International Journal of Emerging Engineering Research and Technology
Volume 2, Issue 4, July 2014, PP 146-154
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

Infraction Forestalling System through SADEC: Stealthy Attack Detection and Mitigation

V.Mayuri[1], B.Neelima[2]

[1]M.TECH, E.C.E, A.I.T.S, TIRUPATHI
[2]ASSISTANT PROFESSOR, E.C.E, A.I.T.S, TIRUPATHI
mayuri.vipparla1@gmail.com
neeli405@gmail.com

Abstract: *In this paper we are catering a effectuation details about simulated solution of stealthy packet drop attack. Stealthy packet drop attack constitutes of four types of attack, which includes colluding collision, packet misrouting, identity delegation and power control. This attack interrupts the packet from reaching the destination through malicious behavior at an intermediate node and can be easily breakdown the multi-hop wireless ad-hoc networks. Observation of the behavior of the neighborhood which is performed by the normal network nodes through overhearing the communication in their neighborhood is one of the common methods for detecting attacks in wireless networks. An instantiation of this technology is local monitoring. 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. A new proposed protocol is called SADEC that can detect and mitigate stealthy packet dropping attack efficiently. It makes use of the local monitoring technique by increasing the number of nodes that can do the monitoring function and they maintain additional information about the routing path so that it can check whether each node is doing its legitimate action. By simulation results, we show that the proposed architecture reduces the drops due to attack and increases the packet delivery ratio.*

Keywords: *Stealthy packet drop, colluding collision, packet misrouting, identity delegation, power control, SADEC.*

1. INTRODUCTION

Now a day's wireless networks are becoming more preferable platforms in many domains but security in wireless is very less as compare to wired (traditional) network. They are becoming important platform for command and control of civilian critical infrastructure and military warfare. Stealthy packet drop attack is a latest threat to wireless ad-hoc networks. Here malicious node evades detection and legitimate node treated as malicious node.

It is suite of four attack types which includes:

1. Misrouting: malicious node misroutes the packet to wrong next hop.

2. Colluding collision: Malicious node with help of its colluding partner over flood the valid next hop resulting in packet drop.

3. Transmission power control: malicious node controls the transmission to its nearest neighbour which is not valid next hop and results in packet drop.

4. Identity delegation: Delegate the relay responsibility to its colluding partner which is close to sender.

To detect such attacks such as wormholes and rushing attacks, traditional mechanism like cryptography alone fails. In this paper we are providing a practical implementation details about solution of stealthy packet drop attack is SADEC protocol. Most of researchers use a behaviour based detection mechanism to detect such attacks. Behaviour based detection includes local monitoring. SADEC also includes local monitoring but adds some checking responsibility to each neighbour in wireless ad-hoc network along with each guard nodes over the network. SADEC improves the efficiency of the wireless ad-hoc network over the base line local monitoring [1]. To mitigate such attacks, many researchers have used the concept of behaviour-based detection.

The notion of behaviour is related to communication activities such as forwarding packets (e.g., [3]). A widely used instantiation of behaviour-based detection is Local Monitoring (e.g., [4],[5], [3], [6],[7], [8], [9]). In local monitoring, nodes oversee part of the traffic going in and out of their neighbours. 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 behaviour. For example, a node may check that its neighbour 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).

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 wireless multi hop ad hoc networks called stealthy packet dropping. In stealthy packet dropping, the attacker achieves the objective of disrupting the packet from reaching the destination by malicious behaviour at an intermediate node. However, the malicious node gives the impression to its neighbours 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 neither end (e.g., 10]) nor hop by hop (e.g., 11]). Due to the resource constraints of bandwidth and energy, much traffic in multi hop ad hoc wireless networks is unacknowledged or only selectively acknowledged [10], [11].

In this paper, we introduce four modes of the stealthy packet dropping attack, such as Misrouting attack, Power Control attack, Colluding Collision, Identity Delegation attack. We provide a protocol called Stealthy Attacks in Wireless Ad Hoc Networks: Detection and Countermeasure (SADEC) that is built using local monitoring and that can mitigate each of the four attack types 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 neighbour.

