ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 1, Issue 8, November 2014

Original Approach With Image Processing For Securing Ad-Hoc Network

Dr.Raman Chadha
Professor, Computer Science Engg. Deptt.
Chandigarh Group of Colleges, Jhanjeri.
Mohali. INDIA
dr.ramanchadha@gmail.com

Mr. A. Aushik
Research Scholar
a_aushik@rediffmail.com

Abstract:
In this article we assess security threats and summarize representative proposals in the context of ad-hoc networks. Here, we review the state of-the-art for original to providing security for wireless networking, namely mobile ad-hoc networks. We recognize the security threats as well as observe the present solution. We additional sum up education erudite, talk about open issues, and recognize future instructions. Mobile ad-hoc network are being expansively deployed at present since they provide some features which are difficult or impossible to be emulate by predictable networks. 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 Ad-hoc network.

Keywords:

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

I. Introduction

1.1 Image Processing

Digital image processing is the use of computer algorithms to perform image processing on digital images. As a subcategory or field of digital signal dispensation, digital image processing has many reward in excess of analog image processing. It allows a great deal wider range of algorithms to be practical to the input data and can evade evils such as the build-up of noise and signal distortion during processing. Since images are defined over two dimensions (perhaps more) digital image processing may be modeled in the form of multidimensional systems. 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 range. Other sources of energy include acoustic, ultrasonic and electronic. Synthetic images are used for modeling and visualization is generating 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

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 1, Issue 8, November 2014

pixel is assigned total 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 account for display.

1.2 MANET

A mobile ad hoc network (MANET) is usually distinct as a network that has a lot of free or independent nodes, frequently composed of mobile devices or other mobile pieces, that can position themselves in various ways and operate without strict top-down network management. There are many different types of setups that could be called MANETs and the potential for this sort of network is still being studied. 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:
Independent- No centralized management entity is available to manage the operation of the different mobile nodes.
Dynamic topology- Nodes are mobile and can be connected dynamically in an random manner. Links of the network vary timely and are based on the proximity of one node to an additional node.
Device detection- Identifying relevant newly moved in nodes and informing about their existence need dynamic update to make easy 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 strictly partial.
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.

Ii. Existing System

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 1, Issue 8, November 2014

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. Pass Points 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 image incorporated 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 method of processing the signature of a customer and then in-between 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 dealings. 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 future 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 smallest amount 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 handset 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 complete

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 1, Issue 8, November 2014

processing of image will support under **UDP (user datagram protocol)** which hold improved speed.

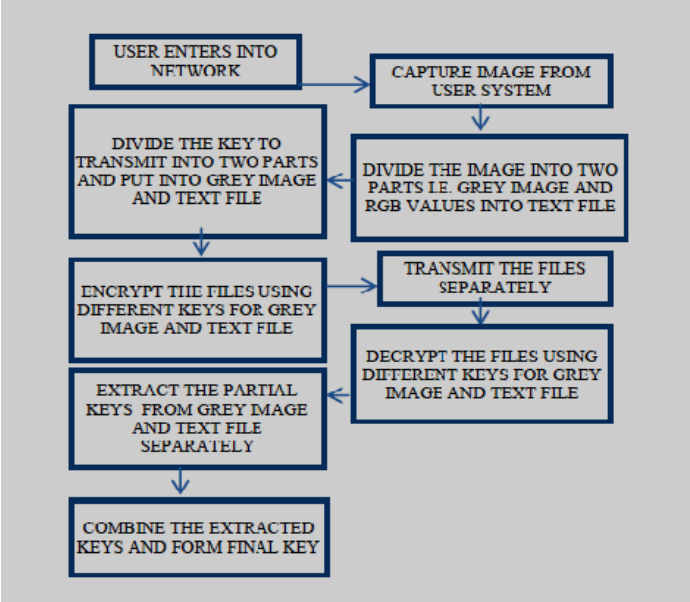

Figure2: Architecture of Proposed System

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
  (i) Grey image with 256 grey levels.
  (ii) 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.

Fig: Snap Shot of Experimental Results

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 1, Issue 8, November 2014

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 dependable in MANET networks. Transfer of authentication keys through nameless midway 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 verification 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 future approach is that we are able to achieve dual level of security in key transfer in MANET networks with encrypted secure key transfer.

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 MATLAB*", 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". [Courtesyof 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

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 1, Issue 8, November 2014

[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]