Mobile Ad Hoc Network Application and Security

Sawsan Abd Al-Hady Mahmood

Abstract

One of the important types of networks is the ad hoc network. In this network the communications nodes don't necessary rely on a fixed infrastructure. Thus, the ad hoc network used in difficult and special environment when we can not use the fixed infrastructure networks. This research will present most important application and special approach security of ad hoc network.

1. Introduction:

In the last few years we have seen the proliferation of wireless communications technologies. Wireless technologies are being widely used today a cross the globe to support the communications needs of very large numbers of end users. There are over1 billion wireless subscribers of cellular services today utilizing wireless devices for voice communications (e.g. phone calls) and data services. Data services include activities such as sending e-mail and instant messages, and accessing the Web. In fact, in some are as of the world wireless technologies are more prevalent than traditional wire line communications technologies.

The wireless technologies themselves have improved tremendously, making it possible to offer both voice and data services over such networks. The resulting allure of anytime, anywhere services makes such services very attractive for the end users.

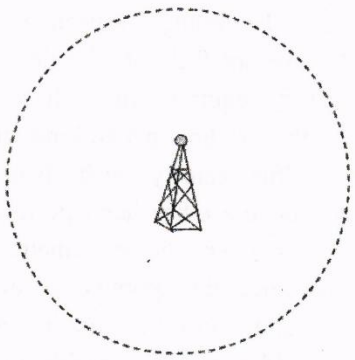
An ad hoc network is a collection of nodes that do not need to rely on a predefined infras- tructure to keep the network connected. Ad hoc networks can be formed, merged together or partitioned into separate networks on the fly, without necessarily relying on a fixed infrastructure to manage the operation. Nodes of ad hoc networks are often mobile, which also implicates that they apply wireless communication to maintain the connectivity, in which case the networks are called as mobile ad hoc networks (MANET). Mobility is not, however, a requirement for nodes in ad hoc networks, in ad hoc networks there may exist static and wired nodes, which may make use of services offered by fixed infrastructure.

As ad hoc networking somewhat varies from the more traditional approaches, the security aspects that are valid in the networks of the past are not fully applicable in ad hoc networks. While the basic security requirements such as confidentiality and authenticity remain, the ad hoc networking approach somewhat restricts the set of feasible security mechanisms to be used, as the level of security and on the other hand performances are always somewhat related to each other. The performance of nodes in ad hoc networks is critical, since the amount of available power for excessive calculation and radio transmission are constrained, as discussed e.g. in. In addition, the available bandwidth and radio frequencies may be heavily restricted and may vary rapidly. Finally,

as the amount of available memory and CPU power is typically small, the implementation of strong protection for ad hoc networks is non-trivial.

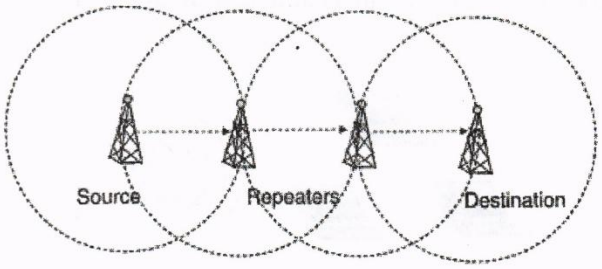
2. Definition of Wireless Ad Hoc Networks:

In wireless networks, nodes transmit information through electromagnetic propagation over the air. The signal transmitted by a node can only be received by nodes that are located within a specific distance from the transmitting node. This distance is typically called the transmission range. The transmission range depends not only on the power level used for the transmission, but also on the terrain, obstacles, and the specific scheme used for transmitting the information. Typically, for simplicity, the transmission range of nodes is assumed to be a circle around the transmitting node, as shown in (Figure1) [1].



(Figure1) Transmission range.

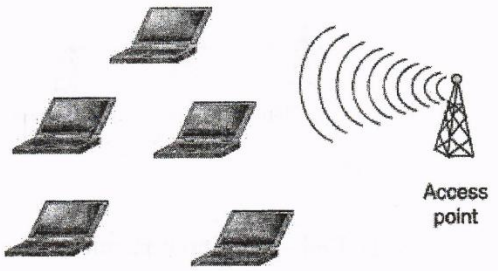
Nodes might need to communicate with other nodes that are out side their transmission range. This is typically accomplished by having other nodes that are within the transmission range of the transmitting node receive and then retransmit the signal. As a result of this retransmission, nodes within transmission range of the node repeating the original signal receive the data. Depending on the location of the destination, multiple nodes may need to retransmit/repeat the data, as shown in (Figure 2).



