Optimized Detection and Isolating Mobile Attacks Through SADEC Lite Protocol In Ad Hoc Networks

M. VIMALA
University Departments
of Anna University,
BITCampus,
Tiruchirapalli
Softline28@gmail.com

ABSTRACT

Four attacks namely data direct to the wrong place, energy control, identity group of representative, and colluding can be easily begin campaign against multi hop wireless ad hoc networks. There is also possibility of Wormhole attack that may be launched by the aggressive elements class from multiple ends of a wireless sensor network against a set of target sensor nodes. Moreover, a legitimate node comes under mistrust. As a result of the attack, the incapacitated data-generating genuine sensor nodes are replaced with malicious nodes that will involve in further malevolent activity against sensory resources. To better utilize protocol for local monitoring by considerably increasing the number of nodes in a neighborhood that can do monitoring. The results signify the need for distributed pattern recognition for detecting malicious attacks in a timely and accurate manner

Keywords
Local Monitoring, Miss placed, multi hop wireless network, energy control, colluding collusion, identity representation, wormhole attack.

1. INTRODUCTION

Wireless Ad hoc is one of the famous and most important platform and the need of this network is increasing day by day. As the need of these network increases many insecured problem raises various attacks make the network to work improperly. The most common attacks like Sybil, DDOS, Wormhole attacks occur in multi hop Ad hoc network. These attacks may cause traffic and time delay in delivering the packet. An ad-hoc network is an autonomous system of hosts connected by wireless RF links without any static infrastructure such as base stations, fixed routing units, or wired links. If two hosts are not within radio range, all message communication between them must pass through intermediate hosts which can also act as routers. Sensor networks are a particular class of wireless ad-hoc networks in which the nodes have micro-electromechanical (MEMS) components,
\

including sensors, actuators and RF communication components. These nodes are multifunctional and capable of sensing, communication, computation, and, sometimes, they can move. Sensor networks typically comprise of large numbers of sensor nodes placed in the environment to be monitored and usually communicate with each other through low-bandwidth communication links. For the purpose of this exposition, we use *sensor nodes* to refer to sensor network nodes, *ad-hoc nodes* to refer to ad-hoc network nodes.

The traffic in WAHAS networks can be classified as *data* and *control* traffic. Control traffic contains information needed to set up the network for data traffic to flow. Typical examples of control traffic are routing, monitoring the liveness of nodes, topology discovery, and system management. Looking further into routing traffic, we find multiple kinds of messages– route request (broadcast) and route reply (unicast) during the initial establishment phase, route maintenance during the lifetime of the data route, and route teardown at the end.

A particular devasting attack is known as Wormhole attack. Here the malicious node keeps an record about the control and data traffic and tunnel the packets from one location to the other. It create an route establishment by preventing the node from find the route that are more than two hops. These attacks may occur in and out of the network bound. Where the Cryptographic key mechanism can prevent the attack occur in the inner nodes of the network bound. But it does not work at the outer network. Cryptographic mechanisms alone cannot prevent these attacks. Many attacks such as wormhole, rushing attacks can be

launched without need of the attacks of cryptographic key check. Many attacks are identified based on Behavior based mechanism the most common techniques.

However, the malicious node gives the impression to its neighbors nodes in local monitoring and routing the packet to the correct destination. This attacks are applicable to the packets even when the packet sends the acknowledgement end to end . Due to the bandwidth and energy level many packets are send unacknowledged or only selectively acknowledged in the multi hop network during heavy traffic occurs. This is particularly more common during data traffic or control traffic. In this paper, we introduce five modes of the stealthy packet dropping attack. We separate the attacks that occur in external network where the cryptographic key mechanism does not work at the malicious node behavior. The other side internal nodes can be protected by cryptographic key mechanism and it easily identify and detect the malicious node within the bound.

Consider a network with five nodes A-B-C-D-E. The packet is forwarded from the node A source to D the destination node. A is forwarding a packet to a compromised node called C. C is supposed to relay the packet to the next-hop node D. The first form of the attack is called packet misrouting. In this mode, C relays the packet to an incorrect next-hop neighbor E. The result is the packet does not reach its destination node (D).Here C is the malicious node in the network. The Node E drops the packet as it is not belongs to its need. To avoid this kind of Misrouting problem we increase the guard node in the network .

