ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

A Novel Approach Using Image Processing for Securing Ad-Hoc Networks

Suresha D[1], Dr. Prakash H N[2]

Research Scholar, Visvesvaraya Technological University, Belgaum, Karnataka, India[1]

Professor and Head, Dept. of CSE, Rajeev Institute of Technology, Hassan, Karnataka, India[2]

Abstract:Mobile ad-hoc networks are being extensively deployed currently since they provide some features which are difficult or impossible to be emulated by conventional networks. The applications ranges from the defence sector (sensor nodes in hostile territory) to general transportation (gadgets used to communicate traffic congestion while traveling) for providing useful infrastructure during disaster recovery. Due to the significance attached to the applications of MANET, security in ad-hoc networks is an important aspect. This paper is focused on using image processing for securing MANET.

Keywords:Device discovery, Image processing, Image Analysis, Limited physical security, Limited resources, Network configuration, Topology maintenance, Security.

I. INTRODUCTION

1.1 IMAGE PROCESSING

Image processing in its broadest sense is an umbrella term for representing and analyzing of data in visual form. Image Processing is the manipulation of numeric data contained in a digital image for the purpose of enhancing its visual appearance. Through image processing, faded pictures can be enhanced, medical images clarified, and satellite photographs calibrated. Image processing software can also translate numeric information into visual images that can be edited, enhanced, filtered, or animated in order to reveal relationships previously not apparent. Image analysis involves collecting data from digital images in the form of measurements that can then be analyzed and transformed. Image analysis provides an accurate digital substitute for rulers and calipers.

Images are categorized according to their source e.g. visual, X-ray and so on. The principal energy source for images is the electromagnetic energy spectrum. Other sources of energy include acoustic, ultrasonic and electronic. Synthetic images are used for modelling and visualization is generated by computer[1]. Digital Images are electronic snapshots taken of a scene or scanned from documents, such as photographs, manuscripts, printed texts, and artwork. The digital image is sampled and mapped as a grid of dots or picture elements or pixels. Each pixel is assigned a tonal value i.e. black, white, shades of grey or color[2], which is represented in binary code as zeros and ones. The binary digits or bits for each pixel are stored in a sequence by a computer and often reduced to a mathematical representation called compressed. The bits are then interpreted and read by the computer to produce an analog version for display or printing.

The fundamental steps in digital image processing include:

- Image acquisition
- Image enhancement
- Image restoration
- Color image processing
- Wavelets and multi resolution processing
- Compression
- Morphological processing
- Segmentation
- Representation and description
- Object recognition

Digital Image Processing and Analysis are used in a wide range of industrial, artistic, and educational applications[3]. Software for image processing and analysis is widely available on all major computer platforms.

Uses of Image Processing:

I. In biotechnology
II. In Medicine
III. In Environmental Science
IV. In Art

1.2 MANET

A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless links. Ad- hoc is Latin and means "for this purpose". An ad-hoc network is a collection of wireless mobile hosts forming a temporary network[4] without the aid of any stand-alone infrastructure or centralized administration. Mobile ad-hoc networks are self-organizing and self-configuring multi hop wireless networks where, the structure of the network changes dynamically. This is mainly due to the mobility of the nodes. Nodes in these networks utilize the same random access wireless channel, cooperating in a friendly manner to engaging themselves in multi hop forwarding. The nodes in the network not only act as hosts but also as routers that route data to/from other nodes in network. In mobile ad-hoc networks where there is no infrastructure support as is the case with wireless networks, and since a destination node might be out of range of a source node transmitting packets. A routing procedure is always needed to find a path so as to forward the packets appropriately between the source and the destination.

Within a cell, a base station can reach all mobile nodes without routing via broadcast in common wireless networks. In the case of ad-hoc networks, each node must be able to forward data for other nodes. This creates additional problems along with the problems of dynamic topology which is unpredictable connectivity changes.

Mobile ad-hoc networks are becoming ever more popular due to their flexibility, low cost, and ease of deployment. However, to achieve these benefits the network must employ a sophisticated routing protocol. Early proposed routing protocols were not designed to operate in the presence of attackers.

Challenges in MANET's

The major open Challenges[4][5][6][7][8] are:

Autonomous- No centralized administration entity is available to manage the operation of the different mobile nodes.

Dynamic topology- Nodes are mobile and can be connected dynamically in an arbitrary manner. Links of the network vary timely and are based on the proximity of one node to another node.

