ISSN 1746-7659, England, UK
Journal of Information and Computing Science
Vol. 7, No. 4, 2012, *pp*. 296-302

Trust Based Selective Forwarding Attacks using Channel Aware Approach in Wireless Mesh Networks

Anand Nayyar

[1] Department of Computer Applications & IT

KCL Institute of Management and Technology, Jalandhar, Punjab, India

(*Received July10, 2012, accepted September 28, 2012*)

Abstract. This Research Paper introduces a channel aware detection (CAD) algorithm that can effectively identify the selective forwarding misbehavior from the normal channel losses. It is a special case of denial of service (DoS) attack in wireless mesh networks (WMNs) known as selective forwarding attack .The CAD algorithm is based on two strategies. With such an attack, a misbehaving mesh router just forwards a subset of packets it receives but drops the others. Channel estimation is the procedure to estimate the normal loss rate due to bad channel quality or medium access collision. Traffic monitoring is to monitor the actual loss rate, if the monitored loss rate at certain hops exceeds the estimated loss rate, those nodes involved will be identified as attackers. To determine the optimal detection thresholds that minimizes the summation of false alarm and missed detection probabilities. In this work the system is free from collision or jamming attacks, when an attacker introduces noise to simulate a noisy channel, it indeed affects the sensing process which in turn leads to inaccurate threshold. This project uses CAD approach to demonstrate the efficiency of discriminating selective forwarding attacks from normal channel losses through extensive computer simulations.

Keywords: Wireless Mesh Network, Selective forwarding attack, Gray Hole Attack, Channel Aware Detection, Optimal Detection threshold.

1. Introduction

Wireless Mesh Network (WMN) is a communications made up of radio nodes organized in a mesh topology. Wireless mesh networks often consist of mesh clients, mesh routers and gateways. The mesh clients are often laptops, cell phones and other wireless devices while the mesh routers forward traffic to and from the gateways which may but need not connect to the Internet. The coverage area of the radio nodes working as a single network is sometimes called a mesh cloud. Access to this mesh cloud is dependent on the radio nodes working in harmony with each other to create a radio network. A mesh network is reliable and offers redundancy. When one node can no longer operate, the rest of the nodes can still communicate with each other, directly or through one or more intermediatenodes. Wireless mesh networks can be implemented with various wireless technology including 802.11, 802.16, cellular technologies or combinations of more than one type. A wireless mesh network can be seen as a special type of wireless ad-hoc network. It is often assumed that all nodes in a wireless mesh network are immobile but this need not be so. The mesh routers may be highly mobile. Often the mesh routers are not limited in terms of resources compared to other nodes in the network and thus can be exploited to perform more resource intensive functions. In this way, the wireless mesh network differs from an ad-hoc network since all of these nodes are often constrained by resources.

1.1 Architecture of Wireless Mesh Network

Wireless mesh architecture is a first step towards providing high-bandwidth network over a specific coverage area. Wireless mesh architectures infrastructure is, in effect, a router network minus the cabling between nodes. It's built of peer radio devices that don't have to be cabled to a wired port like traditional WLAN access points (AP) do. Mesh architecture sustains signal strength by breaking long distances into a series of shorter hops. Intermediate nodes not only boost the signal, but cooperatively make forwarding

decisions based on their knowledge of the network, i.e. perform routing. Such architecture may with careful design provide high bandwidth, spectral efficiency, and economic advantage over the coverage area.

Example of three types of wireless mesh network:

- Infrastructure wireless mesh networks: Mesh routers form an infrastructure for clients.
- Client wireless mesh networks: Client nodes constitute the actual network to perform routing and configuration functionalities.
- Hybrid wireless mesh networks: Mesh clients can perform mesh functions with other mesh clients as well as accessing the network.

Wireless mesh networks have a relatively stable topology except for the occasional failure of nodes or addition of new nodes. The traffic, being aggregated from a large number of end users, changes infrequently. Practically all the traffic in an infrastructure mesh network is either forwarded to or from a gateway, while in ad hoc networks or client mesh networks the traffic flows between arbitrary pairs of nodes.

1.2 Management

This type of infrastructure can be decentralized (with no central server) or centrally managed (with a central server) both are relatively inexpensive, and very reliable and resilient, as each node needs only transmit as far as the next node. Nodes act as routers to transmit data from nearby nodes to peers that are too far away to reach in a single hop, resulting in a network that can span larger distances. The topology of a mesh network is also more reliable, as each node is connected to several other nodes. If one node drops out of the network, due to hardware failure or any other reason, its neighbors can find another route using a routing protocol.

