E-ISSN: 2321–9637
Volume 1, Issue 4, November 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

ENHANCING THE SECURITY IN MANET USING STEGANOGRAPHY

[1]Parag B. Zope [2]Bhagyashree N.Patil [3]Prajkta B. Zope
[1]Department of CSE, PLITMS, Buldana
[2]Department of IT,ACE, Chikhali.
[3]Department of CSE, PLITMS, Buldana
Email: [1] Paragzope1991@gmail.com
[2]Patilbhagyashri53@gmail.com
[3] prajktazope1993@gmail.com

ABSTRACT:"MANET" is a mobile ad-hoc network i.e self configuring infrastructure less network of mobile devices connected by wireless network. As the network is wireless and somewhat insecure due to attacks, we can increase the security of network and make it robust by implementing the Steganography in the data transfer. It guaranties the confidentiality of information. In this paper we are implementing image Steganography using the png Image. By implementing the LSB insertion or HSB insertion method to get more security.

Keyword: LSB insertion, HSB insertion, MANET

1. INTRODUCTION:

MANET is wireless network in which mobile nodes are connected to each other. This is the infrastructure less network. So that every node act as a router itself. The data is transfer with the shortest path. In such network a malicious node can enter in the network and obtain the data from network by breaking a protocols like AODV, TORA.
But by implementing the steganography in the MANET data can securely transfer to the destination node. In steganography the data is encrypted in the image or other file. We are going to implement the Encryption in the image using LSB insertion or HSB insertion.
In this technique the data is hidden in LSB of pixel or HSB of pixel.
Here, we hide data in image while transmission. At receiver side we extract in the image. The node or router should not process any fake request hence the concept of user transfer ID and Request ID is introduced. Implementation of such a security constraints in MANET secure the data transmission eventhough if the malicious node obtain data, decryption become difficult to hacker. In this case the data is more securely transfer if the image is new, so that the malicious node never decrypt the data because decryption happen when embedded image is compare with the original image.

2. TECHNIQUE OF STEGANOGRAPHY :

Steganography means hiding data in image in such way that others can not discern the presence or contents of hidden message. There are two types of image format that can be used in steganography.

1) Lossy Image: The image which is to be sent using internet is compressed so the bit pattern in the image will change such a format is called as lossy. This is not desirable in the image as we are hiding the data in image.
Example: .GIF, TIFF (.TIF & .TIFF), &BMP (.BMP, .DIB) are compressed while sending over so they can not used right now.

2) Lossless Image: The images that are not compressed while sending over the network and the bit pattern is not changed are called as lossless Image. These images are suitable for hiding the data in image to send the data.
Example: Image Files with extension .PNG are lossless.

E-ISSN: 2321–9637
Volume 1, Issue 4, November 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

*3)Cover (Decoy):*Cover serves as medium to hide the message being sent. Making use of graphical images as cover solve many problems readily such as large availability of images, various format of images and variation in size of image

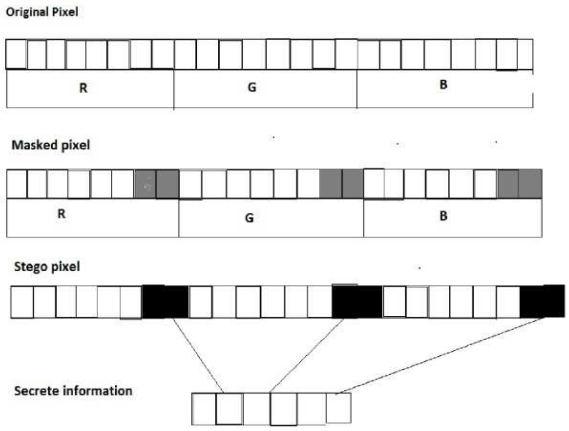

Fig 1: LSB insertion

In the sameway we can do HSB insertion at the leftmost side.

3. ALGORITHM:

The path is decided with the protocols, the transfer id, requet id and path is decided, then the following algorithm is executed

This algorithm is only for embedding a character (8-bit). For embedding the entire message, the steps in the algorithm are repeated. The process of embedding consists of the following steps:

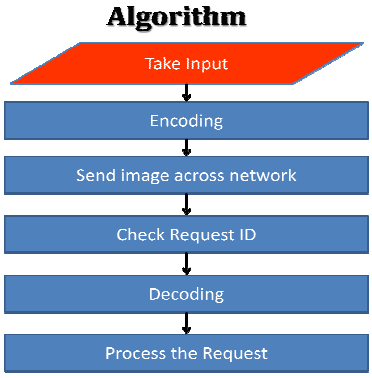

Fig 2: Algorithm of Execution

Step 1: The image is selected initially, in which data has to be embedded.
Step 2: The total number of pixels in the image is calculated by using the formula ‘width x height’.
Step 3: The color intensities of each and every pixel is retrieved and stored in an array. Each pixel constitutes of 3 bytes, where each byte represents one of the three primary colors i.e. RGB.
Step 4: AND operation is performed on each byte of the pixel along with the binary equivalent of 252. The result obtained is the byte value with the last two bits as ‘00
Step 5: The cipher text is AND operated with the binary equivalent of ‘03’ to retrieve the last two bits of the message.