The second mode is called the power control attack. This mode of attacks occurs when the intermediate node reduces its power of transmission to the neighbor and sends the packet. So it causes the packet to drop before it reach its destination. If the intermediate node is malicious node before it transfer it calculate the distance of the reaching node and it reduce its transmission power accordingly. Therefore, the packet does not reach the next hop and attackers can be detected by the help of guard nodes to avoid this problem here we use power control saving mechanism with the help of the Guard nodes in each transmission.

The third form of the attack is called the colluding collision attack. This mode, the attacker uses a colluding node to each other by transferring the packet at same time by two source node to reach at same destination. Therefore, a collision occurs at same destination at same time it drops the packet. This mode of attack can be prevented by the Guard node by using TIM. It allows Multiple Routing mechanisms to reach the same destination and different time using synchronization mechanism. The next mode of stealthy packet dropping is called the identity delegation attack. In this mode, the attacker colludes the node by the compromised node it make another node to compromise with its host placed close to the source node S. E is allowed to use M's identity and transmit the packet. Since E is almost at the id and it relays the packet to the destination so the packet get dropped. In each of these attack types, the adversary can successfully perform the attack without detection through BLM.

Additionally, the main mode of attack that occur during route establishment is known as wormhole attack. This attack occur when the malicious node request for routing to the router and it using Tunelling effect it send the route from one end to the other end of the Tunnel which is also a malicious node. And all these type of attacks cannot be prevented by using behavior based mechanisms. And the other BLM (BaseLine Local Monitoring), Which is not suitable for all attack type five types of attacks and it mainly controls misrouting and power control, a legitimate node is accused of packet dropping.

These attacks can be easily identified with minimum time is required. By increasing the Guard node and it gives the information about the next hop details. And it performs additional checking functionality to avoid traffic. The guard nodes is detected and it changes for the each and every packet delivery based on the region it crosses. Guard nodes are not fixed for all the transaction it is selected on the based it maintains the routing table for all the nodes in the region as whole. It update the routing table for every transfer. Each node keeps the routing table with its neighbor node information.

During the Network Analysis the nodes are made with the separate region. And the nodes in wireless network are in movable the it forms the region of its own and the guard nodes are decided by all the nodes. The Router whose work is to establish the route to source to the destination.

1. A node has a data packet to send but does not know the routing path to the destination, it initiates the route discovery procedure by broadcasting a control packet, called route request (RREQ).
2. When an RREQ reaches the destination, it prepares another control packet, called route reply (RREP), and replies back to the source with the complete route information.

3. Upon receiving an RREP, the source saves the route information in its local memory, called route cache, for later uses.
4. When a node detects a link error during its data transmission, it sends another control packet, called route error (RERR), to the source and deletes the stale route from its route cache.

Since nodes move randomly in a MANET, link errors occur and route information that includes a broken link becomes obsolete. Overhearing improves the network performance by allowing nodes to collect more route information. Nodes in the vicinity of a transmitter would learn about the path to the destination via overhearing.

We Compare BLM with SADEC Lite protocol.BLM could rectify the 45% of these attack and it work with the normal nodes in the network.BLM does not need any extra time to maintain and it takes less memory then SADEC Lite protocol.BLM would isolate the legitimate node as malicious node and it wrongly isolate it. SADEC Lite protocol control all the above attacks mentioned in this paper. But it takes more time for communication between the neighbors as the routing table keeps on changes while nodes are movable. SADEC Lite protocol controls 75% of the mobile attacks and it needs more time than BLM.SADEC Lite would control 100% worm hole attack and detection. SADEC Lite isolate and detect the malicious node correctly than BLM.

2 RELATED WORK

Many researches are moving towards wireless Ad hoc networks and to secure the packet from attacks.

A technique proposed to detect malicious behavior involving in the network in[13], or an out-of-band channel [12]. The other method for detecting and isolating is BLM. For every N data messages (in the above papers N = 1).But this method cause delay and damage to the packet in reaching its destination. In Static topology the attacks can be easily, e.g., [14] to detect wormhole attacks and it is rare case.

The major issue in trusted ad hoc networks has been affected and many researches (e.g., [1], [2], [23], [37]). And they all move with the Dempster-Shafer theory [38] for creating an defined legitimate node in the region.

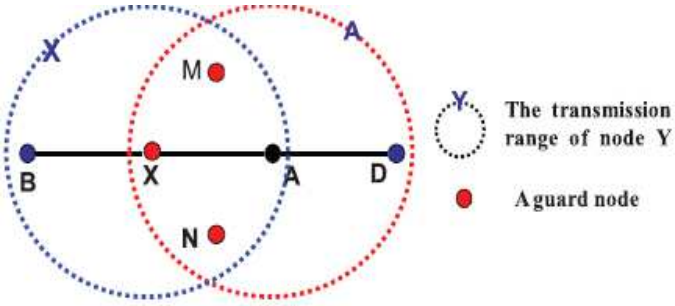

Fig. 1. X, M, and N are guards of A over X → A.

