ISSN (e): 2250 – 3005 || Vol, 05 || Issue,02 || February – 2015 ||
International Journal of Computational Engineering Research (IJCER)

Anonymous Communication for Providing More Privacy and Security

[1]Satish .K. Hatwar , [2] Prof.Vijay.M. Purohit
[1]M.E (EXTC), VIT/ Mumbai University Mumbai, Maharashtra, India
[2]EXTC Dept, VIT/Mumbai University, Mumbai, Maharashtra, India

ABSTRACT

A peer-to-peer network within which interconnected nodes ("peers") shares resources amongst one another without the utilization of centralized administrative systems. In communication network, the foremost common problems are privacy and security. During this network, anonymity is additionally crucial issue. The foremost anonymity for peer-to-peer users involved with the users' identities and actions which may be discovered by the other members. An intruder will get info regarding the content of the information, the sender's and receiver's identities. There are several approaches proposed to produce anonymous peer-to-peer communications. This paper provides anonymous communication with additional privacy and security. Anonymous approaches are designed with the subsequent 3 goals: to safeguard the identity of provider, to safeguard the identity of requester and to safeguard the contents of transferred information between them. This paper presents a new peer-to-peer approach to realize anonymity between a requester and a provider in peer-to-peer networks with trustworthy servers known as supper node in order that the provider won't be able to determine the requester and no alternative peers will determine the two act parties with certainty. This paper shows that the proposed algorithmic rule improved reliableness and has a lot of security. This algorithmic rule, based on onion routing and organization, protects transferring information against traffic analysis attack. The ultimate goal of this anonymous communications algorithmic rule is to permit a requester to speak with a provider in such a way that no-one will confirm the requester's identity and therefore the content of transferred information.

I. INTRODUCTION

In today's rising computational area everyone needs a communication network with full privacy and security. The user need security their personal data and their privacy. Protecting their data and respecting their privacy is prime to maintaining their trust. The privacy and security programs govern in such the simplest way that user data from ensuring the confidentiality of their personal communications and protecting and securing their data. The user is also involved regarding privacy and security of their personal data as they use communication networks. This paper facilitate them user manage a good range of privacy and security which will have an effect on them once using communication network.

Risk includes:

1) Confidentiality of their personal and personal communication
2) Collection of their personal problems
3) Security of their personal data
4) Use of their personal data

There were several approaches to provide privacy and security in wireless communication area. One amongst the means will offer the privacy and security to user data by anonymous communication. In fact, anonymity will be considered a special encryption on the messages to hide correlations between the messages and also the senders. The anonymizing method is performed throughout publishing, communication, searching, and retrieving. Therefore, protecting the messages in communication is important for anonymity. There are several approaches proposed to produce anonymous communications. Existing System are:

Crowds

These are an anonymous web dealing protocol and one amongst the oldest anonymizer networks and only offer requester anonymity. A crowd contains a closed group of collaborating nodes known as jondos and uses a trustworthy third party as centralized crowd membership server referred to as mixer. The new jondo requests crowd membership from the blender, then the blender replies with a listing of all current crowd members. After that, the blender in- forms all previous members of the new member. The requester node selects at random a jondo from the member list and forwards the request to that. The subsequent nodes decide at random whether to forward the request to a different node or to send it to the server.

Hordes

Hordes provide requester anonymity by adopting the Crowds probabilistic forwarding mechanism, and reach provider anonymity by acting a multicast transmission. Since the replying path is that the shortest multicast path from the provider to the requester, Hordes significantly reduces the latency. However, peers in Hordes should participate within the multicast relaying, that incurs an enormous traffic and wastes the bandwidth.

The limitations of existing system contain some attacks against the anonymous communication. The attacker is also system members or intruders from outside.

Therefore to beat the limitation of existing systems there's another conception of using third party as a trusty node is named as supper node in peer to peer network. A peer-to-peer network may be a dynamic and scalable set of computers (also referred as peers). The peers will join or leave the network at any time. The fundamental idea of a peer-to-peer network is to create a virtual layer over the application or network layer. In such AN overlay network all peers interconnect with one another. All peers are both the resource consumers and providers. Currently, file-sharing is that the most well-liked application in peer-to-peer systems.

