Volume 2, Issue 4, April 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Packet Misrouting Attacks in Multi Radio Wireless Networks: Detection and Countermeasure

E.S.Phalguna Krishna*, I.D.Krishna Chandra,
M.Ganesh Karthik
Assistant Professor*
Department of CSE,
Sree Vidyanikethan Engg College,
Tirupati,India
phalgunakrishna@gmail.com

Abstract—**Stealthy packet dropping is a suite for attack such as misrouting and that can be easily launched against multiradio wireless networks. Stealthy packet dropping disrupts the packet from reaching the destination through malicious behavior at an intermediate node. However, the malicious node gives the impression to its neighbors that it performs the legitimate forwarding action. Moreover, a legitimate node comes under suspicion. A popular method for detecting attacks in wireless networks is behavior-based detection performed by normal network nodes through overhearing the communication in their neighborhood. We show that local monitoring, and the wider class of overhearing-based detection, cannot detect stealthy packet dropping attacks. Additionally, it mistakenly detects and isolates a legitimate node. We present a protocol called SADEC that can detect and isolate stealthy packet dropping attack efficiently. SADEC presents two techniques that can be overlaid on baseline local monitoring: having the neighbors maintain additional information about the routing path and adding some checking responsibility to each neighbor. Additionally, SADEC provides an innovative mechanism to better utilize local monitoring by considerably increasing the number of nodes in a neighborhood that can do monitoring.**

Keywords: **Multi radio wireless networks, Stealthy attacks, Local monitoring, Packet misrouting.**

1. Introduction

Multi Radio Wireless Networks (MRWN) is becoming an important platform in several domains, including police, military warfare and delivery services. There are two types of radio networks currently in use around the world: the one-to-many broadcast network commonly used for public information and mass media entertainment; and the two-way type used more commonly for public safety and public services such as police, fire, taxicabs, and delivery services. Many of the same components and much of the same basic technology applies to both [11].

The Two-way type of radio network shares many of the same technologies and components as the Broadcast type radio network but is generally set up with fixed broadcast points (transmitters) with co-located receivers and mobile receivers/transmitters or Tran-ceivers. In this way both the fixed and mobile radio units can communicate with each other over broad geographic regions ranging in size from small single cities to entire states/provinces or countries. There are many ways in which multiple fixed transmit/receive sites can be interconnected to achieve the range of coverage required by the jurisdiction or authority implementing the system: conventional wireless links in numerous frequency bands, fibre-optic links, or micro-wave links. In all of these cases the signals are typically backhauled to a central switch of some type where the radio message is processed and resent (repeated) to all transmitter sites where it is required to be heard[11] [12].

However, the open nature, the fast deployment practices, and the hostile environments where MRWN may be deployed, make them vulnerable to a wide range of attacks against both control and data traffic. Moreover, many MRWN such as wireless networks are resource constrained, primarily with respect to energy and bandwidth. Thus, any security protocol needs to obey these constraints as well. Control traffic attacks include wormhole [5], rushing [4], and Sybil [10] attacks. The most notable data traffic attacks are blackhole, selective forwarding, and delaying, in which, respectively, a malicious node drops data (entirely or selectively) passing through it, or delays its forwarding, and misrouting attack in which the attacker relays packets to the wrong next hop. These attacks could result in a significant loss of data or degradation of network functionality, say through disrupting network connectivity by preventing route establishment.

Cryptographic mechanisms alone cannot prevent these attacks since many of them, such as the wormhole

and the rushing attacks, can be launched without needing access to cryptographic keys or violating any cryptographic check. To mitigate such attacks, many researchers have used the concept of behavior-based detection which is based on observing patterns in the behavior of neighboring nodes and flagging anomalous patterns. The notion of behavior is related to communication activities such as forwarding packets (e.g., [6]) or noncommunication activities such as reporting sensed data. A widely used instantiation of behavior-based detection is Local Monitoring (e.g., [1], [2], [6], [7], [8], [15]). In local monitoring, nodes oversee part of the traffic going in and out of their neighbors. This leverages the open broadcast nature of wireless communication. Different types of checks are done locally on the observed traffic to make a determination of malicious behavior. For example, a node may check that its neighbor is forwarding a packet to the correct next-hop node, within acceptable delay bounds. For systems where arriving at a common view is important, the detecting node initiates a distributed protocol to disseminate the alarm. We call the existing approaches which follow this template Baseline Local Monitoring (BLM). Many protocols have been built on top of BLM for intrusion detection (e.g., [3]), building trust and reputation among nodes (e.g., [1], [2], [14]), protecting against control and data traffic attacks (e.g., [6], [7], [8]), and in building secure routing protocols (e.g., [8], [9]).

