Directional Link Networks: Enabling Technologies for Multimedia Sensor Networks

Deepa Kundur, Texas A&M University, USA
deepa@ece.tamu.edu

The vision of ambient intelligence consists of a multitude of electronic devices and sensors that are seamlessly embedded into people's daily life. Currently, the most promising applications for this environment include home entertainment, healthcare, monitoring, automation, while it is Classically, wireless sensor networks have been envisioned to consist of groups of lightweight sensor nodes that observe *scalar* data, communicate wirelessly, and are densely distributed, collaborative, autonomous, hierarchical and secure. The nodes are distributed in a physical region containing a phenomenon of interest, which is to be monitored and possibly controlled. When the sensor nodes collect diverse types of information such as temperature, humidity, acoustic and visual data simultaneously, they are termed "multimodal sensors". Multiple types of sensing can occur within the same node through the use of distinct sensing technologies or across different nodes each having a single, but distinct sensor type. Multimodal sensors that collect multimedia information such as digital images, video and audio form a multimedia sensor network (MMSN).

Multimedia Sensor Networks: MMSNs represent a form of wireless sensor network in which a subset of sensors often collect higher bandwidth content; MMSNs that sense and process visual information will, in particular, play a critical role in the world's advancement, security and well-being. They can help interface to existing video surveillance infrastructure. For applications including healthcare surveillance, environmental observation and vehicle control, visual and other forms of broadband data are crucial for monitoring. MMSNs can be used for critical tasks often performed by humans such as the monitoring of sick patients. The rich visual signatures of surface currents for oceanographic monitoring makes MMSNs a cheaper alternative to characterize full ocean water columns. In situations where the network *sink* is a human observer, processed visual data from the network can enhance user-interactivity; for example, for unmanned ground or aerial vehicles MMSNs provide the feedback necessary for human operators for make critical motion and target decisions. The proliferation of low-cost portable off-the-shelf media sensing devices has motivated the recent development of vision-rich MMSN system theory, architectures and test beds.

MMSNs possess unique design challenges. First, in contrast to scalar networks, MMSNs require high speed hierarchical networking capabilities to transport broadband data; the improved scalability provided by employing a more hierarchical and power-specialized node architecture is especially advantageous when higher bandwidth communications is involved. Second, MMSNs are heterogeneous where nodes fall in classes with distinct sensing capabilities; for example, scalar sensors such as motion detectors can trigger vision acquisition and the associated traffic patterns may be bursty. Third, given the safety-critical applications facilitated by MMSNs, security and privacy within such networks are of significant concern.

Directional Link Networks: Directional link networks have recently shown potential to address the unique challenges of MMSN systems. Employing directional links provides advantages over traditional omnidirectional transmission for ad hoc sensor networks. By focusing energy in one direction, the potential for spatial reuse is increased while the consumed power and interference are reduced for the same transmission radius; this lengthens network lifetime while providing increased signal strength and reduced multipath components. Similarly, for the same power consumption, longer communicate ranges or higher bandwidth can be achieved facilitating multimedia communications and bursty traffic patterns. Furthermore, security is enhanced due to the reduced spatial signature of the communication signal from a broadcast disk-based model (for omnidirectional communications) to a sector-inspired model, thereby reducing the chances of eavesdropping potentially providing inherent security and privacy. Given these physical layer advantages, there is currently research interest in evaluating directional link technologies for advanced high speed networking systems.

Directional Links at the Physical Layer: Two main technologies exist for directional link communications: free space optical (FSO) and directional radio frequency (RF). **Figure 1** illustrates the idealized differences among the physical layer communication footprints of traditional omnidirectional RF, directional RF and FSO approaches.

