Effective Bandwidth Utilization using Trusted LPEs in Anonymous Communication

B.Durga Anuja
Computer Science & Engineering
SSAIST, Rajahmundry, India

R.Srinivas(Ph.D)
Computer Science & Engineering
SSAIST, Kakinada, India

ABSTRACT
A network consists of autonomous systems that operate mutually for providing communication between the users. The user wants to be anonymous in this communication. The anonymous communication hides the identity of the communication parties. We propose a technique to achieve effective bandwidth utilization using trusted LPE (link processing element) in networks to deliver content from producer to consumers and hide the correspondence between them. In this technique, consumer registers interest for content by sending the Content Request Message (CRM) to the content's producer. Here the LPE that accepts CRM from the consumers merges and processes if they are intended for the same producer. In this process LPE receives number of CRMs from consumers and creates CRM with its identity and forwards to the content's producer as a single message. A producer produces the content requested by LPE that content send to LPE in network. Then LPE forwards content to consumers in reverse direction and duplicates into multiple content messages if necessary.

Keywords
Anonymous communication, LPE, CRM, Producer, Consumer.

1. INTRODUCTION
Anonymity protects the identity of one or both endpoints of a communication. Sender anonymity protects the identity of the original sender from the receiver and receiver anonymity protects the identity of the receiver from the original sender and third parties. For many internet [1] applications, it may be advantageous or essential and even crucial to protect the identity of communication parties. To achieve the anonymous communication the LPE hides the consumers from the producer. The LPE accepts the CRMs from the consumers and transfers that message to the respective producer with its own identity. These multiple LPEs form a LPE network that hides the consumer identity from the producer. An example of a system with such properties is a TYPE-II anonymous remailer [3], at which a user anonymously registers an email account by routing a registration message through a network. In doing so it deposits at the server a data structure that enables the server to route an email back to the (still anonymous) user along the registration path in the reverse direction. In a scenario where there are multiple consumers to which the content should be sent, an anonymous unicast network would have the producer send the content to each consumer individually incurring transmission costs at the producer. In this paper we propose a LPE Element that permits efficient anonymous communication through multicast like mechanism. In our approach each consumer can register individually with the content producer by routing a content request message through the LPE network, though LPE on this path checks the content request message if more than one consumer requested for the same producer content then the LPE merges these CRMS as a single message and forwards it to the content producer. In this way our technique disseminates content to a consumer on a LPE network like multicast "tree" formed by merging content request messages. In particular the producer treats the content request messages from the consumers as a single message.

For example, Fig.1 illustrates one stage of the LPE network where C_1, C_2 are the consumers and P is a producer. C_1, C_2 sends a content request to the producer P via LPE and the reverse of which is used by the producer to route content to these consumers. Here C_1, C_2 share LPE in the network for forwarding content Request message to the producer. In this case, our technique enables P to send only a single content message to LPE with the same computation complexity as if there were only one consumer. Similarly LPE forwards the content messages to consumers or other LPE in the network after processing.Fig.2 illustrates the LPE network where different consumers are connected. Here consumers send a CRM to the LPE for the content. LPE accepts the message, processes and forwards to next LPE or a producer.

