Defending Selective Forwarding Attacks in WMNs

Devu Manikantan Shila ($Student\ Member$, $IEEE$), Tricha Anjali ($Member$, $IEEE$)
Department of Electrical and Computer Engineering
Illinois Institute of Technology
Chicago, IL 60616
Tel:+1-312-567-3384
Email: {dmanikan, anjali}@iit.edu

***Abstract*—Wireless Mesh Networks (WMNs) have emerged recently as a promising technology for next-generation wireless networking to provide wide variety of applications that cannot be supported directly by other wireless networks. In WMNs, security is turning out to be a major concern and little attention has been paid to this topic by the research community. In this paper, we investigate a serious security threat known as the selective forwarding attack (gray hole attack). In a selective forwarding attack, a malicious node refuses to forward all or a subset of the packets it receives. Such selective dropping is challenging to defend against. In this paper, we present an algorithm to defend against selective forwarding attacks based on AODV routing protocol. The first phase of the algorithm is $Counter\text{-}Threshold\ Based$ and uses the detection threshold and packet counter to identify the attacks and the second phase is $Query\text{-}Based$ and uses acknowledgment from the intermediate nodes to localize the attacker. We also present simulation results to illustrate the efficiency of the proposed algorithm. To the best of our knowledge, this is the first paper to present an algorithm for defending selective forwarding attacks in WMN.**

***Index Terms*—Wireless Mesh networks, Selective forwarding attacks, Black hole attacks, Detection threshold, ETX**

I. Introduction

Wireless Mesh Networks (WMNs) [1], [2], [3] have emerged recently as a promising technology for next-generation wireless networking to provide better services that cannot be supported directly by other wireless networks. A WMN consists of two types of nodes: mesh routers and mesh clients. Mesh routers form the backbone and they have minimal mobility which guarantees high connectivity, robustness etc. The mesh client nodes can be stationary or mobile.

Self-organization and self-configuration are the desired features of WMN. These features provide many advantages for WMN's like good reliability, market coverage, scalability and low upfront cost. WMN also gained significant attention because of the numerous applications it supports, e.g., broadband home networking, community and neighborhood networks, delivering video, building automation, in entertainment and sporting venues etc. However, WMNs lack efficient security solutions in various protocol layers [1]. This is attributed to many factors [1], [4]. First, in a wireless network all communications go through shared wireless links which makes it prone to physical security threats as opposed to wired networks. Second, the nodes are mobile and can move in any direction. Whenever the topology changes, the nodes exchange this information to establish a route between source and destination. Since the message are transmitted through wireless links, any malicious node can give incorrect topology updates and other nodes may unknowingly forward the messages. Finally, WMNs have distributed architecture and hence decision making in a WMN will rely on the successful cooperation of nodes. If a malicious node refuses to cooperate with other nodes, then the distributed operation of the network will fail.

In general, WMNs lack efficient and scalable security solutions due to open medium, dynamic topology, and absence of central authority. In a WMN, the mesh clients can access the network through mesh routers or directly via other mesh clients. To support end to end communication, effective routing protocols are required. Hence routing plays an important role in the entire network and therefore focus of certain types of malicious attacks like gray hole attacks, black hole attacks, sybil attacks, sinkhole attacks etc [5], [6].

Although the network layer of WMN is threatened by various attacks, we focus on the selective forwarding (gray hole) attack. Defending selective forwarding attacks in the area of ad hoc and sensor networks have already been studied. Although our work is not about defending security threats in ad hoc and sensor networks, we review the following previous works.

In [4], the authors discuss the routing security issues of mobile ad hoc networks and present a solution for the black hole problem in AODV [7]. But the main limitation of the scheme is that it works on an assumption that the malicious node do not launch group attacks against ad hoc networks.

In [5], the authors provide a detailed description of security threats against routing protocols and the counter measures in the area of sensor networks. Karlof $et\ al.$ first proposed selective forwarding attacks and suggested that multi path forwarding can be used to counter selective forwarding attacks in sensor networks. But multi path forwarding suffers from several drawbacks mainly overhead, poor security resilience [5], [8].

