A WEIGHT BASED SYNCHRONIZATION DETECTION FOR WORMHOLE ATTACK USING PERIODIC UPDATES FRAMEWORK

[I] C. Sudha M.C.A., [II] D. V. Rajkumar M.C.A., M.Phil.,
[I] Research Scholar, Bharathiar University, Coimbatore, [II] Assistant Professor, CS,
[I, II] Dept. of Computer Science, Maharaja Co-Education College of Arts and Science,
Perundurai, Erode – 638052.
[I] Email id: sudharchinnasamy@gmail.com
[I] Contact No:8939667746
[II] Email id: dvrajkumar@gmail.com
[II] Contact No: 7871514680

ABSTRACT

One type of major attacks to neighbor discovery is wormhole attack, in which malicious node(s) relay packets for two legislate nodes to fool them believing that they are direct neighbors. It seems a merit that this kind of attack can enlarge the communication ranges, however, since it causes unauthorized physical access, selective dropping of packets and even denial of services, the wormhole attack is intrinsically a very serious problem especially in case of emergent information transmission. This thesis proposes a wormhole attack resistant secure neighbor discovery (SND) scheme for directional wireless network. In specific, the proposed SND scheme consists of three phases: the network controller (NC) broadcasting phase, the network nodes response/authentication phase and the NC time analysis phase. In the broadcasting phase and the response/authentication phase, local time information and antenna direction information are elegantly exchanged with signature-based authentication techniques between the NC and the legislate network nodes, which can prevent most of the wormhole attacks. To solve the transmission collision problem in the response/authentication phase, we also introduce a novel random delay multiple access (RDMA) protocol to divide the RA phase into M periods, within which the unsuccessfully transmitting nodes randomly select a time slot to transmit. The optimal parameter setting of the RDMA protocol and the optional strategies of the NC are included. In addition thesis proposes the concepts using Substance and Existence Multicast Protocol (SEMP) using the Optimism Max Out algorithms (OPMA) and Randomized Optimism Max Out algorithms (ROPMA) algorithms which nodes use to send updates to their neighbors.

Keywords: Network Controller, Secure Neighbor Discovery, Wireless Network, Random access, Parameter, Authentication

1. INTRODUCTION

1.1. Ad Hoc Wireless Network

Mobile ad hoc network (MANET) is a self-configuring network formed with wireless links by a collection of mobile nodes without using any fixed infrastructure or centralized management. The mobile nodes allow communication among the nodes by hop to hop basis and the forward packets to each other. Due to dynamic infrastructure-less nature and lack of centralized monitoring, the ad hoc networks are vulnerable to various attacks. The performance of network and reliability is

compromised by attacks on ad hoc network routing protocols. In a wormhole attack an intruder creates a tunnel during the transmission of the data from one end-point of the network to the other end-point , making leading distant network nodes to believe that they are immediate neighbors' and communicate through the wormhole link.

In wormhole, an attacker creates a tunnel between two points in the network and creates direct connection between them as they are directly connected. An example is shown in Figure. 1.1. Here R and P are the two end-points in the wormhole tunnel. R is the source node and S is the destination node. Node R is assuming that there is direct connection to node P so node R will start transmission using tunnel created by the attacker. This tunnel can be created by number of ways including long-range wireless transmission ,With the help an Ethernet cable or using a long-range wireless transmission .

