移动自组网络中的选播技术*

严 伟[1+], 倪明选[2]

[1](北京大学 计算机科学技术系,北京 100871)

[2](香港科学技术大学 计算机系,香港)

Manycast in Mobile Ad hoc Networks

YAN Wei[1+], NI Lionel[2]

[1](Department of Computer Science and Technology, Peking University, Beijing 100871, China)

[2](Department of Computer Science and Technology, Hong Kong University of Science and Technology, Hong Kong, China)

+ Corresponding author: Phn: +86-10-62765811, Fax: +86-10-62765813, E-mail: yanwei@net.pku.edu.cn, http://net.pku.edu.cn

Received 2004-11-04; Accepted 2005-02-03

Yan W, Ni L. Manycast in mobile Ad hoc networks. *Journal of Software*, 2005,16(9):1647−1660. DOI: 10.1360/jos161647

Abstract: Manycast is a new "one-to-some-of-many" communication pattern. It is the general communication form of anycast and multicast. With manycast a client can contact several servers to increase reliability or a distributed service can disseminate the important information to more than one server throughout a MANET network. This paper describes the main issues with manycast and mechanisms proposed in the last a few years. It also discusses some possible optimizations by taking advantage of other related work and shows some applications that have already been deployed in practice.

Key words: MANET; routing; manycast; multicast; service location; server selection

摘 要: 选播是一种新型的"1 对一些中的多个"通信模式,是任播和组播通信的通用形式.有了选播的支持,客户端可以与多个服务器建立联系以此增加可靠性,可以被分布式服务用来在移动自组网络中给多个服务器分发重要信息.不仅描述了选播面临的主要问题和最近几年提出的选播机制,而且讨论了借助其他相关技术进行可能的优化方案和实际应用的部署.

关键词: 无线自组织网络;路由;选播;组播;服务定位;服务器定位

中图法分类号: TP393 文献标识码: A

1 Introduction

A mobile Ad hoc network (MANET) is an autonomous system of mobile nodes connected by wireless links[1].

* Supported by the National Natural Science Foundation of China under Grant No.60273002 (国家自然科学基金)

YAN Wei was born in 1961. She is an associate professor at Peking University. Her research areas are next generation computer network, mobile ad hoc network, etc. **NI Lionel** was born in 1950. He is a professor at HKUST. His research areas are next generation computer network, wireless sensor network, etc.

The mobile nodes are free to move at any speed in any direction. Thus, there is no fixed infrastructure and the network's topology may dynamically change in an unpredictable manner. MANETs are characterized by their highly dynamic, multi-hop, and infrastructure-less nature[2]. Such inherently intermittent connectivity and congestion prevent the availability of centralized services in Ad hoc networks. For the sake of enhancing service availability, there are some special requirements for distributed services, such as server replication. A client may supply a gap of unreliability of Ad hoc networks by contacting several servers. Although current networks have implemented the above group communication technologies, they do not consider mobile users who want to locate one or more distributed servers. Casey Carter *et al* proposed a new communication concept, known as manycast, which is suitable for such requirement.

Manycast is a group communication patterns, which enables communication with an arbitrary number of members in a particular group. Manycast has both destination selection ability similar to anycast and one-to-many communication ability similar to multicast, but the number of destinations is variable, specified by a particular client. Anycast[3] is a communication between a single sender and the nearest receiver of a group, while multicast[4] is a "one-to-many" communication between a single sender and all members in a particular group. Anycast and multicast communication are just the special cases of manycast, in which the destination is either one or all, respectively. There have been researches on manycast technologies, as well as network applications using the manycast communication scheme. The research on manycast can be classified into two categories: the network layer and the application layer. However, there is a new trend of implementing manycast in the MAC layer. In this paper, we investigate the difficulties faced in providing manycast communication in an Ad hoc network, study some interesting applications based on manycast, and survey various approaches to manycast. We also discuss a few potential implementation technologies and propose a few possible ways to enhance the performance of manycast.

The rest of the paper is structured as follows. In Section 2, we show some applications and the motivations of manycast. We discuss the implementation problems related to manycast in Section 3. In Section 4, we investigate current researches but focus on network layer manycast technologies, as well as a few candidate methods to enhance the performance of manycast. Section 5 is the conclusions.

2 Applications

High mobility and frequent portioning means that even a low level of availability assurance is hard to be guaranteed in Ad hoc networks. These special features discourage users and may force them to use distributed and replicated services. It is obvious that there is a need to develop a mechanism for distributed clients to discover these distributed servers. Manycast is such a mechanism. Through manycast, applications can discover a good candidate set of service providers and enable efficient communication with those servers. Before investigating current manycast mechanisms in detail, let's study some successful applications which are based on manycast delivery scheme.