Finally, in this paper section 2 contains related work; section 3 contains proposed practical implementation solution to stealthy packet drop attacks. Section 4 contains technology going to be used and features of this project and section 5 contains conclusion.

2. STEALTHY PACKET DROP ATTACKS

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.

2.1 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, 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 argue 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.

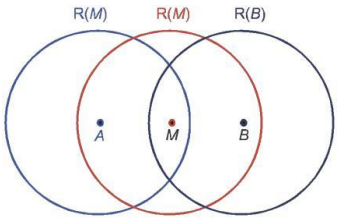

Fig.1. *Drop through Misrouting scenario*

2.2 Drop through Power Control

In this type of attack, a malicious node relays the packet by carefully reducing its transmission power, thereby reducing the range and excluding the legitimate next-hop node. This kind of transmission power control is available in today's commercial Wireless nodes, such as the Crossbow Mica family of nodes.

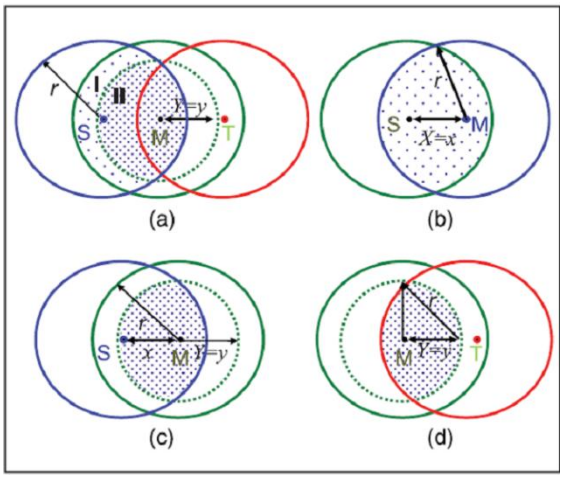

Fig. 2.(*a) The guards of M over S ! M (I and II).*
(b) Separation between S and M ¼ x.
(c) The subset of guards of M over S ! M that has been satisfied by the controlled power transmission of M.
(d) The subset of guards of T over M ! T that wrongly accuses T of dropping the packet.

In the scenario shown in all the guards of Mover S→ M. Fig. 3 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 since more guards can be satisfied and therefore, the stealthier the attack. For this attack to succeed, the attacker must know the location of each neighbor and the detection confidence index ___. Typically, security is not achieved through obfuscate on and therefore, protocol parameters such as are taken to be known to all and location determination is routinely run upon deployment of nodes.

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.

2.3 Drop through Colluding Collision

In many wireless sensor network deployment scenarios, the 802.11 MAC protocol RTS/CTS mechanism that reduces frame collisions due to the hidden terminal problem and the exposed terminal problem is disabled for the sake of energy saving. This is also explained by the fact that packets in some wireless networks such as sensor networks are often quite small and fall below the threshold for packets length for which RTS/CTS is turned on. 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.

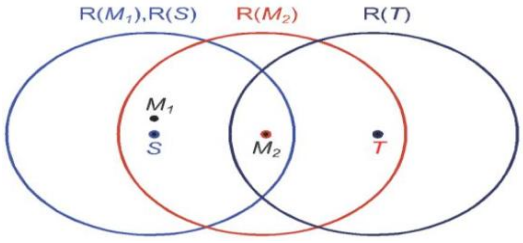

Fig.3. *Drop through colluding collision scenario*

2.4 Drop through Identity Delegation

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 to M2, 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 are all satisfied since these 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.

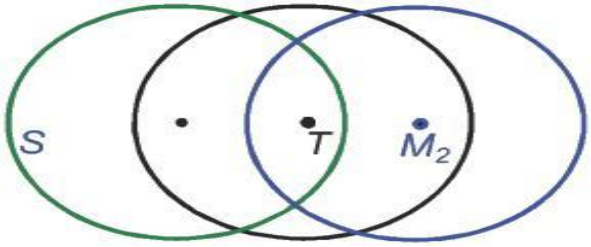

Fig.4. *Drop through identity delegation scenario*

3. EXISTING SYSTEM

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.

