ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

Integrated Collective Node Behaviour Analysis with Onion Protocol for Best and Secured Transmission

Bhavani Raj.R[1], M.K.Nandhini[2], N.Soundharyaa[3] , R.Raja[4]

UG Student, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India [1,2,3]

Assistant Professor, Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, Tamil Nadu, India [4]

ABSTRACT: Electronic Communication is turning into a critical issue now-a-days. Concealing the points of interest of correspondence, content, hubs from the foes like a busybody, programmer and so forth is normally not considering previously. Delay tolerant system (DTN) directing gives a correspondence crude in discontinuously detached systems, for example, combat zone interchanges and human-contact systems. In DTN applications, the namelessness saving component , which conceals the personalities of imparting parties, prompts trouble in finding malevolent hubs. An onion-based mysterious directing with multi-duplicate sending in which L duplicates of a message is permitted now . The conveyance rate, message sending cost, traceable rate, and way and hub secrecy are characterized and broke down at this point. In this paper, an effective system is developed which uses Onion routing but not anonymous one. Each node in the network is provided with needed details (ID , Primary or encryption key, Secondary key , Decryption key) to encrypt in multiple layers and ensure high level security . The system is designed for collecting feedback about neighbouring nodes transmitting packets. Every node's review is analyzed and according to the review analysis , the best route is identified for the packets that involves in transmission.

KEYWORDS : Onion routing , DTN , Encryption , Multiple layer , Feedback , best route

I. INTRODUCTION

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and networkaccessible resources. It is a branch of computer science that involves in securing a computer network and network infrastructure devices to prevent unauthorized access, data theft, network misuse, device and data modification. Delay Tolerant Network (DTN) routing enables message delivery in intermittently disconnected networks such as battlefield communications, bus-to-bus networks [8], PeopleNet [9], pocket switched networks [10], and so on. In these DTN applications, not only is improving the message delivery and minimizing the forwarding cost important, but providing security and privacy preserving mechanisms are also both theoretically and practically important. While the messages exchanged between two nodes can be protected with end-to-end encryption, a large amount of information, including node identifiers, the locations of end hosts, and routing paths, may be revealed by traffic analyses. It is crucial to protect these types of sensitive information in critical communication environments. For instance, in a battlefield, one of the communicating end hosts is most likely to be a commander, and thus, disclosing the location of the end host will likely result in a mission failure. As a defending mechanism, anonymous communications are widely studied to hide where a message comes from and where it goes to, as well as the identities of communicating end hosts. Although significant efforts have been made to design anonymous routing protocols for the Internet and ad hoc networks these approaches are not appropriate for DTNs due to key

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

differences between them. First, the graph representation of a DTN is contact-based, while that of an ad hoc network indicates the physical topology formed by nodes. Second, neither stable end-to-end communication links nor transmission opportunities are assumed due to the fact that intermittent connectivity is very limited. Third, a DTN routing is implemented in the Bundle layer which is located between the transport and application layers. These factors make the existing ad hoc anonymous routing protocol unfeasible in such a network, and therefore, these are the reasons that we again study anonymous communications primarily designed for DTNs.

To the best of our knowledge, very few anonymous routing protocols are designed for DTNs. One of the well-known DTN routing protocols to preserve anonymity is onion routing where layered encryption, each by different secret keys, is applied to a message, and each layer can be peeled off with the corresponding secret key. To accommodate the limited forwarding opportunities, the idea of onion groups is introduced in which a set of nodes form an onion group so that any node in the same onion group is able to encrypt/decrypt the corresponding layer. However, theoretical analysis is yet to be done. Therefore, we are interested in the theoretical aspects of onion-based anonymous routing in DTNs.