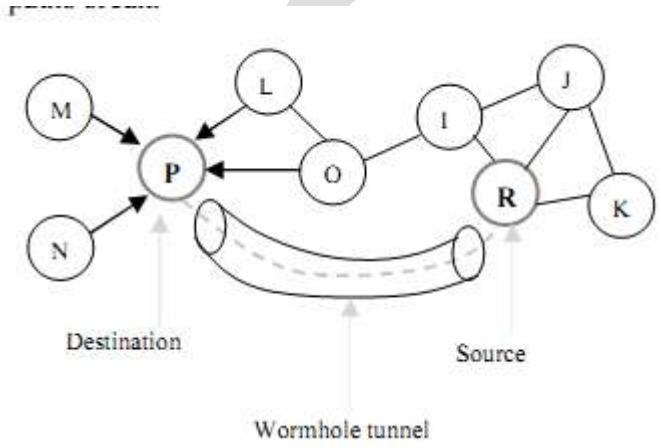

figure 1.1: Warmhole attack

Wormhole attacker records packets at one end in the network and tunnels them to other end-point in the network. This attack compromise the security of networks For example, when a wormhole attack is used against AODV, than all the packets will be transmitted through this tunnel and no other route will be discovered. If the tunnel is create honestly and reliably than it is not harmful to the network and will provides the useful service in connecting the network more efficiently.

A potential solution is to avoid wormhole attack is to integrate the prevention methods into intrusion detection system but it is difficult to isolate the attacker using only software based approach because the packets sent by the wormhole are similar to the packets sent by legitimate nodes .That all the nodes should monitor the behavior of its neighbor nodes. Each node sends REQ messages to destination by using its neighbor node list. If the source does not get back the REP message from destination within a stipulated time, it consider the presence of wormhole attack and adds that route to its wormhole list .On-demand routing protocol (AODP) is being used in dynamic wireless ad hoc networks, a new route will be discovered in response to every route

break . The route discovery requires high overhead. This overhead can be reduced if there are multiple paths and new route discovery is required only in the situation when all paths break.

2. PROBLEM FORMULATION

2.1. Main Objective

1. To reduce the power consumption in switching between the active and sleep mode of the nodes.
2. To schedule the transmission time to the available neighbor nodes.
3. To detect the malicious weight information provided by the nodes during the packet transmission.

2.2. Specific Objectives

1. To extend the generic algorithm and implement the Ability Based Synchronization algorithm to find the winner slot to store the packet data.
2. To extend the Ability Based Synchronization algorithm and implement the Optimism max out algorithm to avoid the inflation attack which is made by sending false maximum weight among the nodes.
3. To extend the Optimism max out algorithm and implement the Randomized Optimism max out algorithm to synchronize all the neighbor nodes by using all the slots.

2.3. Network Model

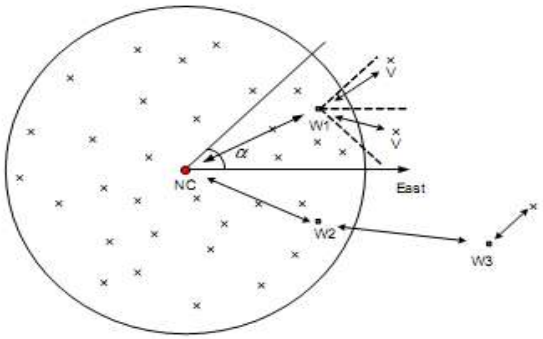

fig. 2.3: Network model under consideration

For 60 GHz directional networks are based on a centralized network structure, i.e., at least one network controller (NC) is deployed, although concurrent point-to-point transmissions are supported between different pairs of devices. Thus, we only consider the infrastructure mode where there exists one NC for access control and resources management of the network.

2.4 Attack Model

This section focuses on an active attack named wormhole attack, in which the malicious node(s) relay packets for two legislate nodes to fool them believing that they are direct neighbors. In particular, there are two types of wormhole attack in the network. One type of attack is that, there is a malicious node, e.g., W1, between the NC and the distant nodes.

In the neighbor discovery procedure, the malicious node relays the packets from the NC to the distant wireless node and vice-versa, to make them believe they are direct neighbor and let the NC offer service to the distant node. Another type of such attack is that, there are two or even more malicious nodes, e.g., W2 and W3, and they collude to relay packets between the NC and a distant legislate wireless node to believe they are direct neighbor. The first type of wormhole attack is only considered, as the proposed SND scheme is also effective for the second attack.

