Ad Hoc and Sensor Networks

Santosh Kumar and Lan Wang
Dept. of Computer Science
The University of Memphis
Memphis, TN 38152-3240, USA

September 24, 2007

Abstract

1 Introduction

While the Internet has penetrated into virtually every aspect of our lives, there are many scenarios where an existing network infrastructure is not available. For example, a hurricane may destroy buildings where the critical networking equipments are housed or cut the power supply to the equipments. In such scenarios, it is extremely important for people living in the disaster area as well as relief workers to communicate with each other using whatever networking devices they have without relying on any existing infrastructure. Such an infrastructureless network is called an *Ad Hoc network*; more specifically, "a network that is setup, literally, for a specific purpose, to meet a quickly appearing communication need [18]." In addition to supporting human communication, an Ad Hoc network may be used for other purposes such as monitoring the physical environment and detecting events (as we will explain later).

An Ad Hoc network can be wired or wireless, but more research effort has been focused on *Wireless Ad Hoc networks* as they are easier to establish and do not restrict users' mobility. In a wireless ad hoc network, each node is equipped with one or more wireless radio transceivers. A node can communicate with nodes in its radio range directly (called single hop wireless); otherwise, it relies on the intermediate nodes to relay its message to a non-neighbor node. The latter mechanism is called *Multi-Hop* wireless communication. In contrast, infrastructure-based networks such as Wireless Local Area Networks (WLANs) and Cellular Networks use only single-hop wireless communication. Moreover, a wireless ad hoc network usually does not have special-purpose relay nodes similar to routers in conventional networks – every node is a potential router (that can relay other nodes' data). Furthermore, the network topology of a wireless ad hoc network is usually much more dynamic than a conventional network, due to node failures and/or node mobility.

A Wireless Ad Hoc Network has several benefits over wired infrastructure-based networks making it a compelling choice for networking in certain application scenarios. We discuss some of these benefits here:

- **Quick to Deploy:** A Wireless Ad Hoc Network, by definition, does not require an existing infrastructure such as wall power or wiring. This significantly reduces the time to deploy a Wireless Ad Hoc Network and have it up and running. Sometimes, the time to deploy may be in minutes or seconds as opposed to days or weeks for an infrastructure-based network.

- **Suitable for a Wider Range of Environment:** A Wireless Ad Hoc Network, can easily be deployed in remote places such as in forests, under water (e.g. rivers, oceans, etc.), on mountain tops, on moving troops in a battlefield, in toxic areas, or on other planets.

- **More Resilient to Failures:** Wireless Ad Hoc Networks are typically more resilient to failures than infrastructure-based networks. This is because communication among nodes can be over multiple hops using intermediate nodes (each of which can act as a router), and because the protocols developed do not assume any existence of infrastructure. Most ad hoc network protocols are/can be designed to quickly reconfigure upon failure, therefore communication among surviving nodes is possible even if several or the majority of nodes have failed (as in a battlefield scenario).

- **Offers Freedom of Mobility:** Since there is no wiring among nodes, the nodes in a Wireless Ad Hoc Network can move freely and still maintain communication with other nodes in the network. The protocols are also designed to adapt quickly to mobility (which may cause frequent changes in the set of neighbors). This makes Ad Hoc Networks especially useful in mobile applications such as among a group of moving soldiers, a fleet of moving vehicles, a fleet of aircrafts flying together, and in disaster locations.

- **Economical:** Due to its low set up overhead (e.g. no wiring and labor), deploying a Wireless Ad Hoc Network is more economical compared to its wired counterpart in several application scenarios.

Although Wireless Ad Hoc Networks have several advantages over infrastructure-based networks, they have their own limitations. For example, the nodes usually have limited lifetime because they typically run on batteries. Moreover, it is often more challenging to develop efficient protocols for the Wireless Ad Hoc Networks, due to mobility and the limitations of wireless communication medium.

Major research issues in wireless ad hoc networks include, but are not limited to, how to ensure connectivity among nodes in the face of unplanned deployment, controlled or uncontrolled mobility, and nodes leaving/joining the network (potentially as a result of failures/repairs); how to efficiently access the shared wireless medium in a distributed fashion; how to route packets to their destinations in the presence of topology dynamics (due to mobility and failures), and sometimes intermittent connectivity; how to meet the Quality of Service (QoS) requirements with distributed resource management. These issues are made even more challenging by the limited resource availability that is typical of a Wireless Ad Hoc network.

Wireless Ad Hoc networks can be classified into several categories. Below are three major categories of Ad Hoc Networks, each of which has become a fertile research area in its own right:

1. **Mobile Ad Hoc Network (MANET):** a MANET is a network of mobile computing devices such as laptops and PDAs. The purpose of forming a MANET is to facilitate communication among mobile host devices that make up this network.

2. **Wireless Sensor Network (WSN):** WSNs are composed of small wireless sensors such as motes [12] that can monitor their surrounding physical environment using various on-board sensors. The purpose of a WSN is to monitor the environment in which it is embedded to either collect data of interest or to detect events of interest such as monitoring its surrounding for illegal intrusion activity.