Peer-to-peer networks are often divided into structured and unstructured categories. Structured peer-to-peer networks map every peer similarly as the index data of every resource into a globally position like Distributed Hash Table (DHT) in an exceedingly highly organized structure. This paradigm has 2 main drawbacks that limit the implementation in real world. First, it cannot support the fuzzy question and second, the DHT structure has massive overhead to individual peers and too tough to maintenance. In Unstructured peer-to-peer networks, peers will join and leave networks merely and there don't seem to be any structured patterns there. This paper focuses on the unstructured peer to-peer networks as a result of this sort of network are best to implement and provide security and anonymity.

There are 3 totally different roles that every peer will play in peer-to-peer networks: a provider (also known as a responder, host or publisher) to supply services upon requests, a requester (also known as AN initiator) to request services, and a proxy (also known as an intermediate peer) during which routs information from a peer to a different peer. Consistent with these roles there are 3 aspects of anonymity in peer-to-peer networks.

Provider anonymity that hides the identity of a provider against different peers, requested anonymity that hides a requester's identity and Mutual anonymity that hides each provider's and requester's identities. Within the most demanding version, achieving mutual anonymity needs that neither the requester, nor the provider will determine one another, nor no alternative peers will determine the two act parties with certainty.

1.1. DUAL-PATH TECHNIQUES FOR REQUESTER ANONYMITY

This paper present the algorithmic rule for achieving requester anonymity with the help of trustworthy third party referred to as supper node that solely keeps networks map. Every peer should send a trigger signal to supper node either sporadically or once it desires to join/leave the network. The ultimate goal of anonymous peer-to-peer networks is to cover the user identities, like the user's ID and IP address. The proposed algorithmic rule is that the means that the requester will connect with arbitrary provider and transfer information with it, in order that any peers like

Provider cannot find the requester's identity. The fundamental principle is relay messages from requester to provider through multiple intermediate peers so truth origin and destination of the messages is hidden from alternative peers. The requester creates a dual-path that contains a path to send request and another to induce respond from provider so the provider cannot compromise the requester's identity. The transferred information between requester and provider is encrypted to safeguard it against eavesdropping. So, during this algorithmic rule there are 2 methods to attach requester to provider: request path and response path. Each of them is initiated by requester at random. The requesters will modification these methods at random whereas connecting to provider at any time. Fig.1.1. illustrates a request and response paths within the network.

Each peer should join the network for obtaining services. The new peer requests a listing of peers within the networks from the supper node. The supper node replies with a listing of all current peers. Afterward supper node informs all peers of the new member. For departure the networks, the peer should send a removing signal for informing the supper node that it desires to go away there. Then, the supper node updates the list of peers what is more it announces alternative peers automatically. Every peer should send a trigger signal to the

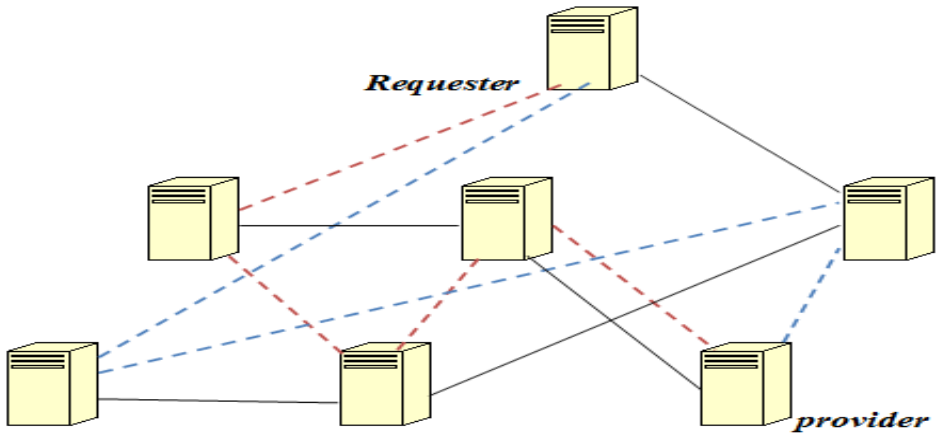


Fig.1.1.Dual path paradigm

Supper node sporadically, to inform the supper node that it's alive. When an amount of time, if the supper node doesn't sense any trigger signal from a peer, it'll take away the peer from the list.