For specificity, we will use [6], [7], [8] as the representative BLM which we will use for comparison with the approach presented in this paper. In BLM, a group of nodes, called guard nodes perform local monitoring with the objective of detecting security attacks. The guard nodes are normal nodes in the network and perform their basic functionality in addition to monitoring. Monitoring implies verification that the packets are being faithfully forwarded without modification of the immutable parts of the packet, within acceptable delay bounds and to the appropriate next hop. If the volume of traffic is high (for data traffic in a loaded network), a guard verifies only a fraction of the packets.

In this paper, we introduce a new class of attacks in multi radio wireless networks called stealthy packet dropping. In stealthy packet dropping, the attacker achieves the objective of disrupting the packet from reaching the destination by malicious behavior at an intermediate node. However, the malicious node gives the impression to its neighbors participating in local monitoring that it has performed the required action (e.g., relaying the packet to the correct next-hop en route to the destination). This class of attacks is applicable to packets that are neither acknowledged end to end nor hop by hop. Due to the resource constraints of bandwidth and energy, much traffic in multi radio wireless networks is unacknowledged or only selectively acknowledged. This is particularly true for the more common data traffic or broadcast control traffic than for rare unicast control traffic.

In this paper, we introduce one mode of the stealthy packet dropping attack. We distinguish between an external malicious node, which does not possess the cryptographic keys in the network, and an internal compromised node, which does and is created by compromising an erstwhile legitimate node. Consider a scenario in which a node called S is forwarding a packet to a compromised node called M. M is supposed to relay the packet to the next-hop node D. The form of the attack is called packet misrouting. In this mode, M relays the packet to an incorrect next-hop neighbor. The result is that the packet does not reach its intended next hop (D) while M appears to the guards as doing its forwarding job correctly.

Additionally, in each attack type, a legitimate node is accused of packet dropping. We acknowledge that the attack model calls for smart adversaries— e.g., they can collude, can position the adversarial nodes, can control transmission power at a fine level of granularity, or can spend significant energy in launching the attacks. On the other hand, note that these attack are not hard to mount for motivated attackers since the requirement for successful instantiation of these attack is fairly humble and practically viable. Therefore, we believe that if the network is critical enough, we do have to worry about such motivated adversaries.

We provide a protocol called Stealthy Attacks in multi radio wireless networks: Detection and Countermeasure (SADEC) that is built using local monitoring and that can mitigate packet misrouting attack type introduced above. SADEC'S detection technique involves two high-level steps: first, having guard nodes that maintain additional next-hop information gathered during route establishment; and second, adding some checking responsibility to each neighbor.

We provide a theoretical analysis for the probability of success of the stealthy packet drop attack in a locally monitored network. We also analyze the resource consumption cost of SADEC. Our analysis shows that SADEC maintains detection coverage above 90 percent for the configuration in which BLM has less than 60 percent coverage. Moreover, the legitimate node isolation of SADEC remains below 2 percent for the configurations in which BLM exceeds 99 percent. Additionally, we build a simulation model for both the power control and the misrouting attacks using ns-2 and perform a comparative evaluation of BLM with SADEC.

Our simulation results show that SADEC can deliver 60 percent of packets to the destination with 20 percent nodes compromised launching misrouting attack, while BLM delivers less than 10 percent. The likelihood of framing of legitimate nodes is also 18-fold reduced with SADEC compared to BLM for the same network. The performance advantages under misrouting attack come at the expense of a slightly higher false isolation (due to natural collisions on the channel) and end-to-end delay in SADEC.

2. RELATED WORK

In the last few years, researchers have been actively exploring many mechanisms to ensure the security of control and data traffic in wireless networks. These mechanisms can be broadly categorized into the following classes—authentication and integrity services, protocols that rely on path diversity, protocols that use specialized hardware, protocols that require explicit acknowledgments or use statistical methods, and protocols that overhear neighbor communication.

A technique proposed to detect malicious behavior involving selective dropping of data, relies on explicit acknowledgment for received data using the same channel or an out-of-band channel. This method would render stealthy packet dropping detectable at the end point. However, the method incurs high communication overhead and has to be augmented with other techniques for diagnosis and isolation of the malicious nodes. A natural extension would be to reduce the control message overhead by reducing the frequency of acking to one in every N data messages (in the above papers N = 1). However, this may delay the adversary detection which may result in significant damage. Statistical measures have been used by some researchers for detection to detect wormhole attacks.