3. **Wireless Mesh Networks:** A Wireless Mesh Network consists of wireless devices mainly used as routers to provide a wireless infrastructure to other devices. A Wireless Mesh Network can provide Internet access to computational devices such as laptops and PDAs, without having to deploy a wired infrastructure.

Each of the above categories can be further classified based on the devices and communication technology they employ. For example, the mobile devices in a MANET can be laptops, PDAs or even cell phones and the communication technology used by these devices can be 802.11, Bluetooth, ZigBee, etc.

Our focus in this article is on the first two categories — MANETs and WSNs (see [1] for a survey of wireless mesh networks). MANETs and WSNs share several key characteristics as both of them rely on the wireless medium for communication and use multi-hop wireless routing. However, they have important differences as well due to the intrinsic differences in their potential applications. For example, typical applications of MANETs include communication on a battlefield and during disaster recovery; therefore, research on MANETs has been focusing on supporting human communication in the face of unconstrained mobility. On the other hand, WSNs are used to monitor the physical environment such as natural habitats and volcanos as well as to detect intrusions in a highly secure area. The sensor nodes are usually stationary and they need to last months without human intervention, so energy-efficiency is a critical issue for WSNs, while ensuring connectivity despite user induced (and hence uncontrolled) mobility has not been a major focus of WSN research.

In the remainder of this article, we first discuss (in Section 2) the common issues in MANETs and WSNs, all of which are important for Wireless Mesh Networks, as well. Then, in Section 3, we describe differences between MANETs and WSNs. Finally, we conclude the article in Section 4.

2 Common Issues in Wireless Ad Hoc Networks

In this section, we discuss issues that are common to most Wireless Ad Hoc Networks.

2.1 The Issue of Connectivity

A Wireless Ad Hoc Network, by its very definition, does not have a preplanned network topology. At the same time, the network needs to facilitate communication among different nodes. For this to be possible the network needs to have some form of connectivity. Depending on the particular network, we may want all the nodes in the network to form a connected graph, or want most of the nodes to form a connected graph, or want the network to provide delay tolerant connectivity [7]. Sometimes, for fault tolerance or to balance the routing load among nodes, k-connectivity in the network may be desired such that k node-disjoint paths exist between every pair of nodes.

Connectivity (or k-connectivity) can be made possible either by increasing the density of nodes, by adjusting the transmission range of individual nodes, or by (controlled or uncontrolled) movement of nodes. If the nodes are mostly static and their location distribution can be approximated by a Poisson process or a random uniform process, then a critical relation exists between the transmission range and node density [10, 24]. Given one of these two parameters, the other can be derived. If the density is given, then the required transmission is called critical, and vice versa. The term critical (in say transmission range) intuitively means that if the transmission range is less than critical value, then the network is disconnected with high probability. On the other hand, if the transmission range is higher than the critical value, then the network is connected with high probability. The connectivity of the network is said to have a phase transition (from disconnected to connected) at this critical value.

When nodes are mobile, similar results exist for the critical relation between the transmission range and density [34]. These results assume that node movements can be approximated by certain mobility models.

While critical density provides a guidance as to what behavior can be expected from a randomly deployed network in terms of connectivity, the results are not directly usable by a practitioner who would like to have a guarantee on connectivity for finite deployment regions. This is because the results derived for critical density are asymptotic, by definition. Recently, a new technique has been proposed to derive density estimates for random deployments that are quite reliable for finite deployment regions [2]. Such work bridge the gap between theory and practice in the area of connectivity since theoretical results can now be readily used in practice.

Another area of research that has received considerable attention is called “Delay-tolerant connectivity.” It means that the network may not be connected at every instant in time, but movement of nodes may facilitate occasional communication among pairs of disconnected nodes. In the extreme case, data mules [16] may be deployed whose sole purpose is to ferry data between source-destination pairs. In other scenarios, nodes that have data packets destined to another node may wait till they come in direct contact to each other, or pass the message to one of their current neighbors, who repeats the process until the data reaches its destination or until its time to live runs out, in which case it is dropped. Figuring out a good approach for message delivery in a mobile network that is not always connected is currently a highly active area of research.

2.2 Distributed Medium Access Control

Because the wireless medium is broadcast in nature, collision can occur when two nodes within each other’s transmission range send packets at the same time. In an infrastructure-based wireless network such as a cell phone network, the access point (or base station) can allocate a different frequency band or a different transmission slot to each node in the same cell. However, in an ad hoc network, there is no centralized controller. Therefore, the first issue that needs to be addressed in any wireless ad hoc network is how to coordinate the transmissions of different nodes without using a centralized controller. The major objectives are to avoid collision (that may lead to loss of all colliding messages and hence loss of bandwidth) in a distributed manner, make efficient utilization of scarce wireless bandwidth, ensure fairness among the nodes, provide real time guarantees to high priority packets, and achieve all these with a mechanism that scales to large network sizes. A protocol that achieves these objectives (or a subset of these) in a distributed manner is called a Distributed Medium Access Control (MAC) protocol[1].