In [8], the authors propose a multi hop acknowledgment scheme for detecting selective forwarding attacks. The intermediate nodes are responsible for detecting the misbehavior of the nodes. If a suspicious behavior is detected, it will generate an alarm packet and deliver to source node. The scheme has two main disadvantages. First, the intermediate nodes in the forwarding path suffer from high overhead. Second, the

978-1-4244-2030-8/08/$25.00 ©2008 IEEE.

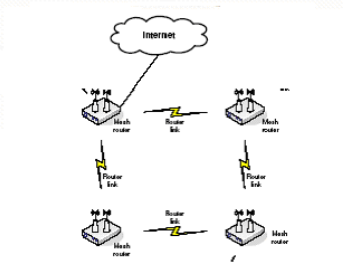

Fig. 1. Infrastructure WMN: Mesh routers are static and form the backbone of the network whereas mesh clients can be static or mobile. Mesh clients rely on mesh routers to forward the data to destination [1]

scheme would not work if a node is compromised during the deployment phase by the attacker.

In this paper we analyze the security threat known as the selective forwarding attack (gray hole attack) and propose an algorithm to defend against the attacks based on AODV [7]. The first phase of the algorithm is $Counter - Threshold\ Based$ and uses the detection threshold and packet counter to identify the attacks and the second phase is $Query\text{-}Based$ and uses acknowledgment from the intermediate nodes to localize the attacker. Although we present the algorithm based on AODV, it can be easily applied to existing routing protocols like DSDV, DSR etc.

The rest of the paper is organized as follows: Section II presents the network architecture and selective forwarding attacks against network protocols in detail. In section III we describe the mechanism to defend against the selective forwarding and black hole attacks. Section IV present an analysis of detection threshold. In section V we describe the simulation setup and the performance results. Finally, we conclude this paper and discuss our future work in Section VI.

II. Problem Statement

A. Network Architecture

We consider a multi-hop infrastructure WMN [1], [11] as shown in figure 1. Infrastructure WMNs are commonly used in community and neighborhood networks. In this type of network, mesh routers are deployed on the roof of houses in neighborhood and they communicate with one another to form a multi-hop static wireless backbone. The client nodes access these static mesh routers to forward the traffic to other nodes. Thus mesh routers take part in the process of forwarding packets, providing end to end communication between nodes not in the direct range.

B. Gray Hole/Selective Forwarding Attacks

In this attack, a malicious node refuse to forward certain packets and simply drop them. If a malicious node drop all the packets, the attack is then called black hole. To launch a selective forwarding attack, an attacker may compromise or hijack the mesh router that belong to the network (known as internal attacks) or attack the network from outside (known as external attacks) by jamming the communication link between the routers. Black hole attacks are easy to detect as opposed to selective forwarding attacks which selectively drops packets originating from a single IP address or a range of IP addresses [12] and forwards the remaining packets.

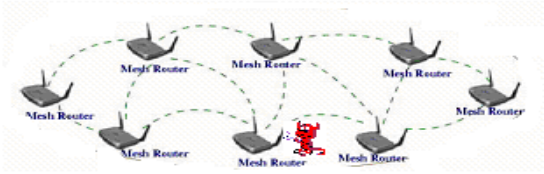

Fig. 2. Single malicious node in the forwarding path

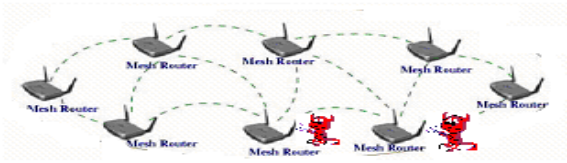

Fig. 3. Two colluding malicious nodes in the forwarding path.

C. Security Attack Model

In this work, we consider only the source and destination mesh node to be trusted because mesh routers deployed in community and neighborhood networks are susceptible to internal attacks or external attacks. Therefore, complete trust cannot be assumed on the intermediate mesh nodes.

Figures 2, 3 shows the deployment of malicious nodes in a infrastructure WMN. Figure 2 shows the presence of single malicious node in the path between source and destination. This attacker can selectively drop the messages for destination. In figure 3, two or more colluding malicious nodes are present in the forwarding path. This kind of deployment makes it very difficult to detect the selective dropping attacks.

