Imperial Journal of Interdisciplinary Research (IJIR)
Vol-3, Issue-4, 2017
ISSN: 2454-1362, http://www.onlinejournal.in

Analysis of MANET Function in Battlefield Environment

Abstract : *In this paper, we present a structure for performance analysis of MANET in fight/battle field environment. We will also study how to MANET functioning in the militarily operation. Research efforts also focus on issues raise during the battle such as topology control, energy efficiency, security and quality of service which already exist in the wired networks and are declined in MANET. This paper examines the application of the MANET and their newest improvement. "We will discuss the metrics used to evaluate these protocols and highlight the essential problems in the evaluation process itself. The results would show better performance with respect to the performance parameters such as network throughput, end-to-end delay and routing overhead when compared to the network architecture which uses a standard routing protocol. Due to the nature of node distribution the performance measure of path reliability which distinguishes ad hoc networks from other types of networks in battlefield conditions".*

1. Introduction

In the current world, "its almost impossible to imagine that someone can live without computers. Computer is an electronic device which is use to setup any type of the network. As the importance of computer in our daily life increases it also sets new demand for connectivity. Wired solution have been around for a long time but there is increasing demand on working wireless solutions for connecting to the internet, sending and reading e-mail message, downloading and uploading, changing information in a meeting and so on. There are many solutions to these needs, one being wireless local area network that is based on IEEE 802.11 standard. However there is increasing need for connectivity in situation where there is no base station" (i.e. back bone connection) available (for example two or more PDAs need to be connectivity).

1.1 Ad Hoc Network-:

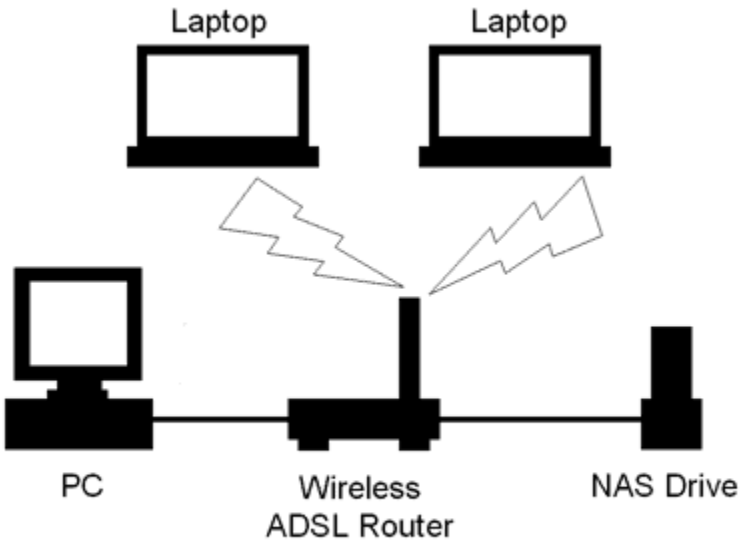
MANET Stands for "Mobile Ad Hoc Network." A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission.

In computing terminology, the term "wired" is used to differentiate between wireless connections and those that involve cables. While wireless devices communicate over the air, a wired setup uses physical cables to transfer data between different devices and computer systems.

A wired network is a common type of wired configuration. Most wired networks use Ethernet cables to transfer data between connected PCs. In a small wired network, a single router may be used to connect all the computers. Larger networks often involve multiple routers or switches that connect to each other. One of these devices typically connects to a cable modem, T1 line, or other type of Internet connection that provides Internet access to all devices connected to the network.

Wired may refer to peripheral devices as well. Since many keyboards and mice are now wireless, "wired" is often used to describe input devices that connect to a USB port. Peripherals such as monitors and external hard drives also use cables, but they are rarely called wired devices since wireless options are generally not available.

While many peripherals are now wireless, some users still prefer wired devices, since they have a few benefits over their wireless counterparts. For example, an Ethernet connection is not prone to signal interference that can slow down Wi-Fi connections. Additionally, wired network connections are often faster than wireless ones, which allows for faster data transfer rates. Some users also prefer wired peripherals since their is no need to replace batteries on a regular basis. Gamers especially prefer wired keyboards and mice since they have lower latency and can be backlit, thanks to the power provided by the USB connection.[1]



Example 2: A wired and wireless peer-to-peer network

1.2 Advantage of mobile ad hoc network:

Self Forming-Nodes that comes within the radio range of each other can setup a network association without any pre-configuration or manual intervention.