2.5 Proposed Wormhole Attack Resistant Scheme

This section first introduces the main idea of the proposed scheme, followed by the detailed description of the three phases in the scheme, namely the NC broadcast (BC) phase, response/authentication (RA) phase and the NA time analysis (TA) phase.

Though the region that each attacker can attack could be a circular area, sectors other than the three plotted sectors can be easily protected from the wormhole attack by using directional authentication, as described in the following. The objective of the proposed SND scheme is to detect whether there are malicious nodes in the NC's communication range R.

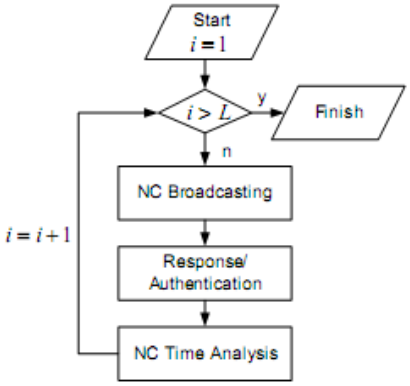

fig. 2.5: Flow chat of the proposed scheme

For the scan of each sector, the NC broadcasts its "hello" message in the specific direction. This period is called "NC BC phase". The legislate nodes in this sector scan its neighbor sector in a counter-clockwise manner starting from a random sector, staying in each sector for tn seconds.

Thus, to guarantee that all the nodes in the sector that the NC is scanning can hear the "hello" message, the NC BC phase should last for at least Ltn seconds. After the NC broadcasts its "hello" message in a septic sector and all the nodes in this sector hear the "hello" message, the node "RA phase" launches. In this phase, either the node(s) in this sector hear the transmission collision and report wormhole attack, or they authenticate with the NC and report their local time information, which can be used by the NC for further detection of wormhole attack in the "NC TA phase".

From the time domain, the process of the proposed worm-hole attack resistant SND scheme is shown in Fig. 3.4, which starts with the NC BC phase, followed by the RA phase and the NC TA phase. In the NC BC phase, the "hello" message is transmitted in each time slot of length ten=2 to guarantee that the nodes in this sector can hear the "hello" message when they enter this sector at a random time and stay there for time duration tn. As shown in Fig. 2.5, the NC TA phase can be pipelined with the RA phase with a delay of td. Note that for the NC BC phase, the length of the "hello" message is larger than tn/4 for security reason.

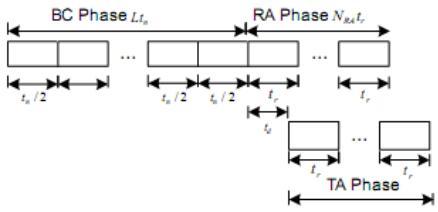

fig. 2.5: Time domain observation of the proposed scheme

2.5.1 ABS: Ability Based Synchronization Algorithm

An algorithm is described first that uses the size of synchronization clusters as a catalyst for synchronization. The algorithm is called ABS—weight based synchronization. As mentioned previously, at the end of each active interval, a node uses the slotArray structure to decide its next transmission time. The slotArray structure has s entries, one for each slot of the next (sleep) interval. The node has to choose one of these slots, called winner slot, and synchronize with it. That is, the node has to advertise the time of its next transmission (its TX value in the CPMP update packet) such that the update packet will be placed into that winner slot by its neighbors.

ABS: Weight Based Synchronization. *initState* resets the local structures. *processPackets* updates the local structures for each received packet. *setTX* determines the winner slot to be the one containing the packet from the largest neighboring cluster of synchronization.