Disadvantage

- It leverages the open broadcast nature of wireless communication.
- It cannot detect the stealthy attacks and
- It mistakenly detects and isolates a legitimate node.

4. PROPOSED SYSTEM

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 hop ad hoc wireless networks is unacknowledged or only selectively acknowledged [29], [30], [39]. This is particularly true for the more common data traffic or broadcast control traffic than for rare uncast control traffic. It can be accomplished by two mechanisms.

Mechanism 1:

Neighbors to maintain additional information about
1) Routing path and
2) Add some checking responsibility.

Mechanism 2:

Considerably increase the number of monitoring nodes.

5. RESULTS

Simulation Model and Parameters

We use Network Simulator Version-2 (NS2) [14] to simulate our proposed algorithm. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. We use the distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage. In our simulation, mobile nodes move in a 1000 meter x 1000 meter region for 50 seconds simulation time. We have varied the node speed as 5,10,15,20 and 25m/s. The transmission range is 250 meters. The simulated traffic is Constant Bit Rate (CBR).The numbers of attackers are varied as 1,2,3,4 and 5.

A) Screenshots for Misrouting Attack

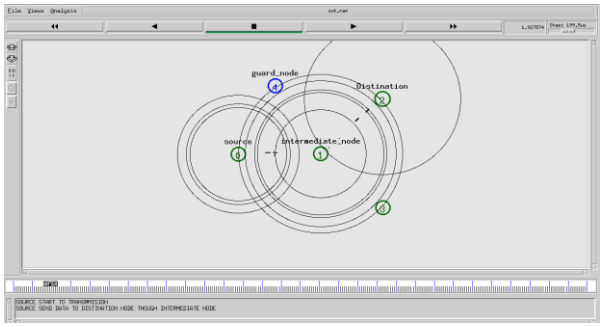

Fig.5.*Source node sends a packet to destination node through intermediate node*

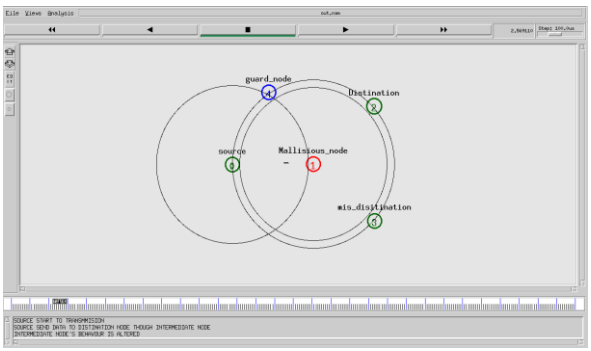

Fig.6.*Intermediate node become malicious node due to misrouting attack*

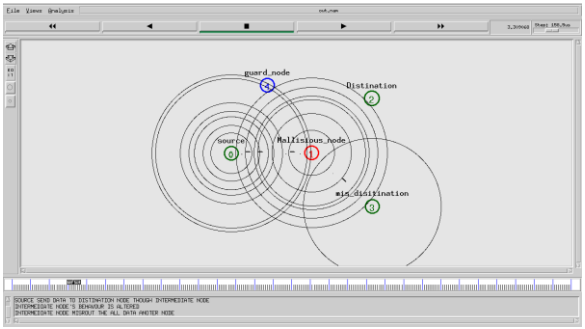

Fig.7.*Due to misbehavior of an intermediate node, it sends a packet to wrong destination.*

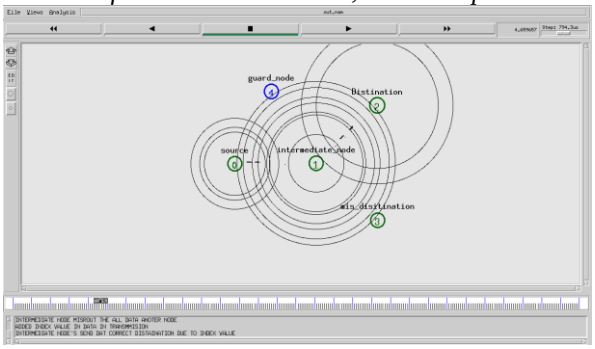

Fig.8. *After mitigating the misrouting attack, intermediate node sends a packet to correct destination*

