Design of a Cyber Security Framework for Surveillance Systems

Ashwini Awale, Rupali Kadam, Priti Kumari, Ashwini Belsare,
Department of Computer Technology, KDKCE, Nagpur

Abstract - The need for increased surveillance due to increase in flight volume in remote or oceanic region outside the range of traditional radar coverage has been fulfilled by the invention of space-based Automatic Dependent Surveillance - Broadcast systems. Systems have the capability of providing air traffic controllers with highly accurate real-time flight data. It is dependent on digital communications between aircraft and ground stations of the air route traffic control centre (ARTCC); however these communications are not secured. Anyone with the appropriate capabilities and equipment can interrogate the signal and transmit.

I. INTRODUCTION

Surveillance is defined as the close observation and monitoring of changing information and it is needed in air transportation systems to track and monitor flights in order to maximize safety and efficiency in the air space. There are three types of surveillance used for air traffic control.

1) Primary surveillance radar: - It provides information about a coordinate system to the Air Traffic Controller, but not the target's identity.

2) Secondary surveillance radar: - It is attached to primary Surveillance radar and is able to interrogate a transponder of an aircraft, determining its altitude, latitude/longitude, and flight number.

Flying and the increase in the number of airplanes that will be used to carry these passengers, there will also be an increase in air traffic. More and more airplanes will be in the skies and there will be a need for a better way to track and monitor aircraft to maintain efficiency and safety in the United States airspace.

II. MODULES

Our project mainly consists of the modules which are described below in detail.

1) Simulation of Entities involve: - Following are the entities involved in the communication system

A. Reference aircraft
B. Other aircrafts
C. Air Route Traffic Control Centre (ARTCC)

In this module we will create the simulation GUI for every entity involved in the communications which are mentioned above. Also it will contain all the necessary information associated with the respective entity.

2) Creation of security framework:- Based on the spoof attacks attempted & detected on the signals we will create a framework for secured transmission of signals so that the data contained by the signals is kept intact form malicious attacks.

There are various methods to implement such security on signals being transmitted.

Further study needs to be done to select the most efficient method by analysing & comparing the effectiveness & accuracy of different methods.

We will be closely observing the factors such as collision risk, signal security, economic implications here as well to get an idea about the effectiveness & accuracy differences between normal &secured communication mode.

Theirs own false data; this is known as spoofing. The possibility of this type of attacks decreases the situational awareness of airspace.

The purpose of this project is to design a secure transmission framework that prevents signals from being spoofed. The ultimate goal of the project is to show that if signals can be secured, the situational awareness can improve and the ARTCC can use information from this surveillance system to decrease the separation between aircraft and ultimately maximize the use of the airspace.

Need for this project: - The reason why this project needs to be implemented is to improve the situational awareness of the aircraft, to reduce the time delay, to maximize the use of the air space and to improve the security in aviation system, to locate exact position of aircraft, accuracy in aircraft to aircraft communication and to avoid collision.

Objective: - The purpose of this project is to design a secure transmission framework that prevents Air Traffic Surveillance System (ATSS) signals from being spoofed & improve situational awareness, decrease the separation between aircraft and ultimately maximize the use of the airspace.

3) Performance Evaluations of framework create: -
In this module we will be comparing the performance of various security methods implemented to come to the conclusion that which method is most effective & accurate as per our methodology. Also the advantages & limitations of most efficient method will be observed here itself.

4) Graphical representation of entire simulation: -
This will be the final module for our project proposed. It will give us the graphical comparison of the things done so far. Also it will provide us with the display of route of the aircrafts depending on the communication between the entities, attacks attempted, collision probability etc.

Cryptography is playing a major role in data protection in applications running in a network environment. It allows people to do business electronically without worries of deceit and deception in addition to ensuring the integrity of the message and authenticity of the sender.

Despite the fact that secured communication has existed for centuries, the key management problem has prevented it from commonplace application. The development of public-key cryptography has enabled large-scale network of users that can communicate securely with one another even if they had never communicated before .This paper considers a Public Key encryption method using RSA algorithm that will convert the information to a form not understandable by the intruder therefore protecting unauthorized users from having access to the information even if they are able to break into the system.

