Survey Paper

Volume 1 / Issue 1 / 2012

Available Online at
www.lbrce.ac.in/ijcc/

IJCC Volume I/Issue 1/2012

Print-ISSN 2319 – 8869
Online-ISSN 2319 – 894X

An Overview of Emerging Technologies & Security Issues in Mobile Ad Hoc Networks

S.Phani Praveen*, T.Bala Murali Krishna#

** CSE Dept., PVP Siddhartha Institute of Engg. & Tech., Vijayawada, India*

#CSE Dept., Paladugu Parvathi Devi College of Engg. & Tech., Vijayawada, India

Abstract

A mobile ad hoc network (MANET), sometimes called a wireless mesh network, is a self-configuring network of mobile devices connected by wireless links. An Adhoc network is a network in which the locations of switches, routers can be mobile. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. Each Node has a router or switch connected by the wireless connection. The Union of connections is in arbitrary topology, allowing people and devices to seamlessly internetwork in areas with no pre-existing communication infrastructure. Traditionally, tactical networks have been the only communication networking application that followed the adhoc paradigm. Recently, the introduction of new Technologies such as the Bluetooth, IEEE 802.11, BRAN, Hyperlan and Hyperlan2 are Helping enable eventual commercial MANET deployments. These recent evolutions have been growing interest in the research and development of MANET. However, they are highly susceptible to attacks and it is very probable that an intruder catches already existing security measures out. This paper attempts to provide a comprehensive overview of this Dynamic field. It first explains the important role that mobile ad hoc networks play in the evolution of future wireless technologies and characteristics and applications. Then, it reviews the latest research activities in security issues in MANETs..

Keywords:Adhoc Network, Bluetooth, Security, wireless sensorNetworks.

1. Introduction

An ad-hoc wireless sensor network (AWSN) is a network composed of a number of simple devices called sensor nodes which are probing their environment via sensors for temperature, light, noise, etc. They offer quick and easy network Deployment in situations where it is not possible otherwise. Ad-hoc is a Latin word, which means “for this or for this only.” Mobile adhoc network is an autonomous system of mobile nodes connected by wireless links; each node operates as an end system and a router for all other nodes in the network. An Ad-hoc network is a collection of wireless mobile nodes

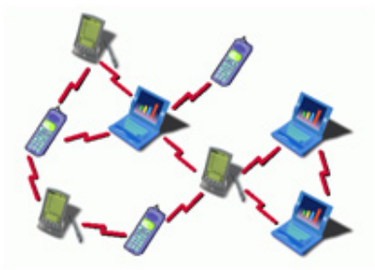

Figure 1: Mobile Network

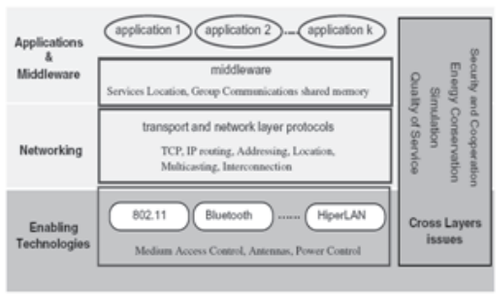

Figure 2: MANET Architecture

Corresponding author : Tel. No. +91 9059639699
E-mail address: phanisurapaneni.pvp@gmail.com.

which dynamically forming a temporary mobile nodes which dynamically forming a temporary network without the aid of any established infrastructure or centralized administration.

1.1 Characteristics of Mobile Ad Hoc Networks

- Seamless interaction
- Peer-to-peer connectivity
- Protocol diversity
- No access point requirement
- Computation and decentralization
- Speed of deployment
- Not any mediator networking device is required for Communications

1.2 Applications

- Military applications
- Emergency operations
- Wireless Mesh networks
- Wireless sensor networks
- Wireless hybrid networks

These low-cost solutions can be used in a large area of applications, including emergency response, medical monitoring, homeland security and environmental monitoring. AWSNs are highly susceptible to attacks, due to both the open and distributed nature of the network, and the limited resources of the nodes. Research on providing security solutions for such networks has focused mainly in enabling access control, encryption and authentication, securing the routing layer and developing secure services and service discovery. All these techniques can be seen as a first line of defence, aimed at preventing malicious nodes to break into the network and preventing it to work as planned, or to retrieve confidential or sensitive information. However, there is a non-negligiblepossibility that an intruder finally becomes successful. Thus, a second line of defence is needed, able to detect third party's attacks and raise alarms, even if the attacks haven't beenexperienced before.