Algorithm 1

```
1. Object implementation ABS extends GENERIC;

2. maxW : int; #max weight over active interval

3. weight : int; #weight advertised in SEMP packets

4. Operation initState()

5. for (i:= 0; i < s; i ++) do

6. slotArray[i] : = new pkt[]; od

7. end

8. Operation setTX()

#compute the maxW value

9. maxW := 0;

10. for (i:= 0; i < s; i ++) do

11. for (j:= 0; j < slotArray[i]:size();j ++) do

12. if (slotArray[i][j]:weight > maxW) then

13. winnerSlot := i;

14. maxW := slotArray[i][j]:weight; fi

15. od od

#determine new TX and weight values

16. if (winnerSlot!= nextSendSEMP % ta) then

17. TX:= winnerSlot;
```

18. nextSendSEMP := tcurr þ TX;

19. weight := maxW + 1;

20. else

21. weight := maxW;

22. fi

23. **end**

24. **Operation** processPackets(t_{curr}: int)

25. pktList := inq:getAllPackets(slotLen);

26. for (i:= 0; i < pktList:size();i ++) **do**

27. index :=((t_{curr} + pktList[i]:TX) mod t_a)/ts);

28. slotArray[index]:add(pktList[i]);

29. **od**

30. **end**

This operation needs to be explicitly performed, since from the last packet received from that cluster, the size of the cluster may have increased—the cluster may have incorporated other nodes. Let n be the number of nodes in a connected network.

2.5.2 OPM: Optimism max out algorithm

The Optimism Max out Algorithm is proposed to address the inflation attack. Instead of relying on subjective information (the weight value contained in SEMP updates), OPMOA allows nodes to build a local approximation of this metric, using only objective information derived from observation—the time of update receptions. OPMOA works by counting the number of packets that are stored in each slot of the current active interval.

Algorithm 2. Optimism Max out Algorithm. setTX finds the slot storing the maximum number of packets and synchronizes with it.

```
1. Object implementation OPMOA extends ABS;

2. maxC : int; #max nr: of packets per slot

3. Operation setTX()

#compute the maxC value

4. maxC :¼ 0;

5. for (i := 0; i < s; i++) do

6. if (slotArray[i]:size() > maxC) then

7. maxC :¼ slotArray[i]:size();

8. winnerSlot := i; fi

9. od

#update the TX value

10. if (winnerSlot! = nextSendSEMP % ta) then

11. TX:= winnerSlot;

12. nextSendSEMP := tcurr + TX;

13. fi

14. end
```

2.5.3 ROPM: Randomized Optimism Max Out Algorithm

This algorithm shows that for the same networks OPMOA is unable to completely synchronize, the situation changes when imperfect channel conditions are considered. Specifically, for a network of 100 nodes with 15 percent packet loss rates, OPMOA synchronizes the entire network in 21,000 s. While in a network with perfect channel conditions clusters created by OPMOA are

stable, packet loss can make nodes move from one cluster of synchronization to another, thus breaking the stability. If enough nodes switch, clusters may engulf other clusters in their vicinity, eventually creating a single cluster of synchronization.

However, relying only on packet loss is insufficient. One of our requirements is that a network synchronizes in a timely manner. To achieve this, we extend OPMOA with randomization: nodes choose to synchronize with their neighbors in a weighted probabilistic fashion. The algorithm is called randomized future peak detection.

This algorithm presents the details of the OPMOAR algorithm, which extends ABS (see Algorithm ABS algorithm). The initState and processPackets methods are also inherited from ABS.

3. EXPERIMENTAL RESULT

The following **Table 3.1** describes experimental result for existing system number of node given average in update data for NC State to receiver data RDMA protocol analysis. The table contains number of node, NC time interval, and receiver update data in RDMA protocol details are shown

Table 3.1Averagae of NC Update data in RDMA Protocol

S.NO	Number of Node	NC Update data (%)	Receiver Update Data in RDMA Protocol (%)
1	N8, N4 [2]	20	40
2	N7, N6, N9, N10 [4]	45	65
3	N5, N12,N14, N21, N23, N8 [6]	58	78
4	N9, N13, N15, N18, N22, N2, N8, N14 [8]	65	85
5	N9, N13, N15, N18, N22, N2, N8, N14, N21,N23 [10]	75	95

The following **Fig 3.1** describes experimental result for existing system number of node given average in update data for NC State to receiver data RDMA protocol analysis. The table contains number of node, NC time interval, and receiver update data in RDMA protocol details are shown.

