1

Introduction

This book assumes that the reader has basic knowledge of wireless communications, including different types of wireless links, an understanding of the physical layer concepts, familiarity with medium access control (MAC) layer role, and so on. The reader is also expected to have a grasp of computer networks protocol stack layers, the Open System Interface (OSI) model, and some detailed knowledge of the network layer and its evolution to Internet Protocol (IP) with protocols such as Open Shortest Path First (OSPF) in addition to Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) over IP. Also, some knowledge of topics such as queuing theory is assumed. In the first part of this book, we will review some of these topics in the context of the tactical wireless communications and networking field before we cover the specifics of the field.

One can divide engineers and scientist in the field of tactical wireless communications and networking into two main groups. One group emphasizes the physical layer and dives into topics such as modulation techniques, error control coding at the data link layer (DLL), and the air interface resource management, and so on. The second group emphasizes networking protocols diving into the network layer, the transport layer, and applications. The first group, primarily composed of electrical engineers, likes to build radios assuming that everything above the DLL that has to interface with the radio is commercial-off-the-shelf (COTS). The second group, mostly composed of computer scientists, assumes that everything below the network layer is just a medium for communications. This book will explain tactical wireless communications and networking in a balanced manner, covering all protocol stack layers. This will provide the reader with a complete overarching view of both the challenges and the design concepts pertaining to tactical wireless communications and networking.

The evolution of tactical wireless communications and networks followed a significantly different path from that of commercial wireless communications and networks. A major milestone of tactical wireless communications development occurred in the 1970s, with the move from the old push-to-talk radios to the first spread spectrum and frequency hopping radios (with anti-jamming capabilities). Since World War II, commanders and soldiers on the ground have effectively communicated with radios forming voice broadcast subnets. These subnets, with their small area of coverage, functioned independent of a core network. Over time, the core networks were created to link tactical command nodes to the command-and-control (C2) nodes and then to headquarters. Commanders on the ground carried push-to-talk

Tactical Wireless Communications and Networks: Design Concepts and Challenges, First Edition. George F. Elmasry.

radios to communicate with their soldiers and relied on communications vehicles to link them to their superiors through a circuit switched network with microwave or satellite links. Although enhanced versions of these technologies are still deployed today, this book will consider them as legacy architecture and "a thing of the past." This text focuses on the Global Information Grid (GIG) vision where the tactical theater is full of IP-based subnets that communicate seamlessly to each other with network management policies that enforce the military hierarchy.

1.1 The OSI Model

Every computer networking book, in one way or another, emphasizes the OSI model. The OSI model has its roots in the IBM definitions of networking computers from the early days. Defining such interfaces, while the science of computer networking was a new field, was an effective approach to accelerate the development of networking protocols. With the OSI model, there are different protocol stack layers, with each stack layer performing some predefined functions. These protocol stack layers are separated and utilize standard upward and downward interfaces. These layers work as separate entities and are peered with their corresponding layers in a remote node. Figure 1.1 demonstrates a conventional OSI with seven layers: the application layer, the session layer, the transport layer, the network layer, the DLL, the MAC layer, and the physical layer. These layers communicate to their peer layers (A and B are peer nodes) as shown by the horizontal arrows. Traffic flows up and down the stack, based on well-defined interfaces as indicated by the vertical arrows. Note that some text books may have different variations of these layers. For example, some textbooks may present a presentation layer under the application layer and before the session layer to perform data compression or encryption. Other models (especially for point-to-point links) omit the MAC layer, but we are especially interested in the MAC layer in this book

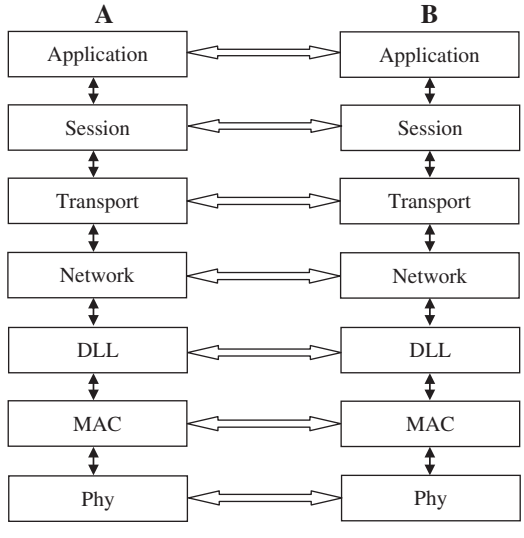

Figure 1.1 Conventional OSI protocol stack layers.