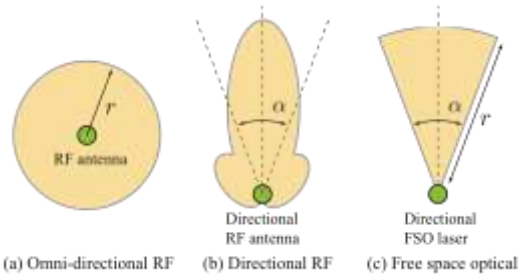

Figure 1. Communication footprints for omnidirectional, directional RF and FSO transmission

The traditional omnidirectional RF paradigm is currently employed in most wireless networking applications; it has the advantage of simplicity for networking protocols (since direction of transmission does not have to be effectively synchronized with other nodes) and improved connectivity given the broadcast nature of communications. However, the bandwidth-power consumption tradeoff is not competitive for MMSNs necessitating wired communication solutions where possible. However, in many applications for which wireless communications is a necessity (e.g., ad hoc networking in geographically remote regions), the link speeds offered by directional RF and FSO technologies demonstrate great potential thus warranting further study.

In the case of FSO communications, the potential for highly compact size (dust-like as proposed for the original Smart Dust) and power efficiency in comparison to RF communications makes them highly favorable for MMSNs. However, atmospheric conditions such as fog, clouds, snow and rain affect link reliability that must be addressed through physical layer processing and network robustness. Furthermore, the line of sight nature of communications makes transceiver alignment a significant issue especially in ad hoc networking contexts where communication may be impeded by physical objects such as buildings or walls. RF communications, in contrast, does not suffer from line-of-sight (LoS) constraints. However, the need for multiple antennas for transmission and/or reception results in node that may be impractically large or costly for lightweight MMSNs. Moreover, there is a beam steering delay that must be accounted for during networking.

Much existing research on directional links has focused on physical layer considerations to maintain bandwidth and security. However, as these devices are connected, networking challenges must also be addressed. For example, coding, modulation and signal processing strategies for various transceiver configurations can significantly improve link quality. However, the existence of the directionality of links due to *node deafness* (i.e., a node s_a cannot be heard by a node s_b within its proximity because s_b's receiver is directional) or *node invisibility* (i.e., s_a cannot transmit s_b because s_a's transmitter is directional) raises fundamental design questions at the networking level. To exploit the physical layer advantages of directional communications network layer mechanisms must be carefully designed to account for a "multi-hop view". In such a context medium access control and routing performance may not improve proportionally to the link speeds due to overhead.

Medium access control strategies must account for any steering involved during transmission and/or reception for directional RF nodes when communicating with immediate neighbors. Temporary node deafness and invisibility results in overhead due to the need for network reconfiguration. On a larger scale, network connectivity and routing issues must be considered. The traditional challenges of reliability, throughput and security must be studied in this new context. Not only does analysis of directional link networks provide performance bounds for emerging MMSNs, but in standard heterogeneous networks in which different devices have distinct communication ranges, directional links may be accommodated to avoid under-utilization and to diminish standard overhead costs.

Connectivity for Directional Networking: The range extension of directional communications can improve the LoS connection between two geographically distant nodes. However, questions arise as to the implications of

directional links to *network connectivity*. Network connectivity for standard bidirectional-link networks requires that at least one sequence of nodes (i.e., a path) exist connecting every possible node pair. For directional networks a notion of a *strongly connected* network is needed. Specifically, a network is strongly connected if for every node pair (s_a, s_b), paths from s_a to s_b and from s_b to s_a exist. For example, **Figure 2** illustrates a unidirectional network that is strongly connected. In contrast to bidirectional links, one sees that the paths from s_a to s_b and from s_b to s_a are necessarily distinct.

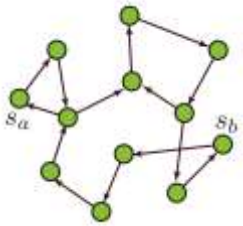

Figure 2. Strongly connected directional link network

The connectivity of a MMSN employing directional links is dependent on the transceiver configuration. Ideally, four transceiver configurations are possible for each directional RF or FSO node as detailed in Table 1. For the omni-omni case, it is clear that there is ideally no issue with unidirectional links. In all other configurations node deafness and/or invisibility is possible causing unidirectional links.