Several distributed MAC protocols have been proposed. Most of them can be classified in two categories:

- **Competitive Protocols:** These protocols subscribe to the philosophy that each node should compete for access to the common wireless channel by itself. Each node makes a local decision on whether to transmit its packets at a given time instant or not. These decisions are based on rules that are expected to maximize the chances of a successful transmission. One common technique is to sense the channel for idleness before starting a new transmission, which is referred to as Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA). The main advantage of these protocols is simplicity and hence scalability. The main disadvantage is inefficient utilization of the wireless channel especially when the number of nodes competing for the channel is high. Examples of such protocols include Multiple Access Collision Avoidance for Wireless LANs (MACAW), Floor Acquisition Multiple Access Protocol (FAMA), Busy Tone Multiple Access (BTMA), Dual BTMA (DBTMA), Receiver Initiated BTMA (RI-BTMA), Multiple Access Collision Avoidance by Invitation (MACA-BI), and Media Access with Reduced Handshake (MARCH).

- **Cooperative Protocols:** These protocols follow a different approach; they are based on the philosophy that nodes should cooperate on deciding a schedule, i.e. who has the right to use the channel at a particular time. In most of these protocols time is divided in slots, and nodes work together on deciding which slots are assigned to which nodes. The main advantage of these protocols is efficient utilization when most nodes have continuous data to send. Another advantage is the guarantee of an upper bound on delay that any node will experience in sending its packets. The major disadvantage is its complexity which arises from its core philosophy of requiring cooperation among nodes. Example of such protocols include Distributed Packet Reservation Multiple Access (D-PRMA), Collision Avoidance Time Allocation (CATA), Hop Reservation Multiple Access (HRMA), Soft Reservation Multiple Access with Priority Assignment (SRMA/PA), and Five Phase Reservation Protocol (FPRP).

Some protocols use a combination of the two philosophies, i.e. use reservation for real-time traffic that need a delay guarantee and use competitive access for regular traffic. An example of such a protocol is MACA with Piggy-Backed Reservation (MACA/PR).

We refer the reader to Chapter 6 in [27] for a description of all the MAC protocols listed above. Some issues that are unique to a MAC protocol in WSN is described in Section 3.5.

2.3 Neighbor Discovery and Multi-hop Routing

Since nodes in a wireless ad hoc network depend on their neighbors to relay packets for them, each node first needs to discover its neighbors after initial deployment ("neighbor discovery") and it needs to update this information as neighboring nodes fail or move out of its transmission range. Moreover, each node needs to figure out to which neighbor a particular packet should be forwarded so that the packet can reach its destination most efficiently. This task is accomplished using a distributed Ad Hoc Routing protocol, which typically takes into consideration the unique characteristics of wireless ad hoc networks, e.g. frequent topology changes, limited power source and low bandwidth resources.

Numerous ad hoc routing protocols have been proposed to date (see [4] and Chapter 7 in [27]) [2]. These protocols perform either **flat** or **hierarchical** routing. In flat routing, a node can potentially obtain a route to all the other nodes in the network. In hierarchical routing, the network is usually divided into many non-overlapping clusters. Each cluster has a clusterhead that handles inter-cluster routing, while other nodes only need to discover routes to nodes within their own cluster. Hierarchical routing protocols are usually more suitable for large networks. Below we focus our discussion on flat routing protocols. Readers are referred to [4] for more discussion of hierarchical routing protocols. Issues that are unique to a routing protocol in WSN is described in Section 3.2.

Flat routing protocols can be classified into one of the following three categories based on when routes are discovered:

[1] Some infrastructure networks such as wireless LANs may also use distributed MAC protocols to avoid collision.

[2] Several of these protocols are being standardized by the Internet Engineering Task Force (IETF) MANET working group (http://www.ietf.org/html.charters/manet-charter.html).

- A **proactive** routing protocol always maintains a route to every destination in a network regardless of whether such a route will be used. The routes are usually computed using a distance vector algorithm or a link state algorithm. The protocols in this category are closest to traditional routing protocols, but they typically include optimizations that reduce bandwidth and processing overhead. They are also able to detect obsolete routes faster, for example, by adding more information in routing messages. Examples of proactive ad hoc routing protocols include DSDV (Destination-Sequenced Distance Vector [31]), OLSR (Optimized Link State Routing Protocol [15]), TBRPF (Topology Dissemination based on Reverse-Path Forwarding [29]), and WRP (Wireless Routing Protocol [28]).

- A **reactive** routing protocol performs route discovery only when a node receives a packet to a particular destination that has no associated route in the node's routing table. In other words, routing overhead will not be incurred for destinations that have no traffic destined to them. Therefore, reactive protocols usually have a lower processing, storage and bandwidth overhead than proactive protocols. The reactive approach is especially suitable for networks with highly dynamic nodes, as the costs of maintaining routes to the dynamic destinations are extremely high. However, the overhead reduction also depends heavily on the traffic pattern in the network. If traffic is evenly distributed among all the destinations, the overhead saving may not be significant. Moreover, since route discovery takes time to complete, networks using reactive routing protocols may have a longer delay in packet delivery. Examples of reactive ad hoc routing protocols include AODV (Ad-hoc On-demand Distance Vector [30]), DSR (Dynamic Source Routing [17]), DYMO (DYnamic Manet On-demand Routing [5]).