since it is an important part of multiple-access tactical radios. Some models also refer to the IP layer as a network sub-layer. Here, we consider the IP layer as the network layer using IP. Regardless of these variations of the OSI model, the wide use of IP today has created a standard network layer with standard interfaces below it (IP ports to radios, point-to-point links, multiple access wired subnets such as Ethernet, optical links, etc.) and IP ports above clients, servers, voice over IP (VoIP), video over IP, and so on.

Let us summarize the OSI model before we jump into the tactical wireless communications and networking open architecture model. You can refer to other computer networking books to read more about the OSI model details.

The ***application layer*** is simply a software (SW) process that performs its intended application. Your e-mail is a simple example of an application process that runs on your PC or phone (which is essentially a network node).

The ***session layer*** has roots in the plain old telephony (POT) networks where call connection information is given to the transport layer. Today, the session layer could be used for authentication, access rights, and so on.

The ***transport layer*** can be understood as two peer processors (in nodes A and B in Figure 1.1) that perform the following necessary functions:

- Break messages down into packets when transmitting, and reassemble when receiving.
- If the layers below are not reliable (packet loss is encountered), a reliable end-to-end protocol may be utilized by this layer.
- Perform end-to-end flow control. Please refer to TCP flow control as an example of this function.
- Session multiplexing (if there are many low rate sessions between the same node pair), and session splitting if there are high rate sessions going between the same node pair.

The ***network layer*** in the OSI model is ideally a single process per node. As you will see later, this convention changes with the tactical model. This layer performs many tasks including packet-based flow control and routing. A network packet has a payload and a header. The header contains the information needed for this process to perform its intended functions (packet flow control, routing, etc.). Notice that with the layer independence of the OSI model, the header information of the network layer is independent of the header information of the DLL layer. With the OSI model, each layer generates its own header information. The network layer packet (including the header) is treated by the DLL as a set of information that needs to be delivered reliably to the peer processor. Each layer generates its own header based on the information it has, or parameters passed from the adjacent layers. The network layer also generates its own control packets (e.g., Link State Updates–LSUs, route discovery packets, etc.). For the remainder of this book, we will adhere to the convention of referring to the IP layer as the network layer.

The ***data link layer***, also known in some textbooks as the *data link control layer*, is a peer processor that ensures the reliability of the underlying bit pipe. The network layer above can send packets reliably, based on the DLL protocols. The DLL treats the network layer packets as a stream of information bits that need to be transmitted reliably. The DLL adds a header and trailer to the packet received from the network layer, forming a DLL frame. Note that this frame length is not constant since the network layer packets are of variable length. The DLL overhead size (headers and trailers) depends on the error control

coding protocol used. Certain DLL protocols can stop transmission in the presence of errors above a specific threshold. Other DLL protocols may not have error correction capabilities and depend on the reliability of the transport layer. Other DLL protocols may have error detection and/or error correction capabilities. How much reliability should be at the DLL; how much reliability should be at the higher layers of the protocol stack (on a hop-by-hop basis); and how much reliability should be left for the transport layer (for an end-to-end path over the network) is a matter of debate. Network coding is an interesting area of research that you should look at to understand this much-debated topic. Cross layer signaling can also be used to optimize the performance of the protocol stack where the tradeoff between DLL overhead and transport layer overhead needed for reliability can be optimized.

The ***medium access control layer***, or MAC layer, plays a major role in multiple access waveforms. Contrary to point-to-point links, with multiple access waveforms, this layer is responsible for managing the multiple access media. Protocols for collision avoidance (making sure two nodes do not transmit on multiple access media at the same time) are at the heart of the MAC layer. In this book, you will see examples of tactical IP radios where different types of medium control are implemented.