E-ISSN: 2321–9637
Volume 1, Issue 4, November 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

Step 6: The OR operation is performed with the output of step 4 and step 5.
Step 7: The output of step 6 becomes the new intensity of the Red color. For Green and Blue color step 4 is repeated and before doing step 5 right bit shifting is performed to the cipher text in the incremental order of 2 till all the 8 bits are embedded.
Step 8: data is send toward the node whose request id is obtained
Step 9: data is accepted at the receiving node and

To retrieve the cipher text from the image, the reverse steps of the algorithm (from 7 to 1) mentioned above is to be performed.

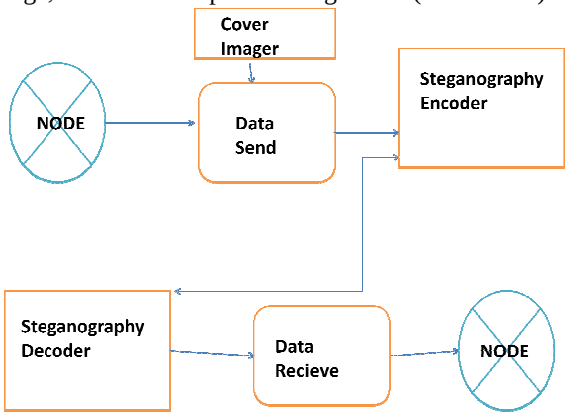

Fig 3:- Working of Steganography in MANET

4. MATHEMATICAL MODEL:

A. Set Theory Analysis

1. Let 'S' be set representing the Mobile node in the network
2. S= {……
   Let U,P, A,M and D are sets such that,

U={u | 'u' is a User Name.}
P={p | 'p' is a password.}
A={a | 'a' is a path.}
D={d | 'd' is destination addr.}
Finally, S = {U,P,A,D,…

2. Identify the process as H(To hide data into image) and I such that,
I={U,P,A,D}
S={ U,P,A,D,I,H …
H= {I,F_h,O_h}
F_h={ f_h| 'f_h' is function to hide data into image.}
O_h={o_h | 'o_h' is output of data hiding.}
$F_h(I)=O_h$

5. Identify process as X(To extract data from image)
S={ U,P,A,D,I,H,X …
X ={O_h, F_x, I}
F_x={ f_x | 'f_x' is function to extract data.}
$F_x(O_h)=I$
6. Identify the process as T(To send data)

E-ISSN: 2321–9637
Volume 1, Issue 4, November 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

S= { U,P,A,D, I,H,X,T …
T= { O_h,F_t}
O_h = {o_h | 'o_h' is steganographed Output}
F_t = {f_t | 'f_t' is a function to send information in the form of O_h}
F_t (O_h) = O_h
7.Identify the process as B(Balance enquiry).
S= { U,P,A,D,I,H,X,T,B …
B= {I, F_b, O_h}
O_h = {oh | 'o_h' is Output in the steganographed form.}
F_b = { f_b | 'f_b' is a function to fetch information in the form of O_h}

F_b(I) = O_h

8. Identify Process as G(To Generate Mini statement)
S={ U,P,A,D ,I,H,X,T,B,F,G …
G={I,F_m,O_g}
F_g={f_g|'f_g' is function to generate Mini statement.}
O_g={o_g|'o_g' is generated Mini statement.}
F_g(I)=O_g

5. ADVANTAGES:

- Fully Secure Data Transmission.
- No Data Loss.
- If anybody get image then it is not possible to extract data from image.
- Image Size not change after encoding.
- No difference between original image and encoded image.
- It can implement in the military zone.

6. DISADVANTAGE:

- If attacker gets original image then, he can retrieve data by comparing stego image with original image .
- No error checking mechanism
- To transfer small amount of data , we require large size of image.

7. FUTURE SCOPE:

- Use of audio Steganography instead of image.
- To design secure ERP model.
- To secure data transfer of confidential data
- Deployable in military zone
- Deployable in disaster affected area

8. CONCLUSION:

Steganography can be used to maintain the confidentiality of valuable information ,to protect the data from possible theft or unauthorized viewing .As we have implemented LSB insertion method in which we can use lossless image format like .png. We can use specially customized images for bank so that other cannot capture image and find data .

E-ISSN: 2321–9637
Volume 1, Issue 4, November 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

REFERENCES:

[1] Mrs Geeta Navale, Mrs Swati S. Joshi,Ms Aaradhana A Deshmukh, "M-Banking Security – a futuristic improved security approach", IJCSI International Journal of Computer Science Issues, January 2010.
[2] Mohammad Shirali-Shahreza "Improving Mobile Banking Security Using Steganography." 2007 IEEE.
[3] Steganography in digital media by Jessica Fridrich
[4] http://en.wikipedia.org/wiki/Steganography.
[5] Zone-H.org (http://www.infosecwriters.com/text_resources/pdf/Steganography_AMangarae.pdf
[6] MANET, Wikipedia http://en.wikipedia.org/wiki/MANET .
[7] Stegnography-new approach in the mobile banking, sagar dalvi, sagar kharche.