2.1 Network time protocol

NTP (Network Time Protocol)[5] is used to synchronize the time of a computer client or server to another server or reference time source, such as a radio, satellite receiver or modem. It provides accuracy typically within a millisecond on LANs and up to a few tens of milliseconds on WANs relative to Coordinated Universal Time (UTC) via a Global Positioning Service (GPS) receiver, for example. Typical NTP configurations utilize multiple redundant servers and diverse network paths in order to achieve high accuracy and reliability.

NTPv4 includes two new association modes, multicast and manycast, which in most applications can avoid per-host configuration altogether. In manycast mode, a client sends a message and expects one or more servers to

reply. From the messages returned, the client selects an appropriate subset of servers and continues in ordinary client/server operation with them. The manycast scheme can provide somewhat better accuracy than the multicast scheme at the price of additional network overhead.

2.2 Public key cryptography

Public key cryptography is one of the most effective security mechanisms for dynamic networks. The ITTC project[6] provides tools and an infrastructure for building intrusion tolerant applications. The ITTC system ensures that the compromise of a few system components does not compromise sensitive security information. Cryptographic keys are distributed across a few servers. The keys are never reconstructed at a single location. PKI (public key infrastructure) is an infrastructure for managing digital certificates. The most important component of PKI is the CA (certificate authority). PKI has been widely deployed in wired networks and some infrastructure-based wireless networks. Mobile nodes may store sensitive information in the infrastructure and maintain minimal information in devices[7].

COCA (cornell on-line certification authority)[8] is a fault-tolerant and secure online certification authority that has been built and deployed both in a local area network and in the Internet. Authority is distributed across several servers by threshold cryptography, any client must contact several servers simultaneously for certification. Yi and Kravets extend above certification concept to MANETs, employ threshold cryptography to distribute the CA functionality over specially selected mobile nodes based on the security and the physical characteristics of nodes[9]. With manycast any client can touch with some selected nodes called MOCAs (MObile Certificate Authority) simultaneously to get certification services.

2.3 Server selection and service location

The most widely used network application today is web browsing of the Internet. To reduce the response time at the end users, as well as the congestion at the servers and in the networks, web caching and server replication techniques are usually introduced. Both techniques place the “content provider” near to the browser clients. Content delivery uses DNS (domain name service) to direct a client request to the best destination. This method has a problem in determining the nearest servers[10]. Due to the potential mobility of web-caches or other servers in Ad hoc network, one or more nodes can act as content providers. Such service scenarios give rise to the problem of “server selection”. Manycast server selection technique can solve these problems. Since the same address can be used from anywhere and routing system would automatically select the best destinations for the clients, it would be transparent to the users.

On the other hand, a new computing device may come into Ad hoc network and know nothing about the service available in the network, there are requirements for some mechanisms of service advertisement or discovery to deal with such a dynamic behavior. J. Wu and M. Zitterbart proposed the “service awareness” concept that includes service discovery, advertisement, and sever selection in mobile Ad hoc environment[11]. Although the proposed system uses an Ad hoc anycast routing policy to allow clients to access services even if some of the providers drop from the network. We think that manycast is also adapted to the concept. Increasing the number of servers not only increases the service availability, for a client may contact more than one server, but also supports a degree of robustness against failure. Instead of relying on elaborate failover mechanisms and DNS to provide backups in case of failure, one needs only systems responding to the same address[10]. In Section 3, we can see that anycast is just a special case of manycast, manycast does more and better than anycast.

2.4 Internet gateways detection

Early in 2000, Shingo Ohmori pointed out that the forthcoming mobile communication systems are expected to

provide a wide variety of services through high data rate wireless channels anywhere in the world[12]. This means that broadband wireless channels have to be connected to broadband fixed networks, such as Internet and local area networks. As more and more wireless devices and applications are deployed, more requirements for mobile nodes to access to Internet are needed. Thus, better connectivity becomes the biggest challenge to the deployment and acceptance of mobile applications.

The solutions based on Mobile IP[13] have extended the coverage to include nodes with a wireless last hop from wired networks. Many approaches have been proposed to support connectivity for the Ad hoc network to the Internet. These approaches can be classified into three categories: proactive schemes[14−16], reactive schemes[17,18] and hybrid schemes[19,20]. Proactive and hybrid schemes can create a virtual backbone which is a mesh structure from a given network topology which includes nodes acting as gateways (for details in Section 4.3). These gateways are assigned well-known addresses. The mobile nodes require connectivity outside the Ad hoc network, contacting one or more gateways by manycast, getting one or several paths from local to outside networks.

In addition to the above applications, we can predict many other applications for Ad hoc networks that could benefit from manycast communication scheme. Peer-to-Peer file sharing systems[21] create an overlay network from end systems. These end systems maintain point-to-point connections as neighboring relationship. So P2P systems based on Ad hoc networks can efficiently locate arbitrary number of best peers by using manycast communication.

