***Bazli B.S.*[1]*, Llewellyn-Jones D.*[2]*, Merabti M.M.*[3]**
[1,2,3]Liverpool John Moores University, Liverpool, United Kingdom
[1]b.bazli@ljmu.ac.uk, [2]d.llewellyn-jones@ljmu.ac.uk, [3]m.merabti@ljmu.ac.uk

EFFICIENT LOOKUP WITHIN SCALABLE UBIQUITOUS COMPUTING NETWORKS

Traditional client-server arrangements within centralized systems using low-level protocols have now been replaced by mobile hosts and dynamic protocols over ubiquitous decentralized systems. Rising costs of data traffic and the need for efficient communication and improved management of systems has created a pressure to roll-out efficient and effective communication methods and address dynamic change of members and resources within ubiquitous P2P networks. This work uses novel allocation and smart lookup technique to initiate efficient routing based on the global availability of the destination node state. Considering the high cost of failed queries within scalable networks, this will improve network efficiency and reduce latency.

Keywords: *Ubiquitous Computing, Scalability; P2P, Overlay Networks, Security, lookup.*

Introduction

The spread, mobility, and granularity of nodes, within scalable networks and the dynamic architecture of the network, makes the resource management complex[1]. The resource management should consider cost, time, and space as well as privacy, fair access, confidentiality, integrity, and availability of resources.

Therefore managing network resources and communication within such distributed systems is becoming more complicated, with important tasks such as routing, resource allocation, service access, and state management becoming increasingly challenging. Traditional client-server arrangements within centralized systems using low-level protocols have now been replaced by mobile hosts and dynamic protocols over ubiquitous decentralized systems which nodes can use to communicate and with processors making decision independent of the network management system.

Rising cost of data traffic and need for efficient communication and improved management of systems has created a pressure to roll-out efficient and effective communication methods and address dynamic change of members and resources within ubiquitous P2P networks. This work will use novel allocation and smart lookup technique to initiate efficient routing based on the global availability of destination node state. This will allow the use of the shortest paths within the ubiquitous computing network without the need for complex changes to the network topology, policy or procedures. Considering the high cost of failed queries within scalable networks, this will improve network efficiency and reduce latency.

The interconnection of autonomous computers and isolated communication networks enables new services and applications to form distributed networks [2, 3]. Despite the typical centralized nature of computer networks, a distributed network operates more efficiently and effectively over a mix of workstations, LAN servers, wireless networks, regional, Web and other servers. As the size of the distributed network grows, managing the network resources, access control and security becomes more complex due to the dynamic and rapid change of network structure, state and flexibility.

There exist several scalable ubiquitous applications and approaches to address the challenges facing scalable ubiquitous networks [3-6]. Researches show that these systems do not support efficient service discovery and performance testing. There is no comprehensive approach to address all challenges facing dynamic change of scalable network structure with hundreds of devices and services joining, leaving, or failing within the system.This work will use novel allocation and state management techniques to allocate Service Centres (SC) within a scalable distributed and ubiquitous system to provide fair and equitable access for existing and new nodes without complex changes to the network topology, policy, or procedures. This is achieved using trusted paired relationships and a structured P2P routing algorithm and proactive state management. By creating new SCs where the network is expanding to serve newly joined nodes ensures the accessibility, availability, and granularity of the network without needing new sets of policies and procedures. Furthermore, the presented design will ensure that existing storage and memory will be sufficient and available to overcome the requirements of new and more scalable networks.

Scalable Ubiquitous Computing

While the evolution of the ubiquitous computing paradigm is generally positive for users, it does introduce security and performance concerns amongst other things.

Nonetheless, privacy measures must be applied carefully, minimizing the impact on users and the system while at the same time maximizing the efficiency and fair resource access in the network. To accomplish this task we will study the overlay structure of ubiquitous computing network with the aim of enhancing the efficiency and effectiveness of the network.

The deployment and use of ubiquitous computing technologies that pervade our everyday lives has significant social and ethical impacts. Scalable, decentralized and self-organizing ubiquitous networks have been popular among communication, file sharing and P2P applications. It is essential to study and consider the impacts and challenges when developing ubiquitous computing systems [1].