The ***physical layer*** transmits a sequence of bits over the physical channel. There are many physical media used today ranging from your cable/digital subscriber line (DSL) modem at home to your cellular phone, Ethernet cable, and optical media. Each medium has its modulation/demodulation technique that maps a bit or a sequence of bits to a signal. Notice that the bit stream from a MAC frame has to be transmitted in a synchronous manner since each bit needs a specific time duration t to be transmitted. The medium's speed or rate in bits per second is $1/t$. The MAC layer emits bits to the physical layer at this rate. Intermit periods between MAC frames (when the MAC layer has no information to send) means that the channel is idle for these periods. Before IP became the standard for the network layer, each physical media needed a MAC or DLL layer that could interface to it, and standardization was a nightmare. Now, we have IP-based modems that can interface to an IP port. IP is the gold standard and should stay with us for a long time. As you will see in the rest of this book, we approach the open architecture for tactical wireless communications and networking as IP-based and thus can bring a wide variety of technologies to the war theater, making them communicate seamlessly.

The OSI concept allowed the science of computer networking to evolve quickly, since the separated entities meant that engineers could focus on developing the layers of their specialties without having to worry about defining interfaces to upward or downward layers. Computer networking relies on this model with some changes.

1.2 From Network Layer to IP Layer

With the IP model, the community has established a five-layer model as shown in Figure 1.2, with the application layer, transport layer, IP layer, DLL/MAC layer, and the physical layer. In addition to the reduction of the OSI layers from seven to five layers, this model refers to the IP as "layer 3" and the DLL/MAC "layer 2" while the physical layer is layer 1.

Notice that the relationship between the network layer and the DLL/MAC is one-to-many. The network layer can send and receive packets from multiple DLL layers (links). This concept evolved with Internet Protocol to become an IP port. An IP router can also have ports dedicated to multiple workstations, servers, and so on, each with its own transport

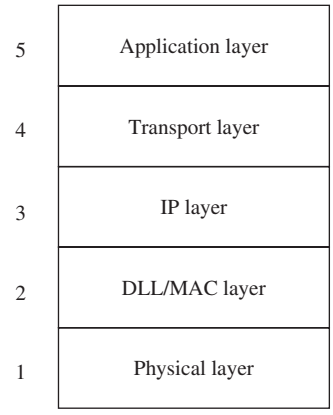

Figure 1.2 The IP as the network layer with a five-layer OSI model.

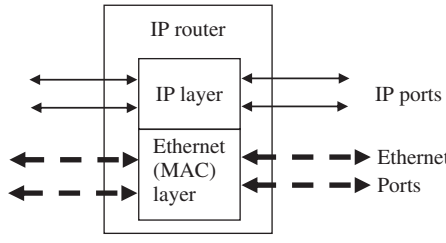

Figure 1.3 IP routers with IP and Ethernet ports.

and session layers. As we dive into tactical networks learning about the tactical edge, we will debate the benefits of relying on the transport layer for reliability versus relying on the tactical edge IP layer, where aggregation of traffic allows us to exploit the benefits of statistical multiplexing in achieving reliability. You will also learn about addressing reliability at the transport layer, tactical edge, DLL, and/or through network coding. You will also be introduced to cross layer signaling through this five-layer model. You will see why IP-based tactical radios can have some layer 3 capabilities with rich cross layer signaling to layer 2.

Figure 1.3 shows a conceptual view of an IP router with both IP ports and Ethernet (MAC) ports. With this naming convention, a workstation carrying a client or a server can be Ethernet-based and can connect to an Ethernet port in a router or a switch. IP-based tactical radios can connect to an IP port. Although the peering of the protocol stack layers still applied to the IP-based model in Figure 1.2, the IP layer is the focal point of this protocol stack model and IP route discovery can be of a client/server, a wired subnet, a wireless subnet, and so on.