Table 1. Wiress transceiver configurations.

transmitter	receiver	Node deafness/ invisbility
omni	omni	neither
directional	omni	node invisibility
omni	directional	node deafness
directional	directional	both

In the remainder of this article, we will focus on the directional-omni transceiver case that is a common model for sensor networks such as Smart Dust that uses FSO communications. Here the nodes are static and are assumed to be randomly deployed in a 1-km by 1-km square geographical region with random position and orientation. Thus, a node can receive information via its omnidirectional receiver if it is within the LoS (i.e., static beam) of another node. **Figure 3** shows a possible realization of such a model for 200 nodes. Given the random nature of the associated network graph, probabilistic methods are used to assess connectivity. Three parameters, the number of nework nodes n, communication range r and beam width α, characterize the properties of the associated *random graph*. **Figure 1**(c) illustrates r and α in the context of the transmission sector of an FSO node.

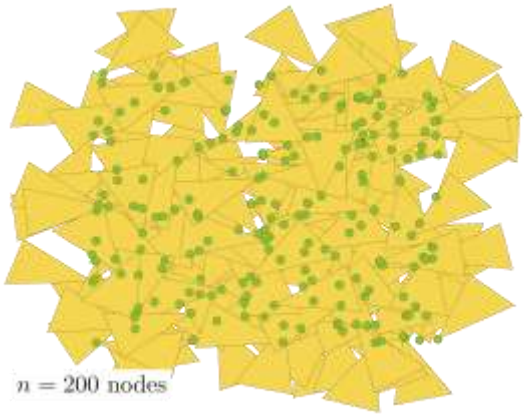

Figure 3. Randomly deployed unidirectional link network

Connectivity is therefore analyzed in terms of what is classically termed the *parameter assignment problem*. The specific problem is to determine the parameters (n, r, α) that guarantee at least a certain probability of connectivity of the associated random graph. Finding an exact expression for this probability of connectivity as a function of (n, r, α) is an open problem. Thus, research bounds this likelihood from above with the probability that there is *no isolated node*.

Node Isolation vs. Network Connectivity: A network node is isolated if it cannot transmit to or receiver from another node in the network. The situation when no network node is isolated not equivalent to the case of a directional network being strongly connected. For example, **Figure 4** shows a situation in which there are no isolated nodes (i.e., every node can communicate to at least one node and is able to receive from at least one node). However, the directional link between s_b and s_a that connects the two loops as well as the partition imply that the network is not strongly connected.

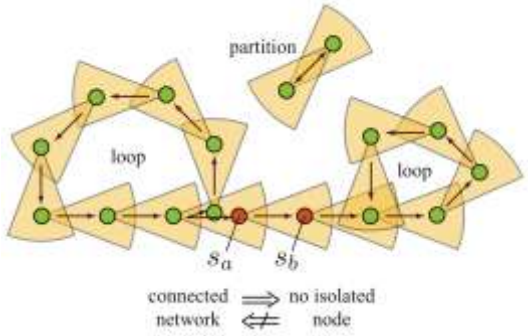

Figure 4. Example of a network with no isolated node that is not strongly connected

An analytic expression for the probability of no isolated node (representing an upper bound on the probability of connectivity) has been derived by the author to be:

$$p_d = \left[1 - e^{-\frac{n\alpha r^2}{2}}\right]^n \left[1 - \frac{e^{-\frac{n\alpha r^2}{2}}}{1 - e^{-\frac{n\alpha r^2}{2}}}\left(1 - \frac{\alpha r^2}{2}\right) \cdot \left(e^{\frac{n\alpha r^2(2\pi-\alpha)}{2\pi(2-\alpha r^2)}} - 1\right)\right]^n$$