The preferential attachment process within a network may lead the most popular nodes to attract connections more than others and cause overloading. Although this process keeps the average shortest path length low and the diameter of the network to an ideal and intended size, overloading of the hubs affects the network efficiency and service availability. However the physical arrangement of nodes and granularity of the network is something that is impossible to manage as this requires allocating newly arriving node to a more suitable place to keep the network structure manageable. The application of privacy and communication within long tail networks which all nodes need to access the central authority for resources and applications is highly complex and less efficient.

The end-to-end authentication of communication within the network is riskier than if applied to P2P connections between neighbouring nodes [7]. Where a network exhibits a power law distribution the ‘preferential attachment’ may lead the network to form a random layout with an unstructured, uneven distribution of nodes which may result in the overloading of the ‘hubs’ and therefore effect network interoperability. Without a clear structure, connection of nodes to SC may form a random network. Because of the nature of ubiquitous computing, it’s particularly difficult to find a comprehensive solution to address scalability and privacy. However, we believe understanding the structure of such networks will be important for establishing a solution.

Network overlay is a virtual network of nodes and logical links that is built on top of an existing physical network to provide services that are not available or limited in the existing networks [7]. It is used for indexing, discovery, data processing and communication independent from the network topology. It helps to utilize the network resources and applications within rapidly growing decentralized network.

Within the network overlay, a peer can contribute to the network or act independently by own processors [12]. This helps developers to customize the network protocols and policies and create their own communication interface and environment. Furthermore overlay networks facilitate flexible routing and alternative communication paths using highly connected and effective network overlays with distributed network environment.

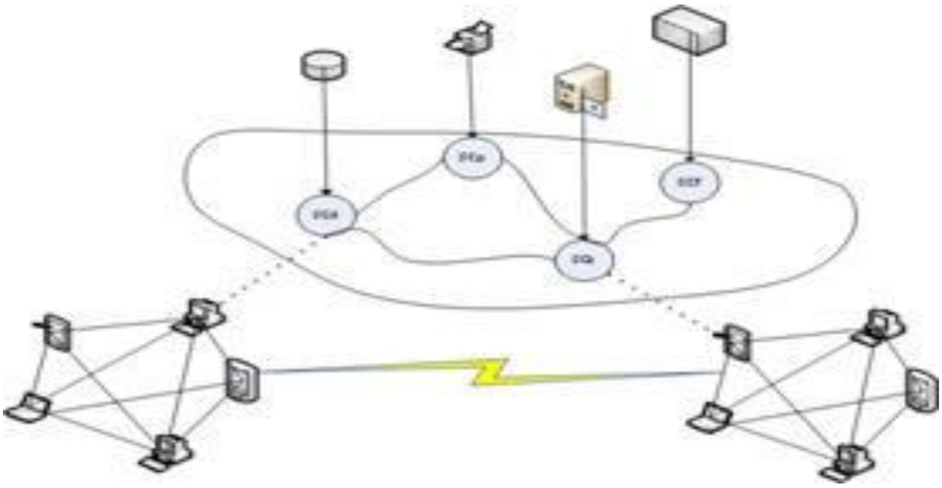


Figure 1. Typical Overlay Network

P2P overlay is popular amongst users for file sharing and communication like Skype (centralized), Bit Torrent and Gnutella (decentralized). Figure 1 is a representation of small network overlay where two sets of network using shared resources via direct link. The SC provide the existing network nodes with the available resources using network overlay which cover a set of nodes within two rings. This brings flexibility, effective communication within the network, and makes management and configuration an easier task.

Network Management

By enforcing the network to follow a power law distribution, the network will become manageable and the joining nodes will be easy to organize. To some extent this will serve the network to achieve efficiency and easy development [1]. Joining a group of hubs with associated nodes will form a network with a power law distribution and maintain the balance of the network. With the policies, services, resources, protocols, and repositories moving to hubs this creates a SC that maintains network reliability, interoperability, and security. The preferential attachment mechanism of the network will naturally create a power-law distribution.

Resource Allocation. We allow some SCs to have more links so that they provide services to demanding areas by assigning specific roles and capabilities to some of the service centres.

In a peered approach the average shortest path will stay as low as possible preventing the random distribution. To keep the average path as short as possible, new service centres will be created to serve the newly attached links. There will be network overlays on top of logical network adjacent and interconnected to each other using live trusted link.