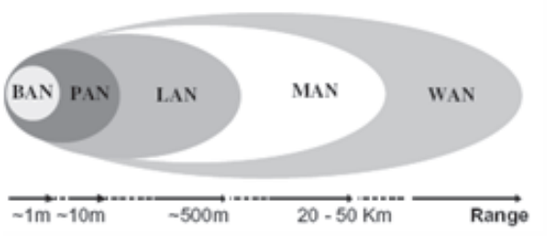

Figure 3: Bluetooth

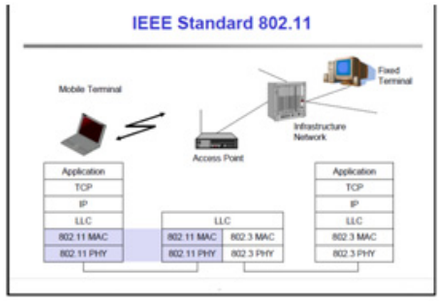

Figure 4: IEEE 802.11 Architecture

2. Bluetooth

Bluetooth is a wireless protocol, which uses a short range radio technology to simplify data transmission over short distances. Bluetooth facilitates a typical way to connect & exchange information between 2 or more devices. Bluetooth is embedded in various products such as mobile devices, laptops, personal computers etc.

Bluetooth network provides a dynamic topology known as PICONET or PAN. The specifications for Bluetooth are licensed by Bluetooth SIG. The following are the criteria satisfied by Bluetooth 1.technical feasibility 2.economic feasibility 3. Market potential 4. Uniqueness 5.compatability. User Scenarios of Bluetooth: Interconnection of peripheral devices, support of adhoc networking, bridging of networks.

2.1 Advantages:

Wireless:when traveling with your laptop or other wireless devices, you'll no longer have to worry about bringing connection cables.

Bluetooth is actually inexpensive:the technology of Bluetooth is cheap for companies to implement, which results in lower costs for the company.

Bluetooth is automatic: Bluetooth doesn't have you set up a connection or push any buttons.

Standardized protocol: Bluetooth is standardized wireless, meaning that a high level of compatibility among devices is guaranteed.

Low interference: Bluetooth devices almost always avoid interference from other wireless devices.

Low energy consumption: As a result of Bluetooth using low power signals, the technology requires very little energy and will use less battery or electrical power as a result.

2.2 Disadvantages:

Battery Use: This occurs mostly on your cell phone but also occurs in other technology such as music players. You're using up more battery power when you leave your Bluetooth enabled on your phone all day.

Bluetooth Internet: Throughout all devices, when using Bluetooth internet, the connection can sometimes run very slow so Bluetooth internet is not highly suggested for all cases.

3. IEEE 802.11

IEEE 802.11 is a set of standards for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6 and 5 GHz frequency bands. They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802). The base version of the standard IEEE 802.11-2012 has had subsequent amendments. These standards provide the basis for wireless network products using the Wi-Fi brand.

3.1 Review of fast connectivity

One of the major trends in the IEEE 802.11 standard is high throughput. The first 802.11 standard had a maximum data rate of 2 Mbit/s. The maximum data rate was increased to 11 Mbit/s (802.11b) and 54 Mbit/s (802.11a and 802.11g). Most recently, 802.11n with a maximum data rate of 600 Mbit/s acquired final approval in September 2009. The increases in data rate have been achieved through the combination of multiple technologies, including MIMO (multi-input multi-output), as shown in the following figure.

