ISSN:2231-0711

Avinash Gundlapally et al | IJCSET |August 2013 | Vol 3, Issue 8, 291-296

A Study on Secure Routing in Wireless Sensor Networks

Avinash Gundlapally,Dr Syed Umar

Department of ECM,
KL University, A.P. INDIA.

***Abstract*— We consider routing security in wireless sensor networks. Many sensor network routing protocols have been proposed, but none of them have been designed with security as a goal. We propose security goals for routing in sensor networks, show how attacks against ad-hoc and peer-to-peer networks can be adapted into powerful attacks against sensor networks, introduce two classes of novel attacks against sensor networks — sinkholes and HELLO floods, and analyze the security of all the major sensor network routing protocols. We describe crippling attacks against all of them and suggest countermeasures and design considerations. This is the first such analysis of secure routing in sensor networks.**

***Keywords*—Spoofing, filtering, defense, wireless.**

I. INTRODUCTION

Our focus is on routing security in wireless sensor networks.Current proposals for routing protocols in sensor networksoptimize for the limited capabilities of the nodes and theapplication specific nature of the networks, but do not considersecurity. Although these protocols have not been designed withsecurity as a goal, we feel it is important to analyze theirsecurity properties. When the defender has the liabilities ofinsecure wireless communication, limited node capabilities,and possible insider threats, and the adversaries can use powerfullaptops with high energy and long range communicationto attack the network, designing a secure routing protocol isnon-trivial.

We present crippling attacks against all the major routingprotocols for sensor networks. Because these protocols havenot been designed with security as a goal, it is unsurprisingthey are all insecure. However, this is non-trivial to fix: itis unlikely a sensor network routing protocol can be madesecure by incorporating security mechanisms after designhas completed. Our assertion is that sensor network routingprotocols must be designed with security in mind, and thisis the only effective solution for secure routing in sensornetworks.

We make five main contributions.

- We propose threat models and security goals for securerouting in wireless sensor networks.
- We introduce two novel classes of previously undocumented attacks against sensor networks1 sinkhole attacks and HELLO floods.
- We show, for the first time, how attacks against ad-hocwireless networks and peer-to-peer networks.These attacks are relevant to some ad-hoc wireless networks as well.be adapted into powerful attacks against sensor networks.
- We present the first detailed security analysis of all themajor routing protocols and energy conserving topologymaintenance algorithms for sensor networks.
- We describepractical attacks against all of them that would defeat anyreasonable security goals.
- We discuss countermeasures and design considerationsfor secure routing protocols in sensor networks.

II. BACKGROUND

We use the term *sensor network* to refer to a heterogeneoussystem combining tiny sensors and actuators with generalpurposecomputing elements. Sensor networks may consist ofhundreds or thousands of low-power, low-cost nodes, possiblymobile but more likely at fixed locations, deployed en masseto monitor and affect the environment. For the remainder ofthis paper we assume that all nodes' locations are fixed forthe duration of their lifetime.For concreteness, we target the Berkeley TinyOS sensorplatform in our work. Because this environment is so radicallydifferent from any we had previously encountered, we feel itis instructive to give some background on the capabilities ofthe Berkeley TinyOS platform.A representative example is the Mica *mote*2, a small (severalcubic inch) sensor/actuator unit with a CPU, power source,radio, and several optional sensing elements. The processoris a 4 MHz 8-bit Atmel ATMEGA103 CPU with 128 KBof instruction memory, 4 KB of RAM for data, and 512 KBof flash memory. The CPU consumes 5.5 mA (at 3 volts)when active, and two orders of magnitude less power whensleeping. The radio is a 916 MHz low-power radio from RFM,delivering up to 40 Kbps bandwidth on a single shared channeland with a range of up to a few dozen meters or so. TheRFM radio consumes 4.8 mA (at 3 volts) in receive mode,up to 12 mA in transmit mode, and 5µ A in sleep mode. Anoptional sensor board allows mounting of a temperature sensor,magnetometer, accelerometer, microphone, sounder, and othersensing elements. The whole device is powered by two AAbatteries, which provide approximately 2850 mA hours at 3volts.

Sensor networks often have one or more points of centralizedcontrol called *base stations*. A base station is typicallya gateway to another network, a powerful data processing orstorage center, or an access point for human interface. Theycan be used as a nexus to disseminate control information intothe network or extract data from it. In some previous work onsensor network routing protocols, base stations have also beenreferred to as *sinks*.