1.3 Applications

Mesh networks may involve either fixed or mobile devices. The solutions are as diverse as communication needs, for example in difficult environments such as emergency situations, tunnels and oil rigs to battlefield surveillance and high speed mobile video applications on board public transport or real time racing car telemetry. A significant application for wireless mesh networks is VoIP. By using a Quality of Service scheme, the wireless mesh may support local telephone calls to be routed through the mesh. For example, miner safety has improved with VOIP phones communicating over a mesh network.

1.4 Multi-Radio Mesh

Multi-radio mesh refers to a unique pair of dedicated radios on each end of the link. This means there is a unique frequency used for each wireless hop and thus a dedicated CSMA collision domain. This is a true mesh link where achieve maximum performance without bandwidth degradation in the mesh and without adding latency. Thus voice and video applications work just as they would on a wired Ethernet network. In true 802.11 networks, there is no concept of a mesh. There are only Access Points (AP's) and Stations. So a Multi-radio wireless mesh node will dedicate one of the radios to act as a station, and connect to a neighbor node AP radio. Single and dual-radio mesh use proprietary means to repeat the signal which means that more than two nodes are in the same collision domain and frequency.

2. Related Work

Y. L. Sun et al [13] have proposed the performance of distributed networks depends on collaboration among distributed entities. To enhance security in distributed networks, such as ad hoc networks, it is important to evaluate the trustworthiness of participating entities since trust is the major driving force for collaboration. We present a framework to quantitatively measure trust model trust propagation, and defend trust evaluation systems against malicious attacks. In particular, we address the fundamental understanding of trust, quantitative trust metrics, mathematical properties of trust, dynamic properties of trust, and trust models. The attacks against trust evaluation are identified and defense techniques are developed. The proposed trust evaluation system is employed in ad hoc networks for securing ad hoc routing and assisting malicious node detection

There are three primary aspects associated with evaluating trust in distributed networks.

- The ability to evaluate trust offers an incentive for good behavior. Creating an expectation that entities will "remember" one's behavior will cause network participants to act more responsibly.
- Trust evaluation provides a prediction of one's future behavior. This predication can assist in decision-making. It provides a means for good entities to avoid working with less trustworthy parties. Malicious users, whose behavior has caused them to be recognized as having low trustworthiness, will have less ability to interfere with network operations.
- Trust definition although definitions and classifications of trust have been borrowed from the social science literature there is no clear consensus on the definition of trust in computer networks. Trust has been interpreted as reputation, Trusting opinion, probability etc.
- Trust metrics trust has been evaluated in very different ways. Some schemes employ linguistic descriptions of trust relationship, such as in PGP quantitative trust models many trust models have been developed to model trust transit through third parties. For example, the simplest method is to sum the number of positive ratings and negative ratings separately and keep a total score as the positive score minus the negative score.

K. Sanzgiri et al [15] have proposed the initial work in ad hoc routing has considered only the problem of providing efficient mechanisms for finding paths in very dynamic networks, without considering security. Because of this there are a number of attacks that can be used to manipulate the routing in an ad hoc network. We describe these threats, specifically showing their effects on AODV and DSR. Our protocol, named Authenticated Routing for Ad hoc Networks (ARAN), uses public-key cryptographic mechanisms to defeat all identified attacks. We detail how ARAN can secure routing in environments where nodes are authorized to participate but untrusted to cooperate, as well as environments where participants do not need to be authorized to participate. Through both simulation and experimentation with our publicly-available implementation ARAN consists of a preliminary certification process followed by a route instantiation process that guarantees end-to-end authentication. The protocol is simple compared to most non-secured ad hoc routing protocols, and does not include routing optimizations present in the latter. It should be noted that these optimizations are the chief cause of most exploits listed. Route discovery in ARAN is accomplished by a broadcast route discovery message from a source node that is replied to by the destination node.
The routing messages are authenticated end-to-end and only authorized nodes participate at each hop between source and destination.

Khalil et al [9] have proposed the multihop wireless systems, such as ad-hoc and sensor networks, the need for cooperation among nodes to relay each other's packets exposes them to a wide range of security attacks. A particularly devastating attack is known as the wormhole attack, where a malicious node records control and data traffic at one location and tunnels it to a colluding node far away, which replays it locally. This can either disrupt route establishment or make routes pass through the malicious nodes. In this paper, we present a lightweight countermeasure for the wormhole attack, called LITEWORP, which relies on overhearing neighbor resource-constrained multihop wireless networks, such as sensor networks.