Device discovery- Identifying relevant newly moved in nodes and informing about their existence need dynamic update to facilitate automatic optimal route selection.

Bandwidth optimization- Wireless links have significantly lower capacity than the wired links.

Limited resources- Mobile nodes rely on battery power, which is a scarce resource. Also storage capacity and power are severely limited.

Scalability- Scalability can be broadly defined as whether the network is able to provide an acceptable level of service even in the presence of a large number of nodes.

Limited physical security- Mobility implies higher security risks such as peer-to- peer network architecture or a shared wireless medium accessible to both legitimate network users and malicious attackers. Eavesdropping, spoofing and denial-of-service attacks should be considered.

Infrastructure-less and self operated- Self healing feature demands MANET should realign itself to blanket any node moving out of its range.

Poor Transmission Quality- This is an inherent problem of wireless communication caused by several error sources that result in degradation of the received signal.

Ad-hoc addressing- Challenges in standard addressing scheme to be implemented.

Network configuration- The whole MANET infrastructure is dynamic and is the reason for dynamic connection and disconnection of the variable links.

Topology maintenance- Updating information of dynamic links among nodes in MANET's is a major challenge.

Security- A mobile link is susceptible to attacks as node mobility renders, any node can enter and leave the network, and providing security for communication is a major challenge in MANETs.

There is an increasing need to develop and deploy highly secure mobile ad- hoc networks (MANET's), particularly for military tactical and other security-sensitive operations in adversarial environments. Since a MANET does not rely on a fixed infrastructure, and network elements are wireless mobile nodes, they can rapidly be deployed with relatively low cost.

The main challenges in assuring MANET networks are due to the fact that a mobile link is susceptible to attacks, and node mobility renders the networks to having a highly dynamic topology. The attacks against routing protocols can be categorized into external and internal attacks. An external attack originates from a router that does not participate in the routing process but masquerades as a trusted router. They can either advertise false routing information or generate floods of spurious service requests, such as a denial of service (DOS) attack. An internal attack originates from a compromised, misconfigured, faulty, or even malicious router inside a network domain.

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. MANET's are a kind of wireless ad-hoc networks that usually has a routable networking environment on top of a Link Layer ad-hoc network.

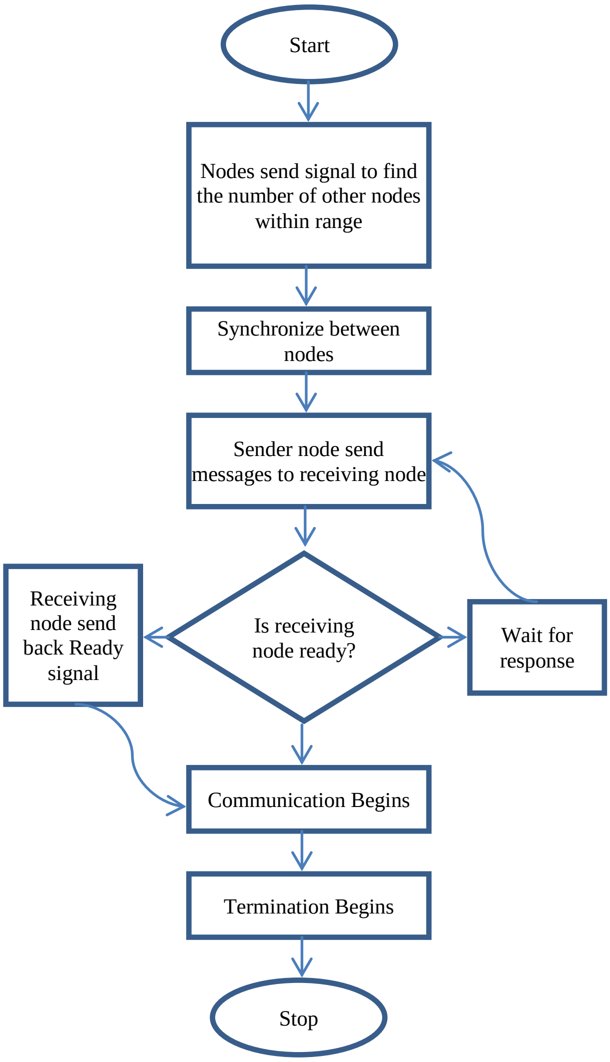
Start
Nodes send signal to find the number of other nodes within range
Synchronize between nodes
Sender node send messages to receiving node
Is receiving node ready?
Receiving node send back Ready signal
Wait for response
Communication Begins
Termination Begins
Stop

Figure1: Working of a general Ad-Hoc Network

An ad-hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any stand-alone infrastructure or centralized administration. Mobile Ad-hoc networks are self-organizing and self-configuring multi hop wireless networks where, the structure of the network changes dynamically. This is mainly due to the mobility of the nodes.

