Performance Analysis of a Selective Encryption Algorithm for securing Text data over Mobile Ad hoc networks

Ajay Kushwaha, Megha Mishra, Subhash Chandra Shrivastava

Abstract*: In recent era security is very much desired for the messages transmitted through the network. The study shows that, even though many approaches have been proposed towards security till date, still the security loopholes also emerging, so constant advancement is crucial for data security. Since all nodes in the network work together as a team to transmit the data, the network may prone to active or passive attacks such as Eavesdropping, Jamming, traffic analysis, Denial of Service, monitoring etc. The research paper introduces a new selective encryption method termed as Selective Significant Data Encryption (SSDE). The SSDE presents adequate protection to the data encryption process by picking up only the significant content from the complete message by referring Natural Language Processing (NLP). As a result, the encryption time overhead will get reduced, and overall performance will improve. Symmetric key algorithms are generally proficient and quick cryptosystem compared to other techniques, so Blowfish system is used for encryption/decryption process. The proposed research work is compared with many conventional methods and found that this approach is more superior to other traditional means.

***Index Terms*: Selective encryption, Mobile Ad hoc Network, Natural Language Processing, Selective significant data encryption, Stop words.**

I. INTRODUCTION

The world is moving towards wireless network because of its decentralized characteristic which does not need any pre-existing infrastructure. The formal definition of ad hoc networks says that it is an independent system capable of routing packets independently. The scale of freedom offered by ad hoc networks is pretty cheaper if compared with other networks. Since ad hoc networks are used these days, so the security can be provided using cryptography. Since every one of the node in the network cooperate as a group to transmit the information, the system is inclined to active and passive attacks such as eavesdropping, jamming, traffic analysis, denial of service, monitoring etc. This paper considers only passive attacks [1] .Without disturbing the transmission; passive attacks intercept the message transmitted onto network and access the valuable information. One can hide information in two ways: one is by masking the presence of the information and the other is by modifying the data to make it meaningless.

Cryptography may be defined as the science and art to alter the information so as to protect it from unintended audience by encrypting it and thus making it pointless. Cryptography uses two styles for data encryption/decryption; that is, Symmetric and Asymmetric methods [2]. The keys used are same for both encryption as well as decryption in case of symmetric methods but are
different in Asymmetric methods. The plain text is changed to cipher text when performing encoding and the cipher text is switched back to the plain text in decryption. This cipher text then transmitted onto the network.

In recent scenario, selective encryption methods are getting more popular because they may reduce the time consumption while encrypting and decrypting data that in turn enhances the competency of the network. This entire task of selecting words for encryption is done with the support of Natural Language Processing. NLP is linked with various branches of computer science. The proposed approach separates the stop words from the entire message and encrypts only the significant data (different words) before transmitting it onto the network. The stop words considered here are those words which are removed before or after from the natural language. These are the commonly used words having little value to the message [3], [4].

II. RELATED WORK

Extensive investigations have been carried out on data encryption and cryptography [5], [6],[14-15]. For data security, various cryptographic techniques were developed such as digital signature, symmetric key, etc. For example, Yonglin et al. [7] developed a probabilistically particular encryption method using symmetric key. It uses the benefits of probabilistic methodology and stochastic algorithm to introduce additional vagueness in data making only entrusted persons decrypting the cipher text. Thamrin et al. [8] proposed a method in cryptosystem for generating pseudo-random number. This mechanism helped in enhancing the reliability and randomness, of key generation. Matin et al. [9] study the results of the new cipher in MANET and wireless LAN networks.

Uthariaraj et al. [10] designed n-way cryptosystem which is used to manage the nodes within a network. This method developed for multicast. They also introduced several functions of key management like key revocation,

Manuscript published on 30 August 2019.
***Correspondence Author(s)**

Ajay Kushwaha (Ph.D. Scholar), associate professor of Computer Science and Engineering at RCET affiliated to Chhattisgarh Swami Vivekanand Technical University, Chhattisgarh.
Dr. Megha Mishra, associate professor at SSGI affiliated to Chhattisgarh Swami Vivekanand Technical University, Chhattisgarh.
Dr. S C Shrivastava, Associate Professor in Mathematics department at Rungta College of Engineering and Technology, Bhilai

rekeying, etc. Zhou and Yang [11] developed a blind signature method. Under this approach, the signer can generate the blind signature and verify, without knowing the text. This technique uses hyper-elliptic curve encryption. Lee et al. [12] proposed a double receiver cryptosystem, which uses two keys for both sender and receiver to encrypt and decrypt the cipher text. Massoudi et al. [13] in his research paper provided a list of assessment standards for JPEG 2000. It includes security, compression, encryption ratio; etc Priyanka et al. [16] depict the basic problems of ad hoc network. The paper also explained the challenges and vulnerabilities of Mobile Ad hoc .Umaparvathi et al. [17] presented a comparison of different symmetric and asymmetric methods of cryptography like AES, Blowfish, DES, and 3DES. The performance evaluation shows that blowfish and 3DES are superior to other methods. Schneier [18], [19-22] introduced a new secret-key block cipher called as Blowfish. The size of block is 64 bits. The length of the key can vary up to 448 bits. Initially, it is a complex phase to initialize the values before encryption. But later on, it works efficiently. It has 16 rounds.