D. Manikantan Shila et al [6] have proposed the Wireless Mesh Networks (WMNs) have emerged recently as a promising technology for next-generation wireless networking to provide wide variety of applications that cannot be supported directly by other wireless networks. In WMNs, security is turning out to be a major concern and little attention has been paid to this topic by the research community. We investigate a serious security threat known as the selective forwarding attack (gray hole attack). In a selective forwarding attack, a malicious node refuses to forward all or a subset of the packets it receives. Such selective dropping is challenging to defend against. In this paper, we present an algorithm to defend against selective forwarding attacks based on AODV routing protocol.
Counter- Threshold Based and uses the detection threshold and packet counter to identify the attacks and the second phase is Query- Based and uses acknowledgment from the intermediate nodes to localize the attacker. We also present simulation results to illustrate the efficiency of the proposed algorithm. To the best of our knowledge, this is the first paper to present an algorithm for defending selective forwarding attacks in WMN.

B. Xiao et al [5] have proposed the Selective forwarding attacks may corrupt some mission-critical applications such as military surveillance and forest fire monitoring in wireless sensor networks. In such attacks, most of the time malicious nodes behave like normal nodes but will from time to time selectively drop sensitive packets, such as a packet reporting the movement of the opposing forces, and thereby make it harder to detect their malicious nature. We propose CHEMAS (Checkpoint-based Multi-hop Acknowledgement Scheme), a lightweight security scheme for detecting selective forwarding attacks. Our scheme can randomly select part of intermediate nodes along a forwarding path as checkpoint nodes which are responsible for generating acknowledgements for each packet received. The strategy of random-

checkpoint-selection significantly increases the resilience against attacks because it prevents a proportion of the sensor nodes from becoming the targets of attempts to compromise them. In our scheme, each intermediate node in a forwarding path, if it does not receive enough acknowledgements from the downstream checkpoint nodes, has the potential to detect abnormal packet loss and identify suspect nodes. They explore the feasibility of our detection scheme using both theoretical analysis and simulations. The simulation results show that our scheme can achieve a high detection rate, even in harsh radio conditions. The communication overhead incurred by our scheme is also within reasonable bounds. One naive approach is to generate a fixed list of checkpoint nodes before the source node sends out the first event packet. However, this approach is infeasible, because checkpoint nodes are responsible for generating ACK packets, and if the checkpoint nodes are compromised, the adversary may crack the network by fabricating ACK packets and without being detected. Therefore, it is important for intermediate nodes to share the probability of being selected as checkpoint nodes as well as the risk of being compromised. We propose a random-checkpoints-selection algorithm, in which a random list of checkpoint nodes is generated by the source node for each event packet. The source node generates a random number as a seed for each event packet, and this seed determines the members of the checkpoint list.

R. Curtmola et al [7] have proposed the vulnerabilities of on demand multicast routing protocols for multi-hop wireless networks and discuss the challenges encountered in designing mechanisms to defend against them. They proposed BSMR, a novel secure multicast routing protocol that withstands insider attacks from colluding adversaries. Our protocol is a software-based solution and does not require additional or specialized hardware. They present simulation results which demonstrate that BSMR effectively mitigates the identified attacks Our protocol ensures that multicast data is delivered from the source to the members of the multicast group, even in the presence of Byzantine attackers, as long as the group members are reachable through non-adversarial paths and a non-adversarial path exists between a new member and a node in the multicast tree. They used an authentication framework to eliminate outside adversaries and ensure that only authorized nodes perform certain operations (e.g., only tree nodes can perform tree operations and only group nodes can connect to the corresponding multicast tree). BSMR mitigates inside attacks that try to prevent a node from establishing a route to the multicast tree by flooding both route request and route reply, unlike the basic multicast protocol presented .which unicasts the route reply. This ensures that if an adversarial-free route exists, then a route is established. BSMR ensures resilience to selective data forwarding attacks by using a reliability metric that captures adversarial behavior. The metric consists of a list of link weights in which high weights correspond to low reliability. Each node in the network maintains its own weight list and includes it in each route request to ensure that a new route to the tree avoids adversarial links. A link's reliability is determined based on the number of packets successfully delivered on that link over time. Tree nodes monitor the rate of receiving data packets and compare it with the transmission rate indicated by the source in the form of an MRATE message. If the perceived transmission rate falls below the rate indicated in the MRATE message by more than a threshold, an honest node that is a direct descendant of an adversarial node updates its weight list by penalizing the link to its parent and then tries to discover a new route to the tree Without loss of generality, we limit our description to one multicast group. Below we describe the previously mentioned authentication framework, the route discovery, the route activation, multicast tree maintenance and the selective data forwarding detection mechanisms.

