Methodology and Challenges of Mobile Adhoc Networks and Types of Attack

Krishan kumar
Ph D (CSE) Research Scholar, Singhania University
Pacheri bari (jhunjhunu) Rajasthan, India

Abstract: in this research paper we will discuss about the proliferation of mobile computing and communication devices (e.g., cell phones, laptops, handheld digital devices, personal digital assistants, or wearable computers) is driving a revolutionary change in our information society. We are moving from the Personal Computer age (i.e., a one computing device per person) to the Ubiquitous Computing age in which a user utilizes, at the same time, several electronic platforms through which he can access all the required information whenever and wherever needed.

Keywords: GPS, static networks, network simulation and security attacks.

I. Introduction and objective of Research Work

A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic.

Such networks may operate by themselves or may be connected to the larger Internet.

MANETs are a kind of wireless ad hoc networks that usually has a routeable networking environment on top of a Link Layer ad hoc network. They are also a type of mesh network, but many mesh networks arenot mobile or not wireless.

The growth of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid- to late 1990s. Many academic papers evaluate protocols and abilities assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other and usually with nodes sending data at a constant rate. Different protocols are then evaluated based on the packet drop rate, the overhead introduced by the routing protocol, and other measures.[1]

II. Review of Literature

The nature of ubiquitous devices makes wireless networks the easiest solution for their interconnection and, as a consequence, the wireless arena has been experiencing exponential growth in the past decade. Mobile users can use their cellular phone to check e-mail, browse internet; travelers with portable computers can surf the internet from airports, railway stations, Starbucks and other public locations; tourists can use Global Positioning System. (GPS) terminals installed inside rental cars to locate driving maps and tourist attractions, researchers can exchange files and other information by connecting portable computers via wireless LANs while attending conferences; at home, users can synchronize data and transfer files between portable devices and desktops.

In present time In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad

Hoc Networks. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes.

The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs. Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. Military networks are designed to maintain a low probability of intercept and/or a low probability of detection. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of the network.[2]

III. METHODOLOGY

The specific MANET issues and constraints described above pose significant challenges in ad hoc network design. A large body of research has been accumulated to address these specific issues, and constraints. In this paper, we describe the ongoing research activities and the challenges in some of the main research areas within the mobile ad hoc network domain. To present the huge amount of research activities on ad hoc networks in a systematic/organic way, we will use, as a reference, the simplified architecture shown in Fig. 2.

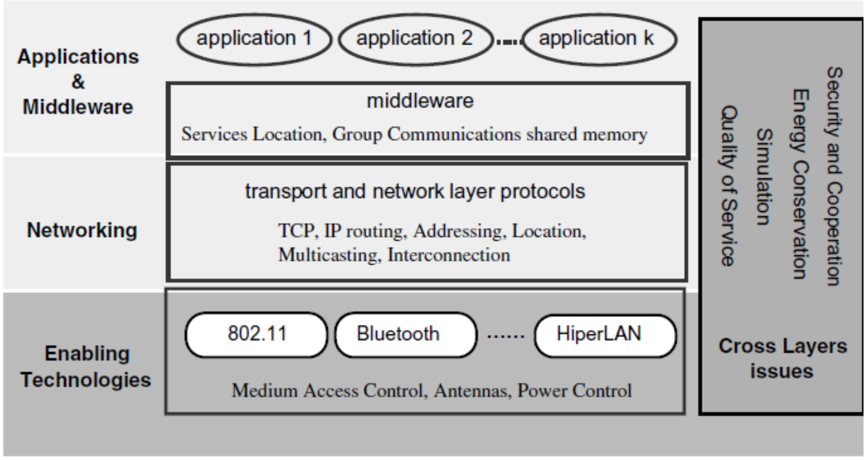
Applications & Middleware
application 1
application 2
application k
middleware
Services Location, Group Communications shared memory
Networking
transport and network layer protocols
TCP, IP routing, Addressing, Location, Multicasting, Interconnection
Enabling Technologies
802.11
Bluetooth
HiperLAN
Medium Access Control, Antennas, Power Control
Security and Cooperation
Energy Conservation
Simulation
Quality of Service
Cross Layers issues

Fig. 2. A simple MANET architecture.