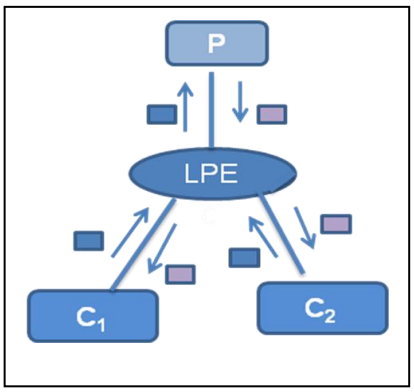

Fig 1: Communication through LPE

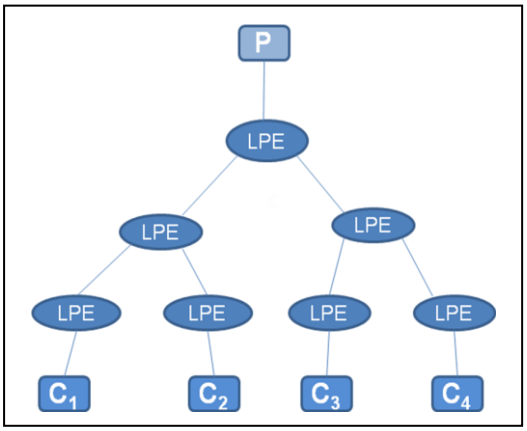

Fig 2: Multicasting through LPE Network

We emphasize that our use of multicast in a system supporting unlinkability is different from the traditional use of multicast to achieve receiver anonymity [3]. Put simply the latter use of multicast sends a unicast message to a single destination by multicasting the message to a group containing that destination [7]. The intended destination recognizes the message as intended for itself either because it expects this message (e.g., as in Hordes [6]), or because the sender addresses the message implicitly, i.e. in a way that only the intended destination can recognize itself as the target. This use of multicast is consumptive in that it delivers messages unnecessarily. The over whelming majority of recipients discard the message. In contrast our goal is to implement multicast in order to save band width over independent unicasts to the same consumers.Fig.3 illustrates the traditional use of multicast where the consumer in the group requested for the producer the content reached to all the consumers in that group [4]. So intended consumer uses the message where as remaining consumers will discard the message which is consumptive and wastes the bandwidth.

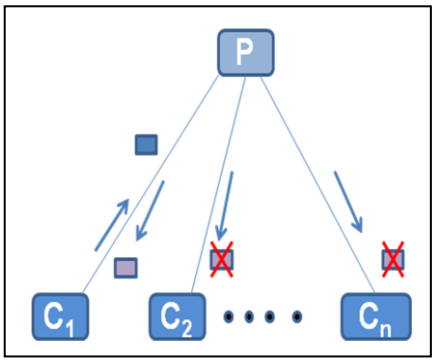

Fig 3: Traditional Multicasting

2. CONTENT REQUEST MESSAGE

We Assume that there is a public key infrastructure [2] by which parties can learn the public key (and network address) of LPE. We also assume that through a mechanism External to our techniques consumers and produces are semi trusted. In LPE network, trusted consumers will send a content request message as shown in Fig.4 for content distributed by a producer. This content Request message is forwarded to the LPE in the network for processing.CRM Contains the following fields.

<page_req , uuid, content key >

Page_req: The page requested by the consumer from producer.Uuid: Universal unique identifier for the Consumer. Content key: This is used by LPE for encrypting the data. This content request message encrypted with the public key of LPE and forward to the LPE network. The next LPE in the path receives the content request message.

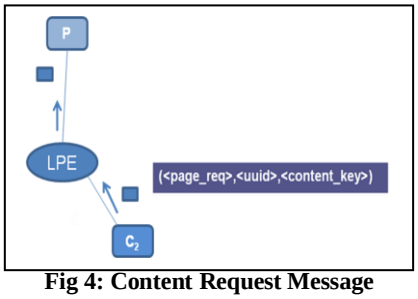

Fig 4: Content Request Message

3. LPE PROCESSING

Each LPE maintains set of tables which are updated with registration message. The LPE uses these tables for processing the content request message which is received from the consumer. The tables are Login table, page_request_count table, content_distribution table,storage_page table.

Table1: Login Table

producer_id	lpe_identity	Passwd
<pname>	<id>	<passwd>

Each entry in the Login table consists of producer_id which is used by the LPE inorder to authenticate with the producer the corresponding <id>,<passwd> will forward to producer for authentication of LPE. If the <id>,<passwd> are accepted by the producer then LPE can communicate with the producer.

Table2: page_request_count

page_req	count	Time	Uuid
<page_req>	<value>	<req_time>	<identity of consumer>

Each entry in the page_request_count contains the fields <page_req>, <count>, <time> <uuid>. Here the LPE maintains another content distribution table which contains the fields <uuid> <pag-req><content_ key>.<page_req includes the page requested,<count> this field will be updated when the page is requested ,<time> : this field contains the time when the request made.