This paper builds on our previous work. In we introduced the stealthy packet dropping attacks and proposed a protocol called MISPAR to mitigate the attacks. In this paper, we quantify the likelihood of mistaken isolation of legitimate nodes due to both natural errors and framing. We also present a thorough analysis of legitimate and malicious node isolation probabilities for both BLM and SADEC under the misrouting attack.

3. FOUNDATIONS

3.1 Attack Model and System Assumptions

3.1.1 Attack Model

An attacker can control an external node or an internal node, which, since it possesses the keys, can be authenticated by other nodes in the network. An insider node may be created, for example, by compromising a legitimate node. A malicious node can perform packet dropping by itself or by colluding with other nodes. The collusion may happen through out-of-band channels (e.g., a wireline channel). However, we do not consider the denial of service attacks through physical-layer jamming [13], or through identity spoofing and Sybil attacks [10].

There exist several approaches to mitigate these attacks—[13] for jamming and [10] for the Sybil attack. A malicious node can be more powerful than a legitimate node and can have high powered controllable transmission capability but is limited to Omnidirectional antennas. The attacks do not affect only a specific routing protocol; rather, they apply to a wide class where an intermediate node determines the next-hop node toward the final destination.

3.1.2 System Assumptions

We assume that all the legitimate communication links are bidirectional. We assume that secure neighbor discovery has been performed and that every node knows both first and second-hop neighbor information. This can be achieved through the protocol described as well as by approaches developed by other researchers [4]. Note that while this knowledge is enormously useful, this by itself cannot mitigate many attack types. For example, further work is needed to detect the wormhole attack. Intuitively, this information subsets the nodes from which a given node will accept packets but does not eliminate the possibility of malicious nodes within that subset. Local monitoring assumes that the network has sufficient redundancy, such that each node has more than an application defined threshold number of legitimate nodes as guards. We assume a key management protocol exists such that any two nodes can communicate securely. We present SADEC for static networks. However, the technique is also valid under mobile situations after adaption to address mobility challenges.

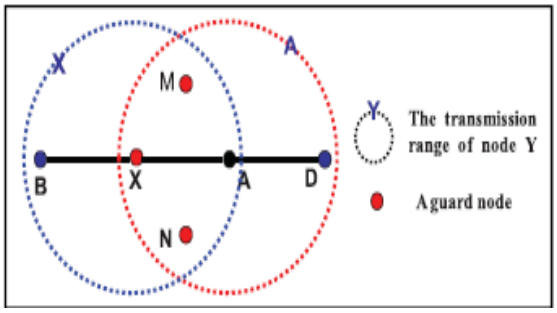

Fig. 1. X, M, and N are guards of A over X -> A.

One of these challenges is the problem of determining the neighbor relation securely. Several such protocols exist in the literature [5], [16], [17]. Additional challenges that need to be addressed include time synchronization and the ability to distinguish between malicious and natural errors which become more frequent due to mobility.

3.2 Background: Local Monitoring:

Local monitoring is a collaborative detection strategy where a node monitors the traffic going in and out of its neighbors. This strategy was introduced in [6] for static sensor networks and here, we give the background needed to understand the concepts presented in this paper.

For a node, say α, to be able to watch a node, say N_2, α must be a neighbor of both N_2 and the previous hop fromN_2, say N_1.We call α a guard node for N2 over the link $N_1 \rightarrow N_2$. We use the notation R (N) to denote the set of all nodes that are within the radio range of N and G (N_1, N2) to denote the set of all guard nodes for N2 over a link $N_1 \rightarrow N_2$. Formally, G (N_1, N2) = R (N_1) ∩ R (N_2) - N_2, where $N_2 \in$ R (N1). For example, in Fig. 1, G(X, A) = {M, N, X}. Information from each packet sent from X to A is saved in a watch buffer at each guard. The guards expect that A will forward the packet toward the ultimate destination, unless A is itself the destination. Each entry in the watch buffer is time stamped with a time threshold, T, by which A must forward the packet. Each packet forwarded by A with X as a previous hop is checked for

the corresponding information in the watch buffer. The check can be to verify if the packet is fabricated or duplicated (no corresponding entry in the buffer), corrupted (no matching hash of the payload), dropped, or delayed (entry is not matched within T). A malicious counter (MalC(i,j)) is maintained at each guard node, i, for a node, j, at the receiving end of each link that i is monitoring over a sliding window of length T_{win}. MalC(i,j) is incremented for any malicious activity of j detected by i. The increment to MalC depends on