- A **hybrid** routing protocol maintains pre-computed routes to some destinations while performing on-demand route discovery for the other destinations. This type of protocols are designed for large networks, where a pure proactive protocol may incur too much control traffic while a pure reactive approach may have too high a packet delay and/or too much control traffic. One example of hybrid routing protocols is ZRP (Zone Routing Protocol [11]).

We now briefly describe DSR and ZRP as an illustration of how ad hoc routing protocols work.

2.3.1 DSR (Dynamic Source Routing [17])

Each node in DSR maintains a cache of discovered routes. When a sender needs to communicate with a new destination, it broadcasts a Route Request (RREQ) message to its neighbors. Each neighbor checks its cache to see if a route to the destination has been discovered before. If not, the node appends its address to the RREQ message and broadcasts this message to its neighbors. This process continues until at least one node identifies a route to the destination in its cache. This node then sends a Route Reply (RREP) message to the original sender of the RREQ message with the entire path in the reply. If no intermediate nodes have a path to the destination, the destination will eventually receive the RREQ message and send a RREP to the sender.

DSR uses source routing in packet delivery, i.e the sender of a packet specifies the entire path in the header of each data packet. Source routing allows a node to use multiple paths to reach the same destination while avoiding packet loops. However, it incurs more message overhead as each packet needs to carry the entire path in its header. Another downside is that the source route may become obsolete when a packet is still on-route to its destination, especially when the nodes are highly mobile.

2.3.2 ZRP (Zone Routing Protocol [11])

In ZRP, each node maintains routes proactively to all the nodes within a certain number of hops. This set of nodes is called a Zone for the node and the number of hops is called a Zone Radius. If a node needs to deliver a packet to a destination outside its zone, it just sends a route request message to those nodes on the boundary of its zone. Those nodes in turn forward the message to the nodes on their zone boundary until a node can locate the destination in its own zone. Since the zone radius determines the routing traffic both within a zone and between zones, the main research issue is therefore how to determine the appropriate zone radius to minimize the overall routing traffic.

2.4 Reliable Data Delivery

The wireless medium typically has a higher error and loss rate than the wired medium due to path loss, multi-path fading and interference. Path loss means that the signal strength weakens after the wireless signal travels for some distance. The remaining signal strength is usually a function of the distance. Multi-path fading occurs when the wireless signal propagates in different directions and finally all the signals arrive at the same destination. These different versions of the original signal may have different phases and strength, so the combination of them may look very different from the original signal. Interference is caused by signals transmitted at frequencies close to each other. It can be reduced to a certain extent by using guard bands between frequency bands and minimizing the transmission range of each node (as described in Section 2.1).

Given the higher error and loss rate of the wireless medium, how to ensure the reliable data delivery without negatively impacting end-to-end throughput becomes a key issue in wireless ad hoc networks. First, unlike wired networks which can rely solely on end-to-end recovery, wireless ad hoc networks also need hop-by-hop link-level error recovery to minimize delay, improve throughput and reduce unnecessary retransmissions by end nodes. Second, the transport layer needs to distinguish losses caused by errors from those caused by congestion. The most popular reliable transport layer protocol is Transmission Control Protocol (TCP). It was designed for wired networks in which most of the losses are caused by congestion, so a TCP sender reduces its speed drastically whenever a loss is detected. This reaction is considered inappropriate for error-triggered losses as the sender should probably be as aggressive as before. As a result, the TCP performance in a wireless network could be problematic. Several extensions to TCP and alternative protocols have been proposed to address these problems. We refer the reader to [27](Chapter 9) for details. A new trend in this research area is for the lower layer to expose more information to the transport layer so that the overall system will be more efficient and effective. Such “Cross Layer Optimization” has been proposed for solving other problems in wireless ad hoc networks as well.

2.5 Security

Securing wireless ad hoc networks is especially challenging [13, 26]. First, privacy and integrity are more difficult to ensure in a wireless network than in a wired network since it is easy for an attacker to snoop on a wireless channel and modify ongoing transmission. Second, because of the infrastructureless nature of wireless ad hoc networks, authenticity is difficult to establish as there is no trusted central authority. Third, since the wireless nodes are more portable than computers in a traditional network, they may be easier to lose and later used by attackers to inject false information. Furthermore, conventional security mechanisms usually have high computational and storage demands which may make their implementation difficult on wireless nodes.

3 What Sets MANETs and WSNs Apart?

Although discussions of Wireless Ad Hoc Networks (which mostly refers to MANETs) often include Wireless Sensor Networks (WSN) as a special case, these two areas have each blossomed into exciting research areas in their own right. This is because these two networks possess several unique characteristics that set them apart. Below we discuss some major characteristics that are unique to each of these networks.

3.1 Typical Usage

MANETs are used mostly for communication between human operated devices such as laptops, PDAs, or Cellular Phones, whereas Wireless Sensor Networks are deployed mostly for data collection and event monitoring. We now discuss some representative applications of each network.

