Intelligent Honeypot Agent for Blackhole Attack Detection in Wireless Mesh Networks

Anoosha Prathapani[1], Lakshmi Santhanam[2] and Dharma P. Agrawal[2]

[1]Department of ECE, [2]Department of CS
University of Cincinnati, Cincinnati, OH, USA
Email: prathaaa@ece.uc.edu, santhal@cs.uc.edu, dpa@cs.uc.edu

Abstract—**Wireless Mesh Networking (WMN), the static mesh routers (MRs) cooperatively relay each other packets to the Internet Gateway (IGW). The routing protocols assume all the nodes in the network to be non-malicious. However, the open architecture of WMNs paves way to malicious attackers who can exploit hidden loopholes in the routing protocol. In this paper, we mainly focus on the vulnerability of the network to a suction attack called blackhole attack. In detecting such attacks, we explore the use of intelligent agents called Honeypots which are roaming virtual software agents that generate a dummy Route Request (RREQ) packets to lure and trap blackhole attackers. We illustrate the performance of our proposed detection approach by extensive simulation results using the ns-2 simulator.**

***KEY WORDS*—AODV, Blackhole, Honey pots, Malicious, Spoofed, Wireless Mesh Networks.**

I. INTRODUCTION

In recent years, Wireless Mesh Network (WMN) [1] is emerging as a new upcoming technology in providing ubiquitous broadband Internet services to a large community of users. The WMNs is a promising technology that offers a good coverage area through multi-hop communication without any degradation in channel capacity. The WMNs are organized in a hierarchical manner and consists of Mesh Routers (MRs), Mesh Clients (MCs), and Internet Gateway (IGW) as shown in Figure 1 [2]. The IGWs are MRs that are connected to the wired network and form the top level of the hierarchy. The MRs (level 2) are inter-connected by an ad hoc network formed by wireless links among themselves [3-4]. The MRs route the traffic of mesh clients to the IGWs in a multi-hop fashion. The mesh clients (level 3) connect to the nearest available MR in a single/multi hop fashion.

Though there are several ongoing research works on WMNs, security is very much in its infancy. The open infrastructure, wireless communication, multi-hop communication, different management styles of the WMNs paves way to malicious attackers in the network [5]. Any malicious attackers in the network can exploit ambiguities in the underlying routing protocols and cause various types of attacks such as Blackhole Attack, Selfish node Attack etc. [6-9].

978-1-4244-5113-5/09/$25.00 ©2009 **IEEE**

In this paper, we specifically focus on the problem of detecting malicious MR that bypasses route lookup process and instead generates spurious route replies to all incoming route request query. It generates route replies in such a way that source would select this MR as an intermediate MR to route its traffic. It falsifies the sequence number field (high) and the hop count (low) field in the reply packet and advertises itself as the best possible route. Upon receiving the data traffic, it unscrupulously drops all the traffic. Thus, in a way the malicious MR imitates the "blackhole" that attracts all particles towards itself due to its enormous gravitational pull in the Universe. Hence, we name this egregious MR as a "blackhole node" or "blackhole MR" in the network and the attack is called "blackhole attack".

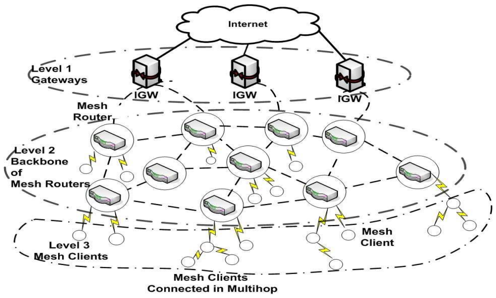


Figure 1. Hierarchical WMN architecture

The only possible counter-measure to prevent the infiltration of such an attack is to authenticate the sequence number and hop-count updates received from other MRs. Though, secure routing protocols such as SEAD [9], Ariadne [10] attempt to address this issue, it is not a complete solution to thwart such an attack as MRs are deployed at public places.