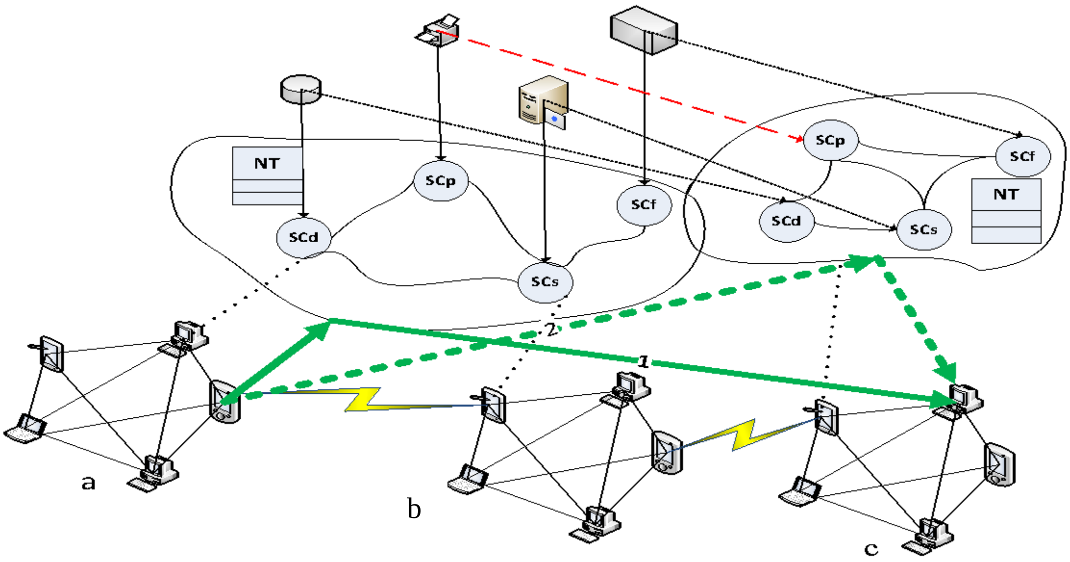


Figure 2. Diverse Short Paths within Multiple Overlay

New overlay will be utilized to serve new nodes and provide the services and applications existed on the neighbouring overlay. This will be the replica of the overlay but some resources that are not possible to virtually replicate e.g. printers. Newly created network overlay will preserve the dimensions of the network naturally by keeping the average shortest path between vertices low. If the number of nodes increases, more SCs are created to keep the service capability at the same level and keep the network scalable, manageable, and interoperable.

In case of newly joined nodes - on the example shown in Figure 2 the 3rd ring of nodes C and subsequently an overlay is created to accommodate newly arrived nodes with the same utilities and resources available in neighbouring overlay. This figure shows how the balance of the network is retained and the path between nodes and network overlay is kept as short as other existing paths within neighbouring node sets. Overlay 2 has similar resources available in overlay 1. There is a direct path between two overlays enabling them to share and update information.

After expansion of the network, new SC 2 and 3 with associated nodes join the network forming balanced structure using power law distribution. CS1, 2, 3, will have direct links with each other allowing them to share the same information, directory services, protocols, and policies providing access to all nodes.

Now if *a* wants to communicate with *b*, despite having further geographical distance, the communication method and approach will be the same as for the two neighbouring nodes b and c as described earlier. This is possible simply because of the direct links between SC1 and SC2. These two SCs will act as a super node to allow direct and secure communication between the two nodes. In this case the identity of the two nodes must also be known and shared by both SCs.

House Keeping. The group of nodes which form an overlay has got an indexing table which stores nodes' IDs, IP address, node state, neighbours' information, and associated attributes. The node state and all other information are stored on 'Naming Table' (NT).

The 'NT' within the SC keeps details of nodes and node sets such as IP addresses, nodeID, node role, type, state, as well as information about the neighbouring nodes and geographical location. A prefix identifying that the node is assigned to particular overlay, therefore knowing the whereabouts of the node is also kept within the 'NT'. This prefix supports globally visible and reachable unique identification, which incorporates the IP addresses assigned to them.