3. Existing Model

An attack, a misbehaving mesh router just forwards a subset of packets it receives but drops the others. Selective forwarding attacks focus on attack detection under the assumption of an error-free wireless channel. This paper has proposed a channel aware detection (CAD) algorithm that can effectively identify the selective forwarding misbehavior from the normal channel losses. In existing system CAD algorithm incorporated with AODV routing protocol. A malicious router may be near to the source router. A malicious router does not have to check the routing table when sending false routing information. In existing system they assume that the system is free from collision and jamming attacks.

4. Methodology

4.1. CAD

Channel aware detection (CAD) algorithm that can effectively identify the selective forwarding misbehavior from the normal channel losses. The CAD algorithm is based on two strategies Channel

estimation is to estimate the *normal loss rate* due to bad channel quality or medium access collision. Traffic monitoring. To monitor the *actual loss rate*; if the monitored loss rate at certain hops exceeds the estimated loss rate, those nodes involved will be identified as attackers. Attack detection is based on the combination of downstream and upstream monitoring. The downstream/upstream monitoring opinions are configured by comparing the monitored loss rates with the downstream/upstream detection thresholds. Due to the randomness nature, even without selective forwarding attack, a burst of normal loss events in certain situations may lead to the false alarm. The CAD approach proposed in this paper departs from the previous solutions in three aspects. CAD considers a practical scenario where a packet loss may be due to bad channel quality, medium access collisions, or purposeful packet dropping; and propose a method to discriminate attacks from those normal loss events. CAD utilizes both upstream and downstream traffic monitoring for enhanced performance; the Watchdog approach relies on downstream monitoring alone. While the existing studies have requirements such as directional antennas, clock synchronization, and guard nodes, CAD is a lightweight algorithm for multihop networks.

CAD Methodology

- The channel estimation is integrated with traffic monitoring to achieve channel-aware detection of gray hole attack, which can effectively identifies selective forwarding misbehavior hidden in the normal loss events due to bad channel quality or medium access collisions.
- In CAD, upstream and downstream traffic monitoring are combined to achieve a versatile detection method. In addition to gray hole attack, the CAD can also detect *limited transmit-power* attack, *on-off* attack and *bad mouthing* attack.
- Based on the analytical model, the optimal upstream/downstream detection thresholds can be computed to minimize the summation of false alarm and missed detection probabilities.
- The thresholds are dynamically adjusted with the channel status to maintain the efficiency of CAD under varying network condition
- We always consider a path with trustworthy source and destination nodes. It is also assumed that the communication on every link between the mesh nodes is *bidirectional*.
- Buffer of infinite size, and a packet can be dropped due to bad channel quality, medium access collision, or presence of an attacker

4.2 Design of CAD Algorithm

The essence of CAD is to identify intentional selective dropping from normal channel losses. A normal packet loss can occur due to bad channel quality or medium access collision under the infinite buffer assumption. In CAD, each mesh node maintains a history of packet count to measure the link loss rate. When a node receives a packet from the upstream, it updates the packet count history with the corresponding packet sequence number. The CAD design requires the destination node to send a PROBE ACK message for every PROBE packet received from the source node. The PROBE ACK message is also secured with digital signature, similar to a PROBE message

- Negative PROBE ACK.
- Positive PROBE ACK
- PROBE ACK Timeout
- On receiving the PROBE, each node in the path marks the PROBE packet with its traffic monitoring information Parameters PROBE packet and PROBE ACK packet for the detection of malicious routers
- Normal loss rate due to channel quality or medium access collision.
- The *channel busyness ratio* is defined as the proportion of time that the channel is in the status of successful transmission or collision

4.3 CAD algorithm at Source Node S

Step 1: Divides the data packets to be sent in **k** equal parts. **DATA [1,….,K];** Initialize **i = 1;**

Comment: Chose channel window size **w**, If total no of data packets **n** then **k = CAD (n/w)**

Step 2: Send ***preface(S,D,ni)*** message to the destination node **D.** Where **ni** is the no of data packets to be sent in current block.

Step 3: Broadcast ***monitor (S, D, NNR)*** message to all its neighbors. Instructing neighbors to monitor next node in the route (PATH).