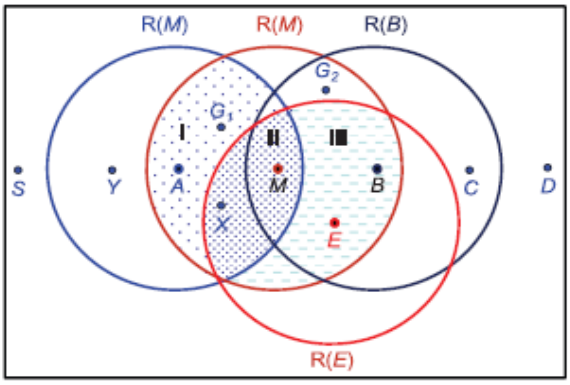

Fig.2. Misrouting scenario

the nature of the malicious activity, being higher for more severe infractions. When the growth in the counter value maintained by a guard node i for node j (MalC(i,j)) crosses a threshold rate (MalCth) over T_{win}, node i revokes j from its neighbor list (called direct isolation since it will henceforth not perform any communication with node j), and sends to each neighbor of j, an authenticated alert message indicating j is a suspected malicious node. When a neighbor N_i gets the alert, it verifies the authenticity of the alert message. When N_i gets enough alert messages about j, it marks the status of j as revoked (called indirect isolation). The notion of enough number of alerts is quantified by the detection confidence index γ. Each node maintains a memory of nodes that it has revoked through a local blacklist so that a malicious node cannot come back to its neighborhood and claim to be blameless. This constitutes local isolation of a malicious node by its current neighbors.

4. STEALTHY DROPPING ATTACK DESCRIPTION

In all the modes of stealthy packet dropping, a malicious intermediate node achieves the same objective as if it were dropping a packet. However, none of the guard nodes using BLM become any wiser due to the action. In addition, a legitimate node is accused of packet dropping. Next, we describe the four attack types for stealthy dropping.

4.1 Drop through Misrouting:

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. The authors in [6] argue that that latter case would be more expensive and dangerous since it gives malicious nodes valid excuses to drop packets. Therefore, they go with the first choice, even though it may result in some false accusations.

Consider the example scenario in Fig. 2. Node A sends a packet to the malicious node M to be relayed to node B. Node M simply relays the packet to node E which is not in the route to the final destination of the packet. Node E drops the packet. The result is twofold: 1) node M successfully drops the packet without being detected since all the guards of M over A →M (regions I and II) have been satisfied by the transmission of M → E, and 2) legitimate node E will be wrongly accused by its guards over M → E (regions II and III) as maliciously dropping the packet

5. STEALTHY DROPPING ATTACK MITIGATION:

In this section, we propose two mechanisms to augment traditional local monitoring to enable the detection of stealthy packet dropping attacks. The first mechanism mitigates stealthy packet dropping through misrouting while the second mitigates the rest of the attack types.

5.1 Mitigating Misrouting Packet Drop:

To detect this attack type, local monitoring has to incorporate additional functionality and information. The basic idea is to extend the knowledge at each guard to include the identity of the next hop for the packet being relayed.

This additional knowledge can be collected during route establishment. Many multihop wireless routing protocols provide this knowledge without any modification while some changes are necessary in others. The first class includes both reactive routing protocols such as Dynamic Source Routing (DSR) and its variants and proactive routing protocols such as TinyOS beacon routing and Destination Sequenced Distance Vector routing (DSDV). In all source routing protocols, the packet header carries the identity of all the nodes in the route from the source to the destination. Therefore, no additional traffic is required to be generated for the guard nodes to be able to detect this form of the attack. Moreover, no additional information is required to be maintained at the guards since each packet carries the required information in its header. In TinyOS beacon routing, the base station periodically broadcasts a beacon to establish a breadth first search tree rooted at the base station. Each node within the transmission range of the base station overhears the beacon, sets its parent to be the base station, sets the hop count to the base station to be one, and rebroadcasts the beacon. Each beacon carries the identity of the broadcasting node, the identity of its parent, and the hop count to the base station. Each guard overhearing the beacon broadcasting saves parent node identity for each neighbor. Later, when a node, say B, is sent a packet to relay, the guard of B can detect any misrouting by B since it knows the correct next-hop en route to the base station

