International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 6, Issue 4, July- August 2017 ISSN 2278-6856

Selective Encryption using Natural Language Processing for Text data in MANET

Ajay Kushwaha [1], Hari Ram Sharma [2] , Asha Ambhaikar [3]

[1] Rungta College of Engineering and Technology, Bhilai, Chhattisgarh, India,

[2] Rungta College of Engineering and Technology, Bhilai, Chhattisgarh, India,

[3] Rungta College of Engineering and Technology,

Abstract

In Today's era security is highly recommended for data which is transferred over network. The paper aims to introduce a selective encryption algorithm for text data encryption termed as Selective Significant Data Encryption (SSDE) adding a noteworthy uncertainty to data while encryption. The SSDE provides sufficient uncertainty to the data encryption process as it selects only significant data out of the whole message using Natural Language Processing (NLP). The SSDE method is found superior to existing ones, that is, toss-a-coin and full encryption method when performance is evaluated based on the extensive set of experiments using python with NLTK and NS2.

Keywords: Mobile Adhoc Network, Selective Encryption, Selective Significant Data Encryption, Natural Language Toolkit

1. INTRODUCTION

The world is moving towards wireless network nowadays and thus ad hoc networks are also acquiring importance. An Ad hoc network is defined as a wireless network in which, all the nodes are able to communicate with each other directly without the need of a central access point. The performance of Ad hoc network is good when less number of nodes are involved, but when the number of nodes increases, the performance gets affected and becomes difficult to manage. The mobile features make the nodes in the Ad hoc network moving. As mobile ad hoc networks is widely used nowadays so the security requirements for the network is also increasing which can be provided by means of cryptography.

1.1 Challenges Faced By MANET

Distributed: As the network is distributed, no central entity will be present, which makes the overall control over the network difficult. [8]

Routing: The changes in the network topology, protocols demanded as reactive rather than proactive, multicast routing, and routes being multi hop increases the challenge in routing. Routing in mobile condition results in link changes, increase in updates, and non-convergence of routing loop.

Security and Reliability: This includes need of different schemes of authentication and key management due to distributed environment reliability problem in wireless connection etc.

Supporting Channel Access: this includes no fixed base station because of distributed environment, difficulties in avoiding packet collisions etc

Dealing with Mobility: Mobility affects signal transmission, multicasting, applications, routing and channel access.

Power management techniques: All wireless activities consume power which reduces the battery rapidly.

Location- aided Routing: This means, if the associated regions are known with the help of positioning information, routing process will be reduced as it will be spatially oriented.

Inter-networking: Internetworking here means connection between ad hoc network (i.e. MANET) and fixed networks. Dealing with such heterogeneous system is a challenge.

Frequent Network Partitions: This disturbs the whole communication process and requires re setup of network for further proceedings.

Quality of Service (QoS): Quality of services to be present in such dynamic environment is difficult to provide and do not possess fixed guarantee.

Utilizing Bandwidth efficiently: In wireless network, the bandwidth is limited and utilizing it in the constantly changing environment is a challenge.

Changing Topology of the Network: This includes challenges to routing protocols to be followed efficiently.

2. LITERATURE REVIEW

Yonglin et al [1] presented a probabilistic selective encryption algorithm which uses the advantages of the

probabilistic methodology that aims to acquire additional uncertainty in text.

Matin et al. [2] focused on the security that is provided at the application level. As the key size of the algorithm is larger, the time required to break an encryption scheme becomes so excessive that undesirable attacks are meaningless.

Shivendra and Aniruddha [3] proposed a combined approach for identification of a given unknown sample of cipher text. In the first part of system, cipher text samples are generated randomly using different cipher algorithms. In the second part; the system analyses sample through a) Block Length/stream Detection b) Entropy/Reoccurrence Analysis c) Dictionary and Decision tree based approach.
Zhou and Tang [4] proposed a complete and practical RSA encrypt/decrypt solution based on the study of RSA public key algorithm. In addition, the encrypt procedure and code implementation is provided in details.

