System aimed to securing the AODV protocol using our Intrusion Detection system. They conclude that AODV performs well at all mobility rates and movement speeds. However, we argue that their definition of mobility (pause time) does not truly represent the dynamic topology of MANETs. In this thesis, the work of has been extended and the proposed protocol is called IDSAODV (Intrusion Detection System AODV). Use of AODV based intrusion detection. Our Intrusion Detection and Response Protocol for MANETs have been demonstrated to perform better than that AODV protocol and presence of Gray Hole Attack, in terms of false positives and percentage of packets delivered. Since the earlier work do not report true positive i.e. the detection rate, we could not compare our results against that parameter with their method[1]. The implementation of the IDSAODV protocol reported in this thesis has shown to work in real life scenarios. IDSAODV performs real time detection of attacks in MANETs running AODV routing protocol. Experimental results validate the ability of our protocol to successfully detect both local and distributed attacks against the AODV routing protocol, with a low number of false positives. The algorithm also imposes a very small overhead on the nodes, which is an important factor for the resource constrained nodes.

4. Proposed methodology

To explain the Gray Hole Attack we added a malicious node that exhibits Gray Hole Therefore, we cloned the "AODV" protocol, changing it to "IDSAODV" as we did "Gray hole" before. To implement the gray hole we changed the receive RREP function of the grayholeaodv.cc file but to implement the solution we had to change the receive RREP and create RREP caching mechanism to count the second RREP message.

In RREP mechanism, "RREP_Insert" function is for adding RREP messages, "RREP_lookup" function is for looking any RREP message up if it is exist, "RREP_Remove" function is for removing any record for RREP message that arrived from defined node and "RREP _Purge" function is to delete periodically from the list if it has expired. We chose this expire time "*BCAST_ID_SAVE*" as 6 (means 3 seconds).

In the "RecvReply" function, we first control if the RREP message arrived for itself and if it did, function looks the RREP message up if it has already arrived. If it did not, it inserts the RREP message for its destination address and returns from the function. If the RREP message is cached before for the same destination address, normal RREP function is carried out. Afterwards, if the RREP message is not meant for itself the node forwards the message to its appropriate neighbor.

We have changed all classes, functions, structs, variables and constants names in all the files in the directory except struct names that belong to AODV packet.h code. We have designed aodv and grayholeoadv protocols to send each other aodv packets.

Therefore we have changed only two files. The changes are explained below.

```
grayholeaodv {
set ragent [$self create-grayholeaodv-agent $node]

}

Simulator instproc create-grayholeaodv-agent

{

node

}

{

set ragent [new Agent/grayholeaodv [$node node-addr]]

$self at 0.0 "$ragent start" # start BEACON/HELLO Messages

$node set ragent_ $ragent

return $ragent

}

}
```

Figure.2 "grayholeaodv" protocol agent is added in "\tcl\lib\ ns-lib.tcl"

The key point in our work is that AODV and Gray Hole AODV protocol will send each other the same AODV packets. Therefore, we did not copy "*aodv_packet.h*" file into the grayholeaodv directory.

5. Simulation Environment

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper.

S.N.	Simulation Environment	Area 800m x 600m
1	Simulation Time	100 ms
2	Mobile Nodes	7 , 20
3	Transferring Mode	Unicast
4	Maximum Speed	10,20,40,60,80,100 (ms)
5	Traffic	CBR
6	Routing Protocols	AODV, Gray-Hole AODV, IDSAODV
7	Packet Size	512 bytes
8	Transport layer	TCP , UDP
9	MAC layer	802.11

Table 1. Table of simulation environment

Performance Metrics:

1. Throughput is the measure of how fast we can actually send through network. The number of packets delivered to the receiver provides the throughput of the network.

2. Packets dropped*:* Some of the packets generated by the source will get dropped in the network due to high mobility of the nodes, congestion of the network etc.

