Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.700 – 704

RESEARCH ARTICLE

Secure Multi-Message Gossiping, with the Assistance of Mobility

[1]Sanjiwani Gugale, [2]Rupali Dhone, [3]Datta Khedakar

sanjeevanigugale@gmail.com, rupalidhone15@gmail.com, kmcdattasir2@gmail.com

Department of Computer Engineering

Abstract - In this paper, the problem of broadcasting multiple messages from one user to many users in wireless dynamic network. Each user can communicate with all other users by exchanging message, video, audio, images or any other file with it. In this paper we communicate overhead of gossip-based information. We communicate in a large n-user wireless dynamic network in which k user wish to share information with all other user. Gossiping has been widely regarded as simple and efficient method to improve quality of service in large scale wireless network. Gossip is a power paradigm in distributed computing. Gossip algorithm spread messages obliviously without centralized control or management with remarkable speed and with inherent fault tolerance. We investigate the dissemination of information or data in large wireless network where user contacts with each other in a random uncoordinated manner. While transferring data from one user to another user, we apply encryption and decryption using RSA algorithm over the data.

Keywords - Gossip Algorithms, Information Dissemination, AES and DES Algorithm, Probabilistic Broadcasting, Dynamic Wireless Random Network, Mobility

1. Introduction

In wireless networks, a variety of scenarios require users to share their individual information or resources with each other for mutual benefits. Information spreading or dissemination in a large network is typically achieved when each user shares its own information or resources with each other user [2]. Broadcasting is an important communication operation in many multi-user systems. Broadcasting refers to a method of transferring a message to all recipients simultaneously. We use the broadcasting concept in this project for gossiping or Communication between multiple users using mobility. Mobility is a wireless device from which we can communicate or gossiping with each other. We design a simple distributed gossip style protocol that achieves near optimal spreading rate for multiple message

dissemination or spreading, with the assistance of mobility. A rumor spreading and partial list includes file sharing [2]–[5], distributed computation and parameter estimation [4]–[5], and scheduling and control [6], [7].

In this paper, we design a gossip style protocol. In the gossip style protocol we broadcast a message to all the other users to achieve the near optimal spreading rate for communicating or gossiping between the users, with the assistance of mobility. And the velocity is also reduced.

In this paper, we investigate the random-push gossip based algorithm where message selection is depends on the users and select messages randomly. This means that, we are using a random-push gossip based algorithm for broadcasting the message. This system is communicates with its Childs or neighbors and then transfer this data to its neighbors and till the all leaf nodes or like a tree structure, that means the root node sends data.. In this way, this system transfers message from the root node to leaf nodes.

Figure shows the system architecture of our system. In this paper, we can apply the encryption and decryption over the data send by the users. User can send the messages as well as video, audio, images and files to the all connected users in dynamic wireless network.

DES Algorithm:

Data Encryption standard(DES)is a symmetric key block cipher published by NIST.1 It encrypts data in 64-bit block.DES is symmetric key algorithm : the same algorithm and key is used for both encryption and decryption. Key size is 56-bit. The encryption process is made of two permutation i.e. p-boxes, which is called initial and final permutation DES use both transposition and substitution and for that reason is sometimes referred to as a product cipher. Its input, output and key are each 64-bits long. the sets of 64-bits are referred to as blocks.

The cipher consists of 16 rounds or iterations. Each rounds uses a separate key of 48-bits.

Fig shows DES encryption algorithm first, the 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the permuted input.

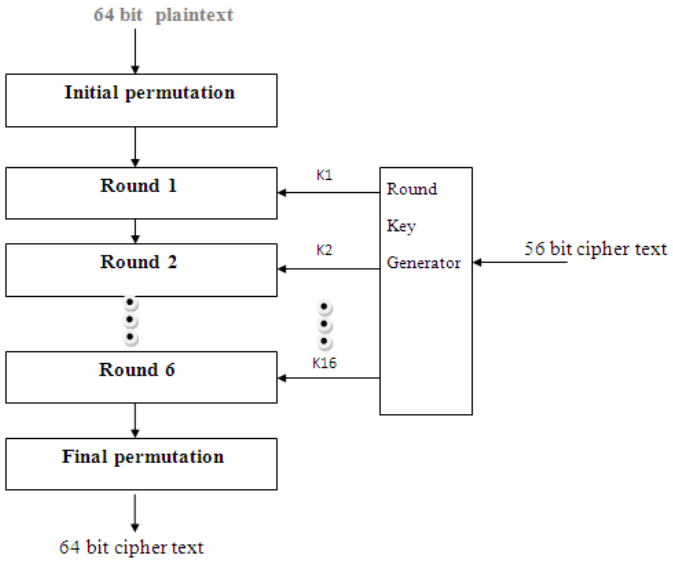


Fig. DES Encryption Algorithm

AES Algorithm:

Advanced Encryption Standard(AES)is symmetric key block cipher published by the NIST in December 2001.In this algorithm variety of consideration, including flexibility, suitability for a variety of hardware and software implement and simplicity, which will make an analysis of security more straight forward.AES is a non-festal cipher that cipher that encrypts and decrypts on number of rounds. The number for 256 bit. Design simplicity. For 128-bits AES, each round contains four steps: 1.byte substitution 2.row shift 3.column mixing 4.round key addition. The input to the encryption and decryption algorithms is a single 128-bit block[12].The block is represented as a row of matrix of 16 bytes. ig shows the overall structure of AES. AES use the several rounds in which each round is made of several stages. data block is transformed from one stage to another. Data block is referred to as state. Block is copied into state array which is modified at each stage of encryption or decryption. After the final stage, state is copied to an output matrix.

2. Existing system

In wireless ad hoc, a variety of scenarios require agents to share their individual information or resources with each other for their benefits. A partial list includes rumor spreading and file sharing, distributed computation and parameter estimation, and control and scheduling.

Because of the huge centralization overhead and unpredictable dynamics in large or complex networks, it is usually more practical to spread or disseminate information and exchange messages in a decentralized and asynchronous manner to combat unpredictable topology changes and the lack of global state data or information. This motivates the exploration of dissemination or spreading information strategies that are inherently simple, asynchronous and distributed while achieving optimal spreading rates.

3. Proposed system

Random gossiping achieves a spreading time for all-to-all spreading over a complete graph , this allows near-optimal spreading time to be achieved within a logarithmic factor from the fundamental lower limit _(n).However, how much benefit can be obtained from more realistic mobility which may be significantly lower than idealized best- Recently, Pettarinet. al explored the information spreading over sparse mobile networks with no connected components of size (log n), which does not account for the dense (interference-limited) network model we consider in this paper . We can transfer or broadcast the messages as well as the video, audio, images and files to the all other users. While transferring the data or information from one user to multiple users, we apply the encryption and decryption over it. In project implementation we use following modules like 1.File transfer server, 2.File transfer client, 3.Gossip, 4.Encryption and Decryption, 5.Establish Dynamic network.

Strategies:

1. Physical-Layer Transmission Strategy:

This strategy is used to achieve efficient spreading, it is natural to resort to a decentralized transmission strategy that supports the order-wise largest number. The following strategy is a candidate that achieves this objective with wireless network communication

2. Message Selection Strategy:

We are interested in a decentralized strategy in which no user has prior information on the number of distinct messages existing in the wireless network. In every time slot: each sender i randomly selects one of the messages it possesses for transmission

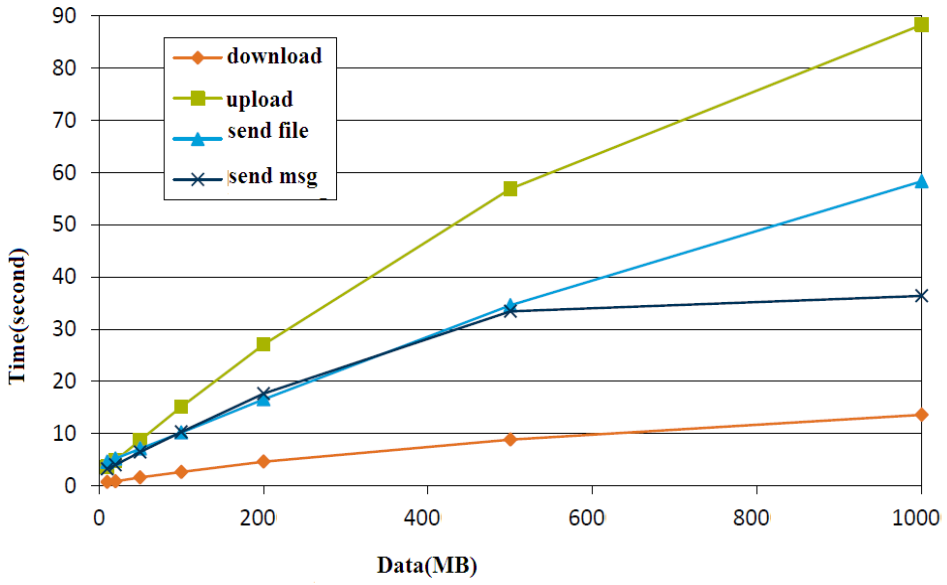
3. Multi-message Spreading in Dynamic Networks with RANDOM-PUSH:

Algorithm for Multi-message Spreading in Dynamic Networks with RANDOM-PUSH

To begin our analysis, we partition the entire unit square as follows:

1. The unit square is divided into a set of non overlapping tiles {Bjg} each of side length √32 log n/n (Note that this is a different partition from sub squares fAjg resulting from the mobility model).
2. The above partition also allows us to slice the network area into vertical strips each of width √32 log n/n and length 1. Label the vertical strips as {Vl} (1 ≤ l ≤√ (32 log n))in increasing order from left to right, and denote by NVl (t) and NVl (t) the number and the set of nodes in Vl that contains M_ by time .
3. The vertical strips are further grouped into vertical blocks {V b} each containing log n strips, i.e. V bj =fVl : (j □ 1) log n + 1 _ l _ j log ng.

Result:



Conclusion:

In this paper, we design a simple distributed gossip-style protocol that achieves near-optimal spreading rate for multimessage dissemination in dynamic wireless network with the assistance of mobility. We used RSA algorithm for encryption and decryption.

Acknowledgement

First and foremost we offer our sincerest gratitude to our college, JSPM's ICOER and our department of Computer Engineering. We extend my heartful gratitude to my guide, Prof.R.N.Phursule and department Computer Engineering, who has supported us throughout our research with their patience and knowledge.

References

[1] IEEE transactions on information theory vol:59 no:6 year 2013, "On The Role of Mobility for multimessage Gossip", Yuxin Chen, Sanjay Shakkottai and Jeffrey G. Andrews.

[2] IEEE INFOCOM 2011 "Sharing Multiple Messages over Mobile Networks", Yuxin Chen, Sanjay Shakkottai and Jeffrey G. Andrews.

[3] The 41st Annual Symposium on Foundations of Computer Science, pp. 565–574, 2000."Randomized rumor spreading," R. Karp, S. Shenker, C.Schindelhauer, and B. Vocking.

[4] J. Tsitsiklis, Problems in decentralized decision making and computation, MIT, PhD dissertation, LIDS,Cambridge, 1984.

[5] IEEE Transactions on Information Theory, vol. 56, no.1, pp. 634 –647, January 2010.K. Jung, J. Shin, and D.Shah, "Distributed averaging via lifted chains".

[6] ACM SIGMETRICS, pp. 27–38, 2006. E.Modiano, G.Zussman, and D. Shah, "Maximizing throughput in wireless networks via gossiping".

[7] IEEE Transactions on Information Theory, vol. 53, no.12,pp. 4640–4654, Dec. 2007. S. Sanghavi, B. Hajek,and L. Massoulie, "Multiple messages with Gossiping".

[8] Revised 21 October 2013; Accepted 22 October 2013 Gang Wang, 1 Zun Lin,1 Wenyang Guan,2 and FengWang "The Performance of Multimessage Algebraic Gossip in a Random Geometric Graph".

[9] IEEE transactions, vol. 52, no. 6, June 2006 S. Boyd,Fellow, IEEE, A. Ghosh, Student Member, IEEE, B.Prabhakar, Member, IEEE, and D. Shah "Randomized Gossip Algorithms".

[10] IEEE transactions on information theory, vol. 53, no.12, December 2007. S. Sanghavi, Member, IEEE, B.Hajek, Fellow, IEEE, and L. Massoulie," Gossiping With Multiple Messages".

[11] IEEE Transactions, Supratim Deb and Muriel M´edard Laboratory for Information & Decision Systems Massachusetts Institute of Technology Cambridge,"Algebraic Gossip.

[12] IJSR "Encryption Algorithms Used for Secured Communication" Chunlei Wang, Guangyi Wang, Yue Sun and Wei Chen