We now discuss how selective forwarding attacks (black hole attacks) can easily happen in AODV [7] routing protocol. AODV is an on-demand routing protocol that creates routes only when required. When a source has data to transmit to an unknown destination, it broadcasts a Route Request (RREQ) for that destination. At each intermediate node, when a RREQ is received a route to the source is created. A receiving node rebroadcasts the RREQ if it has not received this RREQ before, is not the destination and does not have a current route to the destination. If the receiving node is the destination or has a current route to the destination, it generates a Route Reply (RREP) which is unicast in a hop-by-hop fashion to the source. As the RREP flows back to the source, each intermediate node creates a route to the destination. When the source receives the RREP, it records the route to the destination and can begin sending data. If multiple RREPs are received by the source, the route with the shortest metric is chosen.

Figure 4 presents a mesh network of routers. Suppose node A wants to send packets to node D and it broadcasts a RREQ for that destination. We assume that node B is a malicious node that lures the traffic by sending false routing

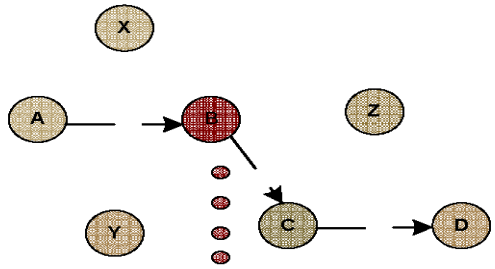

Fig. 4. The selective forward attack problem against network protocols. The malicious node B easily lures the traffic to itself and disrupt the network operation by dropping packets.

information. Node B claims that it has a better route to destination whenever it receives RREQ packets and sends the reply back to source node A. The destination node D and other intermediate nodes may send the reply if it has a fresh route to destination. If A receives the reply from a genuine node first, everything works well. But the RREP from B can reach the source node first due to two reasons [4]. First, a malicious node may be near to source node. Second, a malicious node does not have to check its routing table when sending false route information. As a result, A will think that the route discovery process is complete, ignore all other RREPs and forward data packets to D via B. Node B will refuse to forward some packets and form selective forwarding attack in the network. If B drops all packets, it is known as black hole problem. A similar attack can be achieved with DSR [14], DSDV [15].

III. The Proposed Algorithm

In this paper, our aim is to identify and localize selective forwarding attacks in the area of wireless mesh networks. The characteristics of the defending algorithm [8] should be: 1) able to detect the malicious nodes quickly 2) additional overhead caused by the algorithm should be minimum.

A. Detection of gray hole attackers

In this section, we propose the first phase of algorithm, $Counter - Threshold\ Based$, to achieve our goal of identifying selective forwarding attacks. First, we generate a random set of mesh routers for particular pair of source and destination nodes as shown in figure 3. The path between source and destination mesh nodes are determined using the route discovery feature of AODV protocol [7]. Each node maintains a packet counter for keeping track of the packets received from a particular source node. The source node also maintains a packet counter to keep track of the packets forwarded to destination node.

Two packets, $Control$ packet and $ControlACK$ are used in this detection scheme. The $Control$ packet consists of Source ID, Destination ID, Hash field, Hash-Function [19], [20] and Final-Hash (one way hash chain which encrypts number of packets transmitted from source to destination).

We use hash chains to secure the packet count in a similar way the authors do in [17], [18]. Every time a source forwards a $Control$ packet, it performs the operations as shown in figure

- Sets the Hash field to the packets send by source node to the particular destination

  $Hash = Packets[Source]$

- Sets the Hash function field to the value of the hash function that is going to use

  $Hash\text{-}Function = F$

- Calculates *Final-Hash* by hashing *Packets[Source]* Hop count times.
  The hop count to particular destination can be obtained from the routing table of the source.

  $Final\text{-}Hash = F^{HopCount}(Packets[Source])$

where, F is a hash function and $F^n(y)$ is the result of repeatedly applying the hash function F to y n times

Fig. 5. The operations performed by source node when it transmit a $Control$ packet

Fig. 6. The control packets are included randomly between data packets to avoid complete drop of control packets by the malicious node.