Also the state of neighbouring overlay and nodeID is kept within NTs. Node state and location is transmitted using short aggregate messages. NodeID and state of the node along with its location is available to other network overlays and associated systems. Each node connected to the network will join a global NT and will be assigned nodeID and associated attributes. The role of the node will depend on the location, state, processing power, and memory. For instance, the nodes located behind firewalls cannot be assigned node set leader. A 'NT' will shift the list when a node leaves or a node set is dismantled and will create new space for newly joined nodes and node sets. A minimum of one link exists between adjacent overlays and aggregate message is sent to SC to ensure consistency as well as integrity within the network. In case of failure, a wakeup call message is sent to the neighbouring nodes or node set leader to acknowledge the state and information of nodes is aggregated within a time interval using short messages sent to the NT, which subsequently will be passed to the neighbouring overlays. The NT will maintain the record and update the record periodically. Each node will have active, idle, or unavailable state stored within NTs.

Communication. The communication between every node with each other is peered and therefore it is much more secure than any other approach [8]. Each SC has a direct channel of communication with other SCs, allowing them to share any information they hold. Joining a group of new nodes to the system will create a new SC with the same services available as the other existing centres. We intend to derive an algorithm to limit the number of nodes attaching to each of the SCs to maintain efficiency and minimize overloading the network with new requests. Also, to avoid disturbing the power-law distribution of the nodes, some links will be given particular roles and allowed to attract more nodes than already defined so that demanding areas within the network remain well covered. Figure 3 shows how an alternative path –dotted line- can be taken for a query if the network resource is not available or the initial route is not clear. In this case the query will be directed to the node whose state is 'active' and hold the information requested. This will maintain the shortest path as well as minimal hops increasing network efficiency and avoiding redundancy.

Smart Lookup. In our framework we suggest that before every single query, the source and destination node and routing path is on a clear and ready state to avoid failed lookup and redundant traffic. Considering the high cost of a single query within a scalable network, this will ensure the network efficiency as well as reducing latency. The proposed lookup scheme maps the key to value through a NT within SCs. The source node will send the message to its overlay and overlay will make a decision based on the state and availability of destination node. If the state of the destination source is 'active' then the overlay will grant the look up and create the path to route to the destination with direct or through the available route within adjacent overlay(s). If the destination node is not in active state or not available for any reason then the source node will be informed and will be given alternative resource and path close to the destination node.

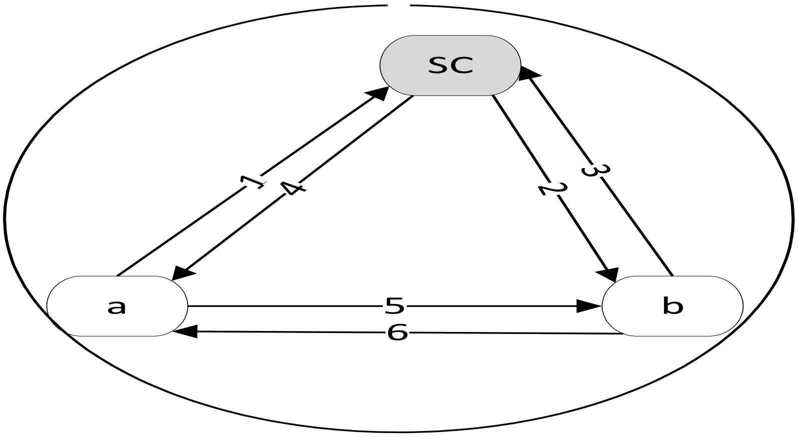


Figure 3. Routing within the same Overlay

Figure 3 shows a simple communication process between two nodes within a single overlay with ring topology within same overlay will use 6 links to establish a communication channel. But the look up between two nodes located on different overlays, although routes through shortest path possible but takes a few more hops than the one happens locally. This is illustrated in figure 4 with corresponding links to establish a communication channel incorporating two SCs.

Suppose node a located within SC1 wants to lookup a file which exists in node b in Figure 5. Since node b does not exist within same ring, SC1 will forward the message to the SC2 associated with node b knowing that node b is in active state and communication channel is clear. Then the look up operation will be granted and routed through a clear communication channel.

If the super-node within SC1 is not available then the message will be forwarded to adjacent CS or a SC close to the destination node. Once the look up is initiated and acknowledged, and then direct communication channel will be created between peers. This will ensure the short path and minimal hops within the look up process. The message will have an identifier so the destination node can be known, allowing the message to be routed to its hub and then onwards to the destination node. If the destination node is available in another node set not adjacent to SC1, then the whereabouts of the destination node, its state and associated node set will be available within in the NT.