Self healing-Node can join or leave rapidly without affecting operation of the remaining nodes.

No infrastructure-In an mobile ad hoc network, mobile nodes from their own network and essentially become their own infrastructure

Peer to Peer-Traditional networks typically support end systems operation in client server mode. In an ad hoc network mobile nodes can communicate and exchange information without former agreement and without confidence on centralized resources.

Predominantly wireless-Historically networks have been mostly wired and enhance or extended through wireless access. The ad hoc environment is essentially wireless but can be extended to support wireless resources.[2]

Highly dynamic-Mobile nodes are continuous motion and ad hoc networking topologies are constantly changing.

1.3. **Function Area**-Some of the function of Mobile Ad hoc Network are-

1. Personal area network and Bluetooth
2. Video Conferencing-
3. Urgent business meeting
4. Disaster relief operation
5. Mining operations
6. Military and BSF exercises

Such network can be used to enable next generation of battlefield application run by military including situation awareness system for manipulation war fighters and remotely deployed unmanned micro-sensor networks.

Ad hoc network can provide the communication for civilian applications such as disaster recovery and message exchange among medical and security personnel involved in rescue operations.

In real life many examples of MANET can be found where an access point and existing infrastructure is not available. Common examples are:

Battlefield situations where truck and even each soldiers gun has wireless card. These nodes from a MANET and communicate with each other in the battlefield. In addition MANETs can be used to detect terrorist's movements in remote area in the Kashmir instead of land mines.

Emergency situations where a building has been destroyed due to fire earthquake or bombs. In such a case it is important to setup quick network MANET are ideal for such situation. For example in emergency operations police and fire fighters can communicate through a MANET and perform their operations without adequate wireless coverage.

2. Characteristic of Mobile Ad Hoc Network-

A MANET consists of mobile platforms (e.g., a router with multiple hosts and wireless communications devices)--herein simply referred to as "nodes"--which are free to move about arbitrarily. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices, and there may be multiple hosts per router.

A MANET is an autonomous system of mobile nodes. The system may operate in isolation, or may have gateways to and interface with a fixed network. In the latter operational mode, it is typically envisioned to operate as a "stub" network connecting to a fixed internetwork. Stub networks carry traffic originating at and/or destined for internal nodes, but do not permit exogenous traffic to "transit" through the stub network. MANET nodes are equipped with wireless transmitters and receivers using antennas which may be omnidirectional (broadcast), highly-directional (point-to-point), possibly steerable, or some combination thereof. At a given point in time, depending on the nodes' positions and their transmitter and receiver coverage patterns, transmission power levels and co-channel interference levels, a wireless connectivity in the form of a random, multihop graph or "ad hoc" network exists between the nodes. This ad hoc topology may change with time as the nodes move or adjust their transmission and reception parameters.[3]
It can be consist of the various device i.e. node can be of different type (printers, routers, laptop, mobile phones) with different computation storage and communication capabilities.
Power consumption can be high because nodes have to be kept alive to forward information sent by other nodes that just happen to be in the neighborhood.It is self organizing and adaptive. This means that a network can be formed without the need for any assistance. This allows speedy exploitation of networks when needed and quick destroy when not needed. Below presents many challenges that participant in MANETs.

The characteristic of these network are summarized as follows

- Node can perform the role of both sender and receiver
- No centralized controller and infrastructure. Inherent mutual trust.
- Dynamic network topology. Frequently routing updates.
- Self-governing, no infrastructure needed.
- Can be setup anywhere
- Energy constraints
- Limited Security.

"Generally, the communication terminals have mobility nature which makes topology which makes the topology of distributed network time varying. The dynamical nature of the network topology increases the challenge of the design of ad hoc networks.[5]

3. Network Security-

Network security extend the computer security thus all the things in computer security are silent valid but there are other things to consider as well. Security is an essential requirement in the mobile ad hoc network. Compared to wired network MANETs are more vulnerable to security attacks due to the lack of trusted centralized authority and limited resources.