This paper builds on our previous work [13]. In [13], We introduced the stealthy packet dropping attacks and proposed a protocol called MISPAR to mitigate the attacks. In this protocol the legitimate node comes under suspicious and it is mistakenly identified and removed. This make us to compare the result analysis of both BLM and SADEC Lite [13]). Here we show the result of both BLM and SADEC with NS-2 simulation. SADEC Lite gives more improvement than BLM and it reduce the count of mistakenly isolation of the legitimate node, this paper presents the results of a testbed experiment using 50 Mica2 motes built to evaluate the overhead of SADEC Lite and its feasibility for resource limited sensor networks.

The Testbed in sensor and Ad hoc network is forming and region and placing the trusted nodes with proper id. The router whose work is the major part in this network. Every nodes maintain its own routing table about its neighborhood details. It communicate whenever the packet is relayed to its destination.

One general method to discover the neighbors node, called the announcer. In sensor node directional antenna is most common type it spread a HELLO message in every direction. Each node that hears the HELLO message sends its identity and an encrypted message, containing the identity of the announcer. Before it responds to its neighbor list, it just check the message authentication using the authentication key. Even the antenna can receive opposite direction and it is informed to the neighbor. This approach is suitable for secure dynamic neighbor detection. And this would help the announcer to find the malicious node easily based on its response. But this method nodes not work with the wormhole attack it just support partially.

Specifically, it only prevents the kind of wormhole attacks in which malicious nodes try to deceive two nodes into believing that they are neighbors. One of the major drawback is the requirement of directional antennas on all nodes may be infeasible for some deployments. At last the protocol may degrade the connectivity of the network by

rejecting legitimate neighbors in their conservative approach to prevent wormholes attack. The other related paper Waterbuck*et al.* [7] present a protocol called ODSBR.
And this protocol will not prevent wormhole but it easily isolate and identify this particular attack. Drawback of this method is it needs an acknowledgement for every packet even it belongs to the same data. And this technique will cause the many packets could be lost before the wormhole is discovered.

3 .FOUNDATION

3.1 ATTACK MODEL

An attacker can affect the internal and external node that even has the authentication key. The internal node which has authentication key to each other, and the external node does not possesses any authentication key. The attack may occur in and out of bound channel. In inner network the malicious node and the compromised node are the major attack. , we do not consider the denial of service attacks through physical-layer jamming [2], or through identity spoofing and Sybil attacks [10]. There exist several approaches to mitigate these attacks—[2] for jamming and [10] for the Sybil attack. A malicious node is more powerful than a legitimate node and it has higher bandwidth and high control transmission capability. but is limited to omnidirectional antennas to broadcast. The attacks do not have target routing protocol it just attack on all the type of routing protocol. The intermediate node will helps the packet to reach the final destination.

If they were malicious then the action of the node would differ and it does not allow the packet to reach the destination. This includes routing protocols specific to WSNs such as the beacon routing protocol. Wormhole attack is launched against such routing protocols, using DSR (Dynamic Source Routing). In DSR method, if a node, say A, needs to discover a route to a destination, say *D*, A floods the network with a route request packet. Any node that accept the request, and the transmission can be done over that path and every packet adds its identity to the source route, and rebroadcasts it.

This Flooding concept would leads to occupy large memory. To limit the amount of memory it occupies due to flooding, each node broadcasts only the first route request it receives and drops any further copies of the same request. For 6 each route request *D* receives, it generates a route reply and sends it back to *S*. The source *S* then selects the best path from the route replies; the best path could be either the path with the shortest number of hops or the path associated with the first arrived reply. However, in a malicious environment, this protocol will fail. When a malicious node at one part of the network hears the route request packet, it tunnels it to a second colluding party at a distant location near the destination. The second party then rebroadcasts the route request.

To Overcome this problem, We use Optimal Path Selection Algorithm for multicast. OPSAM (Optimal Path Selection Algorithm for Multicast) for the static multicast routing problem and the newly defined mobile multicast routing problem. The problem is modeled as one of finding the most probable feasible path, where link weights are random variables.