II. LITERATURE SURVEY

In the year 2014 Qinghua Li, Guohong Cao, Guohong Cao proposed an efficient protocol to obtain the Sum aggregate, which employs an additive homomorphic encryption and a novel key management technique to support large plaintext space. The sum aggregation protocol is also extended to obtain the Min aggregate of time-series data.And also a scheme that utilizes the redundancy in security to reduce the communication cost for each join and leave[1].

In the year 2014, Cong Liu and Jie Wu provided an optimal forwarding protocol which maximizes the expected delivery rate while satisfying a certain constant on the number of forwardings per message. In our proposed optimal probabilistic forwarding (OPF) protocol, we use an optimal proba-bilistic forwarding metric derived by modeling each forwarding as an optimal stopping rule problem. We also present several extensions to allow OPF to use only partial routing information and work with other probabilistic forwarding schemes such as ticket-based forwarding[2].

In the year 2009 , Cong Liu and Jie Wu proposed to avoid the cost associated with °ooding, much e®ort has been focused on probabilistic forwarding, which aims to reduce the cost of forwarding while retaining a high performance rate by forwarding messages only to nodes that have high delivery probabilities. This paper aims to provide an optimal forwarding protocol which maximizes the expected delivery rate while satisfying a certain constant on the number of forwardings per message[3].

In the year 2007 ArunaBalasubramanian, Brian Neil Levine and ArunVenkataramani proposed an intentional DTN routing protocol that can optimize a specific routing metric such as worst-case delivery delay or the fraction of packets that are delivered within a deadline. The key insight is to treat DTN routing as a resource allocation problem that translates the routing metric into per-packet utilities which determine how packets should be replicated in the system.[4].

In the year 2005, ThrasyvoulosSpyropoulos, KonstantinosPsounis, Cauligi S. Raghavendra introduced a new routing scheme, called Spray and Wait, that “sprays” a number of copies into the network,and then “waits” till one of these nodes meets the destination. Using theory and simulations they show that Spray and Wait outperforms all existing schemes with respect to both average message delivery delay and number of transmissions per message delivered[5].

In the year 2000 **,** Amin Vahdat and David Becker proposed techniques to deliver messages in the case where there is nevera connected path from source to destination or when a network partition exists at the time a message is originated. To this end, they introduced *Epidemic Routing*, where random pair-wise exchanges of messages among mobile hosts ensure eventual message delivery. The goals of Epidemic Routing are to: i) maximize message delivery rate, ii) minimize message latency, and iii) minimize the total resources consumed in message delivery[6].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

III. PROPOSED SYSTEM

We develop an effective system which collects Feedback about neighboring nodes transmitting the packets. Every node's review is analyzed and best route is identified only the packets are transmitted. In every node security will be in higher level. Because, we are using onion like security system to protect our data while transfer. For every node there will be a private key for security. While encrypt the data every level of key will be add with previous node till at the end of destination. So the decryption will only made on destination side only. Through this security level is increased.

A)SYSTEM DESIGN

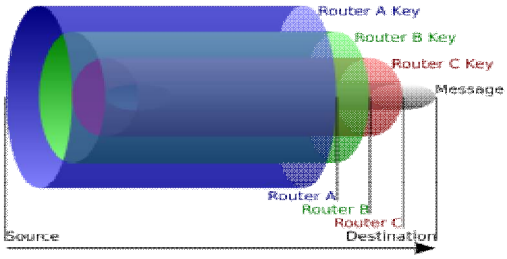

Fig.3.1.Onion Routing Architecture

Fig.3.1. shows that the source of the data sends the onion to Router A, which removes a layer of encryption to learn only where to send it next and where it came from (though it does not know if the sender is the origin or just another node). Router A sends it to Router B, which decrypts another layer to learn its next destination. Router B sends it to Router C, which removes the final layer of encryption and transmits the original message to its destination.