3.2 Advantages:

Very flexible within the reception area: Ad-hoc networks without previous planning possible (Almost) no wiring difficulties:E.g., historic buildings, firewalls More robust against disasters like:E.g., earthquakes, fire - or users pulling a plug

Quite cheap networking infrastructures possible:

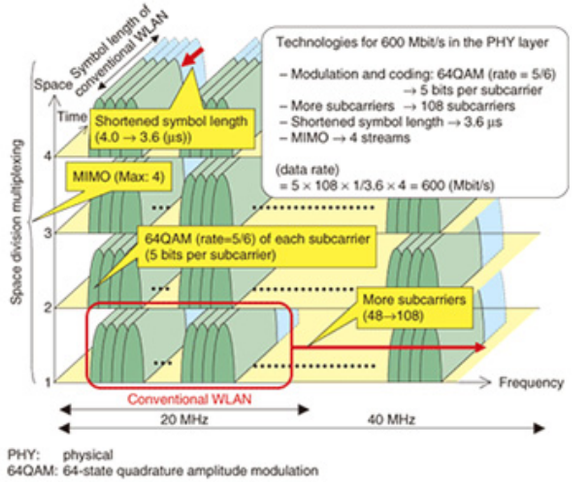

Figure 5: Speeding –up technologies at TGn

3.3 Disadvantages:

Typically very low bandwidth compared to wired networks: 1-10 Mbit/s and error rates of about 10-4 instead of 10-12, Many proprietary solutions, especially for higher bit-rates: Standards take their time, e.g., IEEE 802.11

Products have to follow many national restrictions if working wireless: It takes a vary long time to establish global solutions like, e.g., IMT-2000, Lack of security, “open” air interface, War Driving

4. Hiperlan

A complement to present-day wireless access systems, giving high data rates to end-users in hot-spot areas. Typical app. Environment: Offices, homes, exhibition halls, airports, train stations, etc.Different with Bluetooth, which is mainly used for linking individual communication devices within the personal area network

ETSI standard:European standard, cf. GSM, DECT. Enhancement of local networks and inter-working with fixed networks. Integration of time-sensitive services from the early beginning

HIPERLAN family:One standard cannot satisfy all requirementsRange, bandwidth, QoS support and Commercial constraints.HIPERLAN 1 standardized since 1996 – no products up to now!

4.1 Advantages:

System level simulator, Reconfigurable system-on-chip, and dual-band operations has also been successfully constructed.

4.2 Disadvantages:

There may exist a lot of special filter shapes that can only be realized by means of high-order filters. Burden of installing a VPN-client in all wireless devices

5. Security Issues in MANETs

It is important for maintaining privacy and for mobile e-business transactions. The following explains some of the security problems in mobile and wireless computing systems and solutions for such problems.

Confidentiality: Only destined user must be able to read data.

Integrity: Data integrity needs to be maintained or else the user receives a manipulated message.

Pre-keying: In order to decipher the encrypted messages.

Availability: There may be a denial of service attack.

Non-repudiation: Non – repudiation means that a sender is unable to deny having sent a message or information

Resource Constraint: Resource constraints of a mobile system include CPU runs at a slow, smaller memory availability, and limited battery life.

Power of detection: A mobile device may not detect the signals and therefore get data or message due to attack by jamming signals.

Interception replay: The interception of the signals and after studying the authentication requests and the client responses, attacker can replay the same sequence repeatedly.

Stealing of the subscribed service: Hijacking of user name and password by an attacker results in getting a service subscribed by another client.

Mobility risks: Changed location results in signals routing through paths, which cannot be relied upon.

Spoofing:A node can impersonate an address in a mobile ad hoc network

Reconfiguration: An attack can be network configuration. Network configuration at different periods prevents such attacks.

Eavesdropping: Unsolicited messages from another source during a talk between two sources is called eavesdropping.

Traffic analysis:A security attack can occur by extracting information from the analysis of network traffic.

5.1 Solutions

Direct signaling with restricted signal strengths: Using the directed signals with the signal strengths set such that these are just sufficient to reach and detected successfully

Hardware technique:FHSS is example in hardware used in reduce security risks

Hash: The hash of messages is a set of bits obtained after applying the algorithm

MAC: MAC is the combination of hash and security key

Encryption: Public key and private key encryptions.

SSL: SSL is a protocol in between HTTP and TCP for secure transactions.

Check sum: Checksum and parity are the primitive methods check message integrity

IPSec: IPSec is a method for message integrity check

CHAP: CHAP is a method for authentication of point to point communication

RADIUS: RADIUS is a service for sending the message that the client stands authenticated.