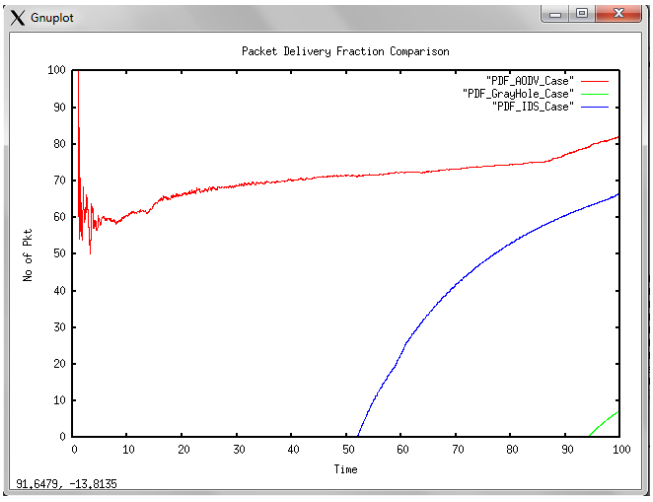
3. Packet delivery ratio**:** The ratio of the data packets delivered to the destinations to those generated by the CBR sources.

4. Normalized routing overhead**:** The number of routing packets transmitted per data packet delivered at the destination. Each hop-wise transmission of a routing packet is counted as one transmission.

5. Optimal path length**:** It is the ratio of total forwarding times to the total number of received packets.

6. Result and Analysis

Gray hole attack from network. IDS recover some percentage of packet delivery ratios. It is the ratio of data packets delivered to the destinations to those generated by the CBR sources is known as packet delivery ratio

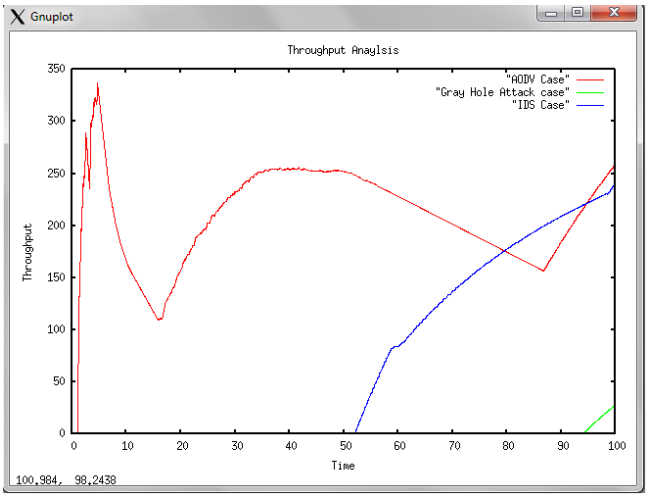


Gnuplot 1 for analyzing Packet Delivery Ratio of AODV, Gray hole AODV & IDSAODV for 7 nodes

- X co-ordinate = Simulation Time
- Y- co-ordinate = Packet Delivery Ratio
- Best Performance (High Throughput) – AODV.
- After Gray hole attack – Lower Ratio.
- Recovery from attack - Good.

Gnuplot 2 for Analyzing Throughput of AODV, Gray Hole Attack & IDS Case For 7 nodes.

Throughput is the average number of packets received per amount of time.



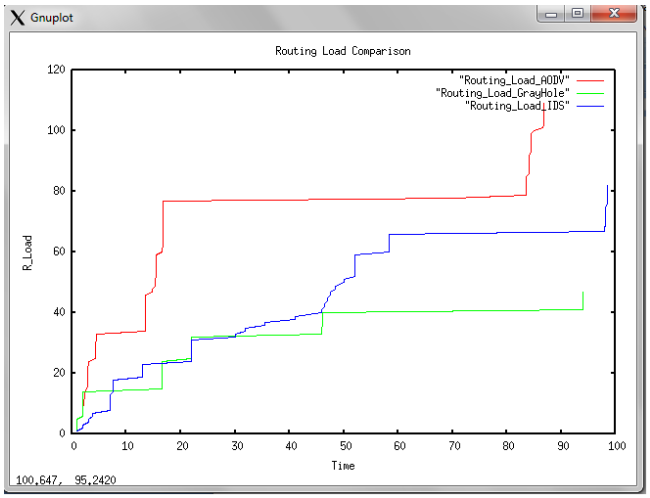
Description:

- X co-ordinate = Simulation Time
- Y co-ordinate = Throughput
- Best Performance –AODV case.
- Attack Time – Throughput is negligible.
- Recovery After IDS Module – Good.