Base stations are typically many orders of magnitude morepowerful than sensor nodes. They might have workstation orlaptop class processors, memory, and storage, AC power, and high bandwidth links for communication amongst themselves.

However, sensors are constrained to use lower-power, lowerbandwidth,shorter-range radios, and so it is envisioned thatthe sensor nodes would form a multi-hop wireless network toallow sensors to communicate to the nearest base station. SeeFigure 2 for a picture illustrating a representative architecture for sensor networks.A base station might request a steady stream of data, suchas a sensor reading every second, from nodes able to satisfya query. We refer to such a stream as a *data flow* and to thenodes sending the data as *sources*.

In order to reduce the total number of messages sent and thus save energy, sensor readings from multiple nodes may be processed at one of many possible *aggregation points*. An aggregation point collects sensor readings from surrounding nodes and forwards a single message representing an aggregate of the values. Aggregation points are typically regular sensor nodes, and their selection is not necessarily static. Aggregation points could be chosen dynamically for each query or event, for example. It is also possible that every node in the network functions as an aggregation point, delaying transmission of an outgoing message until a sufficient number of incoming messages have been received and aggregated. Power management in sensor networks is critical. At full power, the Berkeley Mica mote can run for only two weeks or so before exhausting its batteries. Consequently, if we want sensor networks to last for years, it is crucial that they run at around a 1% duty cycle (or less). Similarly, since the power consumption of the radio is three orders of magnitude higher when transmitting or listening than when in sleep mode, it is crucial to keep the radio in sleep mode the overwhelming majority of the time. It is clear that we must discard many preconceptions about network security: sensor networks differ from other distributed systems in important ways. The resource-starved nature of sensor networks poses great challenges for security. These devices have very little computational power: public-key cryptography is so expensive as to be unusable, and even fast symmetric-key ciphers must be used sparingly. With only 4 KB of RAM, memory is a resource that must be husbanded carefully, so our security protocols cannot maintain much state Also, communication bandwidth is extremely dear: each bit transmitted consumes about as much power as executing 800–1000 instructions [3], and as a consequence, any message expansion caused by security mechanisms comes at significant cost. Power is the scarcest resource of all: each milliamp consumed is one milliamp closer to death, and as a result, nearly every aspect of sensor networks must be designed with power in mind.

This leaves us with a very demanding environment. How can security possibly be provided under such tight constraints? Yet security is critical. With sensor networks being envisioned for use in critical applications such as building monitoring, burglar alarms, and emergency response, with the attendant lack of physical security for hundreds of exposed devices, and with the use of wireless links for communications, these networks are at risk.

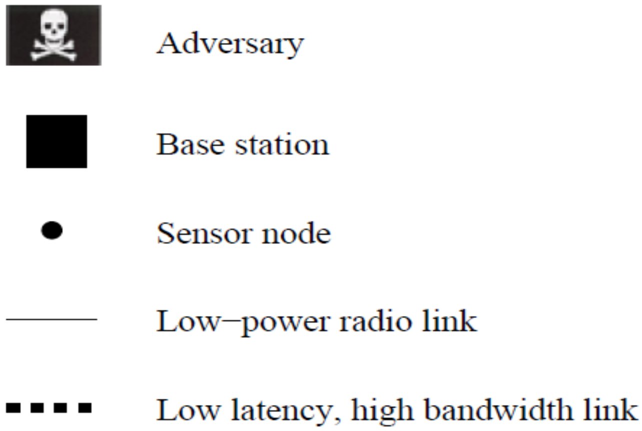

Fig.1. **Sensor network legend.**All nodes may use low power radio links,but only laptop-class adversaries and base stations can use low latency, highbandwidth links.

III SENSOR NETWORKS VS. AD-HOC WIRELESS NETWORKS

Wireless sensor networks share similarities with ad-hoc wireless networks. The dominant communication method in both is multi-hop networking, but several important distinctions can be drawn between the two. Ad-hoc networks typically support routing between any pair of nodes [4], [5], [6], [7], whereas sensor networks have a more specialized communication pattern. Most traffic in sensor networks can be classified into one of three categories:

1) Many-to-one: Multiple sensor nodes send sensor readings to a base station or aggregation point in the network.
2) One-to-many: A single node (typically a base station) multicasts or floods a query or control information to several sensor nodes.
3) Local communication: Neighboring nodes send localized messages to discover and coordinate with each other. A node may broadcast messages intended to be received by all neighboring nodes or unicast messages intended for a only single neighbor[3].