The second class of routing protocols requires modification to the protocol to build the next-hop information at the guards. Examples of these protocols are the reactive routing protocols that use control packet flooding of route requests (REQs) and route replies (REPs) to establish the route between the source and the destination (e.g., LSR [8] and AODV). In these protocols, when a source node desires to send a message to some destination node and does not already have a valid route to that destination, it initiates a route discovery process to locate the other node. It broadcasts a route request packet to its neighbors, which then forward the request to their neighbors, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is located. Along with its own sequence number and the broadcast ID, the source node includes in the REQ the most recent sequence number it has for the destination. During the process of forwarding the REQ, intermediate nodes record in their route tables the address of the neighbor from which the first copy of the broadcast packet is received, thereby establishing a reverse path. Once the REQ reaches the destination, the destination node responds by unicasting a route reply packet back to the neighbor from which it first received the REQ. As the REP traverses along the reverse path, nodes along this path set up forward route entries in their route tables which point to the node from which the REP came.

Next, we show the required changes to the basic version of AODV to enable the guards to build the necessary knowledge for detecting the misrouting attack. The idea behind the solution is to augment the additional information required for detection to the control traffic responsible for route establishment and require the guards to collect that information during the route establishment phase. To collect the next-hop identity information in AODV, the forwarder of the REQ attaches the previous two hops to the REQ packet header. Let the previous hop of M be A for a route from source S to destination D, and the next hop from M be B (Fig. 2). When M broadcasts the REQ received from A, it includes the identity of A and its own identity (M) in the REQ header <S, D, REQ_id, A, M>. When B and the other neighbors of M get the REQ from M, they keep in a Verification Table (VT) <S, D, RREQ_id; A, M, -> (last field is currently blank). When B broadcasts the REQ, the common neighbors of M and B update their VT to include B<S, D, RREQ_id, A, M, B>. When B receives a REP to be relayed to M, it includes in that REP the identity of the node that M needs to relay the REP packet to, which is A in this example. Therefore, all the guards of M now know that M not only needs to forward the REP but also that it should forward it to A.

Two tasks have been added to the functionality of the guards in monitoring the REP packets. First, the guard G of a node N verifies that N forwards the REP to the correct next hop. In the example above, G2 verifies that M forwards the REP to A. Second, G verifies that N has updated the forwarded REP header correctly. In the example shown above, G2 verifies that when the input packet to M from B is <REP, S, D, REQ_id, C, B, M>, then the output packet from M should be <REP, S, D, REQ_id, B, M, A>. Note that M and its guards over the link B →M know that the next hop is A from the information collected in the VT table during the REQ flooding.

Using the additional information mentioned above, SADEC detects misrouting attacks as follows: in the example above, assume that S is sending a data packet to D through a route that includes <Y, A, M, B, C >. The malicious node M cannot misroute the data packet received from A to a node other than the next hop, B since each guard of M over the link A → M has an entry in its VT which indicates B as the correct next hop. This results in an additional checking activity for the guard node involved in local monitoring verifying that the data packet is forwarded to the correct next hop, as indicated by the entry in the guard node's VT. Moreover, M cannot frame another neighbor, say X, by misrouting the packet to X. The guards of X over M →X do not have an entry like <S, D, REQ_id, Y, A, M, X> and therefore, they would not increment the MalC of X when it drops the packet.

6. ANALYSIS

The analysis gives the detection probability for a malicious node indulging in the drop through misrouting and power control attack types. It also provides the probability of false detection of legitimate nodes. We analyze BLM and SADEC under different network conditions. Attacker model The malicious node M uses an omnidirectional antenna. Its goal is to have the effect of dropping the packet from reaching the legitimate next-hop node T.

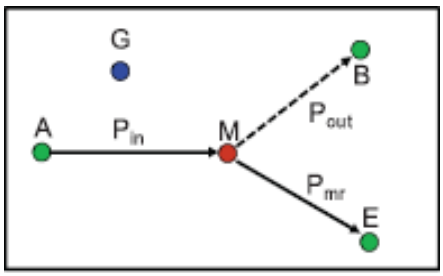

Fig. 3. Misrouting stealthy packet drop scenario.

The detection probability is a lower bound since we assume that the adversary can control the transmission power level to be infinitesimally smaller than that required to reach T. The reduced transmission range of M is represented as y. Output parameters. We define

1. The probability of detection as the probability that a malicious node is detected by a single guard node,
2. The probability of isolation as the probability that the node is directly detected by at least γ neighbors and therefore isolated,
3. The probability of false detection or isolation as the probability that a nonmalicious node is detected by a neighbor or by at least γ neighbors due to natural reasons

such as collision or drop in the communication channel, and

4. The probability of framing detection or isolation is the probability that a nonmalicious node is detected by a neighbor or γ neighbors due to malicious activities.

