Enhancing Security in Ad Hoc Networks through Image Steganography

Amit Kumar , Ganesh Prasad

ABSTRACT:

This project report explores the use of image steganography as a way to improve ad-hoc network security. Discusses various steganography methods, including LSB shift and DCT where this report evaluates their capabilities, imperceptibility, and robustness. The report highlights the limitations of traditional security measures based on the OSI model in ad hoc networks and recommends the use of steganography. Steganography protects against confidential communication, eavesdropping and complements existing security systems. The report includes a practical application that demonstrates the effectiveness of steganography in hiding information while maintaining network performance.

This study contributes to the understanding of ad hoc network security and demonstrates the applicability of steganography in this context.

Keywords: ad hoc network security, image steganography, steganography methods, LSB substitution, DCT, OSI model security

INTRODUCTION:

In the rapidly evolving world of wireless communication, ad hoc networks have gained significant attention due to their flexibility and self-configuring nature. However, the dynamic nature of these networks poses challenges to ensuring robust security. This project report focuses on ad hoc network security through the innovative approach of image steganography.

Steganography is the art of hiding information within digital media, such as images, audio, or video, without raising suspicion. By embedding data within images, steganography provides a covert communication channel that enhances the security of data transmission in ad hoc networks. This report delves into various steganography methods, including LSB substitution, DCT-based analyzing their strengths, limitations, and applicability in the context of ad hoc network security.

Furthermore, the report presents a compelling argument for choosing steganography over the traditional OSI model security approach. While the OSI model provides a layered security framework, it may not be well-suited for the unique challenges of ad hoc networks. Steganography, on the other hand, offers advantages such as covert communication, data confidentiality, anti-tampering capabilities, and resilience against attacks specific to ad hoc networks.

By harnessing the power of steganography, this project aims to contribute to the advancement of secure communication in ad hoc networks, addressing the need for robust security measures in this dynamic and challenging environment.[8][9]

LITERATURE REVIEW:

The literature review conducted for this project report focuses on the security challenges of ad hoc networks and the existing research on image steganography. It explores the limitations of traditional security measures based on the OSI model and examines various steganography techniques, their capacities, imperceptibility, and robustness against attacks in ad hoc network environments.[6][7]

METHODOLOGY:

This project report focuses on addressing the security challenges in ad hoc networks through the innovative approach of image steganography. Ad hoc networks, known for their dynamic and decentralized nature, require robust security mechanisms to protect sensitive information during communication. The report explores various types of steganography methods, such as LSB substitution, DCT-based embedding, and phase encoding, to enhance the security of ad hoc networks. The choice to use steganography over the traditional OSI model security is motivated by its advantages, including covert communication, data confidentiality, anti-tampering capabilities, and resilience against attacks specific to ad hoc networks. By harnessing the power of steganography, this project aims to contribute to the advancement of ad hoc network security, providing a reliable and efficient security solution in this dynamic networking environment.[2][4][9]

CONCLUSION:

This project report highlights the potential of image steganography as an effective security measure for ad hoc networks. By leveraging steganography techniques, such as LSB substitution, DCT, and phase encoding, hidden communication channels can be established, bolstering the confidentiality and integrity of data transmission. The report justifies the adoption of steganography over traditional OSI model security, emphasizing its adaptability to the dynamic and decentralized nature of ad hoc networks. The practical implementation demonstrates the successful integration of steganography in ad hoc networks, providing data concealment without compromising network performance. Overall, this study contributes to the advancement of ad hoc network security by showcasing the practical application of image steganography.[4][6]

SCOPE AND FUTURE WORK:

The project report on ad hoc network security through image steganography has significant scope for further exploration and improvement. The scope of future work includes:

Advanced Steganography Techniques: Investigate and explore more advanced steganography methods, such as transform domain techniques, frequency domain techniques, or adaptive steganography algorithms. These techniques can enhance the security and robustness of data transmission in ad hoc networks. Performance Optimization: Optimize the performance of steganography algorithms to minimize the computational overhead and maximize the data concealment capacity, ensuring efficient and effective utilization of network resources. Security Analysis and Countermeasures: Conduct a comprehensive security analysis to identify vulnerabilities and potential attacks on steganography-based ad hoc network security. Develop countermeasures and mitigation strategies to strengthen the overall security posture. Real-World Implementation and Testing: Implement the steganography-based security mechanisms in real-world ad hoc network scenarios and conduct extensive testing and evaluation to assess their performance, scalability, and effectiveness under various network conditions. Integration with Other Security Measures: Investigate the integration of steganography with other security measures, such as encryption algorithms or intrusion detection systems, to provide a multi-layered security approach in ad hoc networks.[1][10]

REFERENCES :

[1] N. Meghanathan, “Stability and Hop Count of Node-Disjoint and Link-Disjoint Multi-path Routes in Ad Hoc Networks,” Proceedings of the 3 rd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, New York, October 2007.

[2] B. Liang and Z. Haas, “Predictive Distance-based Mobility Management for PCS Networks,” Proceedings of the IEEE International Conference on Computer Communications, Vol. 3, pp. 1377- 1384, March 1999.

[3] T. Morkel 1, J.H.P. Eloff 2, and M.S. Olivier 3, an overview of image steganography, Information and Computer Security Architecture (ICSA) Research Group.

[4] Walaa Abu-Marie, Adnan Gutub and Hussein Abu-Mansour, Image based steganography using Truth Table Based and Determinate Array on RGB Indicator, International Journal of Signal and Image Processing (Vol.1-2010/Iss.3) Abu-Marie et al. / Image Based Steganography Using Truth Table Based and Determinate … / pp. 196-204

[5] Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay And Sugata Sanyal, Steganography and Steganalysis: Different Approaches, Available from: http://arxiv.org/ftp/arxiv/papers/1111/1111.3758.pdf

[6] 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.

[7] www.wikipedia.com

[8] 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.

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

[10] 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.