In this paper, we propose a pervasive monitoring scheme, using intelligent software agents called Honeypots [11]. Honeypots are popular agents that are used in tandem with Intrusion Detection Systems (IDS) to detect the malicious attackers [12]. It has been widely used in corporate networks along with firewalls to prevent the infiltration of Denial of Service Attacks (DoS Attacks) [13]. Rather than deploying them on a MR to camouflage its location, we employ honeypots [13] as mobile software agents that discretely tours the WMN, examining the status of each region. Also, owing to the static nature of WMNs, if a honeypot is deployed on a MR, it results in poor coverage of the detection scheme. Honeypots are synonymous to secret police officers who conduct random investigation.

A honeypot generates a dummy Route Request (RREQ) to a known destination to which it already knows the route. The sole purpose of luring blackhole nodes is to send a falsified reply. Unlike traditional honeypots, that capture only packets directed to them, our proposed mobile mechanism is guaranteed to lure all attackers in the network. Upon observing the RREQ of the honeypot, a malicious blackhole node produces a falsified route reply (RREP). It advertises itself as the best path (high sequence number and shortest hop) to given destination. The malicious blackhole node thus advertises itself as the best path. This primarily exploits the availability of multipath routing option available in WMNs and validates the integrity of a route reply originating from a MR. The logs collected in the honeypots serve as a useful tool to understand the modus operandi of the blackhole node, so that new exploitation trends can be understood. We observe through our extensive simulation, when the network is 20% compromised, MR advertising itself as best path is found to be blackhole with approximately 97% accuracy.

The remainder of this paper proceeds as follows. In the next section, we review some of the related work. Section 3 shows various ambiguities in the route discovery phase of Ad hoc On-Demand Vector (AODV) protocol. In section 4, we outline the architecture of our proposed honeypot based blackhole attack detection scheme. Section 5 gives an overview of the performance analysis of the proposed approach using simulations in ns-2 simulator [14]. Finally, we conclude the paper in Section 6.

II. Related Work

Although our work is not based on security related issues in the ad hoc and sensor networks, we discuss these in the related work. In [6] Ning et al. have mentioned about the misuses of AODV protocol and several classes of insider attacks. Bhargava et al. [7] proposed an Intrusion Detection and Response Model to detect malicious activities that can be carried out in a routing protocol and respond if they found such an activity by observing anomalous behavior using IDM (Intrusion Detection Model) and IRM (Intrusion Response Model) (IRM) to isolate them [7].

Huang et al. [15] proposed a cooperative Intrusion Detection System (IDS) for various kinds of attacks in ad hoc networks where attacker not only affects routing protocol but also IDS. However the results obtained for blackhole attack detection are less pleasing and also appeared to be a costly affair. Ruiz et al. [16] proposed a scheme where they deal with the blackhole attack in the OLSR routing protocol for VoIP calls. Shurman et al. [17] proposed two solutions to detect the blackhole attack and the major drawbacks are: the associated time delay because of shared hops along the redundant paths and also usage of two additional tables that are frequently updated for every node. However, these solutions fail for a group of attackers in the network. Deng et al. [18] consider the routing security issues of mobile ad hoc networks and provide a solution for a blackhole problem in AODV.

Ramaswamy et al. [19] proposed a solution to the cooperative blackhole attack in the network where they introduce an extended Data Routing Information (DRI) table. Although, cross checking helps in identifying and securing against the cooperative blackholes, the power constraints and low processing speeds limit this solution. Karakehayov et al. [20] proposed a routing algorithm called REWARD to detect the blackhole attack cases for a single and group of blackhole attackers in sensor networks using two broadcast messages. However, this technique reduces the vulnerability of the network at the expense of utilizing many message exchanges that consume large amount of energy and power from the batteries. Karlof et al. [21] provided a detailed description of security threats against routing protocols in the area of sensor networks and potential counter measures of selective forwarding. However, sensor networks have several resource constraints like power, memory which may get exhausted due to multipath forwarding [21].

III. Blackhole Attack Illustrated

In this section, we explain operation of blackhole attack by using AODV as an example protocol and then delineate vulnerabilities in AODV protocol.

A. Vulnerabilities of AODV

AODV protocol is an on-demand routing protocol which initiates a route discovery process only when an originating MR desires to send some traffic to an unknown destination. The originating MR broadcasts a Route Request (RREQ) packet, with sequence number set to an unknown value. Then the neighbors re-broadcast the RREQ packets only if it does not have a fresh enough route. This process continues until the RREQ reaches the destination MR or an intermediate MR that has a fresh enough route.