Umaparvathi and Varughese [5] compared the most commonly used symmetric encryption algorithms AES (Rijndael), DES, 3DES and Blowfish in terms of power consumption. A comparison has been conducted for those encryption algorithms at different data types like text, image, audio and video.

Chang et al. [6] presented a powerful and versatile security suite for the AODV (Ad-hoc On-demand Distance Vector) routing protocol. It offers coverage on common security aspects such as encryption and authentication, and it can be easily modified to work with any distance-vector-based routing for MANET (Mobile Ad hoc Networks).

Nawneet et al. [7] concluded a comprehensive summary which discussed the vulnerabilities, challenges and security attacks on ad-hoc routing protocols which leads to difficulties in designing and development of a secure routing protocol and is challenging task for researcher in an open and distributed communication environments.

3. BASIC CONCEPT OF SELECTIVE ENCRYPTION

Selective encryption algorithms are becoming more popular in recent scenario is due to the fact that they reduce the overhead spent on data encryption/decryption, and thus improve the efficiency of the network.

In this section, we have proposed an algorithm for selective encryption and some commonly used techniques of the selective encryption.

The purpose of selective encryption algorithms is to encrypt only certain portions of the messages and provide trustworthy safety so as to secure the transmitted message confidentiality. Selective encryption is proficient to improve the scalability of data transmission and also reduces the processing time.

3.1 Steps of selective encryption

1. Removing special characters like *$&? Etc.
2. Tokenization in which it extracts all the Key words present in the message.
3. Dropping stopwords (common words) and collecting significant data (key words) from the messages
4. All key words are encrypted and rest common words are send as it is along with encrypted keywords on to the network.

A sample code written in Python language shows how keywords are extracted from a message is given in Figure 1.

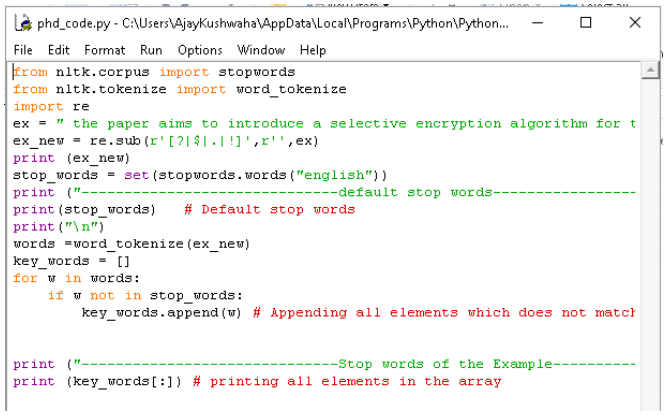

Figure 1 Sample code for information extraction

3.2 Full Data Encryption

In Full Data Encryption whole data that is to be sent over the network is encrypted before transmitted to the receiver side

3.3 Toss-A-Coin Method

This method is a form of Selective Encryption, in which the whole message which is to be transmitted is divided into two groups- even and odd and from the starting of the message, each odd word belongs to odd group and each even word belongs to the even group. The uncertainty involved here is which group will be encrypted i.e. even or odd is not known. As only one group is encrypted, it makes the encryption selective. Now which group will be encrypted is decided by tossing a coin. Here only 50% data is encrypted, thus not much data is reduced and also involvement of uncertainly is less.

3.4 Selective Significant Data Encryption (SSDE)

The approach selects the significant data there in the message and encrypts them prior to sending over the network. Significant data implies the keyword that holds the meaning of entire message. Excluding significant ones, rest commonly used words like articles, pronouns, conjunctions, prepositions, and interjections are sent without encoding. The flowchart of the proposed method (i.e., SSDE) is given in Figure 2 which shows the execution of SSDE algorithm.