3.1-Security problem in MANETs

1. Unreliability of wireless links between nodes- Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants.

2. Dynamic topologies- Nodes are free to move arbitrarily; thus, the network topology- which is typically multihop--may change randomly and rapidly at unpredictable time. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically config.d routing protocol.

3. Lack of Secure Boundaries -The meaning of this vulnerability is self-evident: there is not such a clear secure boundary in the mobile ad hoc network, which can be compared with the clear line of defense in the traditional wired network. This vulnerability originates from the nature of the mobile ad hoc network: freedom to join, leave and move inside the network. Lack of secure boundaries makes the mobile ad hoc network susceptible to the attacks. Due to this mobile ad hoc network suffers from all-weather attacks, which can come from any node that is in the radio range of any node in the network, at any time, and target to any other node(s) in the network. To make matters worse, there are various link attacks that can jeopardize the mobile ad hoc network, which make it even harder for the nodes in the network to resist the attacks. The attacks mainly include passive eavesdropping, active interfering, and leakage of secret information, data tampering, message replay, message contamination, and denial of service [7].

4. **Lack of Centralized Management Facility**- Ad hoc networks do not have a centralized piece of management machinery such as a name server, which lead to some vulnerable problems. Due to absence of centralized management facility problems detection of attacks, path breakages, transmission impairments and packet dropping, breakage of the cooperative algorithm take place because decision making process is decentralized.

5. **Restricted Power Supply**- Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation. The problem that may be caused by the restricted power supply is denial-of-service attacks [6]. Since the adversary knows that the target node is battery restricted, either it can continuously send additional packets to the target and ask it routing those additional packets, or it can induce the target to be trapped in some kind of time-consuming computations. In this way, the battery power of the target node will be exhausted by these meaningless tasks, and thus the target node will be out of service to all the benign service requests since it has run out of power.

6. **Scalability**- Scalability is the problem in the mobile ad hoc network [6]. Unlike the traditional wired network in that its scale is generally predefined when it is designed and will not change much during the use, the scale of the ad hoc network keeps changing all the time: because of the mobility of the nodes in the mobile ad hoc network, you can hardly predict how many nodes there will be in the network in the future. As a result, the protocols and services that are applied to the ad hoc network such as routing protocol and key management services should be compatible to the continuously changing scale of the ad hoc network.

4. Conclusion-As this paper is researches in progress, there have not been sections for discussing laid out here. Nevertheless the issues and highlights about MANET in battlefield areas has been expressed detail. In battlefield ad hoc network can be implemented using the various technologies like Bluetooth and WLAN.the definition itself does not imply any restrictions to implement devices. Ad hoc networks need very specialized security methods. There is no approach fitting all networks because the nodes can be any devices. The computer security in the nodes depends on the type of node and no assumptions on security can be made. In this paper the computer security issues have not been discussed because the emphasis has been on network security".

References

1. J. Haas, Lidong Zhou," Securing Ad Hoc Networks" Department of Computer Science, School of Electrical Engineering.
2. Dave Barker,"Bringing Mobile Ad hoc Networks to the battlefield using COTS open Standerd"Extreme Engineering Solutions.
3. Dr. C. Rajabhushanam,Dr. A Kathirvel, "Survey of wireless MANET Application in Battlefield Operation", (IJACSA) International journal of Advanced Computer science and Application vol. 2 No. 1. January 2011.
4. J. Macker Naval,S. Coeson, " Network Working Groups" Request for Comments: 2501 University of Maryland Category: Informational Research Laboratory January 1999.
5. Mohammad A. Mikki, ―Energy Efficient Location Aided Routing Protocol for wireless MANETs‖, in International Journal of Computer Science and Information Security, Vol 4, No. 1&2, 2009.
6. Amitabh Mishra, Ketan M. Nadkarni, "Security in Wireless Ad Hoc Networks", in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.
7. Zaiba Ishrat, "Security issues, challenges & solution in MANET" Dept. of EC, RGGI (Meerut), India IJCST Vol. 2, Issue 4, Oct. - Dec. 2011 ISSN : 0976-8491 (Online) | ISSN : 2229-4333(Print).