Nodes in these networks utilize the same random access wireless channel, cooperating in a friendly manner to engaging themselves in multi hop forwarding. The nodes in the network not only act as hosts but also as routers that route data to/from other nodes in network.

In mobile ad-hoc networks where there is no infrastructure support as is the case with wireless networks, and since a destination node might be out of range of a source node transmitting packets; a routing procedure is always needed to find a path so as to forward the packets appropriately between the source and the destination. Within a cell, a base station can reach all mobile nodes without routing via broadcast in common wireless networks. In the case of ad-hoc networks, each node must be able to forward data for other nodes. This creates additional problems along with the problems of dynamic topology which is unpredictable connectivity changes.

II. EXISTING SYSTEM

The growth of laptops and 802.11/Wi-Fi wireless networking has made MANET's a popular research topic since the mid-1990s. Many academic papers evaluate different security measures for providing security[9][10] to MANETs and most of the protocols are designed for providing security[11]. And their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measure such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc.

Graphical passwords are to make passwords more memorable and secure. Using a graphical password, users click on images rather than type alphanumeric characters. PassPoints are new and more secure graphical password system[12].

An image authentication can be done by digital watermark[13]. A watermark is a secret code or imageincorporated into an original image which acts to verify both the owner and content of the image. The use of perceptually invisible watermarks is one form of image authentication. A watermarking algorithm consists of three parts:

1. Watermark
2. Marking algorithm
3. Verification algorithm

The Deja Vu approach[14] improve the security of the system which relies on recognition-based, rather than recall-based authentication. Deja Vu authenticates a user through their ability to recognize previously seen images.Secure Authentication using Image Processing and Visual Cryptography for Banking Applications is an algorithm[15] based on image processing and visual cryptography. Which use a technique of processing the signature of a customer and then dividing it into shares. Total number of shares to be created is depending on the scheme chosen by the bank. When two shares are created, one is stored in the bank database and the other is kept by the customer. The customer has to present the share during all of his transactions. This share is stacked with the first share to get the original signature. The correlation method is used to take the decision on acceptance or rejection of the output and authenticate the customer.

III. PROPOSED SECURITY SYSTEM USING IMAGE PROCESSING FOR AD HOC NETWORKS

In the proposed system, whenever the user enters into the ad hoc network an image from the user is taken and that image is divided as one will be the grey image of the original image from the user and the other will the file with color pixel values of the image. Both the image and the file will have the part of key. Then the grey image and file are encrypted with the help of two different types of key. The minimum key sizes will 128 bits. After that again both encrypted files will be joined together and divided into the small packets and each packet again will encrypt with the help of another key. So in this way there are two layer of security before processing the image. Then each packet will pass through the network. At the receiver side after receiving the packet with the help first private we will get separate encrypt d file for grey image and color pixel values after that again we will decrypt with help different private keys of both files and join together for original image. In this proposed system, for manage the better performance, always we will fix the small packet size for transmission and receiver side always buffer space will be more for avoiding the congestion. This entire processing of image will support under UDP (user datagram protocol) which support better speed.