(Figure 2) End – to - End transmissions.

The general wireless networks are dependent on fixed nodes (the radio towers and access points) for connecting the mobile nodes as shown in (Figure 3). In addition, these networks require some fixed infrastructure to interconnect the fixed nodes with each other. This type of architecture has been very successful and widely deployed throughout the world for offering a variety of voice and data services, despite being inflexible (by requiring fixed nodes). This is because the architecture has been sufficient for services typically offered by service providers.

Having a communications network that relies on a fixed infrastructure, however, is not always acceptable for some applications for example, when emergency responders move into an area (say to deal with a disaster), it is possible that the fixed infra structure may have been destroyed or may be unavailable(e.g. in some remote areas). Emergency responders might not have enough time to establish a fixed infrastructure in such cases. A similar situation might also arise in a battlefield environment.



(Figure 3) Typical architecture of wireless network

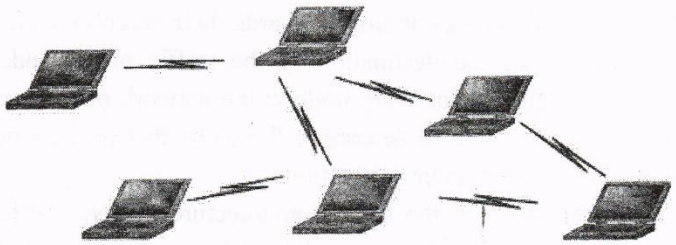
In the past few years, a new wireless architecture has been introduced that does not rely on any fixed infrastructure. In this architecture, all nodes may be mobile and no nodes play any special role. One example of this architecture is the "ad hoc" architecture of as shown in (Figure 4).In this architecture nodes do not rely on

access points to communicate with each other. In fact, nodes reach other nodes they need to

Communicate with using their neighbors. Nodes that are close to each other discover their neighbors. When a node needs to communicate with another node, it sends the traffic to its neighbors and these neighbors pass it along towards their neighbors and soon. This repeats until the destination of the traffic is reached. Such architecture requires that every node in the network play the role of a router by being able to determine the paths that packets need to take in order to reach their destinations.

Networks that support the ad hoc architecture are typically called wireless ad hoc networks or mobile ad hoc networks (MANET). Such networks are typically assumed to be self forming and self healing. This is because the typical applications of such networks require nodes to form networks quickly without any human intervention. Given the wireless links and mobility of nodes, it is possible that nodes may lose connectivity to some other nodes. This can happen if the nodes move out of each other's transmission range. As a result, it is possible for portions of the network to split from other portions of the network. In some applications it is also possible that some nodes may get completely disconnected from the other nodes, run out of battery, or be destroyed. For these reasons, nodes in a MANET can not be configured to play any special role either in the way nodes communicate or in the way of providing communication services (e.g. naming services). This leads to a symmetric architecture where each node shares all the responsibilities. The network needs to be able to reconfigure itself

quickly to deal with the disappearance (or reappearance) of any node and continue operating efficiently without any human intervention [1].



(Figure 3) Ad hoc architecture

In this section we discussed the concept of MANET. We will discuss the application that have motivated of the research on MANETs and are well suited for there use.

3. Application of Mobile Ad hoc Networks:

The MANETs can be used in several cases depending on the application that we need. These networks may be very different from each other, depending on the area of application such as (education, industrial, commercial, emergency and military). The most applications can be shown as follow:

1. **Education (classroom communication):** for instance in a computer science classroom an ad hoc network could be formed between students' PDA's and workstation of the teacher [2].