A "backward-forward" heuristic is proposed which again uses pre labeling of the graph in the backward direction followed by a forward search that attempts to minimize an objective function. The neighbors node also receive the route request and it drop any further legitimate requests that may arrive later on the time. The result is that the routes between the source and the destination go through the two colluding nodes that will be said to have formed a wormhole between them.

The major reasons for the collusion is the two malicious node would send at the same time that it is to short to send even it is more than many hops. Consider Figure 2 in which nodes *A* and *B* try to discover the shortest path between them, in the presence of the two malicious nodes *X* and *Y*. Node *A* broadcasts a route request (*REQ*), *X* gets the *REQ* and encapsulates it in a packet destined to *Y* through the path that exists between *X* and *Y* (*U-V-W-Z*). Node *Y decapus lates* the packet, and rebroadcasts it again, which reaches *B*. Note that due to the packet encapsulation, the hop count does not increase during the traversal through U-V-W-Z. Concurrently, the *REQ* travels from *A* to *B* through *C-D-E*. Node *B* now has two routes, the first is four hops long (*A-C-D-E-B*), and the second is apparently three hops long (*A-X-Y-B*). Node *B* will choose the second route since it appears to be the shortest while in reality it is seven hops long. So *X* and *Y* succeed in involving themselves in the route between *A* and *B*. Any routing protocol that uses the metric of shortest path to choose the best route is vulnerable to the wormhole attack.

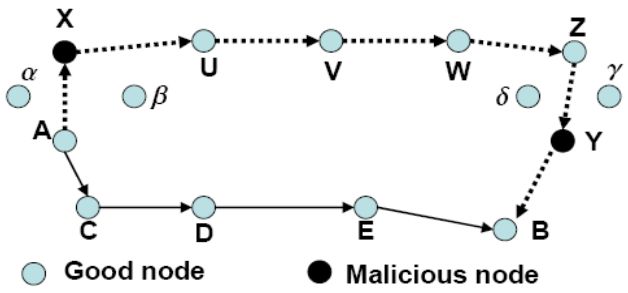

Fig.2. Wormhole through packet encapsulation

This mode of the wormhole attack is easy to launch since the two ends of the wormhole do not need to have any cryptographic information, nor do they need any special capabilities, such as a high speed wireline link or a high power source. A simple way of countering this mode of attack is a by-product of the secure routing protocol ARAN [11], which chooses the fastest route reply rather than the one which claims the shortest number of hops. This was not a stated goal of ARAN, whose motivation was that a longer, less congested route is better than a shorter and congested route.

4. DROPPING ATTACK DESCRIPTION

A malicious intermediate node drop the packet when the attack happens, and the legitimate node comes under suspect. The attack drop the packet in these way through Miss placed, Energy Control, Identity Representation, and collusion. This attacks can be overcome through Multiple routing, Energy Saving, OPST.

4.1Drop through Miss Placed

In the misrouting attack, a malicious node relays the packet to the wrong next hop, which results in a packet drop. Note that, in BLM [6], a node that receives a packet to relay without being in the route to the destination either drops the packet or sends a one-hop broadcast that it has no route to the destination Power saving in PCF is achieved by the coordination of the AP. Each node operates either in AM or PS mode. With PCF, the AP operates in AM and all other mobile nodes operate in PS mode.

The AP periodically sends a beacon for synchronizing mobile nodes in its neighborhood. The beacon includes Traffic Indication Map (TIM), which is a bitmap vector to indicate the traffic and the corresponding receiver. If a node is specified as a receiver in the TIM, it remains awaken to receive a packet during the following data transmission period. It switches off its radio subsystem otherwise.

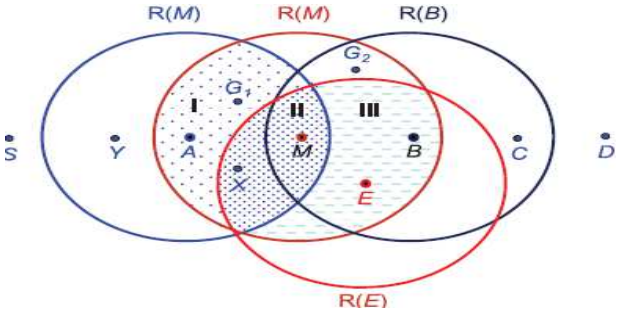

Fig. 3. Miss placed scenario.