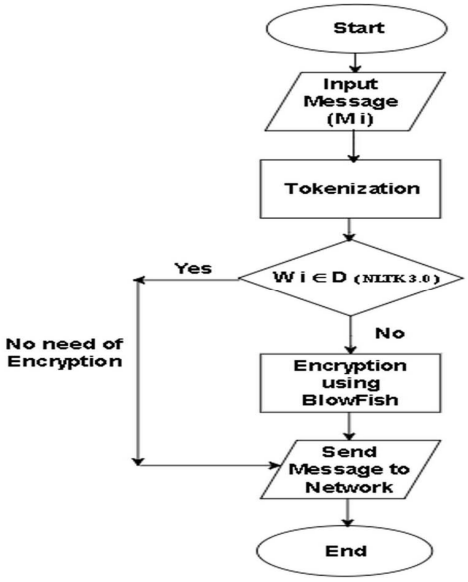

Figure 2 Flow chart of Selective significant data encryption

4 PERFORMANCE EVALUATION

In order to observe the characteristics of SSDE, we carried out an extensive set of experiments within a wireless environment. The experimental setup is done using Red Hat 6.0 32-bit Operating System and NS 2.34, processor: Intel(R) core(TM) i3 CPU M 480 @ 2.67 GHz, 2.66 GHz, 4 GB installed RAM. In this work, the proposed method SSDE is compared with commonly used techniques, that is, Full Encryption and Toss-A-Coin method. Each experiment is run for 50ns of simulation time. During the simulation experiment, the compared systems are all run under the identical scenario. The performance metrics for evaluating the SSDE are Encryption Time, Decryption Time, Battery consumption, End to End Delay and Throughput.

Table 1 Performance Metrics

Performance Metrics	
Encryption Time	Time taken to encrypt plain text into cipher text.
Decryption Time	Time taken to decrypt cipher text into plain text.
End to end delay	Time taken to transfer packets from source to destination.
Battery Consumption	Power consumed during transmission
Throughput	How much encrypted data can be transferred from one location to another in a given amount of time.
Residual Battery	Remaining amount of battery power after transmission.

As stated earlier, two approaches are used as the comparable models with our proposed system. The first approach encrypts all messages without leaving any text unencrypted and thus termed as Full Encryption. In the second approach half of the data is encrypted and is termed as Toss-a-Coin method.

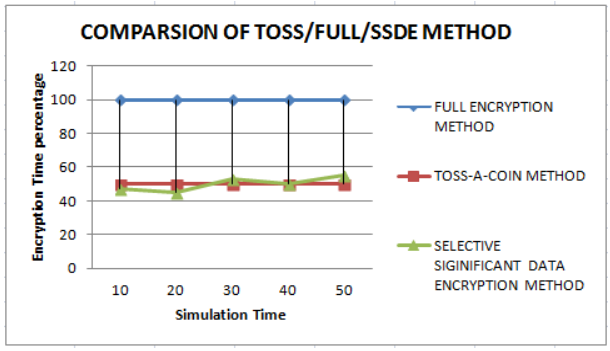

Figure 3 Encryption Time % Vs Simulation Time

Figure 3 and 4 represent the comparison of encryption, decryption and simulation time based on three approaches. Figure 3 show that both toss-a-coin and SSDE have an obvious lower encryption time than full decryption. This advantage is because of selective encryption which reduced the overhead. In Figure 4 the decryption time in full encryption is more as compared to both toss-a-coin and SSDE and thus selective encryption is superior to full encryption for utilization of resources in the network.