2. **Sensors communication:** The widely considered application for MANETs is interconnection of sensors in an industrial, commercial setting. Sensors are typically small devices measuring environmental inputs (such as temperature, motion, light, etc.)and often alerting users and/or taking specific reactions(e.g. starting an air-conditioner)when those inputs reach specific ranges. Sensors have been used extensively in industrial applications and even for applications inside the home(such as in security systems, heating systems, etc.) [1].
3. **Emergency response:** During major emergencies and disasters such as hurricanes or large explosions, the communications infrastructure in the immediate area of the disaster or emergency may be unusable, unavailable, or completely destroyed. When emergency responders' first arrive in the disaster-struck area, it is critical for them to be able to communicate with each other. The communications make it possible for the team to coordinate the relief operations with each other. Since the communication infrastructure is often unavailable, first responders need to be able to establish connectivity immediately. MANETs are well suited for such an application because of their ability to create connectivity rapidly with limited human effort [3].
4. **Battlefield communication:** the most widely considered application of a MANET is battlefield communications. The Department of Defense (DoD) future transformation is based on a key initiative called Network Centric Warfare (NCW). It is expected that there will typically be a large number of

nodes in the battlefield environment that need to be interconnected, including radios carried by soldiers, and radios mounted on vehicles, missiles, unattended air vehicles(UAV), and sensors. In such an environment the network plays a critical role in the success of the military mission.The vast majority of these nodes move around at varying speeds and nodes may lose connectivity to other nodes as they move around in the battlefield because of the terrain(e.g. obstacles may prevent line of sight),distance among the nodes, and soon. Because of the rapid pace and the large degree of unpredictability it is not possible to assume a fixed infrastructure in the battlefield environment. Network administrators have little time to react and reconfigure the networks [1].

4. When MANET Need The Security:

The application areas of ad hoc network are different from each other. Some of these applications work with friendly environment. Thus, the mobile devices not need the special security requirement. Other hand the some application work with hostile environment. In this environment the mobile devices must be need to special security requirement.

There are two different scenarios to explain when we need the special security requirements [6]:

For instance in a computer science classroom an ad hoc network could be formed between students' PDAs and the workstation of the teacher. In another scenario a group of soldiers is operating in a hostile environment, trying to keep their presence and mission

totally unknown from the viewpoint of the enemy. The soldiers in the group work carry wearable communication devices that are able to eavesdrop the communication between enemy units, shut down hostile devices, divert the hostile traffic arbitrarily or impersonate themselves as the hostile parties. As can obviously be seen, these two scenarios of ad hoc networking are very different from each other in many ways: In the first scenario the mobile devices need to work only in a safe and friendly environment where the networking condition is predictable. Thus no special security requirements are needed. On the other hand, in the second and rather extreme scenario the devices operate in an extremely hostile and demanding environment, in which the protection of the communication and the mere availability and operation of the network are both very vulnerable without strong protection.

5. Security For Mobile Ad Hoc Network:

All nodes in any network need to be able to communicate securely with each other. The existence of secure communication channels is especially crucial in MANETs on account of the use of wireless links and other characteristics of such networks. These channels are required form any operations such as exchanging data or exchanging control packets in the case of functions like routing. To make such secure communication possible, it is necessary for nodes to have access to the proper keying material. This is the objective of the key management process. This has lately been a very active area of research in ad hoc networks.

5. 1 Ad Hoc Physical Security:

In ad hoc networks especially mobile nodes are typically significantly more susceptible to physical attacks than wired nodes in traditional networks. However, the significance of the physical security in the overall protection of the network is highly dependent on the ad hoc networking approach and the environment in which the nodes operate. For instance in ad hoc networks that consist of independent nodes and work in a hostile battlefield the physical security of single nodes may be severely threatened. Therefore in such scenarios the protection of nodes cannot rely on physical security. In contrary, in the classroom example scenario the physical security of a node is an important issue to the owner of the node, perhaps for privacy reasons, but the breaking of the physical security does not affect the security of the system as such [4].

5. 2 Key Management with Ad Hoc Security:

The importance of key management can not be over emphasized for both traditional and ad hoc networks. When employing cryptographic schemes, such as encryption or digital signatures, to protect both control and data traffic, a key management service is always required. For secure communication between any two entities, both the entities should possess a secret value or key. The possible ways in which secure communication can be established are for the entities concerned to share a key (symmetric-key system) or for the entities concerned to possess different keys (asymmetric-key system). Key management is the process by which those keys are distributed to nodes on the network and how they are further updated if required, erased, and soon.

There are several steps that key management has to be concerned with for both symmetric key systems as well as asymmetric key systems. These include [5]:

1. Initializing the system users.
2. Creating, distributing and installing the keying material.
3. Organizing the use of the keying material.
4. Updating, revoking, and destroying the keying material.
5. Archiving the keying material.

Key management in ad hoc networks, however, is more difficult than in traditional networks. This is because of several factors, such as the vagaries of wireless links, lack of a central authority, constraints on resources such as power, memory, and bandwidth availability, and the inability to predetermine the neighbors of a node after deployment, which is further worsened on a ccount of the mobility of nodes in such networks [6].