III. METHODOLOGY

There are many ways of classifying data cryptographic algorithms but for the purpose of this paper, they will be classified based on the number of keys that are employed for encryption and decryption. The three common types of algorithms are:

1) Secret Key Cryptography (SKC):

The SKC method uses only a single key for both encryption and decryption. The schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing while block cipher scheme encrypts one block of data at a time using the same key on each block.

The main drawback of this method is propagation error because a distorted bit in transmission will result in n distorted bits at the receiving side. Though stream ciphers do not propagate transmission errors, they are periodic therefore the key-stream will eventually repeat. This normally results in the use of digital signature mechanisms with either large keys for the Public verification function.

2) Public Key Cryptography (PKC):

PKC scheme uses one key for encryption and a different key for decryption. Modern PKC was first described using a two-key crypto system in which two parties could engage in a secure communication over a non-secure communications channel without having to share a secret key. In PKC, one of the keys is designated the public key and may be advertised as widely as the owner wants. The other key is designated the private key and is never revealed to another party. RSA is one of the first and still most common PKC implementation that is in use today for key exchange or digital signatures. The cardinal advantage of this method is that administration of keys on a network requires the presence of only a functionally trusted TTP, as opposed to an unconditionally trusted TTP. Depending on the mode of usage, the TTP might only be required in an "off-line" manner, as opposed to in real time. Many public-key schemes yield relatively efficient signature mechanisms. The key used to describe the public verification function.

IV. REQUIREMENT

Hardware Requirements:

- **System:** Windows based PC
- **Processor:** Dual Core or higher
- **Processor Speed:** 2.0 GHz
- **Memory:** 4 GB RAM
- **Hard Disk Drive:** 160 GB

Software Requirements:

- **Platform:** JAVA
- **Language used:** Java
- **Development tools:** JDK 1.6, Eclipse
- **Database used:** MYSQL

V. ALGORITHM IMPLEMENTATION

The RSA Algorithm for Creating RSA Public and Private Key Pair

The RSA algorithm can be used for both key exchange and digital signatures. Although employed with numbers using hundreds of digits, the mathematics behind RSA is relatively straight-forward. To create an RSA public and private key pair, the following steps can be used:

1. Choose two prime numbers, p and q. From these numbers you can calculate the modulus, *n=pq*
2. Select a third number, *e,* that is relatively prime to (i.e. it does not divide evenly into) the product(p-1)(q-1), the number *e* is the public exponent.
3. Calculate an integer *d* from the quotient(ed-1)/(p-1)(q-1).The number d is the private exponent.
4. The public key is the number pair (n,e). Although these values are publicly known, it is computationally infeasible to determine d from n and e if p and q are large enough.
5. To encrypt a message, M, with the public key, creates the cipher-text, C, using the equation: *C=M^e Mod n.*
6. The receiver then decrypts the cipher-text with the private key using the equation: *M=C^d Mod n.*

How to Use the Keys for Encryption: -

Assuming a sender "A" that wants to send a message to a receiver "B", the sender will take the following steps:-

1. Obtains the recipient B's public key (e,n)
2. Represent the Plaintext message as positive integer *M.*
3. Computes the cipher-text C=M^e Mod n.
4. Send the cipher-text C to B.