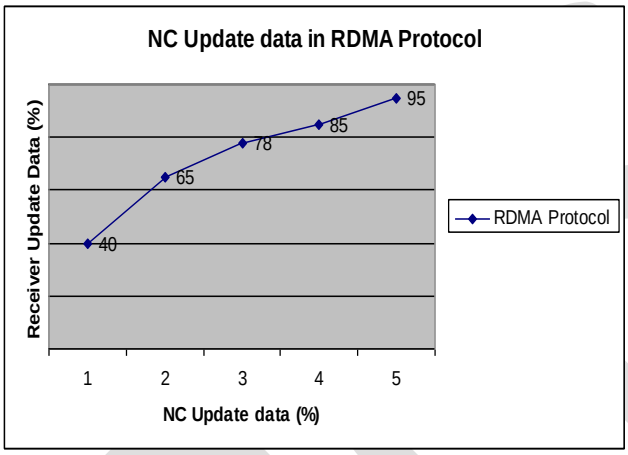

Fig 3.1 Average of NC update data in RDMA Protocol

The following **Table 3.2** describes experimental result for existing system number of node given average in update data for NC State to receiver data SEMP protocol analysis. The table contains number of node, NC time interval, and receiver update data in SEMP protocol details are shown.

Table 3.2 Average of NC Update data in SEMP Protocol

S.NO	Number of Node	NC Update data (%)	Receiver Update Data in SEMP Protocol (%)
1	N8, N4 [2]	20	46
2	N7, N6, N9, N10 [4]	45	72
3	N5, N12,N14, N21, N23, N8	58	83

	[6]		
4	**N9, N13, N15, N18, N22, N2, N8, N14 [8]**	**65**	**89**
5	**N9, N13, N15, N18, N22, N2, N8, N14, N21,N23 [10]**	**75**	**97**

The following **Fig 3.2** describes experimental result for existing system number of node given average in update data for NC State to receiver data SEMP protocol analysis. The table contains number of node, NC time interval, and receiver update data in SEMP protocol details are shown

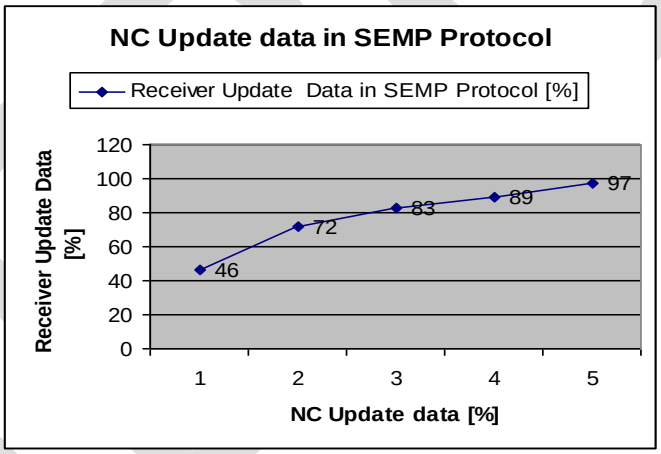

Fig 3.2 Average of NC updates data in SEMP Protocol

The following **Table 3.3** describes experimental result for RDMA and SEMP protocol and average in update data for NC State to receiver data analysis. The table contains number of node, NC time interval, and receiver update data in RDMA and SEMP protocol details are shown

Table 3.3 NC update data in RDMA and SEMP Protocol

S.NO	NC Update data (%)	RDMA Protocol (%)	SEMP Protocol (%)
1	20	40	46
2	45	65	72
3	58	78	83
4	65	85	89
5	75	95	97

