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.

I. INTRODUCTION

Wireless networks are becoming more popular, and Ad hoc networks are following suit. Ad hoc networks are wireless networks in which all nodes can interact directly with each other without the use of a central access point. When a smaller number of nodes are involved, the performance of the Ad hoc network is good, but when the number of nodes increases, the performance gets affected and it becomes hard to manage.

Currently, MANETs are widely used, so they have increased security requirements; for example, cryptography can be used to secure the network. Applications of cryptography are particularly common today in the information era, and typical examples include homeland security, communications between military units, financial transactions, and so on. Symmetric and asymmetric encryption are the two types of data encryption and decryption.

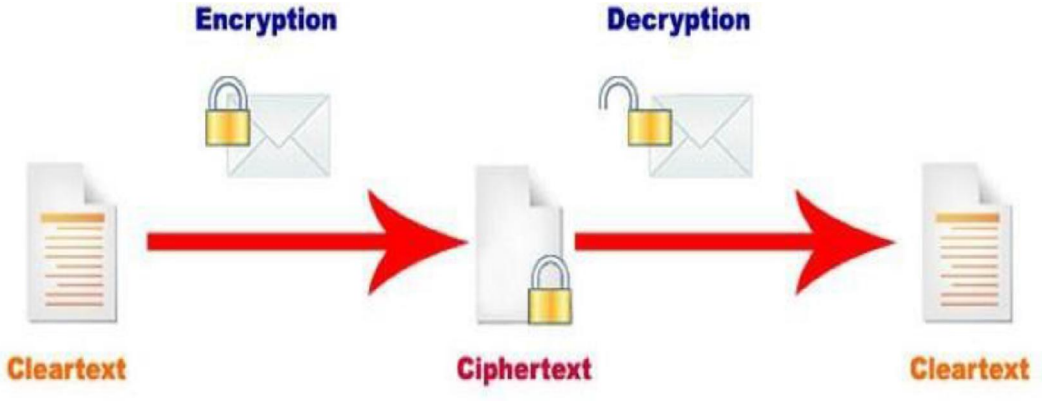


Figure 1: An example of encryption and decryption processes

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

Plaintext is converted to cypher text through encryption, which can then be reversed by decryption. To protect the confidentiality and integrity of data, encryption and decryption are utilised. However, a wireless ad hoc network has particular security and efficiency requirements for conventional cryptographic algorithms due to the features of wireless devices.

Because wireless and mobile devices are often powered by batteries, their computing capabilities are restricted, hence energy conservation is a major challenge in wireless and mobile networks. As a result, an effective selective encryption technique might dramatically reduce wireless device power consumption while also assuring data transmission security. In terms of processing time and security, we will focus on improving the encryption process. Our primary goal is not data transfer through a wireless network, but rather data security against hackers. In an ad hoc network, each node can carry out its own tasks.

To begin, we suggested a selective message data encryption algorithm based on several security measures that selectively encrypts transmitted packets. Selective techniques are made consistent with our proposed scheme, and symmetric key encryption is prevented from having any substantial effect between various communications. Besides sending data between nodes on the wireless network, it is also crucial to protect the data from hackers. Therefore, it effectively protects network data from being exposed to unreliable nodes and reduces the overhead associated with network data protection. We present a method for dealing with dynamic and open situations.

II. Literature Review

Pranay Meshram [1] presents comparative study of three algorithm: Full encryption algorithm, Toss-a-coin selective encryption algorithm, and Probabilistic selective encryption algorithm all take into account certain criteria including encryption time %, encryption time, overall time, and encryption proportion. Finally, we undertake a large number of simulation trials using the ns2 simulator, and our findings suggest that the selected algorithm technique can actually improve message encryption efficiency. Ajay Kushwaha [2] proposes a Selective encryption approach for data encryption called Selective significant data encryption (SSDE). The SSDE provides enough uncertainty to the data encryption process since it selects only significant data from the full message. As a result, the encryption time overhead is reduced and the speed is improved. The encryption is carried out using the symmetric key algorithm. The BLOWFISH algorithm is used for this. It lowers the cost of data protection while yet offering enough uncertainty for increased data security and reliability. The method's performance is evaluated using a large number of experiments.. According to the data, SSDE outperforms alternative wireless network techniques.