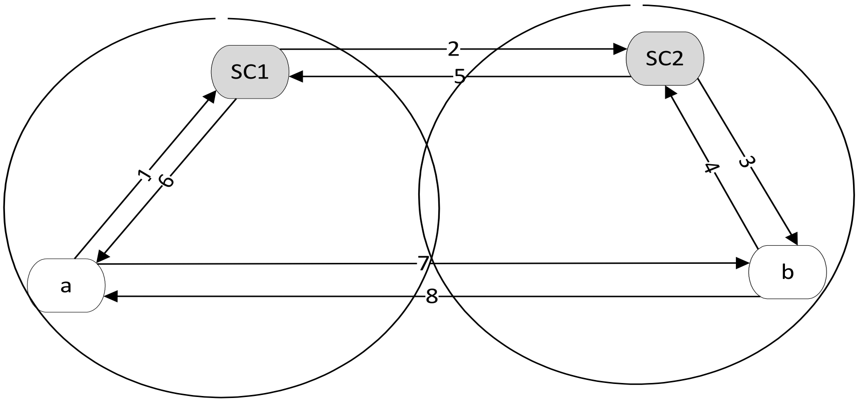


Figure 4. Routing within Different Overlay

If the state of node *b* is unavailable then the associated SC will look at the request and forward it to a node or node set which might be sharing part or some of the attributes related to that request and geographically close to the source node. If the 2nd attempt to reach the resource is failed with same reason then the lookup will continue to the next destination and discard location element on the algorithm to discover the destination node. Since the SC will keep track of nodes and their neighbours ID's in exponentially ascending order, therefore no other algorithm and further calculation required to determine the location of the node within the ring and its distance from the SC. If the node is not available to reach because of departure from the system then the neighbouring nodes should have reported that to the associated node set leader and the attributes of the node would be deleted from the NT. However, the data that node has been holding prior to departure must have cached through replication by neighbouring nodes. One such approach has been taken to improve performance through cache replacement in Freenet [9].

If the state of the node is idle, then a reminder message from SC or a neighbouring node should wake the node up to make its state active and reachable by others. The idle state is occurred between stabilization period and aggregated intervals. The stabilization period is re-arranging the records of entries on NT after eviction of a node or inserting details of new arrivals. If a node became idle before sending a message to the SC informing them of its state, then the wakeup call is initiated to put the idle node to an active state. The look up process then will resume as described in the previous section.

Cost Calculation

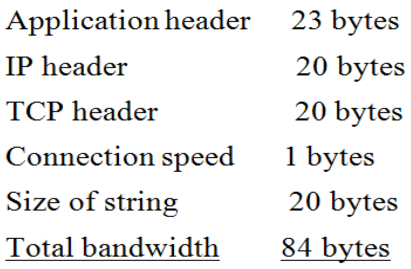
The effective and smart lookup we envision implies that a look up is initiated and granted permission to proceed if the destination node state is in active state and a node is available to reach by the source application. The membership change within scalable unstructured P2P can cause failed lookups therefore generating unnecessary bandwidth and causing redundant traffic over distributed networks. Nodes joining, leaving, and failing enforce extra traffic to the existing bandwidth. The amount of redundant bandwidth enforced by membership change might not seem significant and considered fair if distributed over the network, but one might ask about the size of the fair bandwidth for every node. In a file sharing P2P applications over the internet, a 28kbps bandwidth might not considered significant for a fiber optic user, but it takes half of the average internet connection speed of a dial up user. Considering number of active users within those systems reveals that the amount of redundant bandwidth is distributed amongst just few 'live' users[10]. The probability of bandwidth used in lookups within the same SC and different SC is as follows:

g is the number of overlays of each size, n is the number of nodes;
Total nodes will be g + n;
p (data uses in same SC = $\frac{1}{g}$;
p (within different SC = $\frac{g-1}{g}$;
b (total bandwidth) = [$\left(\frac{1}{g} \times 6\right) + \left(\frac{g-1}{g} \times 8\right)$;
E(bandwidth) $= \sum \mathrm{p(b)x\ b}$.

This is the efficient and cost effective way of communication however; this would not be possible without constant state management and advertisement of nodes. This method also will use minimum routing information, which is low cost and resilient to failures. Additional maintenance protocol ensures a periodical 'sign in' process of the nodes to the local 'NT' so the state is known globally to the other overlay sets. A constant 'sign in' process will reduce the additional maintenance on overhead of multiple overlays; however this will impose extra cost on bandwidth consumption within the network.