Nodes in ad-hoc networks have generally been considered to have limited resources, but as we have seen in Section II, sensor nodes are even more constrained. Of all of the resource constraints, limited energy is the most pressing. After deployment, many sensor networks are designed to be unattended for long periods and battery recharging or replacement may be infeasible or impossible. Nodes in sensor networks often exhibit trust relationships beyond those that are typically found in ad-hoc networks. Neighboring nodes in sensor networks often witness the same or correlated environmental events. If each node sends a packet to the base station in response, precious energy and bandwidth are wasted. To prune these redundant messages to reduce traffic and save energy, sensor networks require in-network processing, aggregation, and duplicate elimination. This often necessitates trust relationships between nodes that are not typically assumed in ad-hoc networks.

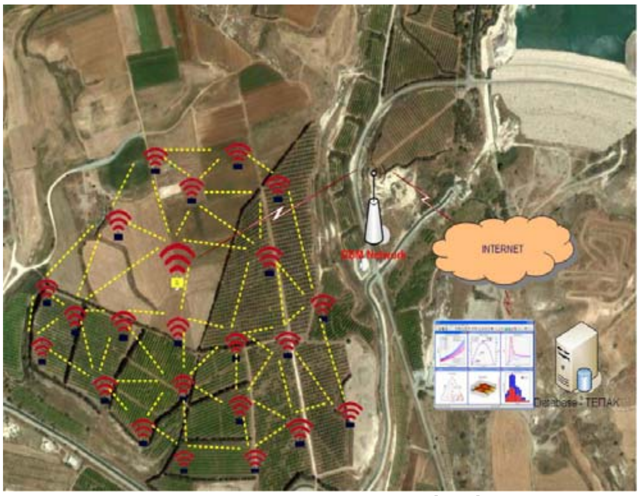

Fig. 2.A representative sensor network architecture.

IV Attacks On Sensor Network Routing

Many sensor network routing protocols are quite simple, andfor this reason are sometimes even more susceptible to attacks against general ad-hoc routing protocols. Most network layerattacks against sensor networks fall into one of the followingcategories:

- Spoofed, altered, or replayed routing information.
- Selective forwarding.
- Sinkhole attacks.
- Sybil attacks
- Wormholes
- HELLO flood attacks
- Acknowledgement spoofing

In the descriptions below, note the difference between attacksthat try to manipulate user data directly and attacks that try toaffect the underlying routing topology.We start with some general discussion of these types ofattacks; in Section V, we show how these attacks maybe applied to compromise routing protocols that have beenproposed in the literature.

*A. **Spoofed, altered, or replayed routing information***

The most direct attack against a routing protocol is to targetthe routing information exchanged between nodes. By spoofing,altering, or replaying routing information, adversaries maybe able to create routing loops, attract or repel network traffic,extend or shorten source routes, generate false error messages,partition the network, increase end-to-end latency, etc.

*B. **Selective forwarding***

Multi-hop networks are often based on the assumption thatparticipating nodes will faithfully forward received messages.

In a selective forwarding attack, malicious nodes may refuseto forward certain messages and simply drop them, ensuringthat they are not propagated any further. A simple form ofthis attack is when a malicious node behaves like a black holeand refuses to forward every packet she sees. However, suchan attacker runs the risk that neighboring nodes will concludethat she has failed and decides to seek another route. A moresubtle form of this attack is when an adversary selectivelyforwards packets.

*C. **Sinkhole attacks***

In a sinkhole attack, the adversary's goal is to lure nearlyall the traffic from a particular area through a compromisednode, creating a metaphorical sinkhole with the adversary atthe center. Because nodes on, or near, the path that packetsfollow have many opportunities to tamper with applicationdata, sinkhole attacks can enable many other attacks (selectiveforwarding, for example).Sinkhole attacks typically work by making a compromisednode look especially attractive to surrounding nodes withrespect to the routing algorithm. For instance, an adversarycould spoof or replay an advertisement for an extremely highquality route to a base station. Some protocols might actuallytry to verify the quality of route with end-to-end acknowledgementscontaining reliability or latency information. One motivation for mounting a sinkhole attack is that itmakes selective forwarding trivial. By ensuring that all trafficin the targeted area flows through a compromised node, an adversarycan selectively suppress or modify packets originatingfrom any node in the area.It should be noted that the reason sensor networks areparticularly susceptible to sinkhole attacks is due to theirspecialized communication pattern. Since all packets share the same ultimate destination (in networks with only one basestation), a compromised node needs only to provide a singlehigh quality route to the base station in order to influence apotentially large number of nodes.