Youngling et al. [3] propose a probabilistic selective encryption strategy that uses probabilistic techniques to increase uncertainty. While sending messages, the sender will randomly produce a value to designate the encryption percentage, which represents how many messages will be encrypted among the transmitted messages. They compared their probabilistic approach to the flip of a coin method, in which every alternate word was encrypted, requiring 50% encryption of the message. However, with probabilistic selective encryption, for each run, a random encryption ratio, er, is generated, which determines what part of the message is to be encrypted because of the uncertainty of value of er, randomness is increased, and a probability variable is used for making decision whether a particular message of whole data, should be encrypted or not.

Patil Ganesh [4] suggests a selective encryption approach in wireless and mobile networks that exploits the concept of entropy to reduce the cost of data security. They can reduce the amount of time spent encrypting and decrypting data and increase network efficiency. The suggested method will encrypt communications with greater entropy selectively while leaving messages with low entropy unencrypted. Passing messages having lower entropy without encryption the transmission is intercepted; only that part of the transmission is accessible which has lower entropy and other higher entropy parts are encrypted. The degree of uncertainty in data encryption is described by the encryption probability factor.

The following parameters were used to study the encryption algorithm by these four authors:

Table: Performance Metric

Encryption Time Percentage	The percentage of time spent encrypting and decrypting selected messages as a percentage of the total time spent encrypting all messages.
Encryption Time	The total time is used to encrypt and decrypt messages.
Overall Time	The total time is used to encrypt all messages.
Encryption Proportion	The proportion of encrypted messages to non-encrypted messages.

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

III. METHODOLOGY

Based on various security measures, we suggested a selective message data encryption algorithm that encrypts transmitted packets using a selected algorithm. Our most important aim is not only to send data on the wireless network from one node to another, but also to secure the data from hackers. As a result, it efficiently prevents data exposure to untrustworthy nodes and reduces the overhead spent on network data protection.

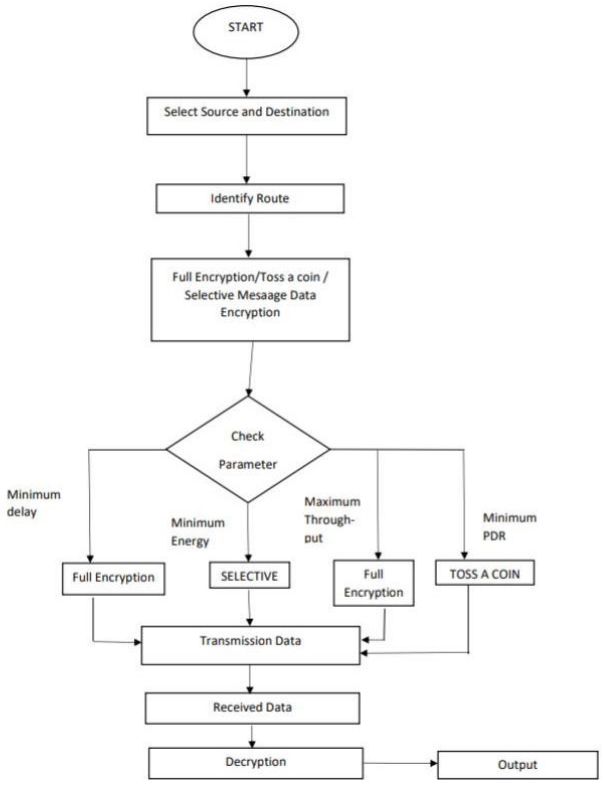
On the basis of the following parameters, we compare our selective message data encryption algorithm to the existing Toss a Coin Algorithm, and full Encryption:

- **Delay**: Delay is the amount of time it takes for a packet of data to travel from one location to another.
- **Energy**: The energy model represents the network's energy level.
- **Packet Delivery Ratio**: The packet delivery ratio (PDR) is the proportion of total packets delivered to total packets sent in a network from a source node to a destination node.
- **Throughput**: The number of packets that successfully arrive at their destinations is measured by throughput.