B)ARCHITECTURE

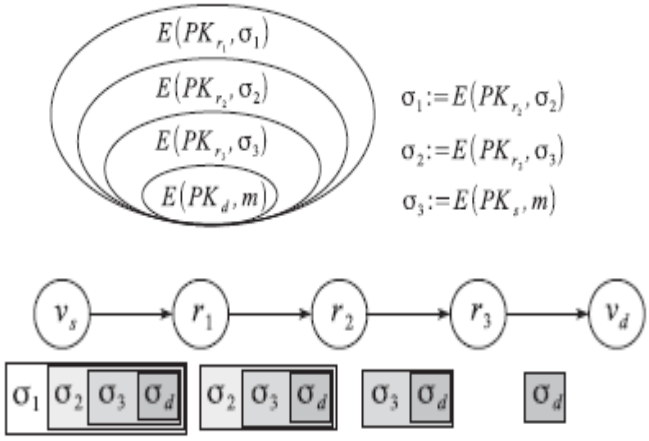

Fig.3.2.Working of Multilayer Encryption

a)NETWORK CONSTRUCTION & ENCRYPTION

In this system, first we have to construct a network which consists of 'n' number of Nodes. So that nodes can request data from other nodes in the network. Since the Nodes have the mobility property, we can assume that the nodes are moving across the network. Network is used to store all the Nodes information like Node ID and other information. Each node contains primary key, secondary key and private key. Also network will monitor all the Nodes

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

Communication for security purpose.The data which is to be transmitted is encrypted before sending the packets to the destination. The data security is ensured using this step. In this system, encryption process is deployed throughout the process of implementation. This encryption process is used in initial process as well as in onion protocol process. Here, RSA algorithm is used for encryption.

b) FEEDBACK ANALYSIS&BEST ROUTE ANALYSIS

Here, the feedback of every node is analyzed and the final review is obtained. Feedback is collected from that node as well as from the predecessor & successor nodes for performance analysis. Overall analysis of a node is concluded based on the overall feedbacks obtained. This process is important to identify the best route to send the packets to the destination so as to reach the destination very effectively & safely.

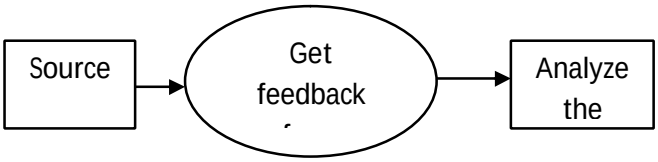

Fig.3.3.Collecting feedback from neighbouring nodes

This subsystem also plays a vital role to identify the best route for effective data transfer. This process will endure the secured data transfer based on the previous data transfer by the corresponding nodes. Overall feedbacks are analyzed and best nodes are identified so that using those nodes, best route is formed. Once the route is identified, data is transferred.

c) ONION PROTOCOL

In this subsystem, onion protocol is implemented. Let us assume N1 to N3 is identified as the best intermediate nodes then the packets flow will be S N1 N2 N3 D.

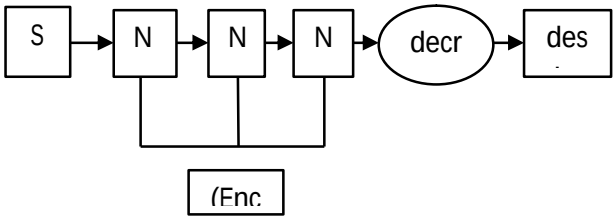

Fig.3.4. Application of Onion Protocol

As per encryption sub system, packets are encrypted and again encrypted using primary key of Destination. This resultant data is again encrypted using primary key of N3 and N2, it is again encrypted by N1 and finally by the destination primary key.While decrypting , the encrypted data will be first decrypted by the decryption key of N1, again decrypted by the decryption key of N2 and then decrypted by decryption key of N3 . Then the node details are verified and decryption is done using RSA algorithm.

IV. RESULTS

Every node will be registered with the details such as ID, primary key, secondary key, Decryption key .At first ,data will be encrypted by RSA algorithm and then it will be encrypted by the primary key of the last node in the path which

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

is before the destination towards the source node . Few snapshots are added below in order to describe the output of this system.