We first describe two applications of MANETs.

- **Facilitating Communication Among a Troop of Soldiers:** Each soldier carries a computing device with Ad Hoc Networking ability. The devices hosted on the soldiers form an Ad Hoc Network as soon as they are turned on. This network allows messages from any node to reach any other node even though the soldiers are allowed to move freely to achieve their operational goals (their movements are not constrained to maintaining a connected network). Therefore, the network of devices needs to take care of maintaining connectivity.

- **Facilitating Communication in Remote Locations:** Cellular phone towers do not cover remote areas (such as mountains and forests). If mobile phones are equipped with Ad Hoc Networking capability (as is being planned), then an Ad Hoc network among the various mobile phones can be formed. This Ad Hoc Network will enable data and possibly voice communication among users even if there are no cellular phone towers in the neighborhood to provide regular coverage.

Now we describe two applications of WSNs.

- **Detecting Illegal Crossing on an International Border:** Wireless sensor nodes are sprayed from an aircraft on the international border. Once these sensors land on ground, they form a multi-hop wireless network. They start monitoring for people or vehicles crossing the border. As soon as such an event is detected by one or more sensors, a detection message is dispatched to a manned station for possible action. The message takes less than a couple of seconds to reach a manned station that may be situated several miles from the point of occurrence of the intrusion event. This system has a potential to significantly improve the border surveillance at a low cost. With this system, the entire border can be continuously monitored instead of spotty surveillance that is done today.
- **Monitoring a Fabrication Plant to Prevent Downtime:** Wireless sensors can be deployed in a fabrication plant to monitor the vibration and acoustic signatures of critical equipments. If the signature matches some specific patterns that typically precede failures, a message is immediately dispatched to a manned station and preventive actions are taken to ensure no downtime occurs. This system has a potential to save millions of dollars by preventing downtime of critical equipment.

As illustrated by the above mentioned applications, the purpose of deploying a MANET is very distinct from that of deploying a WSN. The implication is that new research issues emerge in WSN that had not been so critical in MANET such as the issue of coverage (i.e. ensuring that a WSN provides desired quality of monitoring), tolerance to new types of faults, focus on energy efficiency, etc. Even those issues that are common to both networks such as the design of Medium Access Control, Routing, and other protocols (discussed in Section 2) need to be revisited for WSNs. In the following, we elaborate on these and other differences between MANETs and WSNs.

3.2 Typical Traffic Pattern

Because the typical usage of the two networks are distinct, their typical traffic patterns are quite distinct as well. In a MANET, traffic pattern is usually point to point or point to multi-point. In other words, traffic originating from one node may be destined to one particular subset of nodes at a given time instant, while traffic originating from another node or from the same node but at a different time instant may be destined to a different subset of nodes.

In a wireless sensor network, on the other hand, data traffic either flows from sensor nodes to one or a set of base stations, called source to sink or from the base station(s) to some or all nodes, called sink to source. Examples of source to sink traffic are event detection messages from sensors or sensor data about the environmental variations. Examples of sink to source traffic are the dissemination of a new program to all (or a subset of) sensors or a dissemination of a new value of some parameters to all (or a subset of) sensors. Base stations are sometimes referred to as *sinks* to emphasize this traffic pattern.

Since the traffic pattern in a WSN is so distinct from that in a MANET, the routing protocol used in these two networks are different as well. As mentioned in the previous paragraph, two types of traffic need to be supported by a WSN, information from sensors to sink(s) and from sink(s) to sensors. Traffic from sensors to sink(s) is referred to as *data gathering* and that from sink(s) to sensors is referred to as *data dissemination.* The major issues that need to be addressed in a routing protocol to support each of these traffic patterns are very distinct and hence two different categories of routing protocols have been developed to cater to these two traffic types. MintRoute [36] is an example of a data gathering routing protocol and Deluge [14] is an example of a data dissemination routing protocol.

3.3 Attended vs. Unattended — Implications for Fault-tolerance

MANETs typically consist of human operated devices and therefore are mostly attended by a human being. Several types of faults may easily be detected and repaired (by resetting the device). Battery exhaustion is also not a major concern as the human operator may recharge the device when needed.

A wireless sensor network is typically deployed outdoors and may remain unattended for long periods of time. This unattended nature has several fault-tolerance implications. First, sensor nodes are subject to new types of faults that may come from outdoor environmental conditions such as wind, rain, excessive heat or cold, physical tampering, etc. Excessive heat or cold or excessive battery depletion may cause other types of failures that qualify as byzantine failures [3]. Second, node failures are more frequent in a wireless sensor network. Further, node failures may not be detected immediately and sometimes not detected at all (for example, if message from a healthy sensor node cannot reach the base station). Third, physically repairing or replacing individual nodes may not be feasible (e.g., if the sensors are deployed in inhospitable terrain or in enemy territory), and hence only remote repair of failures is feasible. Fourth, battery recharging may not be feasible (especially if the nodes are not equipped with energy scavenging mechanisms as in solar cells).