4.2 Drop through Energy Control

In this type of attack, a malicious node relays the packet by reducing its transmission energy level. Thus the energy saving mechanisms help to overcome this problem. When the optimal route is selected to deliver the packet the rest of the intermediate node which is not taking part in the transmission will made to sleep mode. When the transaction is completed the nodes in the region is moved to the activation mode .

Consider the node in the region drops the packet through all the guards of Mover S→ M. Fig. 4 shows the set of guards of T over M → T that wrongly accuse T of dropping the packet. The farther T is from M, the better it is for the attacker. The energy level is reduced by calculating the distance of the destination node. When the intermediate malicious node receives the packet it just identify the distance and it automatically controls the energy level and transfer the packet. Then it drops the packet before reaching the destination.

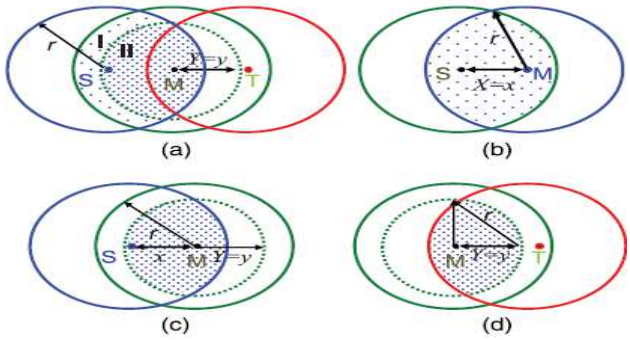

Fig.no.4 Energy control

When the number of guards that are not satisfied by the controlled-power transmission is greater than 1, an intelligent attacker will refrain from lowering the transmission power since it will be detected by all its neighbors either directly or indirectly. Additionally, a successful attack, not only achieves the effect of

dropping the packet, but also causes a subset of the guards of T over M→ T to accuse T of dropping the packet.

4.3 Drop through Colluding Collision

The attacker may exploit the absence of the RTS/CTS frames to launch a stealthy packet dropping attack through collision induced by a colluding node. The colluding node creates a collision in the vicinity of the expected next-hop node at an opportune time. Consider the scenario shown in Fig. 5. The malicious node M1 receives a packet from S to be relayed to T. Node M1 coordinates its transmission with a transmission of some data generated by its colluding partner M2 to T. It has the effect that T is unable to get the packet relayed by M1. The damage caused by this attack is twofold: 1) M1 successfully drops the packet due to a collision at T without being detected, and 2) node T is accused of dropping the packet by some of its guards over the link M1 → T (the guards that are out of the range of M2,region I). Note that for M2 to be able to send data to T, it has to be a legitimate neighbor (compromised by the attacker); otherwise, the attack would be considered a physical-layer jamming [12], which is assumed to be detectable through techniques complementary to that presented in the paper. Drop through Identity Delegate

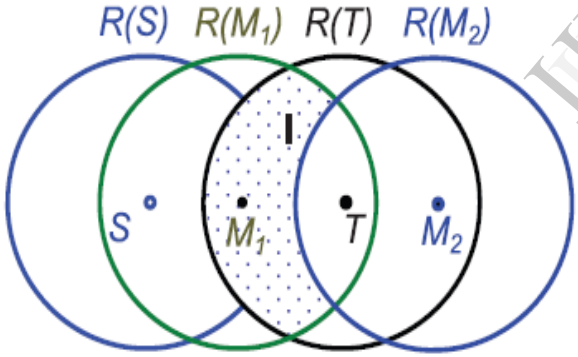

Fig. 5. Colluding collision illustration scenario

In this form of the attack, the attacker uses two malicious nodes to drop the packet. One node is spatially close to the sender. The other node is the next hop from the sender. The first malicious node could be externally or an internally compromised node while the latter has to be an internally compromised node. Consider the scenario shown in Fig. 5, node S sends a packet to a malicious next-hop node M2 to be relayed to node T. The attacker delegates the identity and the credentials of the compromised node M2 to a colluding node M1 close to S. After S sends the packet toM2, M1 uses the delegated identity of M2 and transmits the packet. The intended next hop T does not hear the message since T€ R (M1). The guards of M2 over S → M2 are the nodes in the shaded areas I and II and they are all satisfied since they are in R (M1).

Again, the consequences of this attack are twofold: 1) the packet has been successfully dropped without detection, and 2) the set of nodes in the shaded area II overhear a packet transmission (purportedly) from M2 to T. These nodes are included in G (M2, T) and will subsequently accuse T of dropping the packet.