AAA: AAA is a strategy for authentication

6. Conclusion

In coming years, mobile computing will keep flourishing, and an eventual seamless integration of MANET with other wireless networks, and the fixed Internet infrastructure, appears inevitable.Ad hoc networking is at the centre of the evolution towards the 4th generation wireless technology. Its intrinsic flexibility, ease of maintenance, lack of required infrastructure, auto-configuration, self-administration capabilities, and significant costs advantages make it a prime candidate for becoming the stalwart technology for personal pervasive communication. The opportunity and importance of ad hoc networks is being increasingly recognized by both the research and industry community. In moving forward towards fulfilling this opportunity, the successful addressing of open technical and economical issues will play a critical role in achieving the eventual success and potential of MANET technology.

AWSNs impose new challenges on the design of IDS, which are more imperative than ever due to the unattended operations in open environments. We propose to implement a flexible and efficient intrusion detection system, which can then be used in a variety of wireless network and devices. Our concept is currently being validated through a large and heterogeneous test-bed.

Finally, we would like to state that in the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Since network scenarios cannot rely on centralized and organized connectivity and can be conceived as applications of Mobile Ad-hoc Networks. So, it becomes the best solution of different problems of network.

References

[1] J. Ahola, Ambient Intelligence, ERCIM (European ResearchConsortium for Information and Mathematics) NEWS, N. 47,October 2001.IJCA Special Issue on “Mobile Ad-hoc Networks”MANETs, 2010158

[2] A. Ahuja et al., Performance of TCP over different routingprotocols in mobile ad-hoc networks, in: Proceedings ofIEEE Vehicular Technology Conference (VTC 2000),Tokyo, Japan, May 2000.

[3] B. Kalaavathi, et. Al,http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1470874Raj Kamal, Mobile Computing, Oxford University Press,2009.

[4] G. Anastasi, M. Conti, E. Gregori, A. Passarella, A powersaving architecture for web access from mobile computers,in: Proceedings of the Networking 2002, Lecture Notes inComputer Science, vol. 2345, Springer, Berlin, 2002.

[5] C. Bisdikian, An overview of the Bluetooth wirelesstechnology, IEEE Communication Magazine, December2001.

[6] J. Broch, D. A. Maltz, D. B. Johnson, Y. Hu, J. Jetcheva, APerformance Comparison of Multi-Hop Wireless Ad Hocnetwork Routing Protocols, Proc. Of MobiCom’98, Oct.1998

[7] P. Sinha, R. Sivakumar, V. Bharghavan, CEDAR: a Core-Extraction Distributed Ad hoc Routing algorithm, , IEEEINFOCOM’99

[8] E. R. Royer, C.-K. Toh, A Review of Current RoutingProtocols for Ad Hoc Mobile Wireless Networks, , IEEEPersonal Communications, Apr. 1999

[9] V. D. Park and M. S. Corson, A Highly Adaptive DistributedRouting Algorithm for Mobile Wireless Networks, , IEEEINFOCOM’97, 1997

[10] Special Issue on Wireless Ad Hoc Networks, IEEE Journal

[11] IoannaStamouli, “Real-time Intrusion Detection for Ad Hoc Networks”,Master of Science dissertation, University of Dublin, 2003.

[12] K. Ioannis, T. Dimitriou, F. C. Freiling, “Towards Intrusion Detection inWireless Sensor Networks”, 13th European Wireless Conference, Paris,April 1997.

[13] P. Albers, O. Camp; J-M. Percher, B. Jouga, L. Mé, and R. Puttini,"Security in Ad Hoc Networks, a General Intrusion DetectionArchitecture Enhancing Trust Based Approaches", in Proceedings of the1st International Workshop on Wireless Information Systems, April 2002

[14] R. Roman, J. Zhou, J. Lopez, "Applying Intrusion Detection Systems toWireless Sensor Networks", Consumer Communications andNetworking Conference, 2006, pp. 640-644.

[15] V. Bhuse and A. Gupta, "Anomaly intrusion detection in wireless sensornetworks", Journal of High Speed Networks, Vol. 15, No. 1, pp. 33-51,2006

[16] http://www.computer.org(pervasive Computing(Mobile and Ubiquitous Computing) Magazine from IEEE).

[17] http://www.hpcmag.com (Handheld PC Magazine).

[18] http://www.mobilecomputing.com (Mobile Computing Magazine)

[19] http://www.networkcomputing.com (Network Computing Magazine).

[20] http://www.synchrologic.com (Mobile Computing Newsletter).

[21] http://www.wirelessinternet.com (Wireless Internet Magazine).