When we look at this graph, which is for Throughput of all those three conditions, the throughput of AODV Normal case is better. But attack time data can't be send so that throughput is very low. After attack we attach IDS module in our work so that throughput is recover good.

Gnuplot 3 for Analyzing Routing Load of AODV, Gray Hole Attack case & IDS Case for 7 nodes.

Routing overhead is the number of routing packets transmitted per data packet delivered at the destination. Here, AODV which is in red in the graph shows maximum routing load but case of attack routing overhead is minimum and routing packets minimum is drawback because attacker node can't broadcast routing packet in network so that routing packet flooding is minimum. But after adding IDS Module we recover routing flooding scheme.

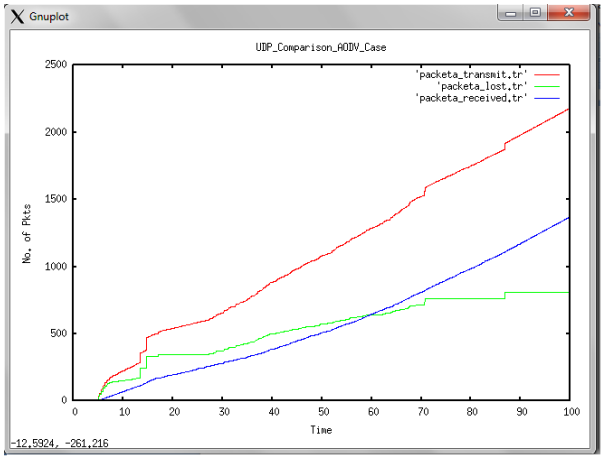


Description:

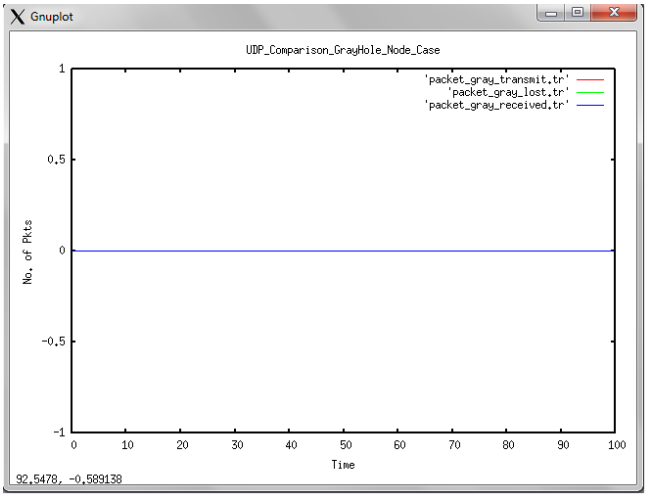
- X co-ordinate = Simulation Time
- Y- co-ordinate = Routing Load
- Best Route flooding – AODV.
- Attack Time – Jamming Routing Packets.
- Routing Recovery after IDS – Very Good.

Gnuplot 4 UDP packet analysis in AODV, Gray hole Attack and IDS Case

Here we generate test traffic UDP packets and analyze all three cases before attack, after attack and IDS case before attack UDP packets receive through genuine receiver and data loss is minimum but after set one node as gray hole attack. Attacker node receives all data packet and can't forward genuine receiver. Here graph show result of UDP packets analysis.