*D. **The Sybil attack***

In a Sybil attack [2], a single node presents multipleidentities to other nodes in the network. The Sybil attack cansignificantly reduce the effectiveness of fault-tolerant schemes such as distributed storage [24], disparity [25] and multipath [26] routing, and topology maintenance [27], [28]. Replicas, storage partitions, or routes believed to be using disjoint nodes could in actuality be using a single adversary presenting multiple identities. Sybil attacks also pose a significant threat to geographic routing protocols. Location aware routing often requires nodes to exchange coordinate information with their neighbors to efficiently route geographically addressed packets. It is only reasonable to expect a node to accept but a single set of coordinates from each of its neighbors, but by using the Sybil attack an adversary can "be in more than one place at once".

*E. **Wormholes***

In the wormhole attack [1], an adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part5. The simplest instance of this attack is a single node situated between two other nodes forwarding messages between the two of them. However, wormhole attacks more commonly involve two distant malicious nodes colluding to understate their distance from each other by relaying packets along an out-of-bound channel available only to the attacker Figure 5 shows an example of a wormhole being used to create a sinkhole. Wormholes can also be used simply to convince two distant nodes that they are neighbors by relaying packets between the two of them. Wormhole attacks would likely be used in combination with selective forwarding or eavesdropping. Detection is potentially difficult when used in conjunction with the Sybil attack.

F. **HELLO** ***flood attack***

We introduce a novel attack against sensor networks: the HELLO flood. Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within (normal) radio range of the sender. This assumption may be false: a laptop-class attacker broadcasting routing or other information with large enough transmission power couldconvince every node in the network that the adversary is itsneighbor.

An adversary does not necessarily need to be able toconstruct legitimate traffic in order to use the HELLO floodattack. She can simply re-broadcast overhead packets withenough power to be received by every node in the network.HELLO floods can also be thought of as one-way, broadcastwormholes.

Note: "Flooding" is usually used to denote the epidemiclikepropagation of a message to every node in the networkover a multi-hop topology. In contrast, despite its name, theHELLO flood attack uses a single hop broadcast to transmit amessage to a large number of receivers.

G. ***Acknowledgement spoofing***

Several sensor network routing algorithms rely on implicitor explicit link layer acknowledgements. Due to the inherentbroadcast medium, an adversary can spoof link layer acknowledgmentsfor "overheard" packets addressed to neighboringnodes. Goals include convincing the sender that a weak link isstrong or that a dead or disabled node is alive. For example, arouting protocol may select the next hop in a path using linkreliability. Artificially reinforcing a weak or dead link is asubtle way of manipulating such a scheme. Since packets sentalong weak or dead links are lost, an adversary can effectivelymount a selective forwarding attack using acknowledgementspoofing by encouraging the target node to transmit packetson those links.

V ATTACKS ON SPECIFIC SENSOR NETWORK PROTOCOLS

All of the proposed sensor network routing protocols are highly susceptible to attack. Adversaries can attract or repel traffic flows, increase latency, or disable the entire network with sometimes as little effort as sending a single packet. In this section, we survey the proposed sensor network routing protocols and highlight the relevant attacks.

A. ***TinyOS beaconing***

The TinyOS beaconing protocol constructs a breadth first spanning tree rooted at a base station. Periodically the base station broadcasts a route update. All nodes receiving the update mark the base station as its parent and rebroadcast the update. The algorithm continues recursively with each node marking its parent as the first node from which it hears a routing update during the current *time epoch*. All packets received or generated by a node are forwarded to its parent (until they reach the base station).

Attacks: The TinyOS beaconing protocol is highly susceptible to attack. Since routing updates are not authenticated, it is possible for any node to claim to be a base station and become the destination of all traffic in the network (see Figure 5).

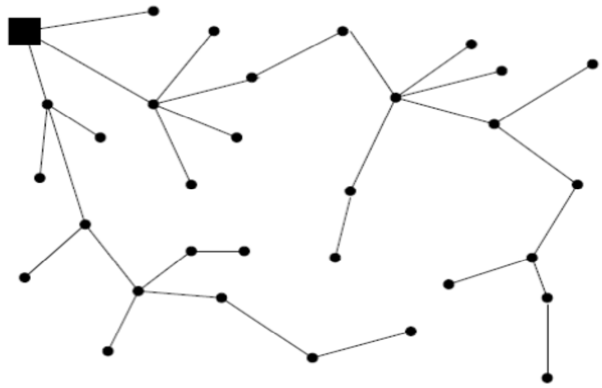

Fig.3. A representative topology constructed using TinyOS beaconing with a single base station.