Consequently, the protocols developed for wireless sensor network needs to be adaptive to these new types of failures. These failure types are not prevalent in a MANET.

3.4 Resource Constraints

The computational capacity, memory size, buffer capacity, and network bandwidth available to a sensor node is an order of magnitude lower than that available to a node in a typical MANET. See Table 1 for a comparison of the hardware specification of a typical WSN device with that of a typical MANET device. Observe that the processor is at least 50 times slower in WSN and RAM size is at least 6,400 times lower. This implies that the protocols and algorithms developed for a WSN need to be considerably simpler than that developed for a typical MANET.

Property	**WSN Device**	**Pocket PC**	**Laptop**
Processor Speed	8 MHZ	400 MHZ	1.8 GHZ
RAM Size	10 KB	64 MB	1 GB
Persistent Storage	1 MB	64 MB	60 GB
Radio Data Rate	250 kbps	11 mbps	54 mbps

Table 1: Comparison of key hardware properties of a typical WSN device (telosb mote), a pocket PC (HP iPAQ), and a typical laptop.

3.5 Energy Efficiency

Sensor nodes, being deployed outdoors and unattended, run on batteries that may not be replaced. Hence, the issue of energy efficiency and network longevity are high priority considerations, whereas this problem is less severe in MANETs that mostly consist of personal digital devices that can be recharged. As a result, every protocol or algorithm developed for wireless sensor network should be designed with a consideration of energy efficiency. For example, the MAC protocols proposed for MANETs are not very appropriate for use in WSN because energy efficiency is not as critical in MANET. In a WSN, even keeping the radio in listening mode for an extended period of time can drain significant energy. Hence, the radio may be completely turned off to save energy and it is turned on only periodically or when needed to receive or transmit data. If the radio is not always in the listening mode, communication (especially of real time data like detection of an intruder) becomes non-trivial. Several MAC protocols to ensure timely communication while ensuring energy-efficiency have been proposed. An example of such a protocol is B-MAC [32].

The issue of energy efficiency is also critical in the process of deployment. If redundant sensors are deployed, the redundant sensor nodes are put to sleep, taking turns, to maximize the lifetime of sensors (as discussed in Section 3.8).

3.6 Mobility

The nodes in a typical MANET are assumed to be frequently mobile. The nodes in a WSN, on the other hand, are mostly static unless moved by wind or other external phenomenon. In future, some sensor networks may consist of mobile nodes, though [35]. In these cases, however, the motion of sensors will be dictated by the network requirement (such as to facilitate data collection from a sensor node disconnected from the base station [16] or to provide temporary coverage in place of a failed sensor node [35]) as opposed to a user-induced motion as in a typical Ad Hoc network. This difference in the mobility pattern affects how the protocols for the two networks are designed.

3.7 Security Threats

New types of security threats are possible in a sensor network due to outdoor and unattended deployment such as physical capture and physical destruction. Since sensor nodes have the ability to receive new program code to replace the currently active program code via wireless channel, an adversary may inject malicious program onto sensor nodes. False sensory data or bogus events can also be injected in the network. Communication can be jammed by accompanying a malicious target (that the network is supposed to detect) with a jammer device. Since the sensors have limited energy reserve, attacks can be played to deplete sensors of their energy such as by sending too many message (from a more powerful device) or causing too many event detections. Designing protocols to mitigate these and other security threats in a WSN is currently an active area of research.

3.8 The Issue of Coverage

Since the main purpose of a WSN is data collection and event monitoring, the issue of coverage becomes a key issue in the deployment and maintenance of sensor networks. The issue of coverage is that of determining methods of initial deployment and subsequent maintenance of the network topology (over time) to ensure that a WSN provides the desired quality of monitoring [21, 20]. This issue does not arise in MANETs since their main purpose is not to monitor events.

When a sensor network is to be deployed, several critical deployment issues arise such as how many sensors should be deployed and in what pattern. Determining how many sensors to deploy becomes more challenging when sensors cannot be deployed at desired locations as when spraying them from an aircraft. Once sensors have been deployed, mechanisms are needed to detect if the network continues to provides the desired quality of monitoring as some sensors may fail unexpectedly due to environmental factors. In the event that the network can no longer provide the desired quality of monitoring, additional sensors may need to be deployed or if the sensors have movement ability then some sensors may need to be repositioned to repair the network. Designing efficient methods of redeployment or reconfiguration continues to be an active area of research.

In order to tolerate unanticipated sensor failures, some redundant sensors may be deployed. In such a case, mechanisms are needed to determine a sleeping schedule [19] for the redundant sensors such that the batteries of the active nodes get depleted at a slower rate ensuring a longer life for the network.

3.9 Localization

Since the main purpose of a wireless sensor network is to monitoring events or collect information about the environment, it is often critical to associate location information with the data collected by a sensor node. For example, if a sensor network is deployed to detect fire, then it is not sufficient to learn that fire has erupted. Location of the fire eruption is a critical part of the information. Further, since installing GPS at every sensor node is prohibitively expensive and energy consuming, the process of localization needs to be performed in a sensor network such that each sensor node knows its absolute location. The process of localization is either not so critical in a typical MANET or installing a GPS unit on each device is within the budget.