As shown in the figure, the research activities will be grouped, according to a layered approach into three main areas:

- Enabling technologies;
- Networking;
- Middleware and applications.

In addition, as shown in the figure, several issues (energy management, security and cooperation, quality of service, network simulation) span all areas, and we discuss them separately.

IV. Enabling technologies

As shown in Fig. 3, we can classify ad hoc networks, depending on their coverage area, into several classes: Body (BAN), Personal (PAN), Local (LAN), Metropolitan (MAN) and Wide (WAN) area networks. Wide- and Metropolitan-area ad hoc networks are mobile multi-hop wireless networks that present many challenges that are still to be solved (e.g., addressing, routing, location management, security, etc.), and their availability is not on immediate horizon. On the other hand, mobile ad hoc networks with smaller coverage can be expected to appear soon. Specifically, ad-hoc singlehop BAN, PAN and LAN wireless technologies are already common on the market [3], these technologies constituting the building blocks for constructing small, multi-hop, ad hoc networks that extend their range over multiple radio hops. For these reasons, BAN, PAN and LAN technologies constitute the Enabling technologies for ad hoc networking. A detailed discussion of Body, Personal, and Local Ad hoc Wireless Net works

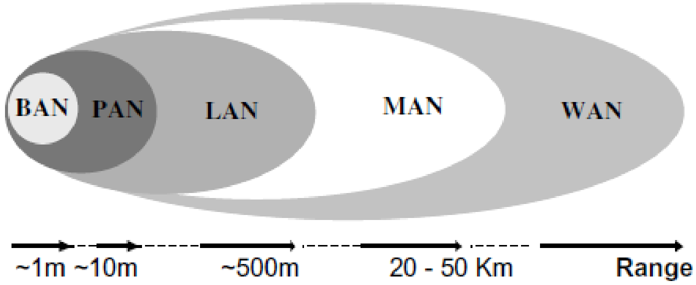

Fig. 3. Ad hoc networks taxonomy.

can be found in [3]. Hereafter, the characteristics of these networks, and the technologies available to implement them, are summarized. A body area network is strongly correlated with wearable computers. A wearable computer distributes on the body its components (e.g., headmounted displays, microphones, earphones, etc.), and the BAN provides the connectivity among these devices. The communicating range of a BAN corresponds to the human body range, i.e., 1–2 m. As wiring a body is generally cumbersome, wireless technologies constitute the best solution for interconnecting wearable devices. Personal area networks connect mobile devices carried by users to other mobile and stationary devices. While a BAN is devoted to the inter-connection of one-person wearable devices, a PAN is a network in the environment around the persons. APAN communicating range is typically up to 10 m, thus enabling the interconnection of the BANs of persons close to each other, and the interconnection of a BAN with the environment around it.

The most promising radios for widespread PAN deployment are in the 2.4 GHz ISM band. Spread spectrum is typically employed to reduce interference and bandwidth re-use. Wireless LANs (WLANs) have a communication range typical of a single building, or a cluster of buildings, i.e., 100–500 m. A WLAN should satisfy the same requirements typical of any LAN, including high capacity, full connectivity among attached stations, and broadcast capability. However, to meet these objectives, WLANs need to be designed to face some issues specific to the wireless environment, like security on the air, power consumption, mobility, and bandwidth

Limitation of the air interface. Two different approaches can be followed in the implementation of a WLAN: an infrastructure based approach, or an ad hoc networking one [4]. An infrastructure-based architecture imposes the existence of a centralized controller for each cell, often referred to as Access Point. The Access Point (AP) is normally connected to the wired network, thus providing the Internet access to mobile devices. In contrast, an ad hoc network is a peer to-peer network formed by a set of stations within the range of each other, which dynamically configure themselves to set up a temporary network. In the ad hoc configuration, no fixed controller is required, but a controller may be dynamically elected among the stations participating in the communication. The success of a network technology is connected to the development of networking products at a competitive price. A major factor in achieving this goal is the availability of appropriate networking standards. Currently, two main standards are emerging for ad hoc wireless networks: the IEEE 802.11 standard for WLANs [5], and the Bluetooth specifications [5] for short-range wireless communications [15,40,179]. Due to its extreme simplicity, the IEEE 802.11 standard is a good platform to implement a singlehop WLAN ad hoc network. Furthermore, multihop networks covering areas of several square kilometers can potentially be built by exploiting the IEEE 802.11 technology. On a smaller scale, technologies such as Bluetooth can be used to build ad hoc wireless Body, and Personal Area Networks, i.e., networks that connect devices on the person, or placed around him inside a circle with radius of 10 m.