We intend to calculate the amount of bandwidth used for a query and compare the result with the proposed method to be able to evaluate the system. To calculate the cost of a typical single query we observe a number of nodes and possible destinations, number of hops taken to reach the destination, and the amount of bandwidth generated and used to perform a query.

For simplicity and relevance we are not considering bandwidth used for downstream because the downstream process is not initiated if a look up fails. In a well-balanced system with known topology, 8 hops as worst-case scenario for a look up is considered which uses 672 bytes as illustrated in figure 5. Considering the packet used for a single search query on a best case scenario, we can calculate the bandwidth used with the following figures (Fig.5):



Application header	23 bytes
IP header	20 bytes
TCP header	20 bytes
Connection speed	1 bytes
Size of string	20 bytes
Total bandwidth	84 bytes

Figure 5. Total Bandwidth in Upstream Process

We are considering two functions to calculate upstream bandwidth used for query over scalable network. First is the number of hops function which considers timing factor by limiting the number of maximum hops attempted to complete a lookup process. This will prevent exhausted lookups. Second function is calculation of generated bandwidth used to initiate the look up. We consider the size of the query, processing, and application cost. Maximum number of reachable nodes within the ring can be determined by:

$$f(n, t) = \sum_{x \le t \ge y}^{t-1} (n-1) \times n,$$

Where*n* is the number of the nodes within the ring; *t* is the mean time of the lookup process. To accurately account for the t we limit the number of hops to between x and y therefore the time to live factor of a query well be x or more hops but no more than y hops therefore avoiding the exhaustive look ups. Bandwidth used for lookup on *n* number of nodes

$$b(n, t, s) = n \times s + f(n, 1, t-1) \times (n-1) x\, s,$$

Where s is the size of the transmitted message over the network and the calculation will consider the number of hops based on number of reachable nodes within the ring. The increase in number of nodes will not have significant impact on distance between them because of the logarithmic distribution of the nodes within the network.

The membership change within a network with numerous queries and requests can lead to unsuccessful look ups increasing network traffic and congestion. It has been observed that a system[11] with 3000 nodes has 20 membership changes and 5 queries per seconds yields 4 GB of data just for a simple string search with static topology and a well-balanced load. If we scale up the system to 10^6 then 625 queries will generate 500 Gbps bandwidth on its own. It is 0.5 Mbps for every node within the distributed users. This might not seem significant because of the distribution of this bandwidth over the network. However experimental analysis shows 10 % of users within Gnutella use 99% of traffic on the network [12]. That means the impact of the redundant look up will be enforced on small cluster of ‘heavy’ users. This also introduces new challenges on scalability of the system and its behaviour under heavy loads.

Each node has got identifier mapping it to the local ‘NT’ and contains information about its neighbours and local ‘NT’. We use Chord look up protocol in a circular topology within an overlay that has keys as much as 2^m – 1, where*m*is the identifier. In a well-balanced network a typical look up will be O(log N). The look up for this routing protocol will use a key to value technique to reach from source to destination.

Membership Change. The membership change within the network is significant which makes some nodes or resources unavailable to lookup or access. This will lead to a considerable amount of failed look ups within a scalable network. The amount of saved data may not be significant but this is only a basic query with minimal links, static topology, and we are not accounting for several other factors which usually generate traffic and use bandwidth.

Calculations shows that implying this figure for a network of 10^6nodes, then the bandwidth used for 500 Gbps of data is required to run a query within the network. If we calculate and apply the failed query to the bandwidth used within a million node network considering the percentage of failed queries as result of constant membership change, then 50 GBps is saved by using the pro-active state management method. The transmission rate and the size of the file is also considered within the look up and routing technique, but not calculated as it has got no effect on the end result intended. Authors avoided using Service Location Protocol (SLP) [15] for this purposes for privacy and anonymity in mind.