Various mechanisms have been proposed to perform localization. For example, a mobile unit with GPS mounted on it can traverse through the network broadcasting its location [8]. Sensors can localize themselves using this broadcast. Alternatively, some anchor nodes can be placed in the network who know their location (possibly using a GPS). These nodes then help other nodes determine their locations by using a localization algorithm. Some mechanisms for localization use time difference of arrivals of radio or acoustic signals [9], while others use radio interferometric techniques where radio signals are transmitted to cause interference (and hence phase difference) at the receivers [23]. Localization in a WSN is still an active area of research.

3.10 Time Synchronization

Since the main purpose of a WSN is to monitor events or collect information about the environment, it is often critical to associate time information with the data collected by a sensor node. For example, if a sensor network is deployed to track the trajectory of a moving target, then time of detection of the target at a specific sensor is necessary to chart the trajectory of target movement.

Time synchronization is also useful in MANETs (especially for implementing some cooperative MAC protocols). However, the clocks of MANET nodes are usually more accurate than that of sensor networks. Also, in MANET devices such as cell phones, time synchronization is provided by a centralized infrastructure. Consequently, the problem of time synchronization is more critical in WSN than in MANET and requires a non-trivial solution.

Several protocols exist for time synchronization in a WSN. They can be classified in two categories — *proactive* and *reactive* [33]. In proactive protocols, a virtual global reference time across the entire network is established and maintained via the exchange of messages. Reference Broadcast Synchronization (RBS) [6] and Flooding Time Synchronization Protocol (FTSP) [25] are examples of proactive protocols. In reactive protocols, time is not synchronized at all. Packets are time-stamped using local unsynchronized times. Synchronization is done after the detection of events. An example of such a protocol is Routing Integrated Time Synchronization (RITS) protocol [22, 33].

4 Conclusion

Wireless Ad Hoc Networks have revolutionized the world of communication by enabling quick and infrastructureless communication at the point of need whether it is in a battlefield, on a mountain, under water, or on a different planet. Wireless Sensor Networks, on the other hand, are revolutionizing many disciplines by providing unprecedented ability to observe our environment and surrounding. By enabling unobtrusive collection and accessibility of real time data from the environment, new research capability is now available in several scientific disciplines such as biology, geology, oceanology, medicine, and elderly care. Also, by enabling real-time and continuous monitoring of environment, new capabilities in surveillance have become possible such as efficient and comprehensive border surveillance. Both of these disciplines, Wireless Ad Hoc Network and Wireless Sensor Network, are relatively young disciplines with highly active research communities. As new applications emerge and as the technologies mature, these two technologies can potentially have a greater impact on our lives than personal computers and the Internet have.

References

[1] I. F. Akyildiz, X. Wang, and W. Wang. Wireless mesh networks: a survey. *Computer Networks*, 47(4):445–487, March 2005.

[2] P. Balister, B. Bollobás, A. Sarkar, and S. Kumar. Reliable density estimates for achieving coverage and connectivity in thin strips of finite length. In *International Conference on Mobile Computing and Networking (ACM MobiCom)*, Montreal, Canada, 2007.

[3] S. Bapat, V. Kulathumani, and A. Arora. Analyzing the yield of exscal, a large scale wireless sensor network experiment. In *IEEE International Conference on Network Protocols (ICNP)*, Boston, MA, 2005.

[4] E. M. Belding-Royer. *Routing Approaches in Mobile Ad Hoc Networks*, chapter 10. Mobile Ad Hoc Networking. Wiley-IEEE Press, 2004.

[5] I. Chakeres and C. Perkins. Dynamic manet on-demand routing, Mar. 2006.

[6] J. Elson, L. Girod, and D. Estrin. Fine-grained network time synchronization using reference broadcasts. In *Proceedings of the Fifth Symposium on Operating System Designand Implementation (OSDI)*, pages 147–163, Boston, MA, 2002.

[7] K. Fall. A delay-tolerant network architecture for challenged internets. In *Proceedings of the ACM SIGCOMM*, Karlsruhe, Germany, 2003.

[8] A. Galstyan, B. Krishnamachari, K. Lerman, and S. Pattem. Distributed online localization in sensor networks using a moving target. In *Third International Conference on Information Processing in Sensor Networks (IPSN)*, Berkeley, CA, 2004.

[9] L. Girod, M. Lukac, V. Trifa, and D. Estrin. The design and implementation of a self-calibrating distributed acoustic sensing platform. In *The Fifth ACM Conference on Embedded Networked Sensor Systems (ACM SenSys)*, Boulder, CO, 2006.

[10] P. Gupta and P. R. Kumar. Critical power for asymptotic connectivity in wireless networks. In *IEEE 37th Conference on Decision and Control*, pages 1106–1110, Tampa, FL, 1998.

[11] Z. J. Haas. A new routing protocol for the reconfigurable wireless networks. In *Proceedings of 6th IEEE International Conference on Universal Personal Communications (IEEE ICUPC'97)*, volume 2, pages 562–566, October 1997.