II. LITERATURE SURVEY

[1] A. K. Datta, M. Gradinariu, M. Raynal, and G. Simon proposed Anonymous Publish/Subscribe in P2P Networks, the fundamental plan of a peer-to-peer network is to create a virtual layer over the application or network layer. In such an overlay network all peers interconnect with one another. All peers are both the resource consumers and providers. Currently, file-sharing is that the most well liked application in peer-to-peer systems.

[2] R.-Y. Xiao proposed Survey on anonymity in unstructured peer-to-peer systems that Peer-to-peer networks will be divided into structured and unstructured categories. Structured peer-to-peer networks map every peer still because the index info of every resource into a globally position like Distributed Hash Table (DHT) during an extremely organized structure. This paradigm has two main drawbacks that limit the implementation in real world. First, it cannot support the fuzzy question and Second, the DHT structure has massive overhead to individual peers and too tough to maintenance. In Unstructured peer-to-peer networks, peers will join and leave networks merely and there don't seem to be any structured patterns there. This paper focuses on the unstructured peer-to- peer networks as a result of this sort of network are best to implement and provide security and anonymity.

[3] L. Xiao, Z. Xu and X. Zhang Mutual anonymity Protocols for Hybrid Peer-to-Peer Systems proposed there are 3 completely different roles that every peer will play in peer-to-peer networks: a provider (also known as a responder, host or publisher) to provide services upon requests, a requester (also known as an initiator) to request services, and a proxy (also known as an intermediate peer) during which routs information from a peer to a different peer. consistent with these roles there are 3 aspects of anonymity in peer-to-peer networks: provider anonymity that hides the identity of a provider against alternative peers, Requester anonymity that hides a requester's identity and Mutual anonymity that hides each provider's and requester's identities. Within the most demanding version, achieving mutual anonymity needs that neither the requester, nor the provider will determine one another, nor no alternative peers will determine the two communication parties with certainty.

[4] Satoshi Togawa, Kazuhide Kanenishi and Yoneo Yano Peer-to-Peer File Sharing Communication Detection System using the Traffic Feature Extraction proposed a traffic visual image system for P2P communication detection, and that we explained a configuration of the paradigm system. And, we have a tendency to explained the results of experimental use and examine. This technique extracts records of P2P communication activities from the collected IP packets and therefore the collected DNS question results, and presents the administrator with a feature map. We have a tendency to develop a paradigm system and experimented to verify its effectiveness. It had been shown that an administrator may examine the results of the feature map.

III. PROBLEM DEFINATION

The limitations of existing system contain some attacks against the anonymous communication. The attackers could also be system members or intruders from outside. The ultimate target is to locate the requester, provider, and what they're transferring.

Time-to-Live Attacks: Time-to-live counters verify the utmost number of hops for a message and are utilized in most peer-to-peer networks to avoid flooding. If an attacker will send a request to a node with such a low time-to-live counter that the packet can most likely not be forwarded, any response relieves that note as the provider.

Denial of Service Attacks: Denial of service attacks may be significantly awkward once nodes will act anonymously, as this might mean that the node acting a Denial of service attack couldn't be known and removed from the system. Whereas anonymous systems cannot stop all Denial of service attacks.

Statistical Attacks: Any attackers are able to get statistical data over a period of long term. Net- works could probably safe for a single run however could reveal data regarding the identities of their peers once all the noticeable messages of a longer run are analyzed for patterns.

Traffic analysis: Making use of the traffic information of a communication to extract data. Interception and cryptanalytic are 2 techniques to analyze the transferred information. The reliable anonymous approach must safe against these types of attacks.

To overcome the on top of limitations exists by the previous systems like Crowds, Hordes, Tor, etc., this paper implementing a system with anonymous communication. During this system, maintaining the anonymity of the sender and also the privacy of the information being transferred between requester and provider.