However, if a malicious blackhole MR is present in the network, it generates a false RREP for all the RREQ packets received by it. During a normal operation, if it is aware of the route to the destination, it generates a RREP to the source. Otherwise, it returns a NULL value. However, a malicious blackhole node is mis-configured to bypass this lookup process and always generates a RREP. It advertises itself to be closest to the destination (stamps lower hopcount value in RREP) and in order to ensure this RREP is favored by the source it also falsifies the sequence number to be an arbitrarily high value. The originating MR then sends the data packets to the malicious blackhole node which then drops all the data traffic unscrupulously. The malicious blackhole node in this manner systematically traps all its neighboring MRs by sucking their data traffic. Thus, the attacker can attract all the traffic towards itself and thereby drops the entire network traffic. Such an attack results in severe performance degradation in WMNs, especially if the malicious blackhole node is located near the IGW. The blackhole node also decreases the network throughput, results in network partitioning, increases end-to-end delay and most severely results in denial of service.

B. Impact of Black Hole Attack

In this sub section, we consider the impact of black hole malicious node in WMNs through simulations in ns-2. We simulate a simple IEEE 802.11s based network with 49 MRs (7 x 7) deployed within a grid like fashion in an area of 1500 x 1500 meters. We randomly attach 2-3 mesh clients to each of these MRs. The MRs communicates with each other using the legacy IEEE 802.11 based interface, forming a wireless backbone. We assume the communication between a MR and a MC does not interfere with the communication between two MRs.

We start flows from the clients that are being serviced by MRs. From here on when we say a flow is started from the MR, we mean that the client has started its flow. We initiate 20 UDP flows sending traffic at a constant rate of 512 bytes. IEEE 802.11 is used for channel arbitration with the transmission range and the channel capacity is set to 250 m and 11 Mbps respectively. AODV is the underlying protocol. The total simulation time is set to 500 seconds. Each simulation has been repeated with 10 different traffic profiles containing randomly chosen traffic sources. One of the MR function is to have flows directed towards the IGW.

We randomly choose one of the MRs as the malicious blackhole MR, which attracts all the network traffic towards itself by advertising itself as a nearest route (highest sequence number and shortest hop count). Figure 2 shows the effect of the blackhole node (MR) on the instantaneous throughput of three affected flows at the IGW, for the randomly chosen traffic profiles. We consider the case where a blackhole MR is randomly selected and initiates the flows from one MR to other MR.

The throughput is very low for those flows with the presence of blackhole MRs when compared to the throughput of other flows with no blackhole MRs. It is observed that the throughput decreases as the number of blackhole MRs in the network increases. In Figure 2, we observe that the throughput of *Flow-1* is high when compared to the other flows, *Flow-2* and *Flow-3*. The maximum throughputs of *Flow-1, Flow-2* and *Flow-3* are observed to be 105kbps, 40kbps and 60kbps respectively.

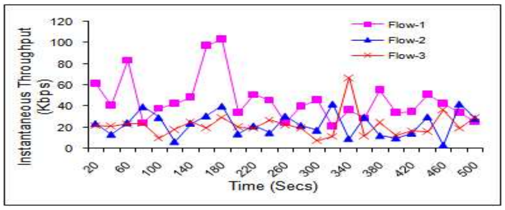


Figure 2. Instantaneous Throughput of flows during attack

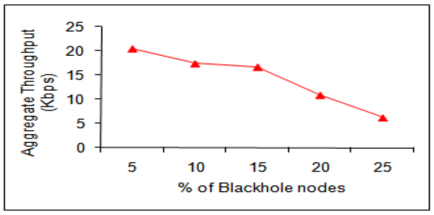


Figure 3. Aggregate Throughput obtained for various Blackhole MRs

IV. HONEYPOT BASED DETECTION SCHEME

In this section, we first present the system architecture and then we describe the proposed detection scheme.

