ADHOC NETWORKS

Prof. Gaikwad Ravi. P.

Institute of Business Management and Rural Development ,Ahmednagar(mh) (India) pin-414111
gaikwadravi2008@gmail.com

Prof. Gaikwad Anil P

Institute of Business Management and Rural Development ,Ahmednagar(mh) (India) pin-414111
anilgaikwad2@gmail.com

Abstract: *In this paper we have covered what Ad Hoc network is and what are the advantages of using it. Also what are airborne networks and how to secure it using Iris recognition? Ad Hoc networks special purpose networks which are created for some particular purpose. They are often created for temporary use. Also they are decentralized wireless networks. Airborne networks are nothing but infrastructure that provides communication transport services through at least one node. Airborne networks are basically used as an war fighting asset which commanders the capability to ascertain the networks operational health and status i.e., network situational awareness. When huge data is sent over these networks their s a need for security. So in this paper we will see the core concepts of Adhoc networks and need for security and how to secure it using Iris recognition by generating living password.*

Keywords:*Ad Hoc networks, Airborne networks, decentralized, security, Iris Recognition.*

JMIJIT
JANUARY, 2011 VOLUME -1 ISSUE 1
©JM ACADEMY ISSN: Print 2229-6115

1.Introduction

Ad Hoc Networks are self organizing, self healing, distributed networks which most often employ wireless transmission techniques. "Ad Hoc" is actually a Latin phrase that means "for this purpose." In computer networking, an ad hoc network refers to a network connection established for a single session and does not require a router or a wireless base station. Examples are organizations, committees, and commissions created at the national or international level for a specific task.

Definition of Airborne networks:

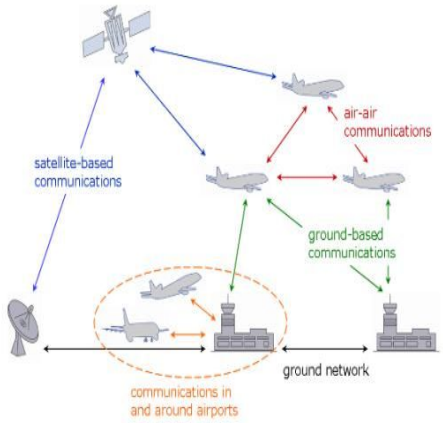
The Airborne Network is defined to be an infrastructure that provides communication transport services through at least one node that is on a platform capable of flight.

WHAT IS MEANT BY ADHOC NETWORKS?

An ad-hoc network is a local area network (LAN) that is built spontaneously as devices connect. Instead of relying on a base station to coordinate the flow of messages to each node in the network, the individual network nodes forward packets to and from each other.

In the Windows operating system, ad-hoc is a communication mode (setting) that allows computers to directly communicate with each other without a router.

Ad Hoc Networks are capable of analyzing the radio propagation environment they operate in to optimize performance. This typically requires that the network nodes have positioning capability as well as memory to recall geographically local conditions.



What we thus observe in the Internet is a very powerful networking medium, but one that is ill adapted to an environment in which the connectivity through the network, and thus its topology, rapidly change in time. That is the reality of wireless military networks, and the reason Internet connectivity is not common in current military systems.

Modern ad hoc networking protocols emerged to bridge this gap during the 1990s. The central idea behind all ad hoc networks is that there is no fixed topology, or the topology is dynamic and rapidly changing. This is a model eminently suited to military networks.

In an ad hoc network, every computer has a router attached to it - either embedded in software, or as a router/radio-frequency modem. We describe each such arrangement as a ‘node’ in the ad hoc network.

In such networks, every node routes if required traffic to and from its peers in the network, which is for all intents and purposes a cooperative network. This is an important distinction from conventional networks, where routers are specialised and most computers do not double up as routers.

The key to the function of all ad hoc networks is the performance of the route discovery protocol in use .Route discovery protocols for ad hoc networks differs

considerably from route discovery protocols used in conventional fixed networks.

