Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 610 – 616

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

Secure localisation of wireless devices with application to sensor networks using steganography

Ankita Tondwalkar[a*] Dr.Preetida Vinayakray-Jani[b]

[a]*Dept of Electronics and Telecommunication Engineering,SPIT,Mumbai-400034,India.*
[b]*Dept of Electronics and Telecommunication Engineering,SPIT,Mumbai-400034,India.*

Abstract

The data collected from the sensor network is meaningful to most of the wireless sensor network applications if and only if it is coupled with the exact positioning of the node. Mere localisation solves the problem of locating an unknown node, however applications like battlefield surveillance or enemy tracking, rescue-operations as well as monitoring of military facilities demand security and reliability of the location information. Therefore secure localisation of non-reference nodes facilitates the localisation system to be robust and secure in adversarial circumstances. The work targets secure localisation of the node position using least significant bit (LSB) insertion technique of steganography. In order for a node to be aware of its position, it sends a cover-image along with the node-id to the Cluster head (CH). The CH which already knows the node position performs LSB embedding on the cover image to generate a stego-image. The stego-image and the cover-image are then compared to get secure position information. The comparison will yield accurate position information only if the cover image is the same. For an adversarial circumstance (different cover image), the security mechanism is robust, and the information will be conveyed to the intended recipient only.

Peer-review under responsibility of organizing committee of the ICISP2015

Keywords–Localisation; security; LSB; Cluster-head; node-id; Steganography; stego-image; cover-image.

1. Introduction

Steganography is an art and science of embedding hidden message in a way that is undetectable to anyone else but the recipient who is aware of the existence of the secret message. The word steganography comes etymologically from the Greek words *Steganos*, meaning secret message and *Graphic*, meaning writing and is literally hide the written message. The military, rescue and search operations as well as the battle field surveillance and other emergency applications require the accurate position information. Any modified or incorrect data deters the success of these applications. Thus if the localisation is not coupled with a security mechanism the entire purpose of localisation is meaningless. This facilitates the need to collaborate the localisation with a robust mechanism to ensure secure transfer of data. The terrestrial architecture is susceptible to many network attacks along with the possibility of the intruder interfering with the localisation process and thereby replaying the false information. There are numerous ways by which security can be achieved. However this paper targets security via steganography as this steganographic technique is robust, involves less overhead wrt to key management. For the

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.107

LSB approach, pointer always points to the LSB bit, so the steganographic approach becomes relatively simpler to implement. If we use steganography on the higher order bits, the difference between the cover and the stego-image will be too large. This will make the secret message vulnerable to any network attack.

Steganography in combination with localisation offers a more reliable and a robust security solution which is of utmost importance in a terrestrial environment. The node position obtained from terrestrial localisation can be securely communicated through Cluster-heads (CHs) via steg-links. The steg-links are established between the communicating entities if and only if both the end points share the same cover image, thus providing for a covert channel. Steganography significantly minimises the problem of unsecured localisation details and provides for authenticate untampered and a secure node position data in a clustered network architecture of Wireless Sensor networks.

Text	Image	Audio/Video	Protocol
Secret message is hidden in a text file.	Secret message is hidden in an image.	Secret data is hidden in an audio signal.	The TCP/IP protocol (header field) is used to hide the secret message.
Most common approach and is rarely used as the text files have a very small amount of redundant data.	The message is embedded using an insertion and extraction algorithm with the same secret key.	Audio embeds Information in an innocuous cover speech in a robust manner and video hides any kind of files in any extension into a video file.	Embeds information within the header field of the network protocols such as TCP/IP.

Concealing data in a message requires the following elements:

- Cover- image (Carrier where data is hidden) to embed the secret message.
- Secret message of any plain text, digital image, or any other form of data.
- Steganographic methods of embedding and extraction of the secret message.
- Stego-key which may be used to insert and extract the data.

The paper has been organised as follows. Section II provides the detail about background followed by System overview in Section III. The proposed system model considers image based steganography approach to find the position of the localised nodes. Section IV analyses the simulation results finally followed by conclusion in Section V.

1.1. Literature Survey

In [3], a new steganographic algorithm is proposed that is use to hide text file inside an image using compression algorithm. This steganographic technique has a maximum compression ratio of 8 bits/ pixel. In the proposed technique an input text file is converted into its binary equivalent and the corresponding number of bits are calculated. A sample cover image for hiding the information is selected and converted to it's corresponding RGB image, with the total count of pixels that make up the image after which the compression function is employed. If the number of bits match the image resolution, the red component of the first character with the first pixel, green of the second character with the first pixel and blue component of the third character with the first pixel is replaced, until all the pixels are exhausted. For cases in which there is a mismatch between the counted pixels and image