Priyadarshini et al. [2] implemented and compared the various cryptographic algorithms like DES, 3DES, AES, RSA, and blowfish by making use of the following metrics like Encryption time, Decryption time, Memory used, Avalanche effect and Entropy. David et al. [23] present a paper on evaluation of load balancing and energy consumption among MANET and Vehicular Ad hoc networks. Sandoval Orozco et al. [24] explained the various common threats to mobile ad hoc networks and assessed several schemes that try to reduce these threats .He discussed various threats like Address Spoofing Threat, Address Space Exhaustion Threat, Address Conflict Threat, False Address Conflict Threat, Denial of Service Threat, Sybil Threat and Negative Reply Threat. The author demonstrated that if new nodes are inserted in MANET during auto configuration can lead to new threats due to behaviour of network. In this research paper Yang et al. [25] emphasized on the basic security issues of shielding the multi-hop network connection between mobile nodes in ad hoc networks. They worked on total security solution for both link and network layer while sending packets over multi-hop wireless network. In this chapter Islam et al. [26] they have analyzed and evaluated in detail on intrusion detection system, key management issues and securing routing. They also provided complete security solutions for Mobile Ad hoc Networks. Bing Wu et al. [27] had a survey on various attacks and their solutions in Mobile Ad hoc Networks. They proposed various solutions to reduce security vulnerabilities. The author also explained vulnerabilities according to protocol layers.

III. CONCEPT OF SELECTIVE ENCRYPTION

In current state, selective encryption approaches are getting more accepted because they decrease the time utilization while encrypting and decrypting the data which augments the competency of the network. The research supports the concept of selective encryption and presents the sketch of some of the picky encryption methodologies. Figure 1 illustrates the process of selective encryption as given below.

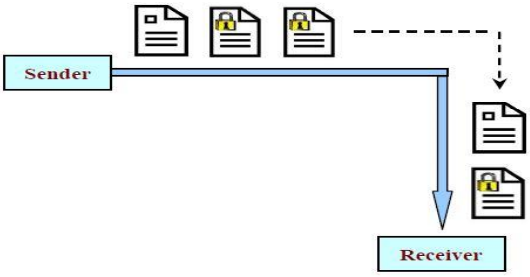
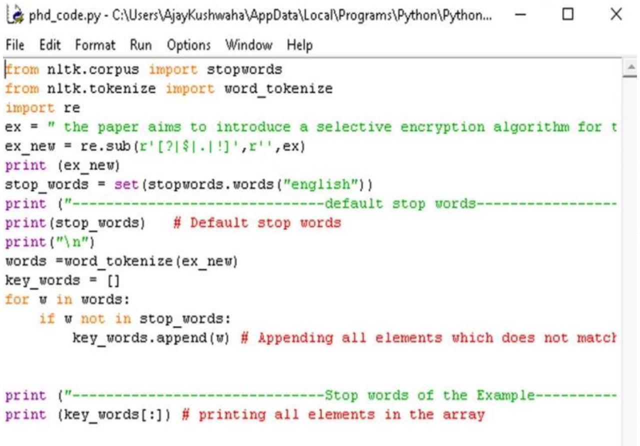


Fig. 1: Schematic diagram of selective encryption algorithm

Selective encryption algorithms are based on the concept of encrypting only selective words of the messages and propose trustworthy safety to the messages transferred through the network. The selective encryption is proficient of getting better scalability for data transfer and also shrinking the dealing out time of encryption and decryption. Natural Language Processing helps to perform selective encryption of the messages. In corpus linguistics, the process of tagging words within sentence based on its classification termed as part of speech tagging. Under this proposed method (SSDE) selective encryption is done by definition and framework of a word in a given message [29-31].