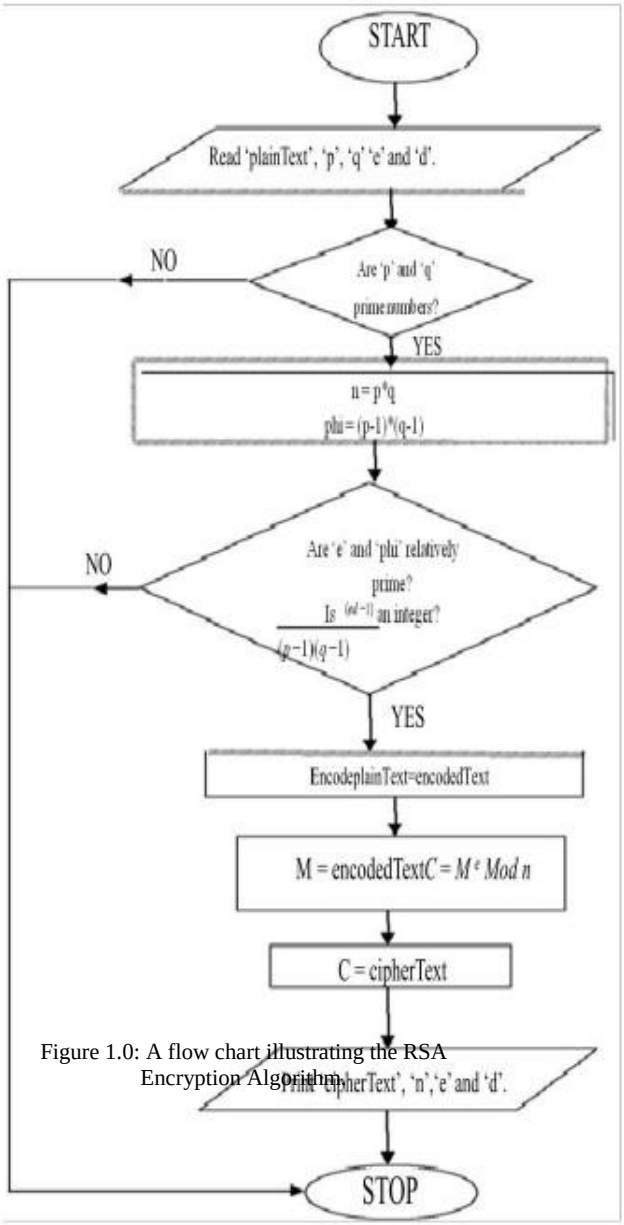

Figure 1.0: A flow chart illustrating the RSA Encryption Algorithm

How to Use the Keys for Decryption

For the recipient "B" to receive the message sent by the sender "A", the recipient will take the following steps:-

1. Uses the private key (n, d) to compute *M=C^e Mod n.*
2. Extracts the plaintext from the Integer representative *M.*

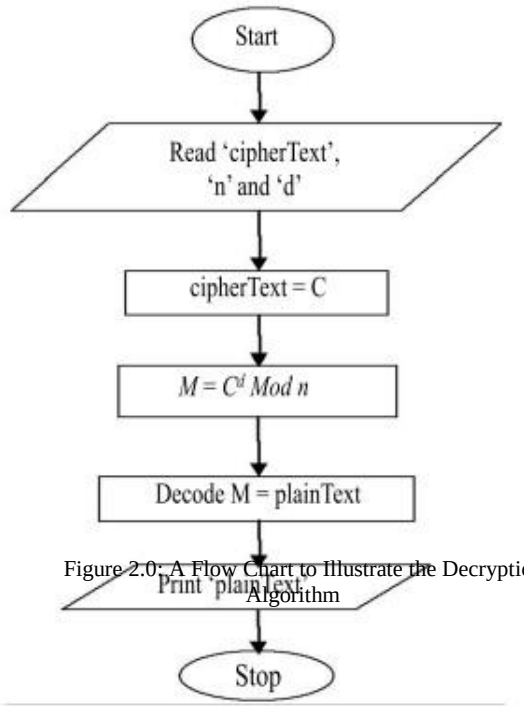

Figure 2.0: A Flow Chart to Illustrate the Decryption Algorithm

VI. RANDOM FUNCTION

Generating a series of random numbers is one of those common tasks that crops up from time to time.In java, It can be achieved simply by using the java,util.Random class.

The first step- as with the use of any API class, is to put the import statement before the start of program class.

Import.java.until.Random;

Next create a random object:

Random rand = new Random();

The Random object provides with a simple random number generator. The methods of the object give the ability to pick the random numbers.

VII. CONCLUSION

Based on the analysis of data and the three simulations, it is recommended that encryption, and in particular symmetric encryption, should be implemented on Radar signals because it has a high level of security strength, low probability of collision, acceptable feasibility, and least economic implications.

FUTURE SCOPE:

The key size of the RSA can be increased and one can use a hybrid encryption to provide a more security. Also military applications can be added such as missile tracking and smart weapons monitoring which can be use for military purpose.

REFERENCES:

1. SaharAmin,Tyler clark, Rennix Offutt, and Kate SerenkoGeogeMasonUniversity,Samin9,tclark11,roffcut "Design of a Cyber security Framework for ADS-B",2014 IEEE
2. 2."Air Traffic".- NextGen Briefing. Federal Aviation Administration,21 Sept 2009.Web.9 Sept 2013.
3. 3."A method for obtaining Digital Signatures and public-key-cryptosystem"- Rivest, R.; Shamir, A. Adleman.