In an ad hoc network, every time a connection is to be established, a node must send out a query which asks 'is a connection to my destination node available, and if so, what routes exist to get there?' In general, research indicates that 'reactive' route discovery techniques, which propagate a query across the network every time a connection is needed, work better than 'proactive' techniques that attempt to maintain a constantly updated table of possible connections. This is for a variety of reasons, but especially since traffic between nodes in close mutual proximity is often dominant.

One of the most popular techniques used is the Dynamic Source Routing (DSR) protocol, proposed by Johnson, which extends the source routing.

- ***Advantages of Ad-Hoc Networks***
- **Lower getting-started costs**
    - no need to install base stations
    - easier temporary setup
- **Well suited to free unlicensed spectrum**
    - significant savings given typical auction prices
- **Inherent scalability**
    - with power control & cooperative relaying, each user contributes to network capacity

What are Airborne Networks?

Airborne Ad Hoc Networks (AAHN) are a form of ad hoc network in which the transceivers and routers are carried by airborne platforms, such as conventional aircraft, High Altitude Long Endurance or conventional Uninhabited Aerial Vehicles, tethered aerostats or dirigibles. As such the AAHN has many quite different characteristics compared to conventional 'terrestrial' ad hoc networks. While AAHNs offer enormous footprint coverage for each node, compared to conventional solutions, this is achieved at the expense of unique problems in antenna placement, transceiver design, protocol design and integration.

Airborne internet has the potential to change the way aircraft receive and send data. Airborne Internet has the potential to change how aircraft are monitored and tracked by the air traffic control system.

The objective of the airborne networks is the use of heterogeneous set of physical links (RF, Optical/Laser and SATCOM) to interconnect terrestrial, space and highly mobile airborne platform themselves, which will be self formed into network with dynamic topology.

Airborne networks are used as an war fighting asset, it provides commanders the capability to ascertain the networks operational health and status -i.e., network situational awareness. Additionally these resources should be configurable to meet the commander's objectives. This paper deals with the framework for critical research technological need for military communications very secretly for airborne networks.

Security Goals

1) ***Availability***
2) ***Confidentiality***
3) ***Integrity***
4) ***Authentication***
5) ***Non-repudiation***

Need for Security

As networks has become a part of our life. We have to send a huge amount of data over the available networks. But hackers are present everywhere who are trying to hack the data that are sent secretly. Encryption is a method that is been used since long which are used to encrypt the data that is been done by some algorithm, but these data were also easily broken

by the hackers. So there is a need to secure the networks.

To secure the recipient data there is a need to design a network with complete security. Here we will see how to secure a Airborne network.

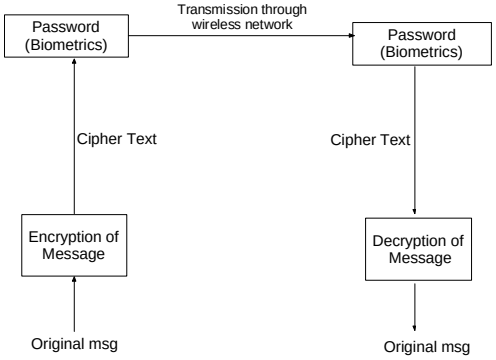


Fig: Security system

In this paper up till now we have seen how airborne networks are useful to send data but the main question that arises here is security of the data so in order to make a data transfer secure we will see certain steps using iris code generations that used along with encryption algorithm will help the data to be send securely.

Steps to generate living password using Iris code generations:

IRIS Recognition

Iris recognition is the process of recognizing a person by analyzing the random pattern of the iris. Iris is a muscle within the eye that regulates that regulates the size of the pupil, controlling the amount of light entering the eye.

There are many biometric techniques that can be used to generate password. But Iris recognition provides more uniqueness compared to fingerprint and face recognition.