The mechanism of eliminating peculiar regular expressions and stop words from the plain text are shown below in Figure 2.


phd_code.py - C:\Users\AjayKushwaha\AppData\Local\Programs\Python\Python...
File Edit Format Run Options Window Help

```
from nltk.corpus import stopwords
from nltk.tokenize import word_tokenize
import re
ex = " the paper aims to introduce a selective encryption algorithm for t
ex_new = re.sub(r'[?|$|.|!]',r'',ex)
print (ex_new)
stop_words = set(stopwords.words("english"))
print ("------------------------------default stop words-----------------
print(stop_words)   # Default stop words
print("\n")
words =word_tokenize(ex_new)
key_words = []
for w in words:
    if w not in stop_words:
        key_words.append(w) # Appending all elements which does not matcl


print ("------------------------------Stop words of the Example----------
print (key_words[:]) # printing all elements in the array
```

Fig.2: Eliminating peculiar regular expressions and stop words

A. FULL DATA ENCRYPTION METHOD

Selective encryption algorithm has benefits of cryptographic techniques, i.e., symmetric and asymmetric algorithms, to assure the safety of transfer of information between the two nodes. In this approach, the whole message sent from sender end to receiver end is entirely encrypted. The encryption ratio is 100%. No data is left unencrypted. It is the safest way to secure data while transmitting from sender end to receiver end.

B. TOSS- A - COIN METHOD

The second approach used to provide sufficient uncertainty to data is Toss- a -coin method. It’s a primary method to give enough uncertainty to data encryption. In this method, the entire message to be transmitted is split into two categories: odd group contains all bizarre number messages like M_1, M_3, M_5….$M_{(2n+1)}$ and even group include all even like M_2……$M_{(2n)}$.

The ambiguity involved here is to choose that on which group encryption is done, even or odd. The decision is done through toss-a-coin method which tells about the group encoded. Under this method, only 50% of data randomly got encrypted and rest is sent as it on the network and thus the amount of data to be encoded is decreased. The encryption ratio is 50% only. The problem with this method is that we need a high degree of randomness in the encrypted message to make difficult for intruder to hack the messages.

IV. PROPOSED METHODOLOGY

This section will explain working of proposed selective encryption method .Our method picks only keywords (significant data) existing in the plain text and encrypts them prior to transmitting over the network. The research work emphasizes only on significant data in SSDE (SELECTIVE SIGNIFICANT DATA ENCRYPTION) method. Significant data are those keywords that hold the significance of the complete message. Apart from significant data, remaining commonly used words like articles, pronouns, conjunctions, prepositions, and interjections are sent with no encryption. The proposed algorithm is as follows:

A. PROPOSED ALGORITHM

```
Step1.   Input Plain text file
Step2.   Sentence Segmentation
Step 3.  Removing special characters
Step 4.  Tokenization
Step 5.  Part of Speech tagging
Step 6.  For each Wi, where i=1 to n
           Check if Wi ϵ D
               If yes go to Step 8
               Else go to   Step 7
Step7.   Encrypt Wi using symmetric key approach and
           transmit the message onto the network.
Step8.   Transmit the message onto the network with no
           encryption.
```

Where

“Wi” means words.
“D” is the database (collection of words like articles, conjunctions, etc.)
“n” is the total number of words in message which is to be encrypted .
“i” is the iteration variable.

Figure 3 illustrates the schematic steps of Selective Significant Data Encryption method which is given below.

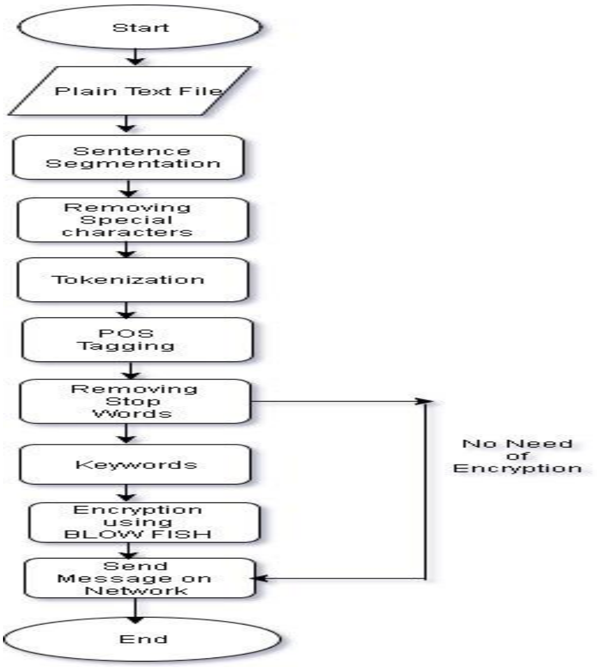


Fig.3: Flow chart of information extraction

B. EVALUATION PARAMETERS

Every Selective Encryption methods have its strengths and weaknesses. Thus, the methods have to be tested taken into consideration the various performance metrics. The paper shows the use and performance study of the following factors:

[1] Encryption

Time required to cryptograph simple text into cipher text is the encryption time. The time relies on the key size, block size of plain text and the mode.