1.3 Pitfall of the OSI Model

The literature is full of criticism of the OSI model and any of its deviations including the IP model. The fact of the matter is that IP technology is now the dominating technology

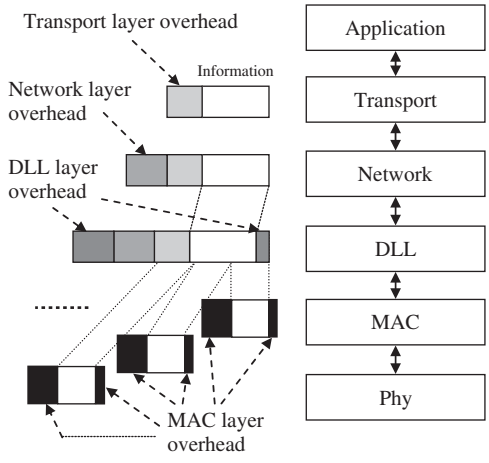

Figure 1.4 Overhead with the OSI stack layers.

and it is with us to stay. Techniques such as cross layer signaling, merging of protocol stack layers (especially layers 2 and 3), tradeoffs between network coding, and transport layer reliability are the path to more optimal performance of both commercial and tactical wireless communications based on the IP model. The attempts to develop a new technology or a super-layer concept are facing many challenges and could take a very long time to materialize, given the dominance of IP. One of the known problems with the OSI model is the amount of overhead bits transmitted over the physical media in comparison to the information bits. Since each layer works independently with its own headers, the ratio of overhead to information contents can be very high. Figure 1.4 demonstrates this problem where the information content in the packet (at the transport layer) is expressed by the white rectangle. The transport layer adds its own header(s) shown in light gray (think of UDP and RTP–real-time protocol–headers or the TCP header). The network layer adds its own header, shown in the medium gray (consider the IP header). The DLL treats the entire packet (information and headers) as a bit stream and adds its own overhead that may contain redundancy bits for error correction, as well as trailers, as expressed in the dark gray portion. The DLL also breaks down the bit stream corresponding to the packet (payload and headers) into small segments (to create MAC frames) with the MAC layer adding its own MAC header and trailers shown in black, and so on. Especially with small payload packets (such as VoIP), the ratio of information bits to the actual bits modulated over the air could be very small.

If you consider the accumulative amount of overhead bits compared to the information bits (for each packet that is carrying application-layer information) and that network protocols at the different stack layers generate their own overhead packets (control packets), you will see how inefficient the OSI model is. Control traffic comes from protocols such as session initiation and session maintenance, negative and positive acknowledgment, and so on. The IP layer introduces a large amount of overhead from routing protocols. Consider Hello packets, links state database (LSD) packets, LSU packets, and so on. In tactical

mobile ad hoc networking (MANET), as the number of nodes per subnet increases, this control traffic volume increases, and considering that some links and radios have limited bandwidth, the ratio of control traffic to user traffic can get extremely high and further increase the inefficiency of the OSI model. Moreover, because of the unreliable nature of tactical wireless links, redundancy packets from error control coding such as network coding can further decrease the available bandwidth resources for user traffic.

1.4 Tactical Networks Layers

The OSI model does not apply directly to the tactical networks for many reasons to include security and information assurance requirements. It is the US National Security Agent (NSA) that defines the Communications Security (ComSec) standards for IP-based networking. NSA defines the High Assurance Internet Protocol Encryption (HAIPE) as the standard for IP-based encryption. Notice that HAIPE differs from commercial Internet Protocol Security (IPSec) in many ways including hardware separation of the plain text IP layer and the cipher text IP layer. HAIPE is the GIG ComSec encryption. Notice also that coalition forces may be required to adhere to a form of ComSec similar to HAIPE. The introduction of ComSec in tactical networks creates two network layers at each node. One is the plain text network layer (sometimes referred to as the red IP layer) and the other is the cipher text network layer (sometimes referred to as the black IP layer) separated by the encryption layer. As will become clear later in this book, the plain text networks are separated from the cipher text core network, creating two independent networking layers. If we take the OSI model in Figure 1.1 and try to create a tactical networks equivalent, we would need to introduce some modification to include ComSec as a layer by itself since HAIPE standards require the plain text and cipher text IP layers to work independently, as separate entities. Also, in a tactical wireless networking protocol stack model, one would need to consider a form of cross layer signaling where control signaling between the stack layers is allowed. Cross layer signaling is covered later in this book where we show how ComSec introduces more complexity to the cross layer approach of tactical networks.