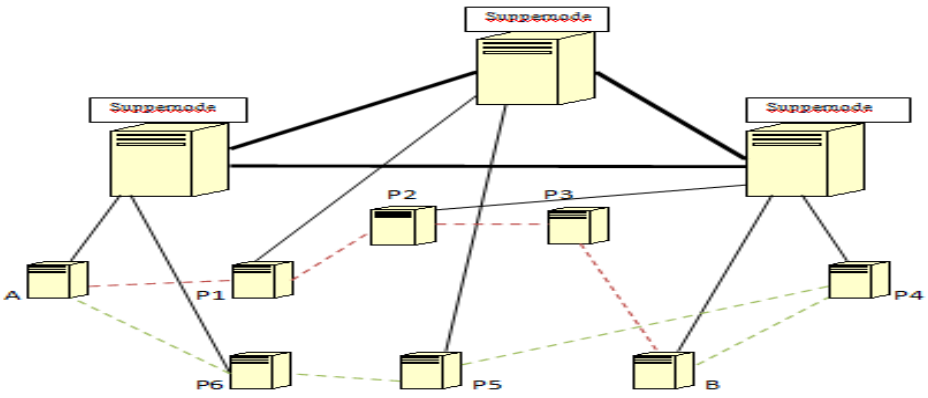
IV. PROPOSED METHODOLOGY

The proposed approach provides requester anonymity to safeguard the identity of the requester and therefore the transferred information against different peers specially the intruders. The proposed algorithmic rule relies on Onion Routine mechanize. Onion Routing is that the technique during which the requester and also the provider communicate with one another anonymously by means of some intermediate peers referred to as onion routers. During this technique, messages route between onion routers. The messages encrypted with onion router's public key. Every onion router learns solely the identity of consequent onion router.

4.1. Process

1) A requester sends a signal to the supper node and requests a list of all current peers.
2) The supper node replies to the peer and sends a list of the live peers within the networks.
3) The requester chooses 2 sets of peers arbitrarily. One in all them is employed for request and therefore the different and also for the response.
4) The requester, requests via the request path and also the response path is embedded in request path by the requester
5) When the provider needs to response the request, it sends the respond message to the peer that determines within the tail of the received message from the requester

4.2. System architecture



Request Path - - - - - - -
Response Path - - - - - - -
Communication between Peers and Suppernodes ——————

Fig.4.2.1. System design

Let's take into account peers P1, P2 and P3 that are chosen arbitrarily by requester for request path and P4, P5 and P6 that are chosen for response path. Additionally think about M, the message that the requester needs to send. During this figure, "A" acts as a requester and "B" acts as a provider. "A" creates 2 methods to communicate with "B" and sends messages via them. "A" should rely messages through P1, P2 and P3 (request path) to send them to provider. Additionally "A" receives the response of its request through P4, P5 and P6 (response path).

After the requester (A) creates the Dual-Path, currently it should create the packet of the messages. To create the packets, the requester (A) should encode the messages by intermediate peers public keys during a layer by layer structure, like onion routing mechanism.