Encryption time = round (stop time – start time, 2)

[2] Decryption

The amount of time used to decrypt cipher text into plain text is decryption time. The time taken for decryption is less compared to encryption time. The time depends on the key size, block size of plain text.

Decryption time = round (Stop time – Start time, 2)

[3] Throughput

The amount of encrypted data that can be transmitted from one place to another in specified time is the throughput. It measured in kbps.

Throughput = round ((File size /Total Time)*(8/1000), 2)

Where
File size in kbps
Total time in seconds

[4] Security

How much secure data communication done between the sender and receiver, making the intruder’s task difficult to hack.

Retrieval Number: I8496078919/19©BEIESP
DOI: 10.35940/ijitee.I8496.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

[5] Entropy

Randomness is a vital property in cryptanalytic processes as a result of information mustn’t be guessed by an intruder. It is a scale of unpredictability within the messages. Entropy study the performance of cryptographic algorithm and it can be calculated using Shannon’s formula.

$$\text{Entropy} = - \sum_{i=1}^{n} \mathrm{p_i} \, log_b(p_i)$$

Where P$_{\mathrm{i}}$ probability of the event happening
b base
n number of different outcomes

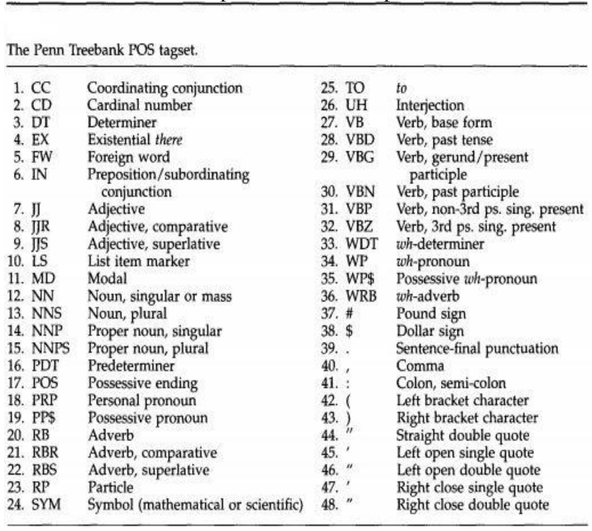
V. PERFORMANCE ANALYSIS AND EVALUATION

A series of simulation performed for validating the various selective encryption methods, within a wireless environment. The software and hardware used for the experiments are Windows 10 64bit Operating System, Python 3.5 with NLTK package, NS 2.34 and i3 processor machine with 4 GB RAM. Throughout the simulation experimentation, all the considered systems are made to run in the same set-up. The performance metrics used to evaluate all methods are encryption time, decryption time, throughput and entropy. In cryptography, entropy is a degree of the unexpectedness. The key taken is of 128-bits, which uniformly generate entropy of 128 bits. On an estimate, it requires 2$^{(128\text{-}1)}$ to crack by any attacker, which is very typical.

Avg per byte encryption for Blowfish = 4.250

Blowfish scores entropy per byte of encryption is far better than other symmetric algorithms. Entropy is a scale of unexpectedness within the information. Blowfish produce high degree of unpredictability in information, as it uses different rounds on S - array and P- array. It makes the output information less susceptible to intruders. A series of simulation performed for validating the various selective encryption methods, within a wireless environment.

There are various lists of parts-of-speech, generally, in most modern language processing on English 48 tag Penn Treebank tag set are used as shown in Figure 3. These tag sets have been used to label a wide variety of corpora, including Wall Street Journal corpus, Brown corpus, etc.



The Penn Treebank POS tagset.