B) Screenshots for Power Control Attack

Fig.9. *Source node sends a packet to destination node through intermediate node.*

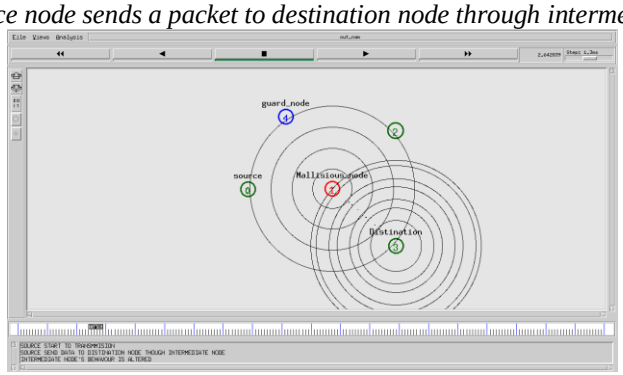

Fig.10. *Due to power control attack, intermediate node becomes malicious node.*

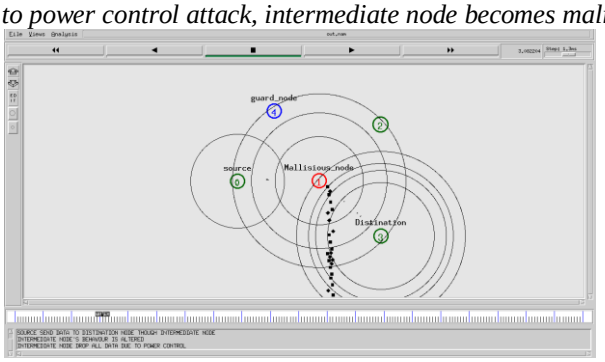

Fig.11. *Packets will be dropped without reaching the destination because of power control attack*

Fig.12. *After mitigating the power control attack, intermediate node sends a packet to destination*

C) Screenshots for Colluding Collision Attack

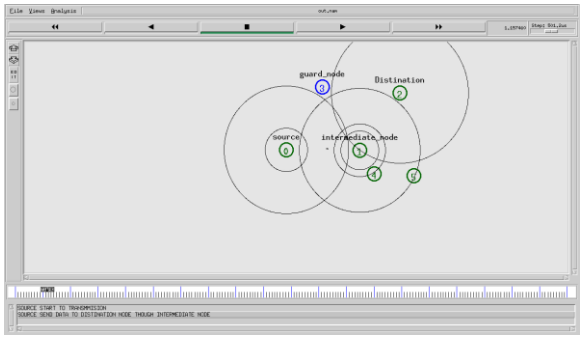

Fig.13. *Source node sends a packet to destination node through intermediate node*

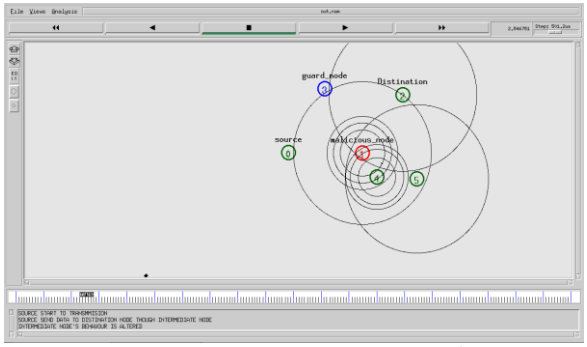

Fig.14.Intermediate node become malicious node because of colluding collision attack

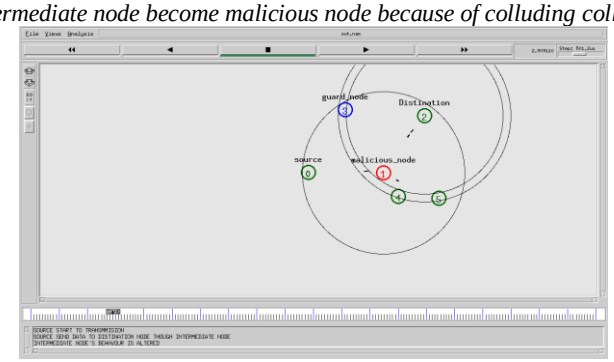

Fig.15 *.Node 5 also sends a packet to intermediate node, due to this collision will occur*