[12] M. Horton, D. E. Culler, K. Pister, J. Hill, R. Szewczyk, and A. Woo. The commercialization of microsensor motes. *Sensors Magazine*, 19(4):40–48, April 2002.

[13] Y.-C. Hu and A. Perrig. A survey of secure wireless ad hoc routing. *IEEE Security & Privacy, special issue on Making Wireless Work*, 2(3):28–39, 2004.

[14] J. W. Hui and D. Culler. The dynamic behavior of a data dissemination protocol for network programming at scale. In *ACM Conference on Ebmedded Networked Sensor Systems (Sensys)*, 2004.

[15] P. Jacquet, P. Mühlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot. Optimized link state routing protocol for ad hoc networks. In *Proceedings of the 5th IEEE Multi Topic Conference (INMIC 2001)*, 2001.

[16] S. Jain, R. C. Shah, W. Brunette, G. Borriello, and S. Roy. Exploiting mobility for energy efficient data collection in wireless sensor networks. *Journal of Mobile Networks and Applications*, 11(3):327–339, 2006.

[17] D. B. Johnson and D. A. Maltz. Dynamic source routing in ad hoc wireless networks. *Mobile Computing*, 353, 1996.

[18] H. Karl and A. Willig. *Protocols and Architectures for Wireless Sensor Networks.* John Wiley & Sons, 2005.

[19] S. Kumar, , T. H. Lai, M. E. Posner, and P. Sinha. Optimal sleep wakeup algorithms for barriers of wireless sensors. In *IEEE BROADNETS*, Durham, NC, 2007.

[20] S. Kumar, T. H. Lai, and A. Arora. Barrier coverage with wireless sensors. In *International Conference on Mobile Computing and Networking (ACM MobiCom)*, pages 284–298, Cologne, Germany, 2005.

[21] S. Kumar, T. H. Lai, and J. Balogh. On k-coverage in a mostly sleeping sensor network. In *International Conference on Mobile Computing and Networking (ACM MobiCom)*, pages 144–158, Philadelphia, PA, 2004.

[22] B. Kusy, P. Dutta, P. Levis, M. Maroti, A. Ledeczi, and D. Culler. Elapsed time on arrival: A simple and versatile primitive for canonical time synchronization services. *International Journal of Ad Hoc and Ubiquitous Computing*, 1(4):239–251, 2006.

[23] B. Kusy, A. Ledeczi, and X. Koutsoukos. Tracking mobile nodes using rf doppler shifts. In *The Fifth ACM Conference on Embedded Networked Sensor Systems (ACM SenSys)*, Sydney, Australia, 2007.

[24] X. Y. Li, P. J. Wan, Y. Wang, and C. Yi. Fault tolerant deployment and topology control in wireless networks. In *International Symposium on Mobile Ad Hoc Networking and Computing (ACM MobiHoc)*, pages 117–28, Annapolis, MD, 2003.

[25] M. Maroti, B. Kusi, G. Simon, and A. Ledeczi. The flooding time synchronization protocol. In *ACM Sensys*, Baltimore, MD, 2004.

[26] A. Mishra and K. M. Nadkarni. Security in wireless ad hoc networks. pages 499–549, 2003.

[27] C. S. R. Murthy and B. S. Manoj. *Ad Hoc Wireless Networks: Architectures and Protocols.* Prentice Hall, 2004.

[28] S. Murthy and J. J. Garcia-Luna-Aceves. An efficient routing protocol for wireless networks. *Mobile Networks and Applications*, 1(2):183–197, 1996.

[29] R. Ogier, F. Templin, and M. Lewis. Topology dissemination based on reverse path forwarding (TBRPF), Feb. 2004.

[30] C. Perkins, E. Belding-Royer, and S. Das. Ad hoc on-demand distance vector (AODV) routing, July 2003.

[31] C. Perkins and P. Bhagwat. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In *ACM SIGCOMM'94 Conference on Communications Architectures, Protocols and Applications*, pages 234–244, 1994.

[32] J. Polastre, J. Hill, and D. Culler. Versatile low power media access for wireless sensor networks. In *ACM Sensys*, 2004.

[33] J. Sallai, B. Kusy, A. Ledeczi, and P. Dutta. On the scalability of routing integrated time synchronization protocol. In *European Workshop on Wireless Sensor Networks (EWSN)*, Zurich, Switzerland, 2006.

[34] P. Santi. The critical transmitting range for connectivity in mobile ad hoc networks. *IEEE Transactions in Mobile Computing*, 4(3):310–317, 2005.

[35] J.-P. Sheu, P.-W. Cheng, and K.-Y. Hsieh. Design and implementation of a smart mobile robot. In *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, volume 3, pages 422–429, Montreal, Canada, 2005.

[36] A. Woo, T. Tong, and D. Culler. Taming the underlying challenges of reliable multihop routing in sensor networks. In *ACM Conference on Ebmedded Networked Sensor Systems (SenSys)*, Los Angeles, CA, 2003.