Authenticated routing updates will prevent an adversary from claiming to be a base station, but a powerful laptop class adversary can still easily wreak havoc. An adversary interested in eavesdropping on, modifying, or suppressing packets in a particular area can do so by mounting a combined wormhole/sinkhole attack.

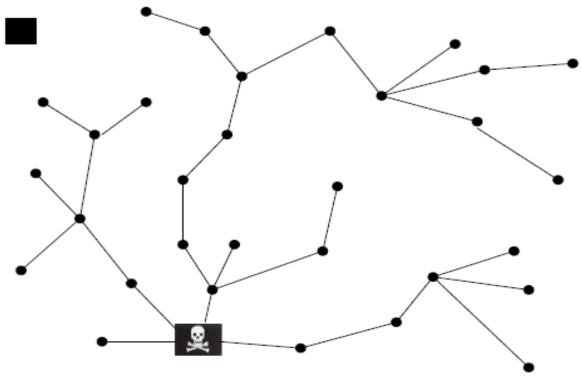

Fig. 4. An adversary spoofing a routing update from a base station in TinyOS beaconing.

The adversary first creates a wormhole between two colluding laptop-class nodes, one near the base station and one near the targeted area. The first node forwards (authenticated) routing updates to the second through the wormhole, who participates normally in the protocol and rebroadcasts the routing update in the targeted area. Since the "worm-holed" routing update will likely reach the targeted area considerably faster than it normally would have through multi-hop routing, the second node will create a large routing sub-tree in the targeted area with itself as the root. As seen in Figure 6, all traffic in the targeted area will be channeled through the wormhole, enabling a potent selective forwarding attack. If a laptop-class adversary has a powerful transmitter, it can use a HELLO flood attack to broadcast a routing update loud enough to reach the entire network, causing every node to mark the adversary as its parent. Most nodes will be likely out of normal radio range of both a true base station and the adversary. As shown in Figure 7, the network is crippled: the majority of nodes are stranded, sending packets into oblivion. Due to the simplicity of this protocol, it is unlikely there exists a simple extension to recover from this attack. A node that realizes its parent is not actually in range (say by using link layer acknowledgements) has few options short of flooding every packet.

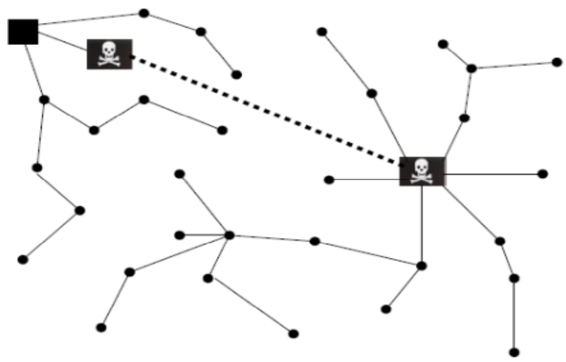

Fig. 5. A laptop-class adversary using a wormhole to create a sinkhole in TinyOS beaconing.

Each of its neighbors will likely have the adversary marked as its parent as well. Routing loops can easily be created by mote-class adversaries spoofing routing updates. Suppose an adversary can determine that node A and node B are within radio range of each other.

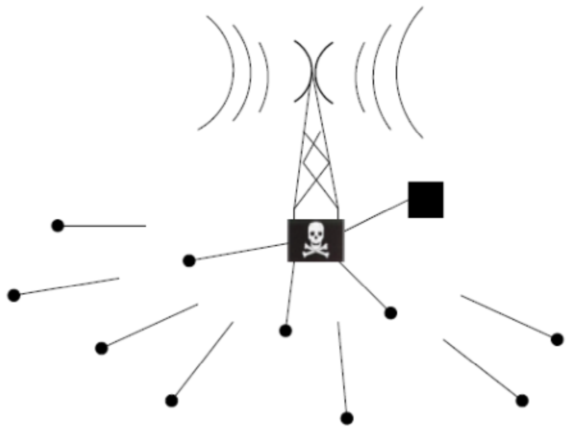

Fig. 6.HELLO flood attack against TinyOS beaconing.