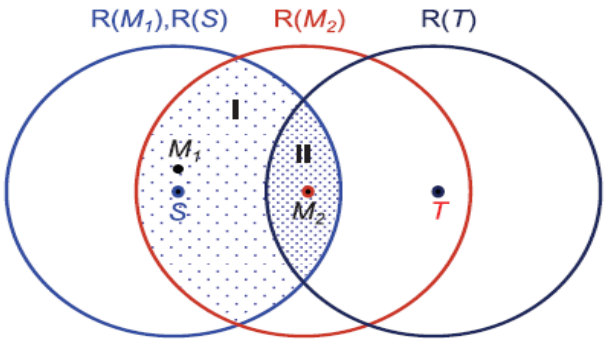

Fig. 6. Identity representation illustration scenario.

Identity representation can be rectified by keeping the secured routing table as described above. The routing table keeps on updating checking function with its neighbor node. The sensor node can be easily isolated and detected based on its table maintained.

Conclusion

The malicious behavior cannot be detected by any behavior based detection scheme presented to date. Additionally, it will cause a legitimate node to be accused. The presented a protocol that successfully mitigates all the presented attacks. It builds on local monitoring and requires nodes to maintain additional routing path information and adds some checking responsibility to each neighbor. The improvement is seen in terms of increase in the probability of isolation of malicious nodes and therefore transmission range of malicious nodes is reduced.

In future work, considering detection techniques for multichannel multi radio wireless networks. The listening activity for detecting malicious behavior is more complicated due to the presence of multiple channels and multiple radios. And also plan to analyze the impact of the detection technique on the network throughput under different adversary models.

References:

[1] A.A. Pirzada and C. McDonald, "Establishing Trust in Pure

Ad-Hoc Networks,” Proc. Australasian Conf. Computer Science
(ACSC ’04), vol. 26, no. 1, pp. 47-54, 2004.

[2] S. Buchegger and J.-Y. Le Boudec, “Performance Analysis of theCONFIDANT
Protocol: Cooperation Of Nodes-Fairness in Distributed Ad-Hoc NeTworks,” Proc. ACM MobiHoc, pp. 80-91, 2002.

[3] Y. Huang and W. Lee, “A Cooperative Intrusion Detection Systemfor Ad Hoc Networks,”
Proc. ACM Workshop Security of Ad Hoc andSensor Networks (SASN ’03), pp. 135-147, 2003.

[4] Y.C. Hu, A. Perrig, and D. Johnson, “Rushing Attacks and Defensein Wireless Ad Hoc Network Routing Protocols,” Proc. ACMWorkshop Wireless Security (WiSe ’03), pp. 30-40, 2003.

[5] Y.C. Hu, A. Perrig, and D.B. Johnson, “Packet Leashes: A Defenseagainst Wormhole Attacks in Wireless Networks,” Proc. IEEEINFOCOM, pp. 1976-986, 2003.

[6] I. Khalil, S. Bagchi, and N.B. Shroff, “MOBIWORP: Mitigation ofthe Wormhole Attack in Mobile Multihop Wireless Networks,”Ad Hoc Networks, vol. 6, no. 3, pp. 344-362, May 2008.

[7] I. Khalil, S. Bagchi, C. Nina-Rotaru, and N. Shroff, “UNMASK:Utilizing Neighbor Monitoring for Attack Mitigation in MultihopWireless Sensor Networks,” Ad Hoc Networks, vol. 8, no. 2, pp. 148-164, 2010.

[8] S.J. Lee and M. Gerla, “Split Multipath Routing with MaximallyDisjoint Paths in Ad Hoc Networks,” Proc. IEEE Int’l Conf. Comm.(ICC ’01), pp. 3201-3205, 2001.

[9] D. Johnson, D. Maltz, and J. Broch, “The Dynamic Source RoutingProtocol for Multihop Wireless Ad Hoc Networks,” Ad HocNetworking, Addison-Wesley, 2001.

[10] C.E. Perkins and E.M. Royer, “Ad-Hoc On-Demand DistanceVector Routing,” Proc. Second IEEE Workshop Mobile ComputingSystems and Applications (WMCSA ’99), pp. 90-100, 1999.

[11] C.E. Perkins and P. Bhagwat, “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers,”ACM SIGCOMM Computer Comm. Rev., vol. 24, pp. 234-244,1994.

[12] B. Dahill, B. N. Levine, E. Royer, and C. Shields, “A secure routing protocol for ad-hoc networks,” ElectricalEngineering and Computer Science, University of Michigan, Tech. Rep. UM-CS-2001-037, August 2001.