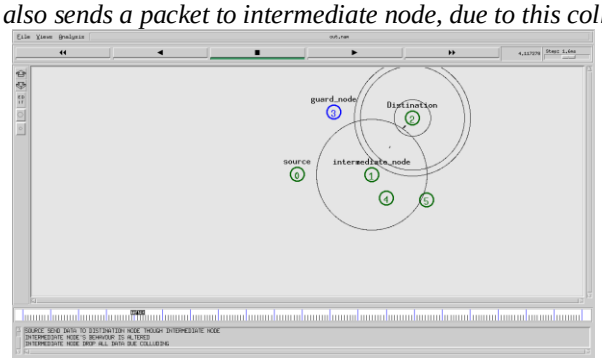

Fig.16.After mitigating colluding collision attack, intermediate node sends a packet to correct destination.

D) Screenshots for Identity Delegation Attack

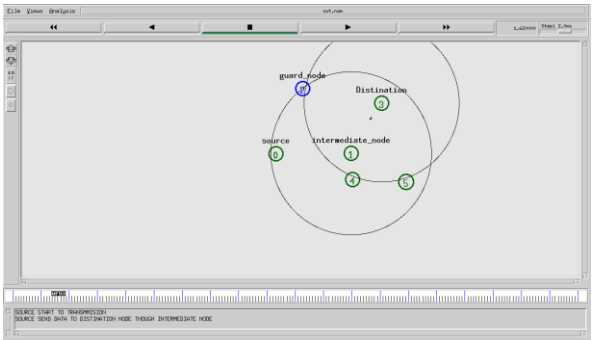

Fig.17. *Source sends a packet to destination node through intermediate node*

Fig.18. *Intermediate node uses the identity of after mitigating identity delegation attack, intermediate sends a packet to correct destination*

6. CONCLUSION AND FUTURE WORK

A new class of attacks called stealthy packet dropping which disrupts a packet from reaching the destination by malicious behavior at an intermediate node. This can be achieved through misrouting, controlling transmission power, malicious jamming at an opportune time, or identity sharing among malicious nodes. However, the malicious behavior cannot be detected by any behavior based detection scheme presented to date. Specifically, showed that BLM-based detection cannot detect these attacks. Additionally, it will cause a legitimate node to be accused. It is then presented by a protocol called SADEC that successfully mitigates all the presented attacks. 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. Showed through analysis and simulation that BLM fails to mitigate most of the presented attacks while SADEC successfully mitigates them. The improvement is seen in terms of increase in the probability of isolation of malicious nodes and decrease in the probability of isolation of legitimate nodes.

In future work, considering the two attacks

i) Colluding Collision

ii) Identity delegation are going to be mitigated by using the NS2 simulator. These attacks mitigation techniques are proposed in project.

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] C. Basile, Z. Kalbarczyk, and R.K. Iyer, "Neutralization of Errors and Attacks in Wireless Ad Hoc Networks," Proc. Int'l Conf. Dependable Systems and Networks (DSN '05), pp. 518-527, 2005.

[12] B. Carbunar, I. Ioannidis, and C. Nita-Rotaru, "JANUS: Towards Robust and Malicious Resilient Routing in Hybrid Wireless Networks," Proc. ACM Workshop Wireless Security (WiSe '04), pp. 11-20, 2004.

[13] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An On-Demand Secure Byzantine Resilient Routing Protocol for Wireless Ad Hoc Networks," ACM Trans. Information and System Security, vol. 10, no. 4, 2008.

[14] "Statistical Wormhole Detection in Sensor Networks," Lecture Notes in Computer Science, R. Molva, G. Tsudik, and D. Westhoff, eds., pp. 128-141, 2005.

[15] D. Liu and P. Ning, "Establishing Pair-Wise Keys in Distributed Sensor Networks," Proc. ACM Conf. Computer and Comm. Security (CCS '03), pp. 52-61, 2003