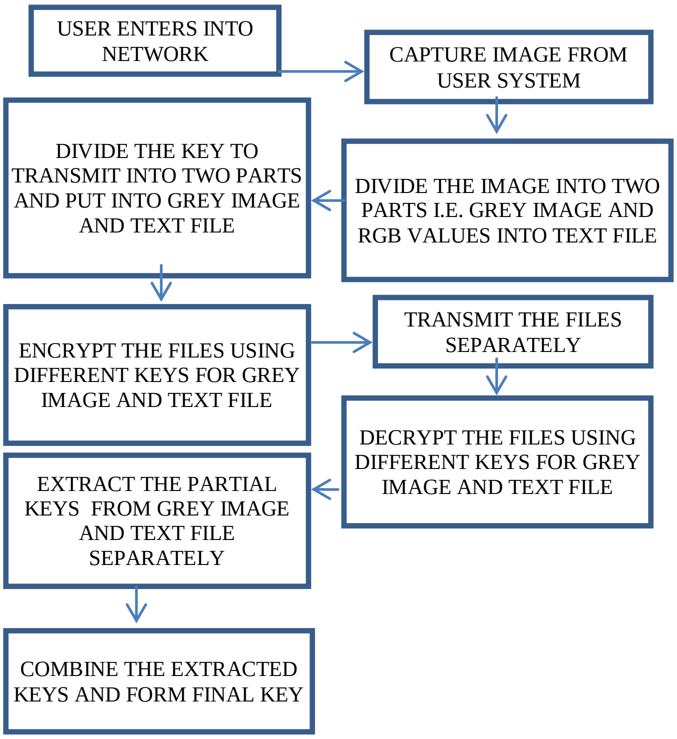
USER ENTERS INTO NETWORK
CAPTURE IMAGE FROM USER SYSTEM
DIVIDE THE KEY TO TRANSMIT INTO TWO PARTS AND PUT INTO GREY IMAGE AND TEXT FILE
DIVIDE THE IMAGE INTO TWO PARTS I.E. GREY IMAGE AND RGB VALUES INTO TEXT FILE
ENCRYPT THE FILES USING DIFFERENT KEYS FOR GREY IMAGE AND TEXT FILE
TRANSMIT THE FILES SEPARATELY
DECRYPT THE FILES USING DIFFERENT KEYS FOR GREY IMAGE AND TEXT FILE
EXTRACT THE PARTIAL KEYS FROM GREY IMAGE AND TEXT FILE SEPARATELY
COMBINE THE EXTRACTED KEYS AND FORM FINAL KEY

Figure2: Architecture of Proposed System

IV. EXPERIMENTAL RESULTS

Whenever user entire into the network and want to have the secure data to transfer with other node in the MANET,

- First users capture/Select the input image and select the key to be transmitted,
- Second user will divide the key into TWO HALF,
- Third the user will divide the input color image into
  1) Grey image with 256 grey levels.
  2) Other will be the text file made up of RGB components of the color image.
- Fourth the divided key will be added to GREY image and TEXT image respectively.
- Fifth the GREY image and TEXT file are ENCRYPTED using one time HASH algorithm of cryptography.
- Sixth the GREY image and TEXT files are transmitted separately in the network that is even the intruder get a file it is hard to get the key as FULL key not present.
- Seventh the GREY image is decrypted separately the original image will be constructed back combining the GREY and RGB image TEXT files.
- Eighth the divided keys are combined to have secure key.

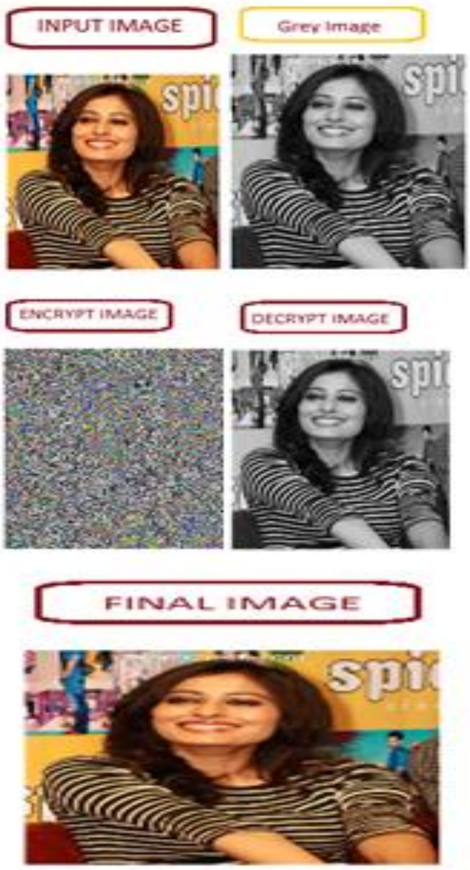

Figure3: Snapshot of Experimental Results

V. CONCLUSION

Secure key transfer is critical for the security of MANET networks. Without knowledge of the identity of intermediate nodes in operation, it is difficult to decide which nodes trustworthy in MANET networks. Transfer of authentication keys through unidentified intermediate nodes is not suitable for use in MANET networks where attackers can monitor to intercept passwords. The use of strong secure key transfer methods that hide authentication keys data is imperative. The proposed system is well suited for secure key transfer in MANET networks, where key is hidden in the image from his system which is different for every user and that image is split into 2 parts and split parts are encrypted for dual level of security. The primary advantage of the proposed approach is that we are able to achieve dual level of security in key transfer in MANET networks with encrypted secure key transfer.