Figure 5 compares the probability of connectivity and no isolated node for 500 nodes. The solid pink line is the probability of connectivity empirically obtained through the averaging of 1000 random deployment realizations and associated test for connectivity. The solid blue line is the analytic expression for the probability of no isolated node shown above, which as predicted is an upper bound. The red line represents the simulated probability of no isolated node and the black dash-dot line is the probability of connectivity compensating for edge effects using a Toroidal distance measure instead of Eucledian. Similar results are found for larger values of beam width α as illustrated in **Figure 6** and **Figure 7**. The latter graph corresponds to the bidirectional communication model that is commonly employed for omnidirectional RF wireless ad hoc networks. In all cases, the probability of no isolated node represents an upper bound on the probability of connectivity. As the beam width grows, this bound naturally tightens. Furthermore, one sees that compensating for edge effects also diminishes any differences between the probabilities. It should be mentioned that hierarchy where a randomly selected subset of nodes (e.g., cluster heads) are connected bidirectionally to one another can be shown to significantly improve connectivity; however, this concept is beyond the scope of this article.

Routing in Directional Networks: Assuming the device and network parameters (n, r, α) are selected for a high likelihood of connectivity, routing protocols can be established for such directional networks. In contrast to traditional ad hoc routing protocols based on reverse path routing, the directional links necessitate that forward and reverse paths between network nodes often be distinct. A circuit-based paradigm, as illustrated in **Figure 8** (where the blue entity is the network sink), must be employed to facilitate bidirectional communications amongst network nodes that primarily transmit via unidirectional links. Here, circuits or loops are the fundamental entity for routing that guarantees one node can communicate to and from another node or network sink. All circuits including the network sink represent an uplink and downlink path from a MMSN node to the sink.

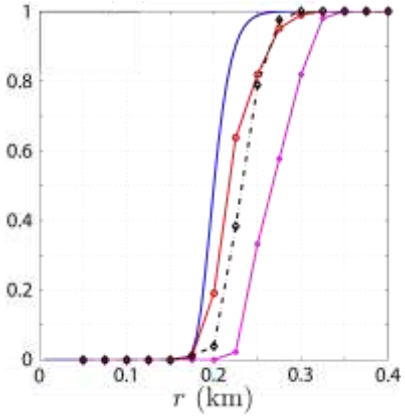

Figure 5. Probability of connectivity and no isolated node for beam width 40 degrees

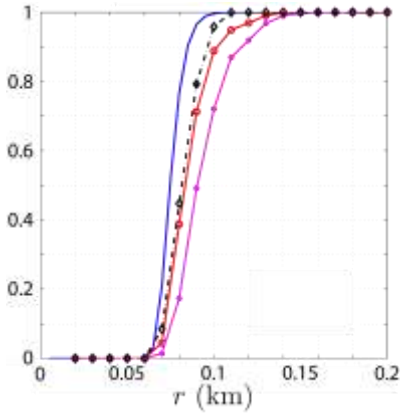

Figure 6. Probability of connectivity and no isolated node for beam width 270 degrees

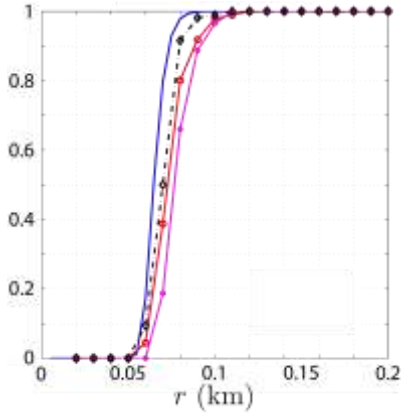

Figure 7. Probability of connectivity and no isolated node for beam width 360 degrees

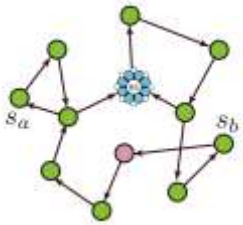

Figure 8. Circuit-based routing facilitates bidirecitonal links

For parameters (n, r, α) that guarantee a high likelihood of connectivity, it can be empirically and analytically shown that the number of hops in a circuit will usually not exceed 6 nodes making such a paradigm for directional link network routing potentially feasible. Topology discovery and route rediscovery mechanisms must account for the asymmetry in uplink and downlink routing, which naturally creates overhead. However, as we discuss next, this asymmetry can aid in network routing security.