An adversary can send a forged routing update to node B with a spoofed source address indicating it came from node A. Node B will then mark node A as its parent and rebroadcast the routing update. Node A will then hear the routing update from node B and mark B as it is parent. Messages sent to either A or B will be forever forwarded in a loop between the two of them.

*B. **Directed diffusion***

Directed diffusion [29] is a data-centric routing algorithmfor drawing information out of a sensor network. Base stationsflood interests for named data, setting up gradients within the network designed to draw events (i.e., data matchingthe interest). Nodes able to satisfy the interest disseminateinformation along the reverse path of interest propagation.Nodes receiving the same interest from multiple neighboringnodes may propagate events along the corresponding multiplelinks. Interests initially specify a low rate of data flow, butonce a base station starts receiving events it will reinforceone (or more) neighbor in order to request higher data rateevents. This process proceeds recursively until it reaches thenodes generating the events, causing them to generate eventsat a higher data rate. Alternatively, paths may be negativelyreinforced as well.There is a multipath variant of directed diffusion [30] aswell. After the primary dataflow is established using positivereinforcements, alternate routes are recursively establishedwith maximal disjointedness by attempting to reinforceneighbors not on the primary path.

Attacks: Due to the robust nature of flooding, it may bedifficult for an adversary to prevent interests from reachingtargets able to satisfy them. However, once sources beginto generate data events, an adversary attacking a data flowmight have one of four goals:

Suppression: Flow suppression is an instance of denial of service. The easiest way to suppress a flow is to spoofnegative reinforcements.

Cloning: Cloning a flow enables eavesdropping. After anadversary receives an interest flooded from a legitimate basestation, it can simply replay that interest with herself listedas a base station. All events satisfying the interest will nowbe sent to both the adversary and the legitimate base station.

Path influence: An adversary can influence the path taken bya data flow by spoofing positive and negative reinforcementsand bogus data events.

VI. Ultimate Limitations Of Secure Multi-Hop Routing

An ultimate limitation of building a multi-hop routingtopology around a fixed set of base stations is that those nodes within one or two hops of the base stations are particularlyattractive for compromise. After a significant number of these nodes have been compromised, all is lost.This indicates that clustering protocols like LEACH wherecluster-heads communicate directly with a base station mayultimately yield the most secure solutions against node compromiseand insider attacks.Another option may be to have a randomly rotating set of“virtual” base stations to create an overlay network. After aset of virtual base stations have been selected, a multi-hoptopology is constructed using them. The virtual base stationsthen communicate directly with the real base stations. The setof virtual base stations should be changed frequently enoughto make it difficult for adversaries to choose the “right” nodesto compromise.

VII. Conclusion

Secure routing is vital to the acceptance and use of sensornetworks for many applications, but we have demonstratedthat currently proposed routing protocols for these networksare insecure.We leave it as an open problem to design a sensornetwork routing protocol that satisfies our proposed securitygoals. Link layer encryption and authentication mechanismsmay be a reasonable first approximation for defense againstmote-class outsiders, but cryptography is not enough to defendagainst laptop-class adversaries and insiders: careful protocoldesign is needed as well.

References

[1] Y.-C. Hu, A. Perrig, and D. B. Johnson, “Wormhole detection in wirelessad hoc networks,” Department of Computer Science, RiceUniversity,Tech. Rep. TR01-384, June 2002.

[2] J. R. Douceur, “The Sybil Attack,” in *1st International Workshop onPeer-to-Peer Systems (IPTPS ’02)*, March 2002.

[3] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, “System architecture directions for networked sensors,” in*Proceedingsof ACM ASPLOS IX*, November 2000.