Step 4: Starts transmitting data packets from the block **Data[i]** to **D.**

Step 5: Sets timeout **TS** for the receipt of the ***preface (D, S, d_count)*** message containing ***d_count***, no of data packets received by D.
Step 6: If **TS** not expired and ***postlude*** message received, if ($ni(1-\mu) \leq d\_count$)
Increment **i** by **1** and go to **Step 8**.
else Start false data removal process. where μ is a threshold value ranges between 0 and 1 indicates the fraction of total packets gets lost due to error prone wireless channel. μ is the permissible packet loss in each node in the route then $\mu = 1-(1-\mu)N$, where N is the total no of nodes in the route (hop count).
Step 7: If **TS** expired and ***preface*** message not received then start removal false process.
Step 8: Continues from **Step 2** when **i** less than equal to **k.**
Step 9: Terminates **S**'s action.

4.4 CAD algorithm at Destination Node D

Step 1 On receiving ***preface (S,D,ni)*** message from **S** extracts **ni** Initialize **d_count = 0.**
Step 2: Sets timeout **TD** for the receipt of the current data sample and waits for the data packets.
Step 3: When **TD** not expired and a data packet received Update **d_count += 1**
Step 4: When **TD** expired send ***postlude(D, S, d_count)*** message to **S.**
Step 5: Terminates **D**'s action.

5. Proposed Model

The channel estimation is integrated with traffic monitoring to achieve channel-aware detection of gray hole attack, which can effectively identifies selective forwarding misbehavior hidden in the normal loss events due to bad channel quality or medium access collisions. In CAD, upstream and downstream traffic monitoring are combined to achieve a versatile detection method. In addition to gray hole attack, the CAD can also detect limited transmit-power attack, on-off attack and bad mouthing attack. Based on the analytical model, the optimal upstream/downstream detection thresholds can be computed to minimize the summation of false alarm and missed detection probabilities. The thresholds are dynamically adjusted with the channel status to maintain the efficiency of CAD under varying network condition. It is considered that a path with trustworthy source and destination nodes, it is also assumed that the communication on every link between the mesh nodes is bidirectional. Buffer of infinite size and a packet can be dropped due to bad channel quality, medium access collision, or presence of an attacker. In proposed system, CAD is integrated with DSR routing protocol. In proposed system, elliptic curve cryptographic techniques will be used to forward data packets.

6. Conclusion and Future Work

In this Research Paper, an effective algorithm to detect and locate the selective forwarding attackers in WMNs has been proposed. The particular challenging scenario considered is that the intentional selective dropping may be interleaved with normal loss events due to wireless channel quality or medium access collisions. The proposed channel aware detection algorithm utilizes the methodologies of channel estimation and upstream/downstream traffic monitoring to discriminate the selective dropping attack from the estimated normal loss rates. It demonstrates how to compute the false alarm and missed detection probabilities for the CAD algorithm, and further derives the optimal detection thresholds to minimize the summation of the false alarm and missed detection probabilities. The presence of normal losses, CAD can detect the attackers efficiently and thereby increase the packet delivery ratio of the network. In this work, the system is free from collision or jamming attacks. When an attacker introduces noise to simulate a noisy channel, it indeed affects the sensing process which in turn leads to inaccurate threshold. Results can be detecting the attackers efficiently and thereby increase the packet delivery ratio of the network. In future, extend CAD algorithm with different routing protocol and encryption techniques to deal with all type of attacks efficiently

7. References

[1] Shila, D.M.; Yu Cheng; Anjali, T.; Mitigating selective forwarding attacks with a channel-aware approach in WMNS, *IEEE Transactions On Wireless Communications*, VOL. 9, NO. 5, May 2010

[2] I. F. Akyildiz and X. Wang, "A survey on wireless mesh networks," *IEEE Commun. Mag.*, vol. 43, no. 9, pp. S23-S30, Sept. 2005.

[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc.International Conference on Mobile Computing and Networking*, Boston, MA, 2000

[4] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Elsevier's AdHoc Networks J.*, vol. 1, no. 2-3, pp. 293-315, Sept. 2003

[5] B. Xiao, B. Yu, and C. Gao, "CHEMAS: identify suspect nodes in selective forwarding attacks," *J. Parallel and Distributed Computing*, vol. 67, no. 11, pp. 1218-1230, Nov. 2007.

[6] D. Manikantan Shila and T. Anjali, "Defending selective forwarding attacks in mesh networks," in *Proc. 2008 Electro/Information Technology Conference* , Ames, IA, May

[7] R. Curtmola and C. Nita-Rotaru, "BSMR: Byzantineresilient secure multicast routing in multi-hop wireless networks," in *Proc. Sensor, Mesh and Ad Hoc Communications and Networks*, June 2007.