1.	CC	Coordinating conjunction	25.	TO	*to*
2.	CD	Cardinal number	26.	UH	Interjection
3.	DT	Determiner	27.	VB	Verb, base form
4.	EX	Existential *there*	28.	VBD	Verb, past tense
5.	FW	Foreign word	29.	VBG	Verb, gerund/present participle
6.	IN	Preposition/subordinating conjunction	30.	VBN	Verb, past participle
7.	JJ	Adjective	31.	VBP	Verb, non-3rd ps. sing. present
8.	JJR	Adjective, comparative	32.	VBZ	Verb, 3rd ps. sing. present
9.	JJS	Adjective, superlative	33.	WDT	*wh*-determiner
10.	LS	List item marker	34.	WP	*wh*-pronoun
11.	MD	Modal	35.	WP$	Possessive *wh*-pronoun
12.	NN	Noun, singular or mass	36.	WRB	*wh*-adverb
13.	NNS	Noun, plural	37.	#	Pound sign
14.	NNP	Proper noun, singular	38.	$	Dollar sign
15.	NNPS	Proper noun, plural	39.	.	Sentence-final punctuation
16.	PDT	Predeterminer	40.	,	Comma
17.	POS	Possessive ending	41.	:	Colon, semi-colon
18.	PRP	Personal pronoun	42.	(	Left bracket character
19.	PP$	Possessive pronoun	43.	)	Right bracket character
20.	RB	Adverb	44.	"	Straight double quote
21.	RBR	Adverb, comparative	45.	‘	Left open single quote
22.	RBS	Adverb, superlative	46.	“	Left open double quote
23.	RP	Particle	47.	’	Right close single quote
24.	SYM	Symbol (mathematical or scientific)	48.	”	Right close double quote

Fig. 4: Modern English 48 tag Penn Treebank Part-of-speech tags set {source Marcus et al., 1993 [28]}

We have prepared two datasets for the assessment of our method. The datasets used are 92 words and 1000 words from Wikipedia.In this segment, we have carried out the evaluation of our proposed system in comparison with other methods. Furthermore, we have shown how frequent words influences the performance of the method.

In Table 1, we have displayed the results of the first dataset of 92 words, which includes 48 keywords / significant data which need to be encrypted and rest 44 common words sent without encryption, making the encryption/decryption process easier by reducing the overall time overhead compared to other methods.

Table 1. POS tag sequences for 92 words

S .NO	POS TAG	TAG NAME	FREQ. %	POS COUNT	KEY WORDS	COMM. WORDS
1	CC	Coordinating conjunction	5.43	5		5
2	DT	Determiner	8.69	8		8
3	IN	Preposition or subordinating conjunction	14.1	13		13
4	JJ	Adjective	16.4	15		15
5	NN	Noun, singular or mass	33.69	31	31	
6	NNS	Noun, plural	8.69	8	8	
7	NNP	Proper noun, singular	1.08	1	1	
8	RB	Adverb	2.17	2	2	
9	TO	to	1.08	1		1
10	VB	Verb, base form	1.08	1	1	
11	VBG	Verb, present participle	2.17	2	2	
12	VBN	Verb, past participle	1.08	1	1	
13	VBP	Verb, non-3rd ps.sing. present	2.17	2	2	
14	VBZ	Verb, 3rd ps.sing. present	2.17	2		2
TOTAL			100	92	48	44

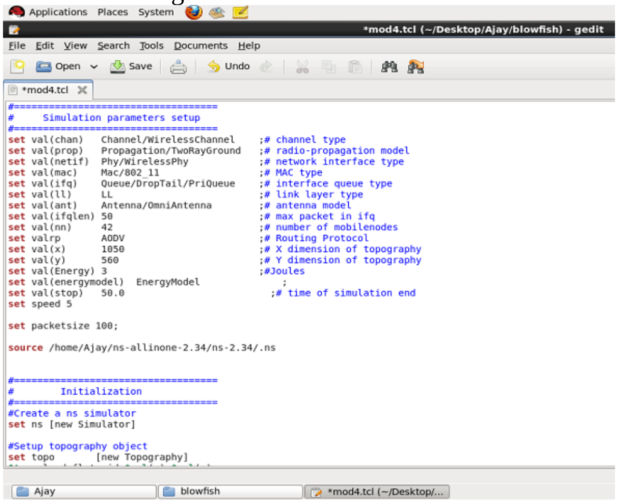
In table 2, we present the performance with a different dataset of 1000 words including 505 keywords / significant data which need to be encrypted and rest 495 common words sent as it is without encryption on to the network.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Table 2. POS tag sequences for 1000 words