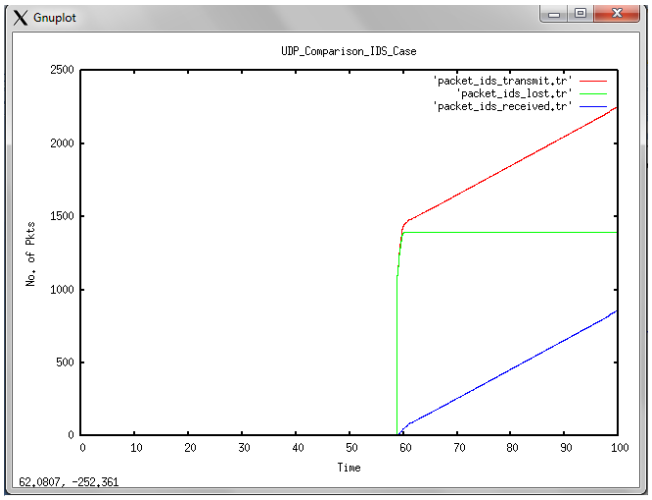


Before Attack with AODV Protocol Gnuplot 4 shows normal condition with AODV routing protocol and UDP packet transmission, lost, and receive graph this result conclude genuine receiver, receive at least 1400 packets out of 2100 packets.



Gnuplot -5 After Gray Hole Attack

Gnuplot 5 results comes after adding gray hole attack with UDP Packets analysis here result conclude gray hole node 0 can's forward any data packets to genuine receiver. so that our genuine receiver can't receive any data packets, result shows 0 packets receive by the receiver.

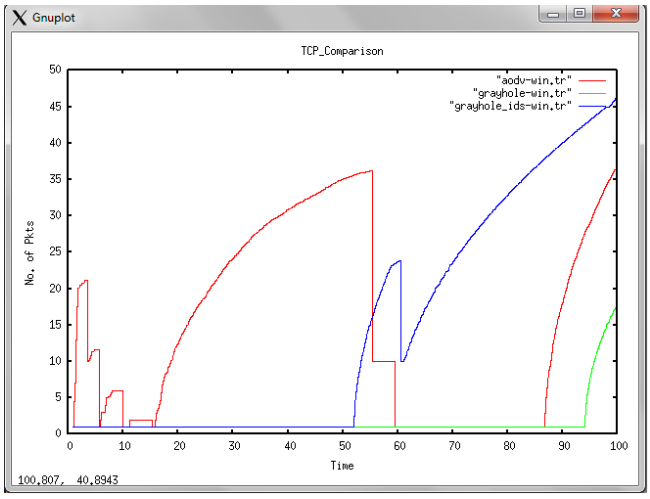


Gnuplot 6 After IDS Module UDP Analysis Graph

Here graph 6 shows recovery of UDP Packets after adding the module IDS in our Project, Result conclude at least 1400 packets receive by the genuine receiver after the 58 ms simulation time, Our IDS gives good recovery.

TCP packet analysis in AODV, Gray hole Attack and IDS Case

Here we analyze TCP Packets in all three conditions such as AODV (Normal case) Gray Hole attack scenario and after IDS Module (Recovery Module). Here Graph shows Through Red Lines Normal AODV case TCP Receive by the receiver, Green lines shows after gray hole attack and blue lines shows after recovery or IDS case. Result conclude after gray hole attack nodes comes in network maximum TCP data has been blocked. But after adding IDS Module maximum recovery results comes.



Gnuplot 7 TCP Packets Analysis in All Three conditions

7. Comparisons gray hole and ids module.

We have compared Routing Load, Throughput and Packet Delivery Ratio of all three conditions. The comparison of before any attack, after gray hole attack and IDS Module on which this project is based is as follows:

Performance Analysis for 7 mobile nodes with recovers

Percentage:

On the basis of above simulation we have concluded that Throughput, Routing Load and Packet Delivery ratio is very good recovered through our IDS in case of Gray Hole Attack. Here table 2 shows result with the simulation of 7 node cases.