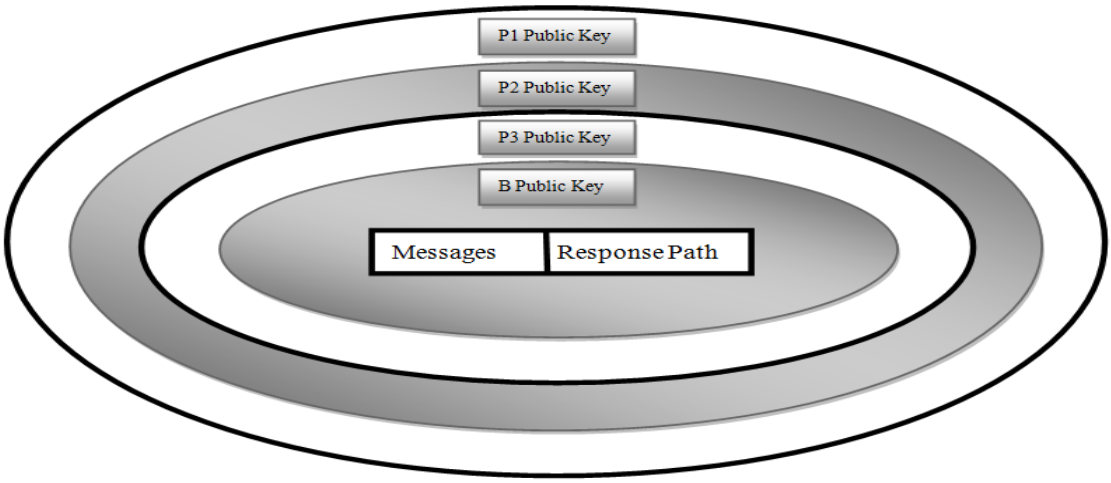


Fig.4.2.2. The structure of request path in wrapped message

When the provider (B) receives the packets, it extracts the message and also the response path packet. Every response packet has 2 elements, the "Next Peer" and also the "Tail". The "Next Peer" part contains subsequent peer during which the message should be sent to that. When extracting the response path packet by provider (B), it encrypts the response message by P4 public key and attaches the Tail" a part of response path packet at end of it. Currently the provider (B) sends the wrapped message to P4. P4 does same method and sends the received messages to P5. P5 sends the messages to P6 and finally P6 sends the messages to the requester (A).

