ISSN:0975-9646

Steganography in Ad Hoc Networks

Rashmi Hegde[#1], Dr. T H Sreenivas[*2]

[#1]PG student, Department of IS&E,
The National Institute of Engineering, Mysore, India

[#2] Professor, Department of IS&E,
The National Institute of Engineering, Mysore, India

Abstract: This paper is a combined contribution to the field of steganography and ad-hoc networks. Various Ad Hoc networks attacks are studied, and steganography methods to help fight them in order to give a new approach to security in ad hoc networks. The proposed solution attracts more importance as it ensures two layers of security through secret asynchronous data sharing through different paths along with using steganographic concepts.

Keywords: Ad Hoc network, steganography, security threats, network security, key exchange, intrusion detection.

I. Introduction

A wireless ad hoc network is a continuously self-configuring, infrastructure-less decentralized type of wireless network shown in Figure 1. An important concern in wireless Adhoc environment is secure transmission of information. Because of no fixed infrastructure flexibility, they can be widely deployed for many applications where supporting structure is unavailable or is unfeasible such as military networks and disaster recovery operations [1, 2].

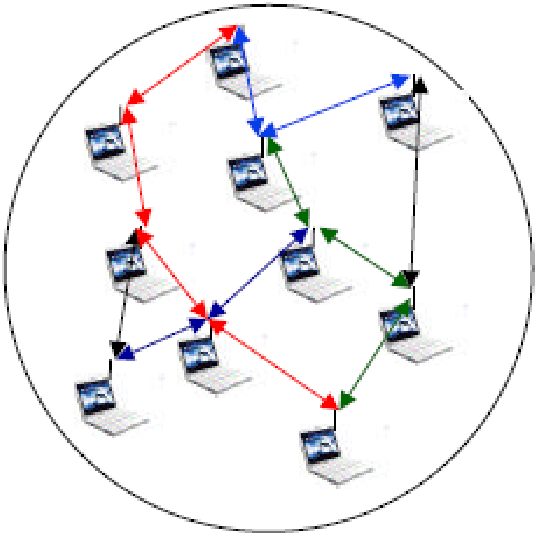

Figure 1: Ad Hoc network

A wireless Adhoc network is one of the growing fields of research at present because of its size, price, power and mobility. These features play an important role in making them to be chosen for many applications irrespective of whether supporting structures are available.

Wireless nodes in ad hoc networks communicate with each other through wireless links or through routers depending upon the distance between the communicating nodes. Network topology of the network changes timely as the nodes are mobile in nature.

Recent progress of technology brings about much more challenges to network security.

Steganography is a method in which information is hidden in an image and the image itself is transmitted across the channel [3]. Steganography can be chosen from all the common encryption methods, as the confidential data is hidden in images and gets away from the eavesdropper even with the knowledge that the confidential encrypted data is present.

Basically the major challenge for employing any efficient security scheme in wireless sensor networks is created by the size of sensors, consequently the processing power, memory and type of tasks expected from the sensors [4].

The purpose of this paper is to integrate steganography method into the wireless Ad Hoc networks communication to enhance security.

The organization is as follows: Attacks in Ad Hoc networks are explained in section 2. Steganography usage is given in section 3. Motivation to this approach is mentioned in section 4. Then, there is a brief overview of the proposed technique in section 5. After that, strength of this technique is seen in section 6. Finally, we will summarize the conclusions and the future work in section 7.

II. Attacks In Ad Hoc Networks[5]

A.Network Layer [5][8][9][10][11][12]

The main network layer attacks include

- **Black hole:** Black holes refer to places in the network where incoming or outgoing traffic is silently discarded (or "dropped"), without informing the source that the data did not reach its intended recipient.
- **Gray hole:** Gray hole is a node in the established routing topology that selectively drops packet with certain probability causing network distraction.
- **Jellyfish attack:** Jelly fish attack is one of the denials of service attack and also a type of passive attack which is difficult to detect. It produces delay before the transmission and reception of data packets in the network.
- **Spoofing:** spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

- **Worm hole:** In a wormhole attack an adversary records information at an origin point, tunnels it (via a faster or direct link) to a destination point more than one-hop away, and retransmits the information in the neighborhood of the destination.
- **Sybil attack:** In the Sybil attack, a malicious node behaves as if it were a larger number of nodes, for example by impersonating other nodes or simply by claiming false identities.
- **Byzantine attack:** Attacks where adversaries have full control of a number of authenticated devices and behave arbitrarily to disrupt the network are referred to as Byzantine attacks.

B. DENIAL OF SERVICE ATTACK

The major denial of service attacks include

- RREQ Flood Attack
- RREP Route loop Attack

C. DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACK

The major distributed denial of service attacks include

- Resource consumption attack
- Replay
- Link spoofing attack or IP spoofing attack
- Flooding attack

D. ATTACKING THE ROUTING PROTOCOL

- Routing Table Poisoning
- Packet Replication
- Route Cache Poisoning
- Rushing Attack

E. SOME OTHER ATTACKS

- Sinkhole attacks
- Location disclosure
- Jamming attack
- Information Disclosure

III. STEGANOGRAPHY USAGE:

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size.