The following **Fig 3.3** describes experimental result for RDMA and SEMP protocol and average in update data for NC State to receiver data analysis. The table contains number of node, NC time interval, and receiver update data in RDMA and SEMP protocol details are shown

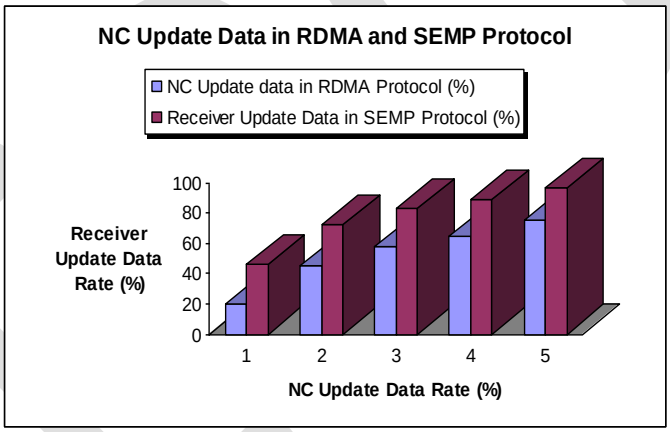

Fig 3.3 NC update data in RDMA and SEMP Protocol

The following **Table 3.4** describes Performances Analysis for RDMA and SEMP Protocol. The table contains NC time interval, and sending data in to designation and its arrival time interval in RDMA and SEMP protocol details are shown

Table 3.4 Performances Analysis for RDMA and SEMP Protocol

S.NO	NC Update Data (ns)	RDMAP Send data To Designation Arrival Details (ms)	SEMP Send Data to Designation Arrival Details (ms)
1	10	163	161

2	20	165	163
3	30	173	170
4	40	176	174
5	50	181	177
6	60	184	182
7	70	185	183
8	80	191	188
9	90	194	190
10	100	197	195

The following **Fig 3.4** describes Performances Analysis for RDMA and SEMP Protocol. The table contains NC time interval, and sending data in to designation and its arrival time interval in RDMA and SEMP protocol details are shown

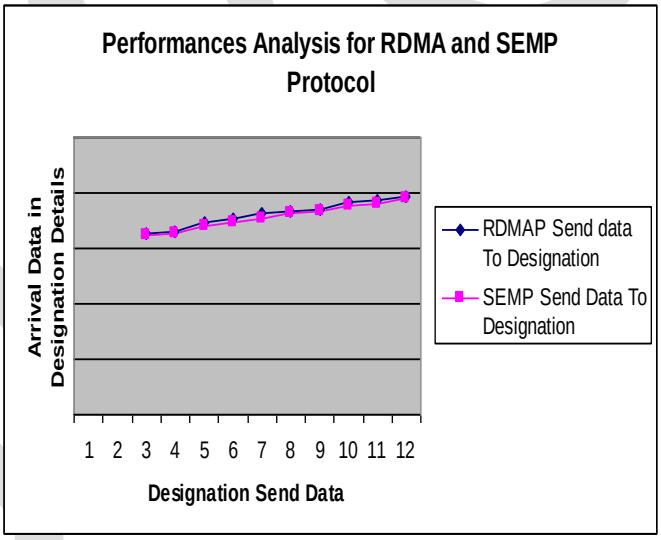

Fig 3.4 Performances Analysis for RDMA and SEMP Protocol

4. CONCLUSSION

The propose system at present several algorithms for synchronization mechanisms. However, the use of random values in winner slot calculation does not cent percent accuracy. So the extension of proposed algorithms with a new algorithm is required for highly efficient communication between nodes.

If the application is tested with real mobile nodes, then it can assist the further proceeding of the algorithm implementation practically. In addition if the experimental application is designed web based, then it can be accessed platform independently and the usage will be more. The new system is designed such that those enhancements can be integrated with current modules easily with less integration work.