S.NO.	POS TAG	TAG NAME	FREQ. %	POS COUNT	KEY WORDS	COMM. WORDS
1	CC	Coordinating conjunction	2.6	26		26
2	CD	Cardinal number	2	20		20
3	DT	Determiner	9.4	94		94
4	EX	Existential *there*	0.3	3		3
5	IN	Preposition or subordinating conjunction	13.2	132		132
6	JJ	Adjective	14.8	148		148
7	JJR	Adjective, comparative	0.7	7		7
8	JJS	Adjective, superlative	0.2	2		2
9	MD	Modal	0.4	4		4
10	NN	Noun, singular or mass	18	180	180	
11	NNS	Noun, plural	10.9	109	109	
12	NNP	Proper noun, singular	5.4	54	54	
13	POS	Possessive ending	0.1	1		1
14	PRP	Personal pronoun	0.2	2		2
15	PRP$	Possessive pronoun	0.1	1		1
16	RB	Adverb	4.6	46	46	
17	RBR	Adverb, comparative	0.3	3	3	
18	RP	Particle	0.2	2		2
19	TO	*to*	1.9	19		19
20	VB	Verb, base form	1.5	15	15	
21	VBD	Verb, past tense	3.3	33	33	
22	VBG	Verb, present participle	2.4	24	24	
23	VBN	Verb, past participle	3.1	31	31	
24	VBP	Verb, non-3rd ps.sing. present	1	10	10	
25	VBZ	Verb, 3rd ps.sing. present	1.3	13		13
26	WDT	Wh-determiner	1.3	13		13
27	WP$	Possessive wh-pronoun	0.1	1		1
28	WRB	Wh-adverb	0.7	7		7
		Total		**1000**	**505**	**495**

The various simulation parameters used in our research work is shown below in figure 5.



```
#====================================
#     Simulation parameters setup
#====================================
set val(chan)   Channel/WirelessChannel    ;# channel type
set val(prop)   Propagation/TwoRayGround   ;# radio-propagation model
set val(netif)  Phy/WirelessPhy            ;# network interface type
set val(mac)    Mac/802_11                 ;# MAC type
set val(ifq)    Queue/DropTail/PriQueue    ;# interface queue type
set val(ll)     LL                         ;# link layer type
set val(ant)    Antenna/OmniAntenna        ;# antenna model
set val(ifqlen) 50                         ;# max packet in ifq
set val(nn)     42                         ;# number of mobilenodes
set valrp       AODV                       ;# Routing Protocol
set val(x)      1050                       ;# X dimension of topography
set val(y)      560                        ;# Y dimension of topography
set val(Energy) 3                          ;#Joules
set val(energymodel)  EnergyModel             ;
set val(stop)   50.0                         ;# time of simulation end
set speed 5

set packetsize 100;

source /home/Ajay/ns-allinone-2.34/ns-2.34/.ns


#====================================
#        Initialization
#====================================
#Create a ns simulator
set ns [new Simulator]

#Setup topography object
set topo       [new Topography]
```

Fig. 5: Simulation parameters in NS 2.34

We have taken random file size to evaluate all the three approaches. Figure 6 shows that SSDE takes the least time for encryption compared to full encryption and toss a coin method for encrypting files of different sizes. Our approach revealed improvement over others.

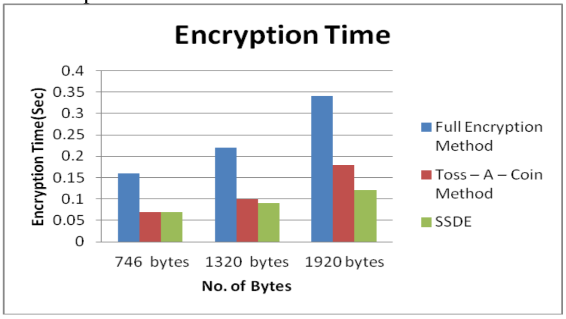


Fig. 6: Encryption Time

Similarly, we have evaluated performance while considering decryption time. Figure 7 shows the time taken for decryption for different file sizes. Our proposed method SSDE has improved performance over other two methods.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

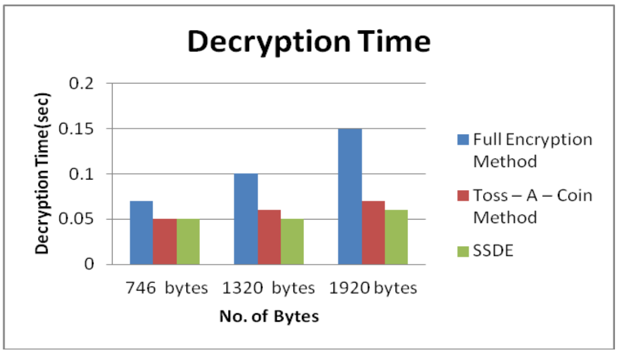


Fig. 7: Decryption Time

Another way to measure the efficiency of any system is to find out the throughput of the system. Here we can see that SSDE proves to be the most efficient methods amongst the three methods, shown in Figure 8.