A. Detection System Architecture

The system architecture of the proposed honeypot detection scheme is illustrated in Figure 4 and has following components:

Route Module: The Route module consists of a Route Reply Analyzer, Dummy Packet Generator, and Constant Bit Rate Unit. The honeypot positions itself next to the 'testee' and generates a RREQ to a certain known destination. When the 'testee' receives such a RREQ, it generates a RREP packet. In order to determine if this RREP is valid or spurious, the Route Reply Analyzer module analyzes the received reply packet. This module analyzes the RREP packet and makes a note of the sequence number and the hop count in the RREP packet. It then triggers the Dummy Packet Generator to generate dummy packets to be given to the testee. These dummy packets are used to determine whether the 'testee' under consideration is malicious or reliable. Such traffic is sent towards a 'testee' to be forwarded to a given destination. The Dummy Packet Generator uses a Constant Bit Rate Unit that generates UDP packets at a constant bit rate. However, the unit is modified such that payload is stuffed and padded with random data.

Feedback Module: The feedback module plays a critical role in the detection of the blackhole MR. The feedback module gives the information that it has learned from the alternate path and dispatches a query packet to the known destination to determine if it has received any traffic packets from the testee. If the packet is received by the destination MR, it acknowledges the receipt of the traffic and unicasts a trace reply to the honeypot. Depending on this answer, the feedback module then declares the 'testee' to be reliable or a malicious attacker.

Alert Module: If a malicious activity is detected by the feedback module, it is fed as input to the alert module. We consider positive output as an indication of a normal condition and a negative output as an indication of an attack. When an attack is detected, an alert is issued by the alert module to block the intrusive activity. The alert module broadcasts the identity of the malicious blackhole to all MRs in the network so that they stop forwarding traffic through it and discard any route reply packets originating from the blacklisted blackhole MR.

Interactive log: This gives the information about the strategies that the honeypot has applied to lure the malicious MR. It also gathers information on the route replies that the attacker uses to lure other MRs in the network. The report of the entire route discovery phase and alerts are lodged in the Interactive log.

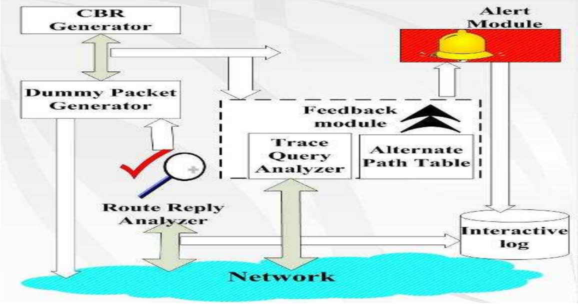


Figure 4. Honeypot System Architecture

B. Honeypot Agents in Detection

We model the detection of blackhole attack using honeypots as software detection agents. We illustrate blackhole attack in in Figure 5. To detect such attack we deploy the honeypots on MRs to lure the malicious attackers and these honeypots are synonymous to the network cops. The proposed scheme is explained through an illustrative Figure 6. We explain various stages as follows:

1. The Honeypot agent sends a RREQ packet to the 'testee'. The source address is that of the MR on which honeypot is residing and the destination address is that of a randomly chosen known destination. We assume that the Honeypot is already aware of a route to the destination and issues an exclusive RREQ to determine the validity of MRs in its neighborhood.

2. The 'testee' sends a RREP packet back to the honeypot that could be valid or spurious. Hence, in the subsequent steps, our honeypot detection scheme enables to distinguish the integrity of RREP packets.

3. Next, the honeypot prepares a testee data packet and forwards it to the 'testee'. The testee packet is like any other regular data packet. However, its payload is masked and padded with random data stream because of which it is not possible for the testee to conclude that it is originating from the honeypot.

4. The honeypot sends a 'Query packet' to the destination about the packet it has already forwarded to the 'testee' in Step 3. It then sends the query packet through this known route. Various fields in the query packets consist of:

a.) Sequence Number: It is the sequence number of the packet generated from the source.

b.) Source IP address: The source IP address is the address of the MR on which the honeypot resides.

c.) Destination IP address: It is the address of the known destination as per the honeypot detection scheme.

d.) Testee id: Source IP address of the testee being evaluated.