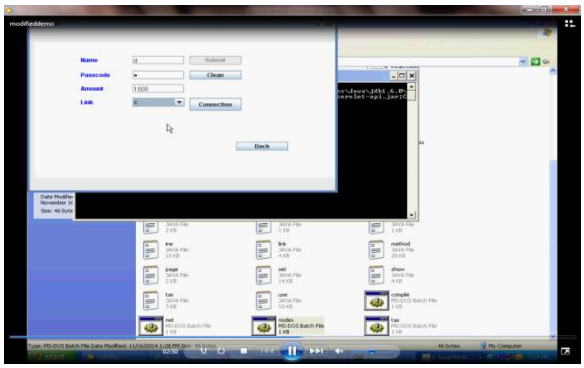

Fig.4.1.Sign Up page

In the above figure each node is registered manually in the signup page by giving name, password, amount and the name of the node which is to be linked. Here node 'd' is registered with passcode , amount and then linked with another node 'c'

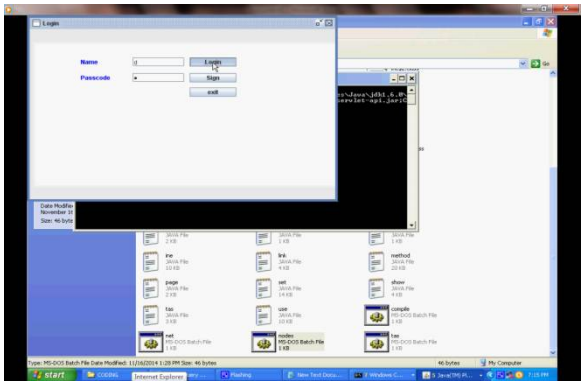

Fig.4.2.Login page

Name and passcode must be entered in order to log in to the node and refer the details or for further operations

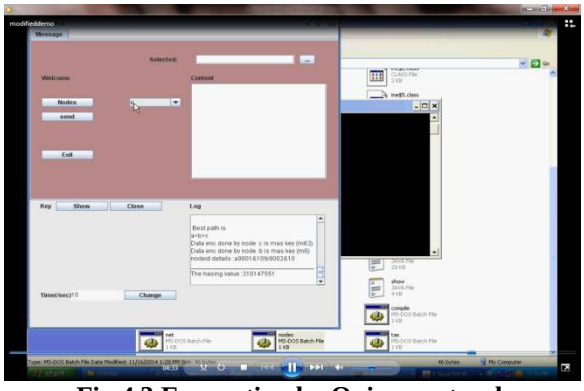

Fig.4.3.Encryption by Onion protocol

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

The possible paths are found and finally the best path among them is also found . Here the layer by layer encryption is done and a hash value is generated which is used while decryption process .

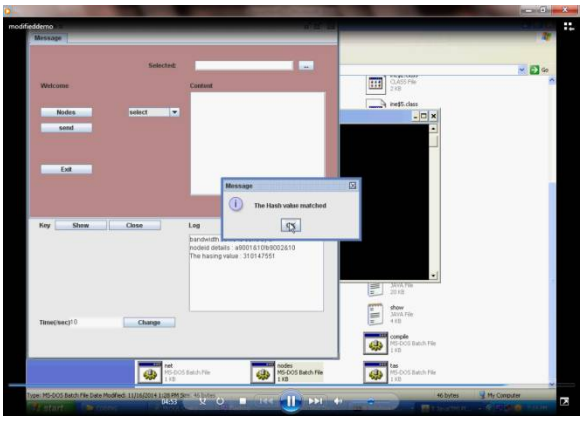

Fig.4.4.Verifying Hash value

While Decryption, the hash value which is generated will be checked for verification.Only if both values are matched , the data will be decrypted

V. CONCLUSION

Onion-based anonymous routing protocol and then extend the existing protocol with group onions into multi-copy forwarding. The main contributions of this paper are performance and security analyses of onion-based anonymous routing for DTNs. The delivery rate is mathematically modeled by incorporating the consideration of any cast-like message forwarding by group onions. The traceable rate of an anonymous routing path is analyzed by reducing the problem to computing the run length of the bit string that represents a routing path. In addition, the path anonymity as well as the node anonymity, both of which are application-dependent entropy-based metrics, are defined and formulated.