[8] A. Perrig, R. Canetti, D. Tygar, and D Song, "The TESLA Broadcast Authentication Protocol," in *RSA CryptoBytes*, Summer 2002.

[9] I. Khalil, S. Bagchi, and N. B. Shroff, "LiteWorp: detection and isolation of the wormhole attack in static multihop wireless networks," *Computer Networks: The International J. Computer and Telecommun. Networking* , vol. 51, no. 13, pp. 3750-3772, Sept. 2007

[10] M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *Proc. ACM Workshop on Wireless Security (WiSe 2002)*, Sept. 2002.

[11] Y. Hu, D. B. Johnson, and A. Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks," *Ad Hoc Networks*, vol. 1, no. 1, pp. 175-192, July 2003.

[12] Y. Sun, W. Yu, Z. Han, and K. J. R. Liu, "Trust modeling and evaluation in ad hoc networks," in *Proc. IEEE GLOBECOM '05*, vol. 3, Dec. 2005. [12] L. F. Perrone and S. C. Nelson, "A study of on-off attack models for wireless ad hoc networks," *Operator-Assisted (Wireless Mesh) CommunityNetworks*, pp. 1-10, Sept. 2006.

[13] Y. L. Sun, Z. Han, W. Yu, and K. J. R. Liu, "A trust evaluation framework in distributed networks: vulnerability analysis and defense against attacks," in *Proc. INFOCOM, 2006*, pp. 1-13, Apr. 2006.

[14] Y. L. Sun, Z. Han, W. Yu, and K. J. R. Liu, "Attacks on trust evaluation in distributed networks," in *Proc. 40th Annual Conference on Information Sciences and Systems 2006*, no. 22-24, pp. 1461-1466, Mar. 2006.

[15] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "Authenticated routing for ad hoc networks," *IEEE J Sel. Areas Commun.*, vol. 23, no. 3, pp. 598-610, Mar. 2007.

[16] Y. Hu, D. B. Johnson, and A. Perrig, "Ariadne: a secure on-demand routing protocol for ad hoc networks," in *Proc. Mobicom'02*, pp. 12-23, 2002.

[17] Y. Hu, D. B. Johnson, and A. Perrig, "Rushing attacks and defense in wireless ad hoc network routing protocols," in *Proc. ACM Workshop on Wireless Security (WiSe)*, pp. 30-40, 2003.

[18] Y. Hu, D. B. Johnson, and A. Perrig, "Packet leashes: a defense against wormhole attacks in wireless networks," in *Proc. IEEE INFOCOM 2003*, vol. 3, pp. 1976-1986, Mar. 2003.

[19] M. E. M. Campista, D. G. Passos, P. M. Esposito, I. M. Moraes, C. V. N. de Albuquerque, D. C. M. Saade, M. G. Rubinstein, L. H. M. K. Costa, and O. C. M. B. Duarte, "Routing metrics and protocols for wireless mesh networks," *IEEE Network*, vol. 22, no. 1, pp. 612, Jan. 2008.

[20] W. Yu, Z. Ji, and K. J. R. Liu, "Securing cooperative adhoc networks under noise and imperfect monitoring: strategies and game theoretic analysis," *IEEE Trans. Inf. Forensics and Security*, vol. 2, no. 2, pp. 240-253, June 2007.

[21] S. Tanachaiwiwat, P. Dave, R. Bhindwale, and A. Helmy, "Location centric isolation of misbehavior and trust routing in energy-constrained sensor networks," in *Proc. IEEE IPCCC*, pp. 463-469, 2004.

[22] S. Buchegger and J. Y. Le Boudee, "Self-policing mobile ad hoc networks by reputation systems," *IEEE Commun. Mag.*, vol. 43, no. 7, pp. 101-107, July 2005.

[23] J. Newsome, E. Shi, D. Song, and A. Perrig, "Sybil attack in sensor networks: analysis and defenses," in *Proc. IPSN '04*, New York, pp. 259-268, 2004.

[24] C. Piro, C. Shields, and B. N. Levine, "Detecting the sybil attacks in mobile ad hoc networks," in *Proc. SecureComm*, 2006.

[25] B. Parno, A. Perrig, and V. D. Gligor, "Distributed detection of node replication attacks in sensor networks," in*Proc. IEEE Symposium on Security and Privacy*, 2004, pp. 49- 63