5. The $Control$ packet is included randomly between data packets as shown in figure 6. The reason to send $Control$ packets randomly between data packets is to avoid complete drop of control packets by the attacker.

When the destination node receives the $Control$ packet, it performs the operations as shown in figure 7 and retrieve the packet count value in $Control$ packet. The destination node then compares the destination packet count with the detection threshold. Our detection algorithm requires the destination node to return an acknowledgment ($ControlACK$) for every received $Control$ packet to the source node. Consider the following scenarios.

1) Scenario I: Positive ControlACK from Destination: If the destination packet count satisfies the detection threshold, a positive $ControlACK$ will be sent to the source node notifying the absence of attacker in the forwarding path.

2) Scenario II: Negative ControlACK from Destination: If the destination packet count is less than the detection

- Applies the hash function *F* Hop count times to the value in the Hash field, and compares that the computed value is equal to the value contained in the *Final-Hash* field. If the *Control* packet is not modified, the destination node will retrieve the number of packets send by source node.

If (Final-Hash $= F^{HopCount}$ (Hash))
  Retrieve the packet count value in the Hash field of the ***Control*** packet.
Else
  Drop the ***Control*** packet

Fig. 7. The operations performed by destination node when it receive a $Control$ packet

threshold, a negative $ControlACK$ will be sent to the source node notifying the presence of attacker in the forwarding path.

3) Scenario III: No ControlACK from Destination: The source node may not receive a reply from the destination for any one of the following two reasons. First, $ControlACK$ packet from destination node is dropped by a malicious node. Second, the $Control$ packet from source did not reach destination and hence destination will not return any $ControlACK$ to source as it does not know that it was expecting any $Control$ packet. To handle this situation, a $Timeout$ is used. After the $Timeout$, source node will initiate the $Query$ based localization algorithm.

The accuracy of the detection of malicious node depends upon detection threshold calculation. We provide an analysis of detection threshold in Section IV and simulation study in Section V.

B. Localization of gray hole attackers

Once the presence of a malicious node is identified by the detection algorithm, the source node invokes the second phase of the algorithm, $Query\ Based$ algorithm. In this phase, source node will query the intermediate nodes in the forwarding path for the received packet counter value. If all the intermediate nodes are queried by source node, it will increase the overhead of algorithm. Hence to improve the performance of the algorithm, a $Counter\ Frequency$ is used to select the intermediate nodes in the path between source and destination. We can determine the appropriate value of $Counter\ Frequency$ based on the experiments on mesh topology. Now, consider the following scenarios.

1) Scenario A: All packets are dropped by Malicious Node: In this scenario, the destination will not receive any packets and hence do not send any $ControlACK$ back to source. After $Timeout$, the source will query the selected intermediate nodes for packet count based on $Counter\ Frequency$. Hop by Hop packet count comparison is employed for selected intermediate node to localize the attacker. In this case, the packet count of the attacker will be higher than the following legitimate node because the attacker is dropping packets without relaying it to the subsequent node.

2) Scenario B: Few packets are dropped by Malicious Node: In this scenario, the destination will send a Negative $ControlACK$ to source to notify the presence of a malicious node. Once the presence of an attacker is detected in the forwarding path, to localize the attacker the source will query the selected intermediate node for packet count based on $Counter\ Frequency$. In this scenario, the packet count of malicious node will be higher than the following genuine node as the malicious node is dropping packets without forwarding it to the subsequent node.

Once the attacker is localized, source node will generate an $Error$ packet to inform other nodes of this attack so that other nodes can discard this localized route in future route discoveries.

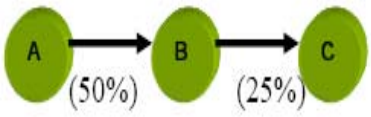

Fig. 8. Three node network topology to illustrate detection threshold; A is the source and C is the Destination.