A classic iris recognition algorithm includes the following steps:

- Image processing
- Feature Extraction
- Pattern matching
- Classifier design

The pattern of human's iris differs from each other. In order to detect iris following steps must be followed:

- Iris radius approximation
- Iris translation
- Iris information extraction
- Gabor filtering
- Generating of iris code
- Comparing iris code

Iris Detection

This is the process for detecting center and radius of an iris given the pupil center and radius. Not at all time pupil and iris are not concentric. So the pupil information does not help directly to determine the parameters of the iris. Having the starting point of the pupil, we guess the potential iris centers and radii. They then integrate over the circumference in order to determine if it is on the border of the iris.

Iris radius approximation

Firstly we have to find the actual iris radius, is to find an approximation of the iris radius. This approximation can be fine tuned to find the actual iris parameters. To find the approximation a single edge of the iris must be found. Most probably eyes are to be distorted in the top and bottom parts due to eyelashes and eyelids, so the best choice for finding an unobstructed edge is along the horizontal line through the pupil center. It happens that for any edge detection it is good idea to blur the image to subtract any noise prior to running the algorithm, but too much blurring can dilate the boundaries of an edge, or make it very difficult to detect. So a special smoothing filter such as the median filter should be used on the original image. This eliminates sparse noise while preserving image boundaries. The original image after running through a median filter works by assigning to a pixel

the median value of its neighbours. Then the image is prepped the edge detection can be done. Since there is such a noticeable rising edge in luminescence at the edge of the iris, filtering with a haar wavelet should act as a simple edge detector.

Iris Translation

Having acquired an approximate radius, a small pad of this value should produce a circle cantered on the pupil which contains the entire iris. Furthermore, with the perimeter of the pupil known, an annuals may be formed which should have the majority of its area filled by the iris.

If the iris is perfectly centered on the pupil, the unrolled image should have a perfectly straight line along its top. However, if the iris is off centered even a little this line is wavy. The line represents the overall distance the iris is at from the pupil center. Itis this line which will help to determine the iris' center and radius. Consequently, an edge detection algorithm must be run on the strip in order to lines' exact location. Once again canny edge detection is used.

Iris Information Extraction

In order to extrapolate the iris' center and the radius, two chords of the actual iris through the pupil must be found. This can be easily accomplished with the information gained in the previous step. Thus easily the information could be retrieved and used for further proceedings.

Gabor filtering

To understand the concept of Gabor filtering, we must first start with Gabor

wavelets. Gabor wavelets are formed from two components, a complex sinusoidal carrier

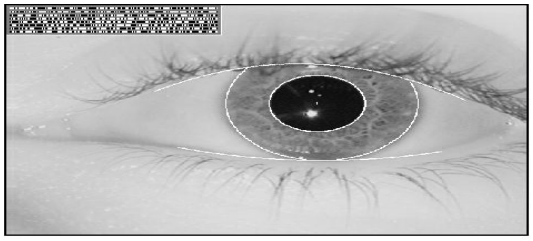
and Gaussian envelope.

G(x,y)=f(x,y) * w(x,y)
The complex carrier takes the form:
F(x,y)=ej(2*pi(uv+vy)+p)
Gaussian Envelope: The envelope has a Gaussian profile and is described by the following equation,
G(x,y)=Ke-pi(a^2(x-x1)^2+b^2(y-y1)^2)
To put it all together, we multiply **f(x,y)** by **w(x,y)**.

Generating an Iris code

We only want to store a small number of bits for each iris code, so the real and Imaginary parts are each quantized. If a given value in the resultant vector is greater than zero, a one stored; otherwise zero is stored.

This iris code generated serves as a password for the system. This password provides a very high security for the system and seems to be unbreakable.



Other applications where iris code password protection can be used are:

- Aviation Security
- Substituting of passports
- Forensic and Military applications
- Network access

Conclusion

In this paper we have seen what Adhoc networks are and what the benefits are of using it. Also we have seen Airborne networks and how to secure them using iris code generation which would act as a living password which would provide high level of security to the networks.

References

1. **www.wikipedia.org**
2. **www.airbornenetworks.co**
3. **www.airborneinternets.com**
4. **www.asdevents.com**
5. **www.biometrics.gov**