Information hiding techniques such as network, audio, image and text steganography can became a powerful tool that can be used to establish secure and stealth communication among trusted agents [6].

Steganography can be used in two major ways as for confidentiality and compression [7].

A. Steganography for Confidentiality:

Steganography, just like cryptography is a method for ensuring confidentiality of a message or information to be sent across an untrusted channel and it is, unlike cryptography, more effective art because it doesn’t attract the attention of the attacker or eavesdropper.

B. Steganography for Compression

A text file, due to high redundant data, can be compressed to smaller size using many lossless compression algorithms including Context Tree Weighting method (CTW) [10], LZ77[11], LZW[12] etc. After encoding text in the image, an index array is obtained which contains the image pixel locations where the text is mapped. For some initial values of the text file size, it is observed that the index array size exceeds the original text but after a certain threshold, the text file size surpasses the index array size and hence compression is achieved in the index array in contrast to the original text. The compression ratio keeps improving until reaching some saturation level where the change in it is almost indiscernible. The amount of compression appears to have a direct relationship with the text size after the threshold point until the saturation is achieved.

IV. MOTIVATION :

Secret Sharing is one of the efficient methods for secured transmission of data. Vinay Rishiwal[8] proposed an image sharing scheme which uses three images instead of single image for steganographic transmission. Mohammad Shirali-Shahreza[9] proposed an improved method for steganography on mobile phone which hunts for empty pixels in the image. Fahad Ullah[7], gave a novel use of steganography for compression and confidentiality through steganography. Krzysztof Szczypiorski[6], showed how steganographic routing is done in multi agent system environment. Rashmi Hegde [5], captured attention in securing Ad Hoc networks through multi path way routing.

V. PROPOSED TECHNIQUE :

Consider an ad hoc network where each node in the network has its own symmetric key called the neighborhood key which is shared between its unique neighbors. There also exists a concept of message specific keys. Secret transmission of data is an important task to preserve the data from the probable threats, during the transmission. The proposed scheme has many stages of encryption and decryption process along with image sharing technique. The algorithm is as follows,

ALGORITHM:

Step 1: Each message is hidden in an image using the message specific key which forms the first level of security.

Step 2: Each image is divided into r pixels.

Step 3: First pixel of each image is taken to form a group of pixels and then second and so on.

Step 4: The shared images are formed from these grouped pixels and encrypted with neighborhood key and passed on to the next node in the network.

Step 5: Each intermediate node decrypts the image and re-encrypts it with shared neighborhood key with the next node and passes on the images.

Step 6: The destination node decrypts the image with neighborhood key and then with message specific key to get back the shared image.

Step 7: This is repeated for all shared images and then the original messages are rearranged back with the help of index numbers.

The difference between original and shared image can be easily identifiable through the images below which gives the shared image an upper hand during attacks.

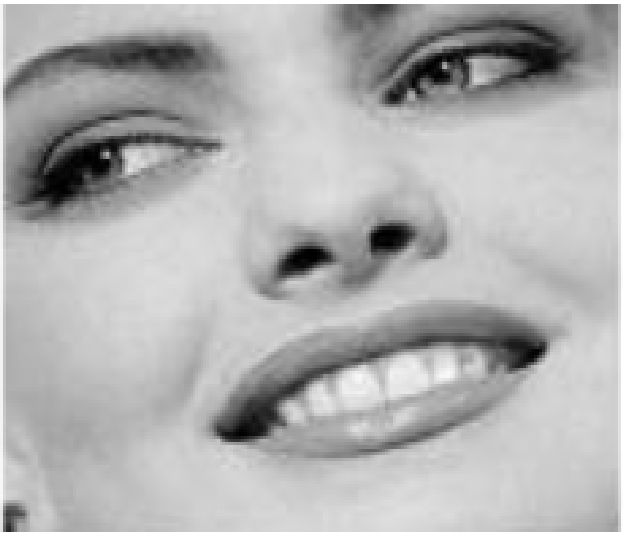

Figure 2: Original image

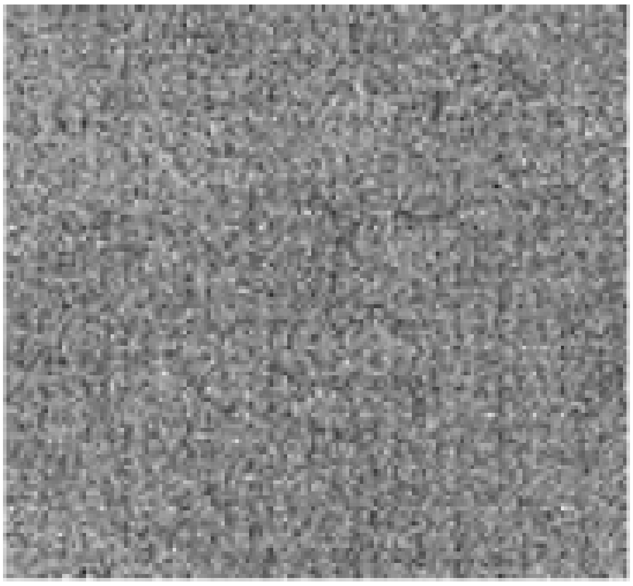

Figure 3: Shared image

Key exchange with only neighborhood nodes aims at reducing crypto-functions processing overheads occurred in a pure reactive approach.