Network Security in Directional Networks: Given the application space of MMSNs, security is of fundamental importance. Directional communications naturally lends itself to a more secure solution at the physical layer due to the more limited size of the communication footprint (see **Figure 1**), which makes interception of a communication beam more difficult. However, questions naturally arise as to whether there are any higher-level network security benefits of directional transmission paradigms.

The conventional threat model for ad hoc and sensor networks includes a high likelihood of insider attack. Thus, any network entity (excluding the sink) can potentially become corrupt. Given the high degree of coordination for such tasks as routing, even the corruption of a single node may have significant effects. A common strategy of legitimate network nodes is therefore to avoid collaboration with potentially corrupt nodes; thus, identification of such nodes is essential.

We assert in this paper that the asymmetry in communications warranted by directional link networks makes the network more secure. First, if traditional mechanisms to ensure successful data delivery are employed (e.g., via the use of ACK packets), a corrupt node in an uplink path would not be able to influence an ACK coming through a downlink path, thus alerting the network of a potential problem. Furthermore, for an attacker to hide such unwanted behavior, it would have to influence both the uplink and downlink paths thus raising the difficulty of the attack. For example, an attacker would have to corrupt two nodes in appropriate positions (depending on the topology) of the network.

Standard routing attacks geared for reverse path routing mechanisms no longer apply to a circuit-based approaches also providing inherent protection against naïve hackers. Future research efforts of the author and her group involve quantitative assessment of the trade-off between connectivity and security of directional link MMSNs.

Final Remarks: As MMSN systems emerge, we are at an exciting phase of development in which novel devices for sensing, communications and actuation must be employed. One class of such devices makes use of directional link communications to facilitate high-speed communications at lower power consumption. This article introduced some interesting aspects of directional link networking research and highlighted emerging challenges.

Useful Links:

1. Wireless Optical Sensor Networks: Connectivity, Routing and Security (Publications): http://www.ece.tamu.edu/~deepa/pub.html#wosn
2. Directional RF Sensor Networks: Connectivity and Security (Publications):

http://www.ece.tamu.edu/~deepa/pub.html#dirrf

Deepa Kundur received the B.A.Sc., M.A.Sc., and Ph.D. degrees all in Electrical and Computer Engineering in 1993, 1995, and 1999, respectively, from the University of Toronto, Canada. In January 2003, she joined the Department of Electrical Engineering at Texas A&M University, College Station, where she is a member of the Wireless Communications Laboratory and holds the position of Associate Professor. Before joining Texas A&M, she was an Assistant Professor at the Edward S. Rogers Sr. Department of Electrical and Computer Engineering at the University of Toronto where she was the Bell Canada Junior Chair-holder in Multimedia and an Associate Member of the Nortel Institute for Telecommunications.

Dr. Kundur's research interests include protection of scalar and broadband sensor networks, multimedia security, and computer forensics. She is an elected member of the IEEE Information Forensics and Security Technical Committee, vice-chair of the Security Interest Group of the IEEE Multimedia Communications Technical Committee and on the editorial boards of the IEEE Transactions on Multimedia and the EURASIP Journal on Information Security. More recently, she has been a guest editor for the 2007 EURASIP Journal on Advances in Signal Processing Special Issue on Visual Sensor Networks and the 2009 EURASIP Journal on Information Security Special Issue on Enhancing Privacy Protection in Multimedia Systems. She has been the recipient of the 2005 Tenneco Meritorious Teaching award, the 2006 Association of Former Students College Level Teaching award, and the 2007 Outstanding Professor Award in the ECE Department.