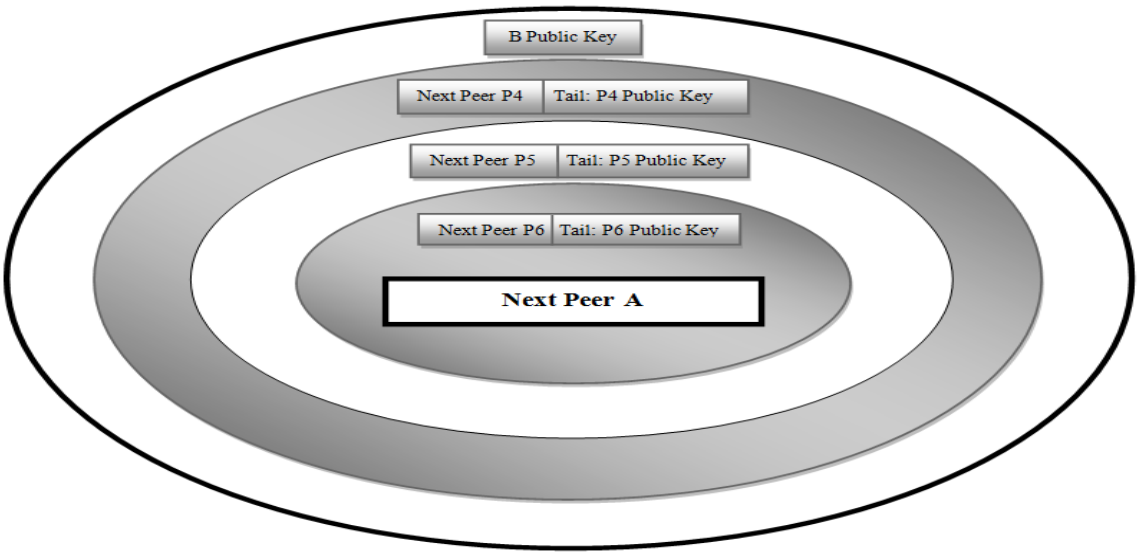


Fig.4.2.3. The structure of response path in wrapped message

4.3. Data Flow

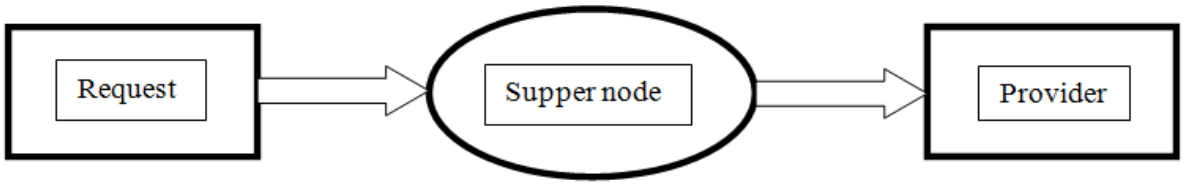
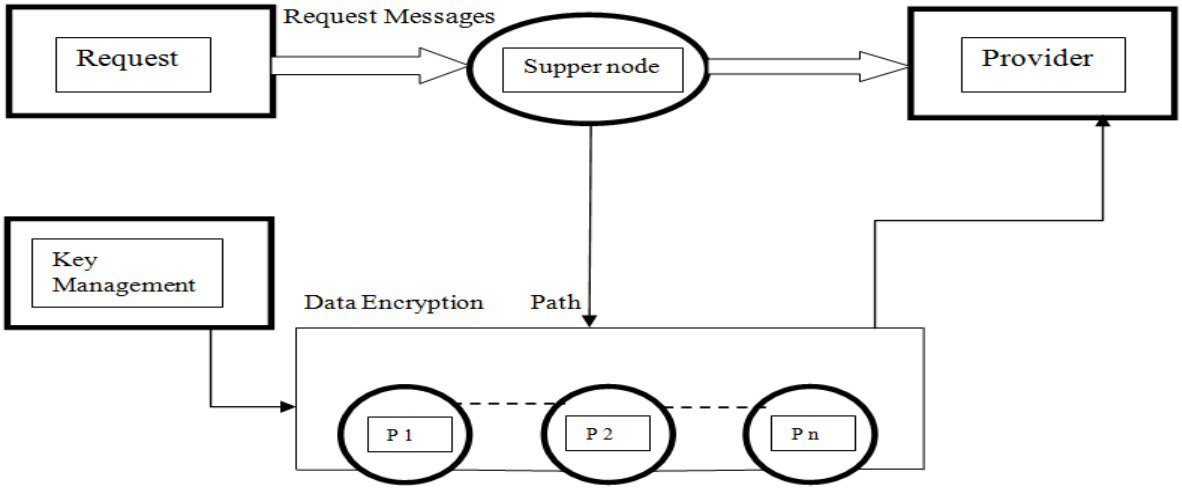


Fig.4.3.1.Data Flow 1



Peer: P1, P2…Pn

Fig.4.3.2.Data Flow 2

V.CONCLUSION

The proposed peer-to-peer anonymous algorithmic rule provides versatile layer for the requester to decide on dual-path to attach to the provider. This algorithmic rule provides additional responsibility and additional Security. additionally it will increase its fault tolerance because the connection between the requester and also the provider isn't depend upon intermediate peers, and if every intermediate peer downs, the requester will modification the dual- path to continue its connectivity. We tend to algorithmic rule our rule for achieving requester anonymity with the help of trusty third party referred to as supper node that only keeps networks map. Super-nodes are used to recover the group formation of network nodes. Super-nodes are generated based on this data to represent the closeness between nodes.

REFERENCES

[1] *A. K. Datta, M. Gradinariu, M. Raynal, and G. Simon*, Anonymous Pub- lish/Subscribe in P2P Networks, in Proc. International Parallel and Distributed Pro- cessing Symposium (IPDPS'03), pp. 47a, 2003.

[2] *R.-Y. Xiao*, Survey on anonymity in unstructured peer-to-peer systems, Journal of Computer Science and Technology, pp. 660-671, 2008.

[3] *L. Xiao, Z. Xu, and X. Zhang*, Mutual Anonymity Protocols for Hybrid Peer-to-Peer Systems, in Proc. of the 23rd International Conference on Distributed Comput- ing Systems, pp. 68.

[4] *Satoshi Togawa, Kazuhide Kanenishi and Yoneo Yano*, Peer-to-Peer File Sharing Communication Detection System using the Traffic Feature Extraction.2006 IEEE International Conference on Systems, Man, and Cybernetics October 8-11, 2006, Taipei, Taiwan.

[5] *Guowei Huang, Zhi Chen, Qi Zhao Gongyi Wu*, Activity Monitoring to Guarantee File Availability in Structured P2P File-sharing Systems. 26th IEEE International Symposium on Reliable Distributed Systems

[6] *Bing Li and Dijiang Huang*, Modeling Anonymous MANET Communications Using Super-nodes. 2013 IEEE Military Communications Conference.