The watchdog, path-rater and feedback system gives a much more boost to the security of the nodes and the routing paths. Watchdog identifies misbehavior and path rater rates nodes according to their reliability.

HELLO messages are periodically sent to the nodes in the group. To forward the information the RREQ and RREP messages are used by each intermediate node to establish the route between the source and the destination nodes in the network. To detect any sort of intrusion, watchdog and path-rater are used. Figure 7 illustrates a watchdog and path-rater operation [5] in a MANET.

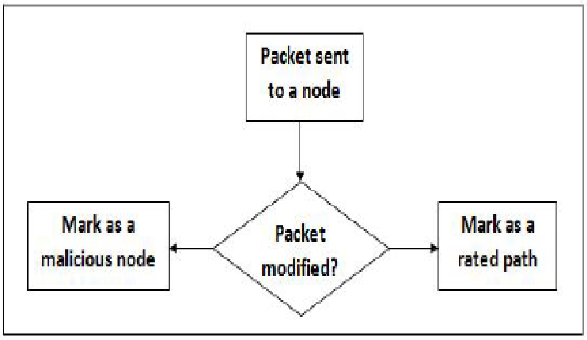

Figure 4: Illustration of watch dog and path rater actions

Fake feedbacks are feedbacks about transactions that never actually occurred. A malicious node may try to provide several bad feedbacks about another node in order to reduce its reputation. To overcome this, each node must provide the proof of its judgement about which packet was dropped by its neighbour identified by the index number or about its malicious behaviour. This must be signed by each node individually [5].

VI. Strength Of This Technique :

The explanation of how this algorithm can reinforce any wireless ad-hoc network against various security threats is given in this section. The basic idea of sharing, transmitting the shares asynchronously via multiple disjoint paths and redundancy in the number of shares well addresses more or less all common possible attacks. In addition to that, steganography lets the attacker to confusion about the location and encryption of the message in the images. This gives two stages of security.

The network layer attacks would be resolved by the asynchronous and multipath routing method. The steganographic integration into this method prevents the attacker from getting a share of the confidential data.

VII. Conclusion

In this paper steganography is integrated to give Ad Hoc networks a boost in security fight. This scheme fights against many attacks that are possible in the network.

The scope of future work is to strengthen this method and also to extend the resistance to much more type of attacks.

Acknowledgement:

We are greatly thankful to our family and friends for the continuous support that has provided a healthy environment to drive us to do this project. We also thank the Principal and the Management of NIE for extending support to this work.

REFERENCES

[1] Hassan A. Karimi, Prashant Krishnamurthy "Real-time routing in mobile networks using GPS and GIS techniques", Proceedings of the 34th IEEE Hawaii International Conference on System Sciences – 2001

[2] Luiz A. DaSilva, Jeff H. Reed, William Newhall, Tutorial on "Ad hoc networks and automotive applications", Mobile and Portable Radio Group, Virginia Polytechnic Institute and State University, 2002

[3] Artz D., "Digital steganography: hiding data within data", Internet Computing, IEEE, vol. 5, Issue: 3, pp. 75-80, May/Jun 2001.

[4] Al-Sakib Khan Pathan, "Security in Wireless Sensor Networks: Issues and Challenges", Feb. 20-22, 2006 ICACT2006

[5] Hegde, Rashmi, and H. D. Phaneendra. "ANew APPROACH TO SECURITY IN AD HOC NETWORKS." *organization* 4.2 (2015).

[6] Krzysztof Szczypiorski, "Steganographic Routing in Multi Agent System Environment", Journal of Information Assurance and Security 2 (2007) 235-243

[7] Ullah, Fahad, et al. "Novel Use of Steganography for Both Confidentiality and Compression." *International Journal of Engineering and Technology* 2.4 (2010): 361-366.

[8] www.wikipedia.com

[9] Kaur, Amandeep, and Deepinder Singh Wadhwa. "Effects of jelly fish attack on mobile ad-hoc network's routing protocols." *IJERA* 2248.9622 (2013): 1694-1700.

[10] Barapatre, Mr Mukesh, and Vikrant Chole. "Spoofing Attack Detection and Localization in Adhoc network using Received Signal Strength (RSS)."*environments* 3.5 (2014).

[11] Lazos, Loukas, et al. "Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach." *Wireless Communications and Networking Conference, 2005 IEEE*. Vol. 2. IEEE, 2005.

[12] Newsome, James, et al. "The sybil attack in sensor networks: analysis & defenses." *Proceedings of the 3rd international symposium on Information processing in sensor networks*. ACM, 2004.