Related Works

Proposes distributed object location and routing technique pastry[13], by creating overlay of networks and interconnecting them over the internet to provide data storage, file sharing, and naming over a large scale of a distributed network. While the proposed framework uses naming technique and prefixes a number to the nodeID to serve the granularity of the nodes, Pastry determines the distance between two nodes using given IP addresses and proximity measures to locate the clients and route the message through using logarithmic hops to reach from source to destination. Although Pastry is a great method, which is used by many systems to address scalability and state management, it presumes availability of destination node with more optimistic approach on successful look-ups. In the Pastry system, the look up result is either success or failure. In other words the message either reaches the destination after several attempts or accesses the resource by any means, or it reaches to a point where it determines the destination is not available or reachable. Although this does not leave the process with uncertain results, but the guaranteed success may lead to exhaustive search which uses any means and route to reach the destination. The proposed algorithm takes extra measure to minimize the failed look up which occurs as result of membership change.

Dixon et.al. [14] offers a primitive lookup method chord over distributed large scale network by associating the key to data location and efficiently mapping the pair concurrently. Chord successfully adapts membership change within the nodes and dynamics of the network. Although this proposes an efficient routing and provides high success rate but it uses one dimensional mapping method based on geographical location of nodes. This technique introduces discrepancies on different topological domains and scalable cross channel communications. Chord takes an active approach to replace the failed nodes with their neighbouring nodes, however, this all happens after the look up was initiated and passed the point of no return. Although this yields a success or fail result but using state management reduces those failed result therefore making the lookup process within a complex and distributed system more efficient and reduces costs to users and networks.

Short path and direct communication has been tested as an efficient and secure communication which is employed by method proposed by Ying Le et al. [1] addresses security over long range communication by encrypting messages using private keys and choosing multiple routing paths called multiple descriptions (MD) method. MD method observes limited number of links between nodes on application layer to develop a low congested communication channel and will suffer on a distributed scalable network while our proposed method uses alternative paths and short paths to communicate which lead to higher success rates in lookups.

Conclusion

The security, privacy, efficiency, and effectiveness of direct communications using trusted relationships has been tested, analyzed, and confirmed by various researchers in real world networks. Structured P2P overlays are an efficient way of secure communication through trusted paths over a distributed, decentralized network. However the number of failed attempts to lookup resources which either failed or no longer exist will cause traffic congestion and routing failures therefore reducing network efficiency and increasing the cost. If a query to contact a node is failed because the node failed or no longer exists, it will force high cost to network bandwidth and cause congestion on highly scalable network, something that if avoided will increase network efficiency. By identifying the need for improvement, we use smart lookup scheme by pro-active state management approach so the state of the node will be known the source channel using trusted route to reduce redundancy and failed lookups within the network. This technique will be combined with existing P2P application solutions to provide cost effective and efficient routing and lookup with P2P network overlay.

References

1. Li Y., Tian C., Diggavi S., Chiang M., Calderbank A. Network resource allocation for competing multiple description transmissions // IEEE Trans. Commun., vol. 58, no. 5, pp. 1493–1504, May 2010.
2. Papers R., Meng J. Paper Communications and Networking, vol. 2, no. 1, 2008.
3. Panda G. K., Tripathy B. K., Jha S. K., Security Aspects in Mobile Cloud Social Network Services, Int. J., vol. 2, no. 1, 2011.
4. Dixon C., Uppal H., Brajkovic V., Brandon D. ETTM : A Scalable Fault Tolerant Network Manager, Network.
5. Greenberg B. A., Hamilton J. R., Kandula S., Kim C., Lahiri P., Maltz A., Patel P., Sengupta S. VL2 : A Scalable and Flexible Data Center Network, Access Yournal vol. 09, pp. 95–104, 2009.
6. Edwards W.K., Grinter R. E. At Home with Ubiquitous Computing : Seven Challenges 2 The Seven Challenges, Seven., year.
7. Wei T., Wang C.-H., Chu Y.-H., Chang R.-I. A Secure and Stable Multicast Overlay Network with Load Balancing for Scalable IPTV Services // Int. J. Digit. Multimed. Broadcast., vol. 2012, no. i, pp. 1–12.
8. Chung Y. Distributed denial of service is a scalability problem // ACM SIGCOMM Comput. Commun. Rev., 2012, vol. 42, no. 1, p. 69, Jan.
9. Nguyen D. T., Nguyen B. L., Vu D. L. Improving Freenet’s Performance by Adaptive Clustering Cache Replacement / 2009 IEEE-RIVF Int. Conf. Comput. Commun. Technol., 2009, pp. 1–7.
10. Rasti A. H., Stutzbach D., Rejaie R. On the Long-term Evolution of the Two-Tier Gnutella Overlay / Proc. 25TH IEEE Int. Conf. Comput. Commun., 2006, pp. 1–6.
11. Ritter J. Why Gnutella Can’t Scale. No, Really, 2001, 13 p., http://www.cs.rice.edu
12. Sen S., Wang J. Analyzing Peer-To-Peer Traffic Yournal, vol. 12, no. 2, pp. 219–232, 2004.
13. Rowstron A., Druschel P. Pastry : Scalable, distributed object location and routing for large-scale peer-to-peer systems / Proceedings of the IFIP/ACM International Conference on Distributed Systems Platforms Heidelberg, London, Springer-Verlag, 2001, pp. 329-350.
14. Stoica I., Morris R., Liben-Nowell D., Karger D. R., Kaashoek M. F., Dabek F., Balakrishnan H. Chord: a scalable peer-to-peer lookup protocol for internet applications // IEEE/ACM Trans. Netw., Feb. 2003, vol. 11, no. 1, pp. 17–32.
15. Kempf J., Pierre R. St., Pierre P. St. Service Location Protocol for Enterprise Networks: Implementing and Deploying a Dynamic Service Finder. John Wiley & Sons, year.