[4] V. D. Park and M. S. Corson, "A highly adaptive distributed routingalgorithm for mobile wireless networks," in *IEEE INFOCOM '97*, 1997,pp. 1405–1413.
[5] C. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing,"in *MILCOM '97 panel on Ad Hoc Networks*, 1997.
[6] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hocwireless networks," in *Mobile Computing*, Imielinski and Korth, Eds.Kluwer Academic Publishers, 1996, vol. 353.
[7] C. Perkins and P. Bhagwat, "Highly dynamic destination-sequenceddistance-vector routing (DSDV) for mobile computers," in *ACM/SIGCOMM'94 Conference on Communications Architectures, Protocols and Applications*, 1994, pp. 234–244.
[8] L. Zhou and Z. Haas, "Securing ad hoc networks," *IEEE Network Magazine*, vol. 13, no. 6, November/December 1999.
[9] F. Stajano and R. J. Anderson, "The resurrecting duckling: Securityissues for ad-hoc wireless networks," in *Seventh International SecurityProtocols Workshop*, 1999, pp. 172–194.
[10] J. Hubaux, L. Buttyan, and S. Capkun, "The quest for security in mobilead hoc networks," in *Proceedings of the ACM Symposium on Mobile AdHoc Networking and Computing (MobiHOC 2001)*, 2001.
[11] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing robust andubiquitous security support for mobile ad-hoc networks," in *ICNP*, 2001,pp. 251–260.
[12] M. G. Zapata, "Secure ad-hoc on-demand distancevector (SAODV) routing,"
[13] H. Luo, P. Zefros, J. Kong, S. Lu, and L. Zhang, "Self-securing adhoc wireless networks," in *Seventh IEEE Symposium on Computers andCommunications (ISCC '02)*, 2002.
[14] J. Binkley and W. Trost, "Authenticated ad hoc routing at the link layerfor mobile systems," *Wireless Networks*, vol. 7, no. 2, pp. 139–145,2001.
[15] B. Dahill, B. N. Levine, E. Royer, and C. Shields, "A secure routingprotocol for ad-hoc networks," Electrical Engineering and ComputerScience, University of Michigan, Tech. Rep. UM-CS-2001-037, August2001.
[16] J. Kong, H. Luo, K. Xu, D. L. Gu, M. Gerla, and S. Lu, "Adaptivesecurity for multi-layer ad-hoc networks," *Special Issue of WirelessCommunications and Mobile Computing, Wiley Interscience Press*, 2002.
[17] Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distancevector routing for mobile wireless ad hoc networks," in *Proceedings ofthe 4th IEEE Workshop on Mobile Computing Systems and Applications(WMCSA 2002)*, June 2002
[18] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demandrouting protocol for ad hoc networks," Department of Computer Science,Rice University, Tech. Rep. TR01-383, December 2001.
[19] S. Basagni, K. Herrin, E. Rosti, and D. Bruschi, "Secure pebblenets,"in *ACM International Symposium on Mobile Ad Hoc Networking andComputing (MobiHoc 2001)*, October 2001
[20] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hocnetworks," in *SCS Communication Networks and Distributed SystemsModeling and Simulation Conference (CNDS 2002)*, January 2002.
[21] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Sixth annual ACM/IEEE Internation Conference on Mobile Computing and Networking*, 2000,
[22] S. Buchegger and J.-Y. L. Boudec, "Nodes bearing grudges: Towardsrouting security, fairness, and robustness in mobile ad hoc networks," in*Proceedings of the Tenth Euromicro Workshop on Parallel, Distributedand Network-based Processing*. Canary Islands, Spain: IEEE ComputerSociety, January 2002, pp. 403–410.
[23] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar, "SPINS:Security protocols for sensor networks," in *Proceedings of MobileNetworking and Computing 2001*, 2001.
[24] Castro and Liskov, "Practical byzantine fault tolerance," in *OSDI: Symposiumon Operating Systems Design and Implementation*. USENIXAssociation, Co-sponsored by IEEE TCOS and ACM SIGOPS, 1999.
[25] A. Banerjea, "A taxonomy of dispersity routing schemes for fault tolerantreal-time channels," in *Proceedings of ECMAST*, vol. 26, May 1996, pp.129–148.
[26] K. Ishida, Y. Kakuda, and T. Kikuno, "A routing protocol for finding twonode-disjoint paths in computer networks," in *Internation Conference onNetwork Protocols*, November 1992
[27] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed energyconservation for ad hoc routing," in *Proceedings of the Seventh AnnualACM/IEEE International Conference on Mobile Computing andNetworking*, 2001.
[28] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, "Span: Anenergy-efficient coordination algorithm for topology maintenance in adhoc wireless networks," *ACM Wireless Networks Journal*, vol. 8, no. 5,September 2002.
[29] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: Ascalable and robust communication paradigm for sensor networks," in*Proceedings of the Sixth Annual International Conference on MobileComputing and Networks (MobiCOM '00)*, August 2000.
[30] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient,energy-efficient multipath routing in wireless sensor networks," *MobileComputing and Communications Review*, vol. 4, no. 5, October 2001