5.3 Access control:

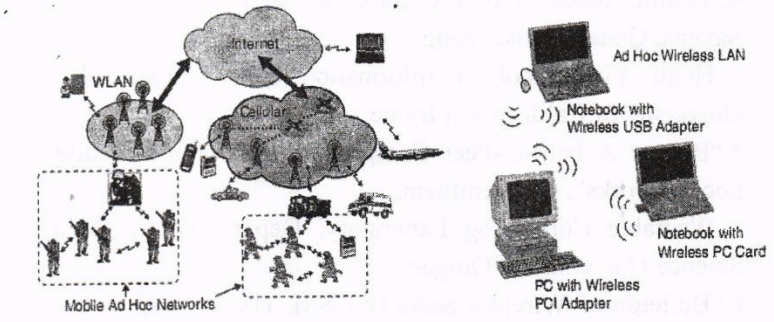
Access control consists of the means to govern the way the users or virtual users such as operating system processes (subjects) can have accesses to data (objects). In networking, access control can e.g. involve the mechanisms with which the formation of groups of nodes is controlled. Only authorized nodes may form, destroy, join or leave groups. Access control can also mean the way the nodes log into the networking system to be able to communicate with other nodes when initially entering the network. There are various approaches to the access control: Discretionary Access Control (DAC) offers the means for defining the access control to the users themselves. DAC allows the restriction of access to objects

based on the identity of subjects or groups of subjects. Mandatory Access Control (MAC) involves centralized mechanisms to control the access to objects with formal authorization policy. DAC and MAC are often applied together so that DAC allows the system user subjects to control access of other subjects, while MAC controls and restricts the operation of DACs in the system in general. This kind of approach prevents the system from failures generated by the actions of careless users. Finally, Role Based Access Control (RBAC) applies the concept of roles within the subjects and objects. In RBAC systems subjects can have several roles of which one is at a time active and therefore the accesses to objects are defined with respect to roles, not subjects. As stated in [4], RBAC does not necessarily involve the controlling of access to information only, but also the restriction of access to functions within the system. Thus roles are group-oriented sets of transactions associated to roles that the specific users can perform to given objects. For example, in banking applications using RBAC users with different roles may have the same set of accesses to the same objects as such, only with different limits in the amount of transferable money. In DAC and MAC systems these kind of definitions could not be directly be applied [2, 3].

6. Discussion:

The term Mobile Ad hoc NETworks (MANETs) refers to ad hoc networks in which the nodes forming the ad hoc network are mobile. Most ad hoc networks allow their nodes to be mobile and are therefore MANETs.

In other words, these networks are formed on an as-needed basis and do not require the existence of any infrastructure. This property makes ad hoc wireless networks suitable for use in various scenarios like disaster recovery, enemy battlefields or in areas where user density is too sparse or too rare to justify the deployment of network infrastructure economically. (Figure 4) shows some examples of ad hoc wireless networks.



(Figure 4) Examples of Ad Hoc Networks

Ad hoc networks have two major limitations:

a) There are no dedicated routing devices (since there is no infrastructure available)

b) The network topology may change rapidly and unpredictably as nodes move.

In the absence of any routing infrastructure, the nodes forming the ad hoc networks themselves have to act as routers. A MANET may therefore be defined as an autonomous system of mobile routers (and

associated hosts) connected by wireless links the union of which forms an arbitrary graph.

References:

1. "Security for Wireless Networks", Farooq Anjum and Petros Mouchtaris, wiley 2007.

2. "Security in Ad Hoc Networks", vesa karpijoki, Hut Tml 2000.

3." Securing Ad Hoc Networks", LidongZhou, Department of Computer Science, ZygmuntJ.

Haas, School of Electrical Engineering CornellUniversity,

4."Identity-based Access Control for Ad Hoc Groups", Nitesh Saxena, Gene Tsudik, Jeong

Hyun Yi, School of Information and Computer Science University of California at Irvine.

5."Proem: A Peer-to-Peer Computing Platform for Mobile Ad-hoc Networks", GerdKortuem,

Wearable Computing Laboratory, Department of Computer Science University of Oregon.

6."Bulletproof Wireless Security GSM, UMTS, 802.11 and Ad Hoc Security", Praphul

Chandra, Elsevier 2005.