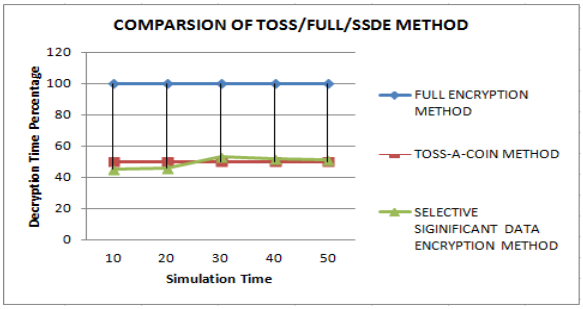

Figure 4 Decryption Time % Vs Simulation Time

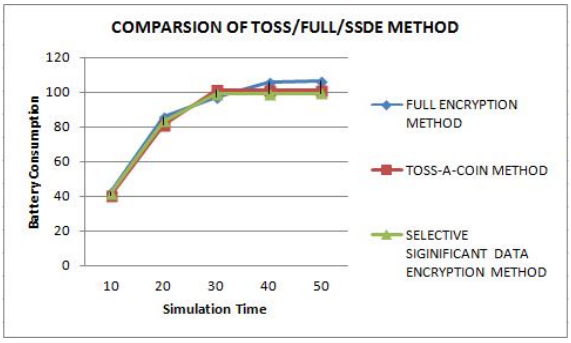

Figure 5 Battery Consumption vs. Simulation Time.

Figure 5 compare the battery consumption of toss-a-coin, full and SSDE respectively. Figure 5 displays that SSDE has lower battery consumption than full method and more than toss-a-coin. As it is difficult to identify what parts of messages are encrypted in SSDE, thus gives an added

advantage. It is evident that SSDE is more efficient and time saving when compared with full and toss-a-coin method in all aspect like encryption ,security etc.

5 CONCLUSION

This paper introduces a better solution for data encryption in wireless networks. The approach is based on Selective encryption, which is one of the most promising solution nowadays to reduce cost of data protection as well as providing sufficient uncertainty for reliability and improved data security. The performance of the method is evaluated based on the extensive set of experiments. The results demonstrate the effectiveness of SSDE over other methods in wireless networks. Thus the provided solution gives a feasible solution for secure wireless communication in Mobile Ad hoc network. This method can be used in social chatting apps, military security, corporate world communication, and government activities involving text data encryption. This method can be used for text data only. In future, this method can be extended for other file formats (i.e. audio, video etc).

References

[1] Boukerche, A., Mokdad, L., Ren, Y.: Performance Analysis of a Selective Encryption Algorithm for Wireless Ad hoc Networks. In: Wireless Communications and Networking Conference, pp. 1038- 1043. IEEE, (2011)

[2] Matin, M.A., Hossain, M. M., Islam, M.F., Islam, M.N., Hossain, M.M.: Performance Evaluation of Symmetric Encryption Algorithm in MANET and WLAN. In: International Conference for Technical Postgraduates (TECHPOS), pp. 1 – 4. IEEE , Kuala Lumpur , (2009)

[3] Mishra, S., Bhattacharjya A.: Pattern Analysis of Cipher Text: A Combined Approach. In: International Conference on Recent Trends in Information technology (ICRTIT), pp. 393 – 398. IEEE,(2013)

[4] Zhou, X., Tang, X.: Research and Implementation of RSA Algorithm for Encryption and Decryption. In: International Conference on Strategic Technology (IFOST), pp. 1118 – 1121. IEEE,(2011)

[5] Umaparvathi, M., Varughese, D.K.: Evaluation of symmetric encryption algorithms for MANETs. In: International Conference on Computational Intelligence and Computing Research (ICCIC), pp. 1 – 3. IEEE , Coimbatore, (2010)

[6] Chang, J.T., Gundala, Moh, S., Moh, M.: VESS - a Versatile Extensible Security Suite for MANET Routing. In: Pacific Rim Conference on Communications, Computers and Signal Processing, pp. 944 – 950. IEEE, Victoria,(2009)

[7] Raj, N., Bharti, P., Thakur, S.: Vulnerabilities, Challenges and Threats in Securing Mobile Ad-hoc Network. In: Fifth International Conference on Communication Systems and Network Technologies, pp. 771 – 775. IEEE, (2015).

[8] Vinti Parmar, Rahul Rishi Priyanka Goyal.: MANET :Vulnerabilities, Challenges, Attacks, Application, International Journal of Computational Engineering & Management, vol. 11, pp. 32-37, (2011)

Abstract

Ajay Kushwaha received his MTech.(CSE) degree in Computer Science Engineering from CSVTU in the year 2009. Currently pursuing Ph.D. in Computer science and Engineering from CSVTU.