Table3: content_distribution_table

Uuid	page_request	content_key
<identity of consumer>	<id of page requested>	<key>

The entries of content distribution table <uuid> :unique identification of LPE <pag-reg> for which page they have requested <content_key>:this key used for encrypting the content this key is used by the LPE for encryption of content and forwards to consumers. By using these tables the LPE processes content Request message received from the consumers. Whenever consumer sends a content request message to a producer then the LPE in the network receives the message and updates the <page-req> <content key> <uuid> of a content distribution table and updates the <count> filed present in the page_request_count table. LPE maintains two fields count and req_time. When the count reaches certain threshold then the LPE sends a request message to the producer for the content or req_time reaches threshold value then also LPE forwards a request message to producer. In this scenario the LPE compares the request received time with current system time. If waiting time is more than the threshold value, then it automatically sends a request message to the producer for content without waiting for CRMs from other consumers. Here if threshold value is too small performance will be degraded if it is too large waiting time increases so threshold value should be optimal.

LPE receives the content from the producer, it duplicates the content and encrypts the content with corresponding content key of a consumer and forwards to the consumers. In the scenario where Just after sending a request to producer, consumer requested for the same producer the consumer has to wait until the count threshold reached. In order to avoid annoyance in this technique the content is temporarily stored at LPE in table called storage_page.

Table4: storage_page

Producer_id	Page_request	Content
<name of a producer>	<requested page id>	<content>

Whenever consumer requested for the same page then immediately LPE forwards the content to the consumers.

4. PRODUCER AND CONSUMER PROCESSING

The LPE in the network receives the Encrypted content request messages made for the producer. It receives and decrypts the message updates the table and creates CRM with its identity encrypted with public key of producer forwards single request message to the producer. Whenever producer ready to accept the request first it will checks for authentication of LPE. If the LPE is authenticated then producer will accept the request message from LPE and in return it produces content. The LPE sends a content key in the request message that key is used by the producer in order to encrypt the content. After receiving the encrypted message from the producer the LPE decrypts the message and duplicates when necessary.

The consumer sends a content Request message for content to the producer via LPE. This message is received by LPE and processed. The LPE receives content form the producer and encrypts the content with content key send by the consumer then forward to the consumer. Wherever consumer receives the content message, decrypts the message and recovers content.

5. CONCLUSION

In this paper, we presented an anonymous multicast technique which allows producers to multicast content to consumers. Consumers will send a content request message to the producer through LPE network. The LPE presented in the network receives the CRMs from different consumers. If they request same content from producer then LPE stores the information about the consumer[s] and creates a content message for producer with identity of LPE. So the producer receives a single request message from the LPE and produces the content.LPE receives content from producer and duplicates content for different consumers who requested for content. This technique avoids annoyance in traditional multicasting and provides anonymous communication with bandwidth savings.

6. FUTURE SCOPE

Anonymous communication through LPE networks can be implemented to allow producers to multicast content to consumers while providing unlinkability against a global adversary in control of both the producer and some set of LPEs. The Content Request Message can be transferred with layered encryption technique so that security will be strongly provided.

7. REFERENCES

[1] Pfitzmann A and Waidner M. 1987 “Networkswithout use observability” y.Computers & Security,2(6):158-166.

[2] Ballardie. T 1994 “Scalable multicast key distribution” IETF RFC 1949.

[3] Mazieres D and Kaashoek M.F 1998 “The design, implementation and operation of an email pseudonym server”. In Proceedings of the 5th ACM Conference on Computer and Communications Security. pages 27-36.

[4] Grosch C 2000 “Frame work for anonymity in ip-multicast environments”. In Globecom.

[5] J.Sterbenz, R Krishnan,et.al,2002,”Survivable Mobile wireless networks:Issues Challenge and research Directions” proceedings of ACM WiSE.

[6] Albert R.Z and. Barabasi A.L 2002 “Statistical mechanics of complex networks". Reviews of Modern Physics, 74(1):47-97.

[7] Shields C and Levine B N “A protocol for anonymous communication over the internet”.

[8] Ginger Perg Michael K.Reiter 2006 “M2: Multicasting Mixes for Efficient anonymousCommunication.”Proceedings of the 26th IEEE International Conference on Distributed Computing Systems (ICDCS’06).

[9] Ren J 2008“Anonymous communication in Overlay networks” Military communication conference.

[10] Zhang J 2010 “Analysis of Anonymity in P2P Anonymous Communication Systems”.

[11] SV Pokraev et al.”Model-driven semantic integration of service-oriented applications”.

[12] Ismail,AR et al.”Investigating British customers’ experience to maximize brand loyalty within the context of tourism in Egypt: Netnography & structural modeling approach”.