In the following, we analyze a representative attack from proposed mechanisms to detect stealthy packet dropping. The misrouting stealthy packet dropping, we provide the results for baseline local monitoring (BLM) and SADEC.

6.1 Misrouting Stealthy Packet Dropping:

Consider the scenario in Fig. 3 below. A node A is relaying a packet (P_{in}) to the next-hop node M, which is malicious. Node M is supposed to relay the packet to the legitimate next-hop node B as P_{out}. Instead, M relays the packet to a wrong next hop E as P_{mr}.

There are four different possibilities for the guard G in Fig. 3:

1. G misses both Pin and Pmr → missed detection.
2. G misses Pin but gets Pmr → detection as fabricate (which is incorrect since the malicious action is misrouting).
3. G gets Pin but misses Pmr → detection as drop (incorrect).
4. G gets both Pin and Pmr → successful misrouting detection for SADEC and missed detection for BLM.

7. CONCLUSION:

We have introduced a new class of attack which disrupts a packet from reaching the destination by malicious behavior at an intermediate node. This can be achieved through misrouting. However, the malicious behavior cannot be detected by any behavior based detection scheme presented to date. Specifically, we showed that BLM-based detection cannot detect this attack. We then presented a protocol called SADEC that successfully mitigates all the presented attack. SADEC builds on local monitoring and requires nodes to maintain additional routing path information and adds some checking responsibility to each neighbor. Additionally, SADEC's new detection approach expands the set of neighbors that are capable of monitoring in a neighborhood, thereby making it more suitable than BLM in sparse networks.

In future work, we are considering other detection techniques for multiradio wireless networks such as power control, colluding collision and identity delegation. The listening activity for detecting malicious behavior is more complicated due to the presence of multiple channels and multiple radios.

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 the CONFIDANT 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 System for Ad Hoc Networks," Proc. ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '03), pp. 135-147, 2003.

[4] Y.C. Hu, A. Perrig, and D. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," Proc. ACM Workshop Wireless Security (WiSe '03), pp. 30-40, 2003.

[5] Y.C. Hu, A. Perrig, and D.B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," Proc. IEEE INFOCOM, pp. 1976-986, 2003.

[6] I. Khalil, S. Bagchi, and N. Shroff, "LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks," Proc. Int'l Conf. Dependable Systems and Networks (DSN '05), pp. 612-621, 2005.

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

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

[9] S.J. Lee and M. Gerla, "Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks," Proc. IEEE Int'l Conf. Comm. (ICC '01), pp. 3201-3205, 2001.

[10] Q. Zhang, P. Wang, D. Reeves, and P. Ning, "Defending against Sybil Attacks in Sensor Networks," Proc. Int'l Workshop Security in Distributed Computing Systems (SDCS '05), pp. 185-191, 2005.

[11] Minho Shin, Seungjoon Lee and Yoo-ah Kim, "Distributed Channel Assignment for Multi-radio Wireless Networks", pp.417-426, 2006.

[12] Krishna N. Ramachandran, Elizabeth M. Belding, Kevin C. Almeroth and Milind M. Buddhikot, "Interference-Aware Channel Assignment in Multi-Radio Wireless Mesh Networks".

[13] R. Muraleedharan and L.A. Osadciw, "Jamming Attack Detection and Countermeasures in Wireless Sensor Network Using Ant System," Proc. Wireless Sensing and Processing, vol. 6248, p. 62480G, 2006.

[14] S. Buchegger and J.L. Boudec, "Robust Reputation System for P2P and Mobile Ad-Hoc Networks," Proc. Workshop Economics of Peerto- Peer Systems, 2004.

[15] I. Khalil, S. Bagchi, and N. Shroff, "SLAM: Sleep-Wake Aware Local Monitoring in Sensor Networks," Proc. 37th Ann. IEEE/IFIP Int'l Conf. Dependable Systems and Networks (DSN '07), pp. 565-574, June 2007.

[16] N. Sastry, U. Shankar, and D. Wagner, "Secure Verification of Location Claims," Proc. ACM Workshop Wireless Security (WiSe '03), pp. 1-10, 2003.

[17] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks," Proc. Network and Distributed System Security Symp. (NDSS '04), pp. 131-141, 2004.