3.1 Steps:

- Step 1: Start
- Step 2: Select Source and Destination
- Step 3: Identify Route
- Step 4: Apply Encryption algorithm Full Encryption /
    - Toss a coin / Selective Message Data Encryption for Encryption message
- Step 5: Check Parameters such as Delay, Energy, PDR, Throughput.
- Step 6: Received Data
- Step 7: Decryption
- Step 8: Output

3.2 Flowchart



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

IV. GRAPH

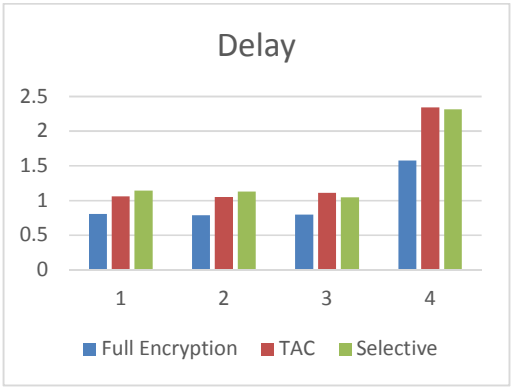


Fig 1. Delay

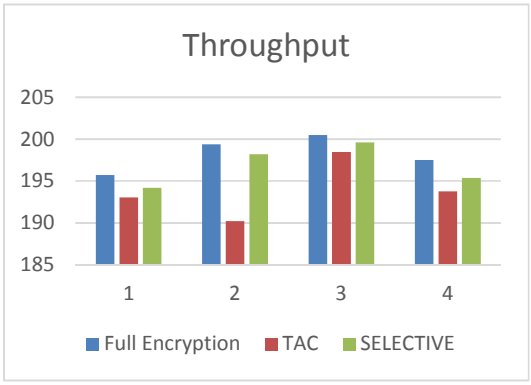


Fig 2. Throughput

In fig 1, we conclude that Delay is minimum in Full Encryption.
In fig 2, we conclude that Packets will arrive successfully to destination in Full Encryption.

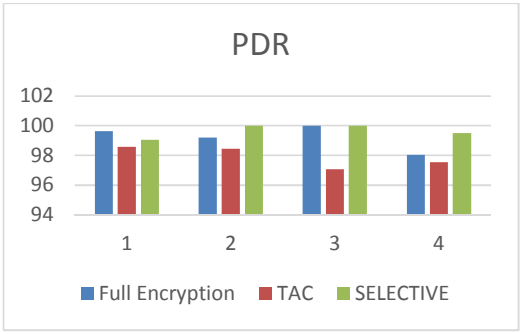


Fig 3. Packet Delivery Ratio

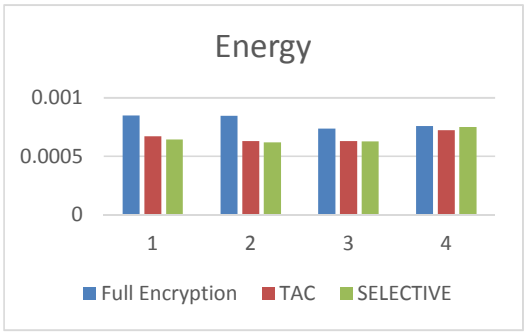


Fig 4. Energy

In Fig 3. we conclude that Packet Delivery Ratio is maximum in Selective Message data encryption and Full Encryption In Fig 4. we conclude that Energy will is minimum in Selective Message data encryption required less in Toss a Coin and Selective Message Data Encryption Algorithm for packets tranfer.

V. CONCLUSION

We will provide a new selective encryption approach in this study to ensure excellent data protection. The Toss a Coin Algorithm, Full Encryption, and Selective Message Data Encryption algorithms are all compared. We infer that the Delay of the Full Encryption Algorithm is the shortest possible.. Energy of Selective message data encryption algorithm and Toss a coin algorithm is Minimum then Full Encryption algorithm. Throughput is maximum in Full encryption algorithm. Packet Delivery Ratio is Maximum in Full Encryption and Selective Message Data Encryption Algorithm.

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

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

[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.

[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.