IV. Analysis of Detection Threshold

We determine the appropriate value of detection threshold (d_{thresh}) based on the routing metric ETX (expected transmission count) [10]. ETX is defined as the expected number of data transmissions needed to successfully deliver a packet from a sender to the receiver, including retransmissions. ETX of a link is computed using the forward and reverse delivery ratios of the link. The forward delivery ratio, d_f, is the measured probability that a data packet is successfully delivered at the receiver and the reverse delivery ratio, d_r, is the probability that the acknowledgment packet is successfully received by the sender. The ETX of a link is computed as

$$ETX = \frac{1}{d_f \times d_r} \tag{1}$$

The inverse of ETX corresponds to the delivery ratio of the link. The detection threshold d_{thresh} of a route is computed as the inverse of the summation of ETX of all the links i along the path p.

$$d_{thresh} = \frac{1}{\sum_{linki \in p} ETX_i} \tag{2}$$

$$AR = N \times d_{thresh} \tag{3}$$

where, AR is the Acceptance Rate and N is the number of packets transmitted by the source node. For example, consider the three node network (figure 8). In this topology, node A wants to communicate with node C. Let N be the number of data packets transmitted by A to C. Suppose the delivery ratios of the link AB is 50% (ETX = 2) and that of link BC is 25% (ETX = 4) . d_{thresh} of route AC is computed as the inverse of the summation of the ETX of links AB and AC i.e. $\frac{1}{6}$. Only $\frac{1}{6}$ of the packets send from source A will reach the destination node C. If node C receives packets less than AR ($N \times d_{thresh}$), then a malicious node is present in the path. Now we will examine whether the proposed Counter-Threshold based algorithm is able to detect the malicious attack accurately. Suppose a malicious node respond back to the RREQ of source with a better route information (high delivery ratio) to lure the traffic to itself as seen in figure 4. Since the detection threshold of the route is computed based on the throughput of each link, if a attacker drops packets, the packets received by the destination node will be less than AR and the presence of malicious node between sender and receiver can be easily detected.

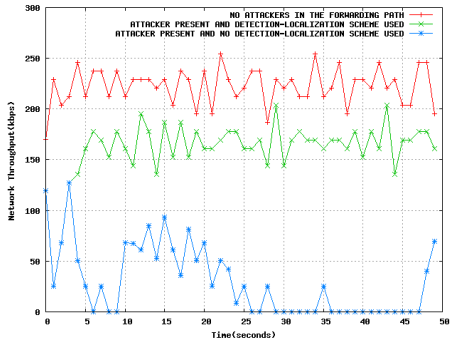

Fig. 9. Network Throughput in the presence and absence of attackers.

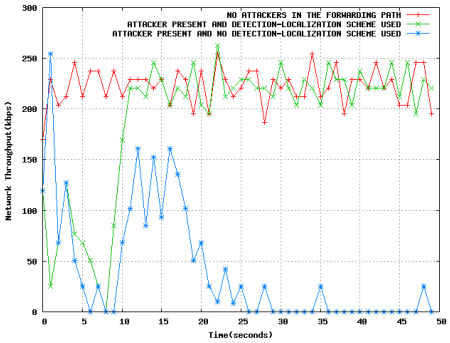

Fig. 10. Two or more colluding attackers are present in the paths between source and destination

V. Performance Evaluation

The proposed algorithm is implemented in ns2 [21] and the performance is evaluated in terms of network throughput, overhead of the algorithm and sensitivity of the algorithm to detection threshold.

A. Simulation Parameters

The network topology consists of a square grid of 36 mesh nodes located in $1000m \times 1000m$ area. In our simulations traffic sources are modeled as bulk TCP transfers. Packets have a size of 1024 bytes and are sent at a deterministic rate. The transmission range is set as 250m while the carrier sensing range is set as 550m. One stationary source and one stationary destination is placed on the opposite sides of the grid with multiple forwarding paths between them. The malicious nodes are randomly located in the forwarding path of source and destination. We integrate the ETX metric into AODV routing protocol to select the path between source and destination. We set the maximum number of $Timeouts$ as 2 before the source node initiates the localization algorithm. The $Control$ packets are generated randomly by the source node to avoid complete dropping of packets by the attacker.

B. Performance Results

In this section we evaluate the performance of the algorithms in terms of network throughput, overhead and sensitivity to detection threshold.