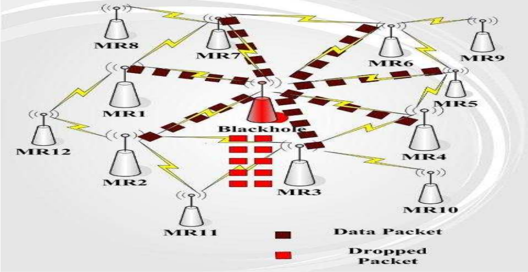


Figure 5. Illustration of Blackhole Attack

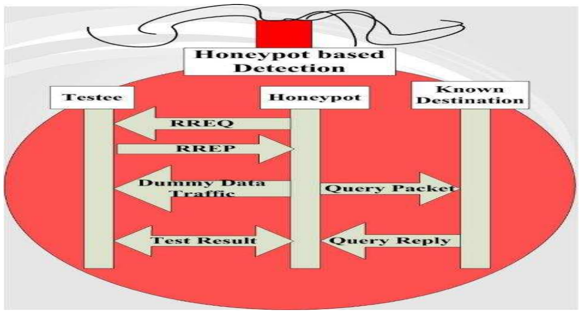


Figure 6. Honeypot based Blackhole Attack Detection

5. When a destination receives such a trace query, the destination processes it by examining its Most Recently Received Traffic Cache, including the source ids, a timestamp when it was received and count of number of packets received from this source

6. If the destination finds the testee id in its traffic cache, it prepares a "Query reply packet", the destination address of which is equal to the source address of honeypot from which query packet came. The query reply packet also includes the following data in its information field: count of number of packets received and the timestamp of last received packet. Thus, the Query reply packet is unicast to the honeypot using the same route on which trace packet came. Various fields in the Query reply packet are same as the fields in Query Packet and are explained as follows:

a.) Sequence Number: This is the sequence number of the IP packet being originated at the destination.

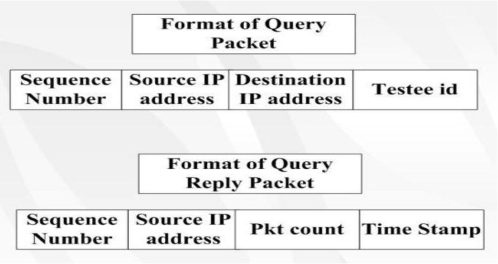
b.) Source IP Address: Address of destination MR that the packet is being sent from.

c.) Destination IP Address: Address of the MR on which honeypot resides.

d.) Packet Count: Keeps count of the number of packets received from the testee under consideration.

e.) Time Stamp: Time information about the last packet that it received.

7. When the honeypot agent receives the Query reply packet, it hands it to the feedback module. Depending on the content of the information field, integrity of the testee is determined. If the packet was received at the destination, the 'testee' is considered to be "Good MR". If the field is empty, then the 'testee' is considered to be a malicious attacker. The format of the Query packets is shown in Figure 7. The feedback module uses the alternate path to retrieve the information.



Format of Query Packet

Sequence Number	Source IP address	Destination IP address	Testee id

Format of Query Reply Packet

Sequence Number	Source IP address	Pkt count	Time Stamp

Figure 7. Format of Query Packets

8. The alert module in the honeypot then advertises that the 'testee' under consideration is a malicious blackhole attacker. Thus, other MRs in the network avoids forwarding its packet through the malicious blackhole MR.

9. This information is also sent to the IGW which then passes it to the Internet Service Provider (ISP) to remove a malicious MR.

Thus, honeypots act as network cops, examining the integrity of the routing module of the MRs in the network. The mobile honeypot can be made to move along the pre-configured itinerary in the network. Honeypot can also conduct random walk in the network, starting from IGW to the leaf MRs in a depth first fashion.

V. PERFORMANCE ANALYSIS

In this section, we study the performance of our proposed detection of blackhole attack using honeypots as detection agents with simulations performed using ns-2 [14]. We use the same scenario described in Section 3. The total simulation time is set to 150 seconds. We compromise for about 20% of MRs, observe the effect of blackhole attack on the network and calculate the throughput of the network, and evaluate the following metrics:

- True Positives (TP): Number of times an alert is raised, when an attack is present,
- False Negatives (FN): Number of times an alert is not raised when an attack is present,
- False Positives (FP): Number of times an alert is raised, but attack is not present and
- True Negatives (TN): Number of times no alert is raised, when an attack is present.

The performance of our scheme is based on the TPR (True Positive Rate) and FPR (False Positive Rate).