REFERENCES

[1] Q. Li, G. Cao, and T. F. L. Porta, “Efficient and privacy-aware data aggregation in mobile sensing,” IEEE Trans. Depend. Secur. Comput., vol. 11, no. 2, pp. 115–129, Mar./Apr. 2014.
[2] W. Gao, Q. Li, and G. Cao, “Forwarding redundancy in opportunistic mobile networks: Investigation and elimination,” in Proc. IEEE INFOCOM, 2014, pp. 2301–2309.
[3] C. Liu and J. Wu, “An optimal probabilistic forwarding protocol in delay tolerant networks,” in Proc. 10th ACM Int. Symp. Mobile Ad Hoc Netw. Comput., 2009, pp. 105–114.
[4] A. Balasubramanian, B. Levine, and A. Venkataramani, “DTN routing as a resource allocation problem,” in Proc. Conf. Appl. Technol. Archit. Protocols Comput. Commun., 2007, pp. 373–384.
[5] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, “Spray and wait: An efficient routing scheme for intermittently connected mobile networks,” in Proc. SIGCOMM Workshop Delay-Tolerant Netw., 2005, pp. 252–259.
[6] A. Vahdat and D. Becker, “Epidemic routing for partially-connected ad hoc networks,” Duke University, Durham, NC, USA, Tech. Rep. CS-200006, 2000.
[7] S. Jain, K. Fall, and R. Patra, “Routing in a delay tolerant network,” in Proc. Conf. Appl. Technol. Archit. Protocols Comput. Commun., 2004, pp. 145–158.
[8] X. Zhang, J. Kurose, B. N. Levine, D. Towsley, and H. Zhang, “Study of a bus-based disruption-tolerant network: Mobility modeling and impact on routing,” in Proc. Annu. ACM Int. Conf. Mobile Comput. Netw., 2007, pp. 195–206.
[9] M. Motani, V. Srinivasan, and P. S. Nuggehalli, “PeopleNet: Engineering a wireless virtual social network,” in Proc. Annu. ACM Int. Conf. Mobile Comput. Netw., 2005, pp. 243–257.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

[10] S. Wang, M. Liu, X. Cheng, and M. Song, "Routing in pocket switched networks," IEEE Trans. Wireless Commun., vol. 19, no. 1, pp. 67–73, Feb. 2012.
[11] J. Ren and J. Wu, "Survey on anonymous communications in computer networks," Comput. Netw., vol. 33, no. 4, pp. 420–431, 2010.
[12] M. Backes, A. Kate, S. Meiser, and E. Mohammadi, "(Nothing else) MATor(s): Monitoring the anonymity of Tor's path selection," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., 2014, pp. 513– 524.
[13] S. B. Mokhtar, G. Berthou, A. Diarra, V. Qu_ema, and A. Shoker, "RAC: A freerider-resilient, scalable, anonymous communication protocol," in Proc. IEEE 33rd Int. Conf. Distrib. Comput. Syst., 2013, pp. 520–529.
[14] S. Basagni, K. Herrin, D. Bruschi, and E. Rosti, "Secure pebblenets," in Proc. ACM Int. Symp. Mobile Ad Hoc Netw. Comput., 2001, pp. 156–163.
[15] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile Ad Hoc networks," in Proc. IEEE 24th Annu. Joint Conf. IEEE Comput. Commun. Soc., 2005, pp. 1940–1951.