The problem of synchronizing the periodic transmissions of nodes in ad hoc networks, in order to enable battery lifetime extensions without missing neighbor's updates is studied. Several solutions, both lightweight and scalable but vulnerable to attacks is proposed. Extension of generic algorithm to use transmission stability as a metric for synchronization is made. The implementation and simulations show that the protocols are computationally inexpensive, provide significant battery savings, are scalable and efficiently defend against attacks.

5. SCOPE FOR FUTURE ENHANCEMENTS

Several algorithms are proposed for synchronization mechanisms. However, the use of random values in winner slot calculation does not cent percent accuracy. So the extension of proposed algorithms with a new algorithm is required for highly efficient communication between nodes.

- If the application is tested with real mobile nodes, then it can assist the further proceeding of the algorithm implementation practically.
- In addition if the experimental application is designed web based, then it can be accessed platform independently and the usage will be more.

The new system becomes useful if the above enhancements are made in future. The new system is designed such that those enhancements can be integrated with current modules easily with less integration work.

6. REFERENCE

[1] X. An, R. Prasad, and I. Niemegeers, "Neighbor discovery in 60 ghz wireless personal area networks," in Proceedings of IEEE International Symposium on World of Wireless Mobile and Multimedia Networks .IEEE, 2010, pp. 1–8.

[2] S. Vasudevan, J. Kurose, and D. Towsley, "On neighbor discovery in wireless networks with directional antennas," in Proceedings of IEEE INFOCOM 2005 , vol. 4, 2005, pp. 2502–2512.

[3] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in Proceedings of Network and Distributed System Security Symposium . San Diego, 2004

[4] R. C. Daniels and R. W. Heath, Jr., "60 GHz wireless communi-cations: Emerging requirements and design recommendations," IEEE Veh. Technol. Mag., vol. 2, no. 3, pp. 41–50, Sept. 2007.

[5] Z. M. Chen and Y. P. Zhang, "Inter-chip wireless communication channel: Measurement, characterization, and modeling," IEEE Trans. Antennas Propagat., vol. 55, no. 3, pp. 978–986, Mar. 2007.

[6] A. Burrell and P. Papantoni-Kazakos, "Random access algorithms in packet networksła review of three research decades," International Journal of Communications, Network and System Sciences, vol. 5, no. 10, pp. 691–707, 2012.

[7] L. Georgiadis, L. Merakos, and P. Papantoni-Kazakos, "A method for the delay analysis of random multiple-access algorithms whose delay process is regenerative," IEEE Journal on Selected Areas in Communications, vol. 5, no. 6, pp. 1051–1062, 1987.

[8] R. Mudumbai, S. Singh, and U. Madhow, "Medium access control for 60 ghz outdoor mesh networks with highly directional links," in Proccedings of IEEE 1

[9] G. Acs, L. Buttyan, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 5, no. 11, pp. 1533-1546, Nov. 2006.

[10] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-Tolerant Routing for Wireless Networks," Computer Comm., vol. 29, no. 2, pp. 216-230, 2006.

[11] S. Dosh i, S. Bhandare, a nd T.X. Brow n, "An On-Demand Minimum Energy Routing Protocol for a Wireless Ad Hoc Network," ACM SIGMOBILE Mobile Computing and Comm. Rev., vol. 6, no. 3, pp. 50-66, 2002.

[12] L.M. Feeney, "An Energy Consumption Model for Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks," Mobile Networks and Applications, vol. 6, no. 3, pp. 239-249, 2001.

[13] D.B. Johnson, D.A. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks," Ad Hoc Networking, Addison-Wesley, 2001.

[14] Y.-C. Hu, A. Perrig, and D. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. In Proceedings of the ACM Conference on Mobile Computing and Networking (Mobicom), 2002.