In addition to the IEEE standards, the European Telecommunication Standard Institute (ETSI) has promoted the HiperLAN (HIgh Performance Radio Local Area Network) family of standard for WLANs. Among these, the most interesting standard for WLAN is HiperLAN/2. The HiperLAN/2 technology addresses high-speed wireless network with data rates ranging from 6 to 54 Mbit/s. Infrastructure-based and ad hoc networking configurations are both supported in HiperLAN/ 2. To a large degree, HiperLAN is still at the prototype level, and hence we will not consider it more in detail. More details on this technology can be found in. [6] surveys the off-the-shelf technologies for constructing ad hoc networks; while [4] presents an in depth analysis of 802.11-based ad hoc networks, including performance evaluation and some of the open issues. The ad hoc network size in terms of the number of active nodes is the other metric used to classify MANETs. As defined in [181], we can classify the scale of an ad hoc network as small-scale (i.e., 2–20 nodes), moderate-scale (i.e., 20–100 nodes), largescale (i.e., 100+ nodes), and very large-scale (i.e., 1000+ nodes). In [107], it was shown that in anad hoc network with n nodes the per-node throughput is bounded by $c/\sqrt{n},$, where c is a constant. Unfortunately, experimental results [104] indicate that with current technologies the pernode throughput decays as $c'/n^{1.68}$, and hence, with current technologies only small- and moderate- scale can be implemented in an efficient way.

V. TYPES OF ATTACKS

5.1. External vs. Internal attacks

External attacks, in which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services. Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors. The security attacks in MANET can be roughly classified into two major categories, namely passive attacks and active attacks are as described in the figure 1.The active attacks further divided according to the layers.

5.2 Passive Attacks

A passive attack does not disrupt the normal operation of the network; the attacker snoops the data exchanged in the network without altering it. Here the requirement of confidentiality gets violated. Detection of passive attack is very difficult since the operation of the network itself doesn't get affected. One of the solutions to the problem is to use powerful encryption mechanism to encrypt the data being transmitted, there by making it impossible for the attacker to get useful information from the data overhead.

5.3. Active Attacks

An active attack attempts to alter or destroy the data being exchanged in the network there by disrupting the normal functioning of the network. Active attacks can be internal or external. External attacks are carried out by nodes that do not belong to the network. Internal attacks are from compromised nodes that are part of the network. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation, modification, fabrication and replication.

VI. CONCLUSION

In the end of research paper In this survey paper, we try to inspect the security threats in the mobile adhoc networks, which may be a main disturbance to the operation of it. Due to nature of mobility and open media MANET are much more prone to all kind of security risks as covered. As a result, the security needs in the MANET are much higher than those in the traditional wired networks. During the survey, we also find some points that can be further explored in the future, such as to find some effective security solutions and protect the MANET from all kinds of security risks. We will try to explore deeper in this research area.

REFERENCES

[1] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication," International Journal of Computer Science and Security (IJCSS) Volume: 4 Issue: 3.
[2] Sukla Banerjee , "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks", Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.
[3] M. Conti, Body, personal, and local wireless ad hoc networks, in: M. Ilyas (Ed.), Handbook of Ad Hoc Networks, CRC Press, New York, 2003 (Chapter 1)..
[4] W. Stallings, Local & Metropolitan Area Networks, Prentice Hall, Englewood Cliffs, NJ, 1996..
[5] Web site of the IEEE 802.15 WPA.N Task Group 1: http://www.ieee802.org/15/pub/TG1.html..
[6] G. Zaruba, S. Das, Off-the-shelf enablers of ad hoc networks, in: S. Basagni, M. Conti, S. Giordano, I. Stojmenovic (Eds.), Ad Hoc Networking, IEEE Press Wiley, New York, 2003.