IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

Imperative Study of Selective Encryption Algorithm Using NS2

Er. Pranay Meshram[1], Ritika Ahirkar[2], Pratiksha Navghare[3], Ritika Kawale[4], Tanvi Channawar[5]
Assistant Professor, Department of Computer Science and Engineering[1]
BE Scholars, Department of Computer Science and Engineering[2,3,4,5]
Priyadarshini J L College of Engineering, Nagpur, Maharashtra, India

Abstract: *Security is one of the most complex features of Internet and Network applications. Symmetric key algorithms are a typically efficient and fast cryptographic system, so it has significant applications across many domains. Cryptosystems based on symmetric key methods, as well as other forms of security, are excellent for an ad hoc wireless network with limited computational resources. We introduce the concept of selective encryption in the context of data protection strategies. To begin, we look at the notion of selective encryption and present a symmetric key-based selective message data encryption algorithm. This paper performs comparative study of three algorithm: Full Encryption, Toss-a-coin selective encryption algorithm and Selective Data Message encryption algorithm considering certain parameters such as Delay, Energy, Packet Delivery Ratio and Throughput. Only the entrusted receiver can decipher the ciphertext, and other unauthorised nodes are unaware of the entire communication, thanks to probabilistic algorithms that introduce adequate uncertainty into the encryption process. In addition, we also use additional security mechanisms to enhance the safety of our proposed system. We show that selected algorithms can indeed improve the efficiency of message encryption as a consequence of our comprehensive simulation studies utilising the NS2 simulator.*

Keywords: Wireless Security; Data Confidentiality; Symmetric Key Encryption; Wireless Ad hoc Networks.

REFERENCES

[1]. Pranay Meshram, S.J Karale, Pratibha Bhaisare, "Comparative Study of Selective Encryption Algorithm for Wireless Adhoc Network" International Journal of Research in Education and Science vol-2,issue-2,February-2012.
[2]. Kushwaha Ajay and H. R Sharma, "A Novel Selective Encryption Method for Securing Text over Mobile Ad hoc Network" 7th International Conference on Communication, Computing and Virtualization 2016 Procedia Computer Science 79 (2016) 16 – 23
[3]. Yonglin Ren, Azzedine Boukerche ,Lynda Mokdad, "Performance Analysis of a Selective Encryption Algorithm for Wireless Ad hoc Networks", IEEE WCNC 2011-Network.
[4]. Patil Ganesh, Madhumita A Chatterjee "Selective Encryption Algorithm for Wireless Adhoc Networks ", International Journal on Advanced Computer Theory and Engineering ISSN (Print) : 2319 – 2526, Volume-1, Issue-1, 2012
[5]. Probabailistic selective encryption algorithm based on AES for wireless adhoc network " ICCC-2012 International Conference on Computer Co" Performance Analysis of selective Encryption Algorithm for Wireless Adhoc Networks ICRACS International conference on recent in computer science, Organised by godwurl Institute of Engineering and Techonology.
[6]. Anish Goel, Kaustubh Chaudhari "FPGA Implementation of a Novel Technique for Selective Image Encryption" IEEE-2016 2nd International Conference on Frontiers of Signal Processing pp.15-19.
[7]. Garima Mehta, Malay Kishore Dutta, Carlos M. Travieso-González & Pyung Soo Kim" Edge Based Selective Encryption Scheme for Biometric Data Using Chaotic Theory" 2014 International Conference on Contemporary Computing and Informatics (IC3I)IEEE-2014 pp.383-386.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, April 2022
Impact Factor: 6.252

[8]. Prati H utari Gani, Maman Abdurohman" Selective Encryption of video MPEG use RSA Algorithm" IEEE- 20 14 1st International Conference on Information Technology, Computer and Electrical Engineering (ICITACEE) pp.124-128.

[9]. M.S. Corson, J.P. Maker, and J.H. Cernicione, Internet-based Mobile Ad Hoc Networking, IEEE Internet Computing, pages 63–70, July-August 1999.

[10]. Kejun Liu, Jing Deng, Member, IEEE, Pramod K. Varshney, Fellow, IEEE, and Kashyap Balkrishnan, Member, IEEE, "An Acknowledgement-based approach for the detection of routing misbehavior in MANET" IEEE Transaction on mobile Computing, VOl.6 No.5, May 2007.