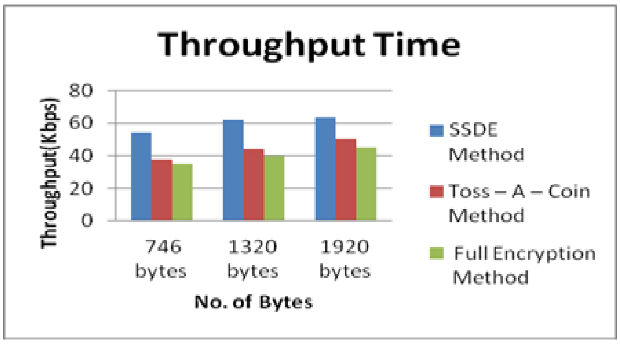


Fig. 8: Throughput time

I. CONCLUSION

The results reveal that the SSDE is seen as promising solution to lessen the cost of data security for Mobile Ad hoc networks. The approached solution is having a foundation of Selective encryption. Selective encryption proves to be quite a capable solution to lessen the price of data fortification and also giving adequate uncertainty for dependability and enhanced data protection. The SSDE method gives sufficient uncertainty to data communication when traveling from the sender to the receiver. The aspect of picking up only the significant data from the entire message brings vagueness. We carried out a comparison of all the approaches, and it is found that both the approaches SSDE and toss-a-coin shows a lower percentage of encryption time compared to full encryption, and this is achieved by the use of selective encryption. It signifies that data communication can be made faster by SSDE and toss-a-coin. As SSDE is encoding only the uncommon words (i.e., significant words) this makes the intruder’s job complex. Toss-a-coin uses less time but ignore significant words. SSDE encrypts random words and makes it difficult for the intruders to recognize what part of messages is encoded, thus gives an additional benefit. It is apparent that SSDE is more proficient and time-saving in comparison to the full encryption and toss-a-coin technique in all facets of encryption, security, etc. Consequently, the presented solution provides a viable key for securing wireless communication in Mobile Ad-hoc network..

REFERENCES

1. W. Lou, W. Liu, and Y. Fang, “SPREAD: enhancing data confidentiality in mobile ad hoc networks,” Proceedings of 23rd Conference of the IEEE Computer and Communications Societies, pp. 2404–2413, 2004.
2. Priyadarshini Patil, Prashant Narayankar, Narayan D G, Meena S M. “A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish”, Procedia Computer Science 78 (2016), pp. 617 – 624.
3. Church K. W., Rau L. F. “Commercial Application of Natural Language Processing”, communication in ACM, 1995, Vol. 38: 11.
4. Eric Brill. “A simple rule-based part of speech tagger”, In Proc. of the workshop on Speech and Natural Language, February 1992, pp. 112-116.
5. Olutobi Owoputi, Brendan O'Connor, Chris Dyer, Kevin Gimpel, Nathan Schneider, and Noah A. Smith. “Improved Part-of-Speech Tagging for Online Conversational Text with Word Clusters”. In Proc. of the Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, June 2013, pp. 380-391.
6. D. Jena, S. K. Panigrahy, and S. K. Jena, “A novel and efficient cryptosystem for long message encryption,” Proceedings of Int. Conference on Industrial and Information Systems, pp. 7–9, 2009.
7. Azzedine Boukerche, Lynda Mokdad Yonglin Ren, "Performance Analysis of a Selective Encryption Algorithm For Wireless Ad hoc Networks," IEEE, 2011, pp. 1038- 1043.
8. N. M. Thamrin, G. Witjaksono, and A. Nuruddin, Eds., “An Enhanced Hardware-based Hybrid Random Number Generator for Cryptosystem”, Proceedings of International Conference on Information Management and Engineering, pp. 152–156, 2009.
9. Matin MA, Hossain Md. Monir, Islam Md Foizul, Islam Muhammad Nazrul, Hossain M Mofazzal,” Performance Evaluation of Symmetric Encryption Algorithm in MANET and WLAN” International Conference for Technical Postgraduates (TECHPOS), at Kuala Lumpur, 14-15 Dec. 2009.
10. V. R. Uthariaraj and A. J. Prakash, "Multicrypt: A Provably Secure Encryption Scheme for Multicast Communication," in Proceedings of 1st Int. Conference on Networks and Communications, 2009, pp. 246–253.
11. X. Zhou and X. Yang, "On certain integrals of Lipchitz-Hankel type involving products of Bessel functions," in Proc. of Pacific-Asia Conf. on Knowledge Engineering and Software Engineering, 2009, pp. 186-189.
12. T. Diament, H. K. Lee, and A. D. Keromytis, Eds., “The dual receiver cryptosystem and its applications,” Proceedings of the 11th conference on Computer and communications security, pp.330–343, 2004.
13. A. Massoudi, F. Lefebvre, and C. De Vleeschouwer, Eds., “Secure and Low-Cost Selective Encryption for JPEG2000”, Proceedings of 10th IEEE International Symposium on Multimedia, pp. 31–38, 2008.
14. Haojie Shen; Li Zhuo; Yingdi Zhao, "An efficient motion reference structure based selective encryption algorithm for H.264 videos" Information Security, IET, 2014, pp.199-206.
15. K. T. Talele, and S. T. Gandhe U. Potdar, "Comparison of MPEG video encryption algorithms," in Proceedings of Int. Conference on Advances in Computing, Communication, and Control, 2009, pp. 289-294.
16. Vinti Parmar, Rahul Rishi Priyanka Goyal, "MANET: Vulnerabilities, Challenges, Attacks, Application , "International Journal of Computational Engineering & Management, vol. 11, pp. 32-37, January 2011.
17. Umaparvathi M., Varughese Dharmishtan K. “Evaluation of Symmetric Encryption Algorithms for MANETs” International Conference on Computational Intelligence and Computing Research (ICCIC) at Coimbatore IEEE 28 - 29 Dec. 2010.
18. B. Schneier. “The Blowfish Encryption Algorithm” In Dr. Dobb's Journal, pp. 38–40, April 1994.
19. Schneier B. (1994) “Description of a new variable-length key, 64-bit block cipher (Blowfish)”. In: Anderson R. (eds) Fast Software Encryption. FSE 1993. Lecture Notes in Computer Science, vol 809. Springer, Berlin, Heidelberg.
20. Schneier B., "Applied Cryptography Second Edition: protocols, algorithms, and source", Beijing: China Machine Press, 2000.
21. Schneier B., "The Blowfish Encryption Algorithm", Retrieved, 2008.
22. Stallings W., “Cryptography and Network Security Principles and Practice” 4th Ed. Prentice-Hill Inc. 2005.
23. S David, R Navaneetha krishnan. “Energy consumption and load balancing compared with VANET and MANET”, International Journal of Pure and Applied Mathematics Volume 116 No. 12 2017, 257-265.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