With IP-based tactical wireless communications and networks, as you will see in subsequent chapters, the physical, MAC, and DLL layers form what we will refer to as the radio. The network layer plays a major role on top of the radio with ComSec encryption creating two independent IP layers. Figure 1.5 shows the mapping of the OSI model to the tactical networks model. Notice that the radio implementation of the DLL and MAC layer can have a different mutation specific for each tactical or commercial radio. Also notice the presence of plain text IP and cipher text IP as two independent layers separated by ComSec encryption.

With the model shown in Figure 1.5, COTS-based IP routers can interface to a tactical radio that has IP ports and has an IP layer that peers to the IP layer of the router. COTS-based IP routers can also interface to tactical links that have a simple IP modem. In either case, we will refer to the layers below the IP layer as the radio, to maintain consistency and to present tactical wireless networking in an open architecture theme.

The remainder of the first part of this book will cover some of the important theoretical bases for each of the tactical networks stack layers modeled in Figure 1.5. These theoretical

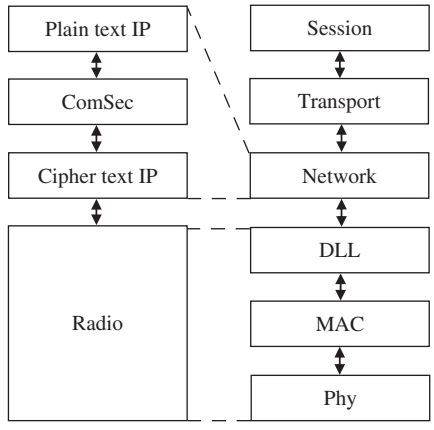

Figure 1.5 Mapping of the OSI to the tactical networks stack layers.

bases are presented in the context of tactical MANET, explaining the challenges and design concepts of tactical wireless communications and networks.

1.5 Historical Perspective

One can argue that computer networking has its roots in the T-carrier system developed by Bell Labs in the 1960s for digital telephony. The term integrated services digital network (ISDN) was coined when a worldwide telephone network was developed. Following IBM's introduction of the OSI concept, many proprietary networking techniques started to appear. The DARPA NET project was a major breakthrough in linking computers, not only the telephone sets. This project then turned into the Internet, and IP began taking root. Now, the tactical communications and networking field is in the path to be completely IP-based. The vision of the global information grid reaching the tactical theater requires that a network of networks should offer seamless communications to the warfighter anywhere in the world, and IP was selected to be the way forward for this vision. Today, the war theater could potentially be full of sensors, robots, unmanned vehicles, and so on. Also, there is a new generation of warfighters who are from the information age and are used to texting and sending images and short video clips. In addition, there is an explosion of potential applications that can aid the warfighter in his mission. All these factors created the need for greater capacity in the tactical theater and the need for seamless communications between the different subnets, leading to a new generation of tactical radio such as the Joint Tactical Radio System (JTRS) radios and the research in cognitive radios, as well as exploring the use of commercial wireless technologies in the tactical theater. This opens the door for tactical wireless communications and networking to utilize an open architecture approach. One can expect, as time goes by, that the boundaries between tactical and commercial wireless research topics to gradually lessen to where both communities are interested in cognitive radios, cross layer signaling, layer merging, the role of network coding, and so on.

Bibliography

1. Bertsekas, D. and Gallager, R. (1994) *Data Networks*, 2nd edn, Prentice Hall.
2. Schwartz, M. (1987) *Telecommunication Networks Protocols, Modeling and Analysis*, Addison-Wesley.
3. Tanenbaum, A. (1996) *Computer Networks*, 3rd edn, Prentice Hall.
4. Elmasry, G. (2010) A comparative review of commercial vs. tactical wireless networks. *IEEE Communications Magazine*, **48**, 54–59.
5. Lee, J., Elmasry, G., and Jain, M. Effect of security architecture on cross layer signaling in network centric systems. Proceedings of Milcom 2008, NC9-3.
6. Elmasry, G. and D'Amour, C. Abstract simulation for the GIG by extending the IP cloud concept. Proceedings of Milcom 2005, U503.