1) Scenario I: A single attacker present in the forwarding path: In this scenario, an attacker is randomly selected in the forwarding path between source and destination. Figure 9 shows the network throughput as a function of time. Two observations are made from figure 9. First, network throughput is degraded in the presence of malicious nodes. Second, after using detection and localization phase of the algorithm, the network performance is improved because the proposed algorithm detects the attacker and initializes the $Query - Based$ phase to localize the attacker. Once the attacker is localized, the source node sends an $Error$ packet to all other nodes and initiates a new route discovery process that avoids the malicious node. It is seen from figure 9 that the proposed algorithm defends the attacker at time 3s and the throughput is improved thereafter.

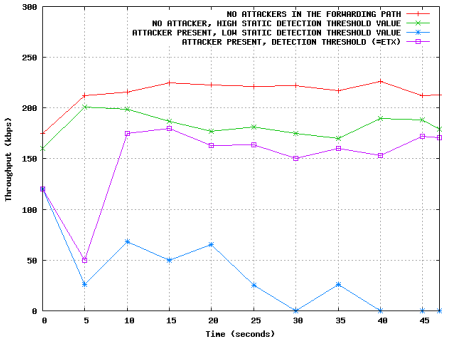

Fig. 11. Sensitivity of Detection scheme with different threshold values

2) Scenario II: Colluding attackers present in multiple forwarding paths between Source and Destination: In this scenario, two or more attackers are randomly selected in the multiple forwarding paths between source and destination. Figure 10 shows the network throughput as a function of time. It is seen from figure 10 that the network performance is improved using detection and localization algorithm after time 7s because the proposed algorithm identifies the attacker in the time interval $0 - 7s$ and initiates a new route discovery process that avoids the malicious node.

3) Scenario III: Analysis of Detection Threshold: In this scenario we compare the efficiency of the proposed algorithm with different detection threshold values. It is observed that using ETX as detection threshold results in high throughput in the presence and absence of attackers. From figure 11, two observations are made.

Case 1: When d_{thresh} is lower than ETX

It is seen that the network performance is very low when the value of detection threshold is less than throughput of the path. When the destination node receives the $Control$ packet, it checks the received packets with the detection threshold. Since the detection threshold is low, the number of received packets will be greater than the $Acceptance$ rate (AR) and hence the destination will always respond with a positive $ControlACK$ to source. As a result, attackers will go undetected and the network throughput will degrade.

Case 2: When d_{thresh} is higher than ETX

It is seen in figure 11 that even in the absence of an attacker,

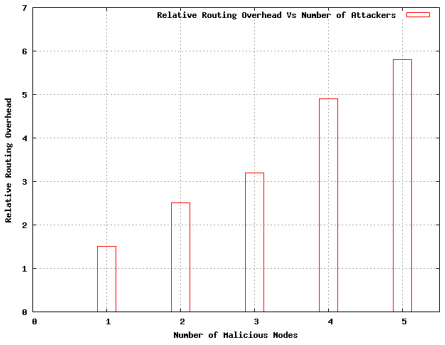

Fig. 12. Overhead of the algorithm vs Number of Malicious Nodes

the throughput is low when the detection threshold is higher than throughput of the path. In this case, when the destination node receives the $Control$ packet, it checks the received packets with the detection threshold. Since the detection threshold is higher than the throughput of the path, the number of received packets will be less than the $Acceptance$ rate. Therefore, the destination node will always respond with a negative $ControlACK$ to source. As a result, the source node enables the localization phase of the algorithm and hence the legitimate nodes are avoided in the future route discovery process.

4) Scenario IV: Relative Routing Overhead of proposed algorithm: Relative routing overhead is computed as the ratio of the overhead incurred in implementing the proposed algorithm as opposed to the one that does not. Figure 12 shows the relative overhead of the algorithm with the increase in number of attackers. As the number of attackers increase, the initialization of the localization process and route discovery process increases. As a result, the overhead of the system increases with the number of attackers.