TABLE 2 Comparisons between All Three Conditions

Sr. No	Category	AODV	Gray Hole attack	IDS
1.	Throughput	Good	Very low	Good Recovery (92.69%)
2.	Routing Load	Flooding good	Jamming	75.22% good
3.	Packet Delivery Ratio	Good	Very low	80.40% good

8. CONCLUSION

Every protocol being simulated using the same parameters that had been discussed to ensure the simulation produced accurate results. In MANET we can find the performance and QoS of the various matrices and overcome the destroyed packet and drop rate, Transmission rate of these three metrics and compare with the AODV Protocols. The analysis had been done through simulation using commercial and highly reliable tool like Network Simulator (NS2).The performances comparison of the four routing protocols for mobile ad hoc networks.Here we gives summarize result in normal AODV protocol case, Gray Hole Attack case and IDS case that time we take parameter total number of packets send, total number of packets receive by the genuine receiver, routing load packet delivery ratio, Average end to end delay etc.

9. FUTURE SCOPE OF WORK

In this work we detect only gray hole attack and recover through IDS, and only routing misbehavior detection are done. In future we enhance through detection every layer misbehavior detection and transmission rate of metrics compare with the all Protocols. We also update IDS module and 100% recovery procedure done. We can also apply the other techniques like packet capturing, false route forwarding, changing source and destination addresses etc.

10. REFERENCES

[2] Sukla Banerjee "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks" Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA

[3] S. Marti, T. J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehavior in Ad Hoc Networks", Proc. 6th Annual Int'l. Conf. Mobile Comp. and Net., Boston, MA. pp. 255-265. August 2000.

[4] P. Misra,. "Routing Protocols for Ad Hoc Mobile Wireless Networks",http://www.cse.wustl.edu/~jain/cis78899/adhoc_routing/index.html, 14 May 2006.

[5] Piyush Agrawal and R. K. Ghosh," Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks".

[6] YONGGUANG ZHANG, WENKE LEE, AND YI-AN HUANG. Intrusion detection for wireless Ad Hoc networks. In Mobile Networks and Applications. ACM, 2002.

[7] H. Deng, W. Li and D. P. Agrawal, "Routing Security inWireless Ad Hoc Networks". University of Cincinnati, IEEE Communication Magazine, October 2002.

[8] HU, Y.-C., PERRIG, A., AND JOHNSON, D. B. Ariadne: A Secure On Demand Routing Protocol for Ad Hoc Networks. In Eigth ACM International Conference on Mobile Computing and Networking (Mobicom 2002) (Sept. 2002).

[9] D. E. DENNING, "An Intrusion Detection Model", IEEE Transactions in Software Engineering, vol. 13, no2, February 1987.

[10] S. BHARGAVA, D. P. AGRAWAL, "Security Enhancements in AODV protocol for Wireless Ad hoc Networks", in IEEE Semi-annual Proceedings of Vehicular Technology Conference (VCT'01), 2001.

[11] SCOTT CORSON AND JOSEPH MACKER, "Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations". Internet-Draft, draft-ietf-manet-issues-01.txt, March 1998. Work in progress.

[12] I. STAMOULI. Real-time intrusion detection for ad hoc networks. Master's thesis, University of Dublin, September, 2003.

[13] C. E. Perkins, E. M. Belding-Royer, and S. R. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing.

[14] K Fall and K. Varadhan, "The NS Manual" , November 18, 2005, http://www.isi.edu/nsnam/ns/doc/ns_doc.pdf ,25 July 2005.

[15] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[16] K. Elissa, "Title of paper if known," unpublished.

[17] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[18] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[19] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[20] Electronic Publication: Digital Object Identifiers (DOIs): Article in a journal:

[21] D. Kornack and P. Rakic, "Cell Proliferation without Neurogenesis in Adult Primate Neocortex," Science, vol. 294, Dec. 2001, pp. 2127-2130, doi:10.1126/science.1065467. Article in a conference proceedings:

[22] H. Goto, Y. Hasegawa, and M. Tanaka, "Efficient Scheduling Focusing on the Duality of MPL Representatives," Proc. IEEE Symp. Computational Intelligence in Scheduling (SCIS 07), IEEE Press, Dec. 2007, pp. 57-64, doi:10.1109/SCIS.2007.357670.