TPR: This is the ratio of number of alerts when there is an attack to total number of attacks as:TPR $=TP / (FN + TP)$

FPR: This is the ratio of number of alerts when there is no attack to total number of attacks as: FPR= $FP/(TN+FP)$

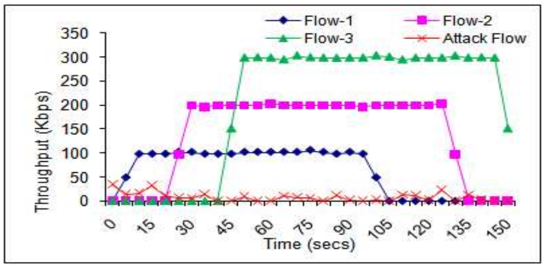


Figure 8. Instantaneous Throughput of the flows with our scheme

We determine instantaneous throughput for the flows initiated with a randomly chosen malicious MR. We start a set of flows at different MRs and observe the throughput of each flow in the presence of blackhole MRs. Figure 8 shows the improvement in the instantaneous throughput due to the incorporation of our scheme. The traffic flow *Flow-1* shown in the Figure 8 has a throughput of the 100kbps which is an improvement over the default case. *Flow-2* has a throughput of 200kbps and *Flow-3* has the throughput of 300kbps. From Figure 9, we observe that, with the implementation of the scheme there is almost 80% of improvement in the aggregate throughput than the aggregate throughput in the default case, in the first instance when 5% of network is compromised. As the percentage of compromised MRs in the network increase, the aggregate throughput decreases in both the cases but still the throughput with the scheme is very high than in the case wihtout any honeypot based detection scheme. In Figure 9. it is observed that when the network attackers have been increased from 5% to 20%, the TPR falls from 100% to 87% approximately. This shows that the scheme is detects almost all the network attackers, even when the number of attackers have been increased.

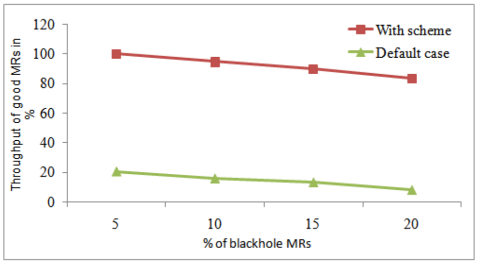


Figure 9. Aggregate Throughput with Scheme and Default Case

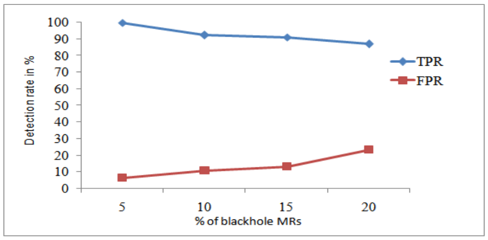


Figure 10. TPR vs FPR Variation

As the number of attackers increased, the FPR also increases. The graph in Figure 10 shows that the proposed honeypot based detection scheme has a very high TPR

(100%) and a low FPR (23%) and therefore, detects malicious attackers accurately and efficiently.

Next we study the Receiver Operating Characteristics (ROC) curve (TPR vs. FPR). The ROC curve reflects the tradeoffs in the sensitivity of the detection algorithm. Figure 11 shows the ROC curve for our detection scheme. We observe that in our scheme very few innocent MRs are reported to be malicious MRs as seen from the value of FPR which is 0.05 and all the compromised blackhole MRs to be correctly detected and reported as seen from the value of the TPR which is very close to 1. Similar kind of low FPR vs. high TPR values are observed by varying the percentage of the number of malicious blackhole attackers in the system.

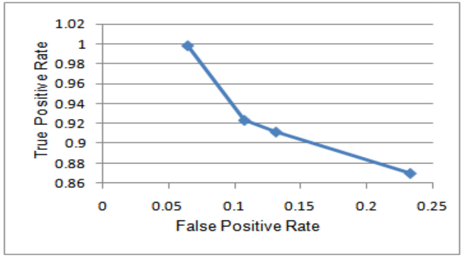


Figure 11. RoC Characteristics

CONCLUSION

In this paper, we have proposed an intelligent honeypot based detection system to identify the blackhole attackers in WMNs. Through extensive simulations, we demonstrate that our honeypot based detection model aids in the increase of throughput in a WMN with blackhole MRs and has a high detection rate and low false positive rate. As a part of our future work, we plan to use honeypot detection agents to detect various other attacks. We also plan to use the Weighted Cumulative Expected Transmission Time as a routing technique to detect blackhole attackers in WMNs.