VI. Conclusions

Wireless Mesh Networks (WMNs) have emerged recently as a promising technology for next-generation wireless networking to provide wide variety of applications that cannot be supported directly by other wireless networks. In such networks, security is turning out to be a major concern and little attention has been paid to this topic by the research community. In this paper, we discuss the routing security threat known as the selective forwarding attack that can be easily deployed against a WMN and present an algorithm to defend against selective forwarding attacks based on AODV routing protocol. The first phase of the algorithm is Counter-Threshold Based and uses the detection threshold and packet counter to identify the attacks and the second phase is Query Based and uses acknowledgment from the intermediate nodes to localize the attacker. The algorithm presented in this paper can be easily applied to existing routing protocols like DSR, DSDV. We also present a simulation study that shows the efficiency of the proposed algorithm in the presence of selective forwarding attackers.

Our future work is to investigate the performance of the proposed algorithms when different existing link quality metrics are used as the detection threshold.

References

[1] I.F. Akyildiz and X. Wang, "A survey on Wireless Mesh networks," in *IEEE communication Magazine*, September 2005.

[2] J. Jun and M. L. Sichitiu, "The nominal capacity of wireless mesh networks," in *IEEE Wireless Communications*, October 2003.

[3] Jane-Hwa Huang, Li-Chun Wang, and Chung-Ju Chang, "Coverage and Capacity of A Wireless Mesh Network," in *Wireless Networks, Communications and Mobile Computing*, June 2005, pp. 13–16.

[4] H. Deng, W. Li, and D.P. Agrawal "Routing Security in Ad hoc Networks," in *IEEE Communications Magazine*, October 2002.

[5] 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.

[6] A. Hamid, Mamun-Or-Rashid, C. Hong, "Defense against lap-top class attacker in wireless sensor network," in *Advanced Communication Technology, 2006. (ICACT 2006) The 8th International Conference*, Feb 2006.

[7] I.D. Chakeres and E.M. Belding-Royer, "AODV Routing Protocol Implementation Design," in *Proceedings of the International Workshop on Wireless Ad Hoc Networking (WWAN)*, Tokyo, Japan, March 2004.

[8] B. Xiao, B. Yu and C. Gao "CHEMAS: Identify suspect nodes in selective forwarding attacks," in *Journal of Parallel and Distributed Computing*, pp.1218-1230, June 2007.

[9] David B Johnson and David A Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile Computing*, Imielinski and Korth, Eds., vol. 353. Kluwer Academic Publishers, 1996.

[10] D.S J De Couto, D.Aguayo, J.Bicket, and R.Morris, "A High-Throughput Path Metric for Multi-Hop Wireless routing," in *ACM Mobicom*, 2003.

[11] T. Wu, Y. Xue, Y. Chi, "Preserving traffic privacy in wireless mesh networks," *World of Wireless, Mobile and Multimedia Networks, 2006. WoWMoM 2006*, June 2006.

[12] Mishra, A. Nadkarni, K. Patcha, A, "Intrusion Detection in Wireless Ad Hoc Networks," *IEEE Wireless Comm*, Feb 2004.

[13] W. Lee and Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," *Wireless Networks. Kluwer. 2003. ACM/Kluwer Wireless Networks Journal*, September 2003.

[14] D.B.Johnson and D.A.maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," in *Mobile Computing*, 1996.

[15] C.Perkins and Bhagwat, "Highly Dynamic Destination-Sequence DistanceVector Routing (DSDV) for Mobile Computers," in *ACM SIGCOMM Computer Communication Review*, October 1994, pp. 234–244.

[16] L. Lamport, "Constructing digital signatures from one-way function," in *technical report SRI-CSL-98, SRI International* , October 1979.

[17] Manel Guerrero Zapata, "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing," *Mobile Ad Hoc Networking Working Group*, August 2001.

[18] Y.C Hu,D.B. Johnson and A. Perrig, "SEAD: Secure effiecient distance vector routing for mobile wireless ad hoc networks," *The 4th IEEE Workshop on Mobile Computing Systems and Applications*, June 2002.

[19] C. Madson and R. Glenn, "The use of HMAC-MD5-96 within ESP and AH," *Internet Request for Comment, RFC 2403*, November 1998.

[20] C. Madson and R. Glenn, "The use of HMAC-SHA1-96 within ESP and AH," *Internet Request for Comment, RFC 2404*, November 1998.

[21] Kevin Fall and Kannan Varadhan, *NS notes and documentation*, The VINT Project, UC Berkely, LBL, USC/ISI, and Xerox PARC, 1997.