UOT 004.7

Bazlı Behnam S.[1], Llewellyn-Jones David[2], Merabti Məcid M.[3]
[1,2,3]Liverpul Con Mur Universiteti, Liverpul, Böyük Britaniya
[1]b.bazli@ljmu.ac.uk, [2]d.llewellyn-jones@ljmu.ac.uk, [3]m.merabti@ljmu.ac.uk

Genişlənən universal kompüter şəbəkələrində effektiv axtarış

Kliyent-server texnologiyalarının mərkəzləşdirilmiş sistemlər çərçivəsində aşağı səviyyəli protokollardan istifadə edən ənənəvi mexanizmləri hazırda mobil hostlarla və universal mərkəzləşdirilməmiş sistemlər üzərində dinamik protokollar ilə əvəz olunur. Verilənlər trafikinə qiymətlərin artması və effektiv kommunikasiya və sistemlərin idarə edilməsinin təkmilləşdirilməsi zərurəti effektli və təsirli kommunikasiya metodlarının tətbiqini və universal P2P-şəbəkələrdə üzvlərin və resursların dinamik dəyişməsi probleminin həllini tələb edir. Bu işdə təyinat qovşağının vəziyyətinin qlobal əlyetərliliyi əsasında effektli marşrutlaşdırmaya başlanması üçün yeni paylanma və intellektual axtarış metodundan istifadə edilir. Bu metod, genişlənən şəbəkələr daxilində uğursuz sorğuların yüksək dəyərini nəzərə alaraq, bu şəbəkənin effrektliliyini yaxşılaşdırmağa və gözləmə vaxtını azaltmağa imkan verəcəkdir.

Keywords: *Paylanmış hesablamalar, genişlənmə; P2P, overley şəbəkələr, təhlükəsizlik, axtarış.*

УДК 004.7

Behnam B. Bazli[1], David Llewellyn-Jones[2], Madjid M. Merabti[3]
[1,2,3]Ливерпульский Университет Джона Мура, Ливерпуль, Великобритания
[1]b.bazli@ljmu.ac.uk, [2]d.llewellyn-jones@ljmu.ac.uk, [3]m.merabti@ljmu.ac.uk

Эффективный поиск в рамках масштабируемых универсальных компьютерных сетей

Традиционные механизмы клиент-серверных технологий в рамках централизованных систем с использованием протоколов низкого уровня в настоящее время заменяются мобильными хостами и динамическими протоколами надуниверсальных децентрализованных систем. Рост цен на трафик данных и необходимость эффективной коммуникации и улучшенного управления системами требуют развертывания эффективных и действенных методов коммуникации и решения проблемы динамического изменения членов и ресурсов в универсальных P2P-сетях. Эта работа использует новый способ распределения и интеллектуального поиска для инициирования эффективной маршрутизации на основе глобальной доступности состояния узла назначения. С учетом высокой стоимости неудачных запросов в рамках масштабируемых сетей это позволит улучшить эффективность сети и снизить время ожидания.

Ключевые слова: *распределенные вычисления, масштабируемость. P2P, оверлейные сети, безопасность, поиск.*