References

[1] N. Nandiraju, D. Nandiraju, L. Santhanam, B. He, J. Wang, and D. P. Agrawal, "Wireless mesh networks: current challenges and future directions of web-in-the-sky," in *IEEE Communication*, Aug.2007, vol.14, no.4, pp. 2-12.

[2] I. F. Akyildiz and X. Wang, "A survey on Wireless Mesh Networks," in *IEEE Communication*, Sept. 2005.

[3] D. P. Agrawal, and Q. –A. Zeng, *Introduction to Wireless and Mobile Networks*, 2nd Edition, Brookes Cole Publishing, April 2005.

[4] C. Cordeiro, and D. P. Agrawal, *Adhoc and Senor Networks: Theory and Application*, World Scientific Publishing, Spring 2006.

[5] N. Ben Salem and J. P. Hubaux, "Securing Wireless Mesh Networks," in *IEEE Wireless Communications*, Apr. 2006.

[6] P. Ning and K. Sun, "How to misuse AODV: a case study of insider attacks against mobile ad hoc routing protocols," *Ad Hoc Networks*, vol. 3, no.6, pp. 795-819, 2005.

[7] S. Bhargava and D. P. Agrawal, "Security Enhancements in AODV protocol for Wireless Ad Hoc Networks," *IEEE Vehicular Technology Conference*, VTS 54th, 2001, vol. 4, pp. 2143-2147.

[8] L. Santhanam, A. Mukherjee, R. Bhatnagar, and D. P. Agrawal, "A Perceptron based Classifier for Detecting Malicious Route Floods in Wireless Mesh Networks," In *3rd Intl Conference on Wireless and Mobile Communications*, March 4-9, 2007 - Guadeloupe,.

[9] Y . Hu , D. B. Johnson, and A. Perrig , "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," *Ad Hoc Networks*, 2003, pp. 175-192.

[10] Y. Hu, A. Perrig, and D. B. Johnson, "Ariadne: a secure on-demand routing protocol for ad hoc networks," In *Proc. of ACM Mobicom*, pp. 12-23, 2002.

[11] The Honeynet Project, (http://www.honeynet.org/)

[12] S. Khattab, R. Melhem, D. Mosse, and T. Znati, "Honeypot back-propagation for mitigating spoofing distributed Denial-of-service attacks," *Journal of Parallel and Distributed Comp.*, vol. 66, pp. 1152-1164, April 2006.

[13] L. Spintzer, "The Honeynet Project: Trapping the Hackers," *IEEE Security and Privacy Magazine*, vol .1, no. 2, March 2003.

[14] Network Simulator (NS-2), http://www.isi.edu/nsnam/ns/index.html

[15] Y. -A. Huang and W. Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks," *Proceedings of 1st ACM Workshop on Ad hoc and Sensor Networks*, pp. 135-147, 2003.

[16] J. –C. Ruiz, J. Friginal, D. –Andres and P. Gil, "Blackhole Attack Injection in Ad hoc Networks," *Fault Tolerance Systems Group* (GSTF), http://www.ece.cmu.edu/~koopman/dsn08/fastabs/dsn08fastabs_ruiz.pdf

[17] M. A. –Shurman, S. -M. Yoo, and S. Park, " Blackhole Attack in Mobile ad Hoc Networks," In *Proceedings of ACM of 42nd annual South-East Conference Regional Conference*, pp. 96-97,2004.

[18] H. Deng, W. Li, and D. P. Agrawal, "Routing Security in Wireless Ad Hoc Network," *IEEE Communications Magazine*, vol. 40, no. 10. October 2002.

[19] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, " Prevention of Cooperative Black Hole attack in Wireless Ad Hoc Networks," *Proceedings of the International Conference on Wireless Networks*, June, 2003.

[20] Z. Karakehayov, "Security-Lifetime tradeoffs for Wireless Sensor networks," *Emerging Technologies & Factory Automation, ETFA*, IEEE, pp. 246-250, Sept., 2007

[21] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," in *First IEEE International Workshop on Sensor Network Protocols and Applications* (SNPA 03), pp.113-127, May 2003.