ACKNOWLEDGMENT

First of all I would like to express my heartfelt thanks to Dr. Prakash H N, Professor and Head, Department of Computer Science and Engineering, Rajeev Institute of Technology, Hassan, Karnataka, India for their highly appreciable encouragement and support. Their guidance has been the constant driving force behind my preparation to this Paper. I would also like to thank all who have been instrumental in inspiring and motivating me with all guidelines. I'm glad to admit that the paper has been a great learning experience and I would certainly look forward to future opportunities like this.

REFERENCES

[1] Rafael C. Gonzalez, Richard Eugene Woods, *"Digital Image Processing",* 3rd edition, Pearson. Pp.23-775.

[2] Suresha D, Dr. Ganesh V. Bhat, "*A Survey - Mathematical Morphology operations on Images in MATLA*B", International Journal of Advanced Scientific Research and Technology, Issue 2, Vol.3, June-2012, ISSN No. 2249-9954.

[3] Digital Image Processing.
[Courtesy of http://en.wikipedia.org/wiki/ Digital_image_processing]

[4] Suresha D, Sathisha M S, Alok Ranjan, Prasanna Kumara, *"Implementation of Protected Routing to Defend Byzantine Attacks for MANET's* ",2012 International Journal of Advanced Research in Computer Science, Volume 3, No. 4, July- August2012, ISSN No. 0976-5697.

[5] Andreas Tønnesen, "*Mobile Ad-Hoc Networks*", 802.11 illustrations by LarsStran.
[Courtesy of http://www.olsr.org/docs/wos3-olsr.pdf]

[6] Dipesh Patel, Dr. Rakesh Nagi, "Ad hoc Wireless Networks", A Presentation October 17, 2001.
[Courtesy of http://www.acsu.buffalo.edu/~nagi/courses/ 684/adhoc.pdf]

[7] Lidong Zhou, Zygmunt J. Haas, "*Securing Ad Hoc Networks*", IEEE network, special issue on network security, November/December, 1999.
[Courtesy of http://www.cs.cornell.edu/home/ldzhou/adhoc.pdf]

[8] Ad hoc network specific attacks.
[Courtesy of http://www.spies.informatik.tu-muenchen.de/lehre/seminare/WS0304/UB-hs/burg-ad_hoc_specific_attacks-paper.pdf]

[9] Panagiotis Papadimitratos and Zygmunt J. Haas, "*Secure Routing for Mobile Ad hoc Networks*", In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002.
[Courtesy of http://people.ece.cornell.edu/haas/wnl/Publications/cnds02.pdf]

[10] Haiyun Luo, Petros Zerfos, Jiejun Kong, Songwu Lu and Lixia Zhang, " Self-securing Ad Hoc Wireless Networks".
[Courtesy of http://www.hciteseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.3...pdf]

[11] Suresha D, Shashidhar M S., "Implementation of Secure Biometric Authentication Using Kerberos Protocol", International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE), Volume 3, Issue 3, March 2013, ISSN: 2277 128X

[12] Susan Wiedenbeck Jim Waters, Jean-Camille Birget, "*Authentication Using Graphical Passwords: Basic Results*".
[Courtesy of http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.133.1931]

[13] Raymond B. Wolfgang and Edward J. Delp, "Overview of image security techniques with applications in multimedia systems", Proc. SPIE 3228, Multimedia Networks: Security, Displays, Terminals, and Gateways, 297 (February 1, 1998).
[Courtesy of http://proceedings.spiedigitallibrary.org/proceeding.aspx?articleid=932842]

[14] Rachna Dhamija, Adrian Perrig, "Vu: A User Study Using Images for Authentication".
[Courtesy of https://sparrow.ece.cmu.edu/group/pub/old-pubs/usenix.pdf]

[15] Hegde, C. Manu, S. ; Deepa Shenoy, P. ; Venugopal, K.R., "Secure Authentication using Image Processing and Visual Cryptography for Banking Applications". Advanced Computing and Communications, 2008. ADCOM 2008.
[Courtesy of ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4760429]