24. Sandoval Orozco, A. L., J. García Matesanz, Luis Javier García Villalba, J. D. Márquez Díaz, and T- H. Kim. "Security issues in mobile ad hoc networks." International
25. Journal of Distributed Sensor Networks 8, no. 11 (2012).
26. Yang, Hao, Haiyun Luo, Fan Ye, S. W. Lu, and Lixia Zhang. "Security in mobile ad hoc networks: challenges and solutions." (2004): 38-47.
27. Islam, Noman, and Zubair Ahmed Shaikh. "Security issues in mobile ad hoc network." In Wireless networks and security, pp. 49-80. Springer, Berlin, Heidelberg, 2013.
28. Bird, Steven, Edward Loper and Ewan Klein (2009),” Natural Language Processing with Python”. O’Reilly Media n Inc.
29. Marcus, M. P., Marcinkiewicz, M. A., & Santorini, B. (1993). “Building a large annotated corpus of English: The Penn Treebank”. Computational linguistics, 19(2), 313-330.
30. Kushwaha, A., Sharma, H.R. and Ambhaikar, A., 2016. A novel selective encryption method for securing text over mobile ad hoc network. Procedia Computer Science, 79, Pp.16-23.
31. Kushwaha, A. and Sharma, H.R., 2014, November. Designing an Enhanced Selective Encryption Method for Securing Mobile Ad Hoc Network. In 2014 International Conference on Computational Intelligence and Communication Networks (pp. 793-798). IEEE.
32. Kushwaha, A., Sharma, H.R. and Ambhaikar, A., 2018. Selective Encryption Using Natural Language Processing for Text Data in Mobile Ad Hoc Network. In Modeling, Simulation, and Optimization (pp. 15-26). Springer, Cham.

AUTHORS PROFILE

Ajay Kushwaha (Ph.D. Scholar) I am an associate professor of Computer Science and Engineering at RCET affiliated to Chhattisgarh Swami Vivekanand Technical University, Chhattisgarh. Currently, I am pursuing Ph.D. in Computer Science and Engineering from Chhattisgarh Swami Vivekanand Technical University .My research concentrates on Natural Language processing, Mobile Ad hoc Networks, & Cryptography.

Dr. Megha Mishra working as associate professor at SSGI affiliated to Chhattisgarh Swami Vivekanand Technical University, Chhattisgarh.

Dr. **S C Shrivastava** completed her Bachelor of Science and Master of Science degrees in Mathematics from Pt. Ravishankar Shukla university, Raipur. He Received his Ph.D. degree from the same university in mathematics in 2012. Presently he is working as Associate Professor in Mathematics department at Rungta College of Engineering and Technology, Bhilai (affiliated by CSVT University, Bhilai). His research areas are Fixed Point Theory and Fractal Theory. Vivekanand Technical University, Chhattisgarh.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)