A sensor network is comprised of many small power devices with special sensing capabilities. It is just a static Ad hoc network because of nodes stability. Sensor nodes can detect and determine events that lead to safe operations, such as malfunctions, failures and natural disasters. When a variety of sensors are deployed in large numbers for detecting temperature, pressure, electromagnetic fields, acoustics, optical, chemical, and biological radiation and humidity etc, a mobile data collector can use manycast mechanism to collect sensitive datum from some sensors.

Distributed applications[22], distributed database of cache coherence applications can benefit from manycast delivery scheme too. Manycast communication enables such applications to discover a subset of peers with the best performances, thus isolate the application from underlay network transports.

3 Challenges to Manycast

Manycast is a group communication scheme in which one client contacts simultaneously to ***k*** servers from ***m*** members of a group, and the first explicit concept is defined by Ref.[23]. These servers are better for the client according with special application purpose. In terms of manycast semantic, the set of receivers for a particular transmission will be different for different communication source, due to the dynamic nature of Ad hoc networks. Thus manycast can not be deployed globally without serious consideration of a few key issues. Before investigating the problems of providing manycast communication in an Ad hoc network, let’s have a look at the manycast service definition in detail.

3.1 Manycast

Manycast fills the gap between anycast and multicast communication. In fact, Anycast and multicast are special casts of the manycast. Some manycast’s features are also found in anycast and multicast. Similar to multicast, manycast enables one client contact simultaneously with multi-servers, and the better servers in the group are selected by network itself like anycast.

Manycast supports bidirectional communication which follows such a one-to-many-to-one model. Thus, manycast provides a symmetric channel suitable for request/response communication between client and servers.

3.2 Global routing

The biggest difference between manycast and multicast is that receivers of transmission are better nodes with closer, less delay, minimum hops, greater bandwidth etc. Because of the inherently high dynamics, multi-hop, and infrastructure-less nature, multicast mechanisms are not suitable for manycast. There are some challenges when generally deploying manycast communications. Global routing may be the import problem.

Similar to anycast, global manycast also destroys the route aggregation because it allows the same address to be assigned to several nodes in different subnets. Only one of the subnets having a manycast address can match net prefix and be aggregated by routers. All other subnets of the manycast address must have individual route entries in routing tables. Thus routing tables will grow unbounded and routing speed will be significantly impacted when deploying manycast in a large scale. For effective, widely available and scalable new routing mechanisms, delivery methods and infrastructure for manycast should be supported.

3.3 Stateful connection

Some network applications which use stateful connections, such as TCP, require both peers to know enough about each other and the communication ongoing so far. Without sufficient knowledge, the connection-oriented protocol will not understand what is going on and when the connection will be terminated. Therefore, it is very important that the two ends of a stateful connection are in synch state. Although unicast delivery can guarantee a unique destination for a given address, manycast can not. Because any two manycast packets may arrive at different set of nodes, the stateful protocol can not be used on top of manycast communication without being modified. That is why most applications using manycast are the brief request/response transactions.

If applications need a long-term and stateful connection, a feasible and instant method would be as follows. First, using a brief manycast mechanism to discovery $\boldsymbol{k}$ servers, and then using unicast communication to create a long-term stateful session for peers. Some complicated solutions can be used for the above second phase. Scott Weber and Liang Cheng proposed a Five-Way Handshake in Ref.[10]. When a request comes in at the manycast address, the host can simply reply with its unicast address, and then take up the three-way handshake to create a stateful connection like TCP. A different approach, known as Source Identification Option, based on IPv6, has been presented in Ref.[24]. IP header option combined with the extra header option enables the destination awareness of the manycast address associated with the packet. Engel *et al*. proposed another easy solution, Source Route Option[25]. The method simply uses the existing source route option to force packets to follow a fixed route. These solutions all need to modify the protocol stack to some degree.

3.4 Manycast conflict

Manycast may be implemented in the application layer without the support of routing protocol. In such a case, manycast modules must reside in each node in the network. Manycast conflict occurs when replies are propagated back to the requesting source. Whenever a user performs a manycast delivery, the modules flood a transmission throughout the whole network. Since most routing protocols in Ad hoc network are on demand, there is a need of a wide network flood for every unicast route discovery. One manycast transaction for a group of $\boldsymbol{m}$ members requires $\mathbf{1}+\boldsymbol{m}$ network-wide floods, one for client request and $\boldsymbol{m}$ for responses from m servers. This excess of network-wide floods results in two important side effects on packet loss.

The first problem is broadcast implosion, a reverse broadcast storm. A member of a manycast group usually responses to the request towards the requesting source by the flooding scheme. Flooding will result in serious redundancy, contention, and collision on source network, causing collisions and loss of many of the responses. Several schemes, such as namely probabilistic, counter-based, distance-based, location-based, and cluster-based schemes, have been proposed in Ref.[26] to alleviate this problem.

Even if the reverse routing discoveries are successful, many unicast responses may result in another problem, such as ARP Harmful problem. ARP is the last hop delivery and at the interface between network and data link layer. When so many replies are delivered back, there is a rise and ARP broadcasts "implode" into the source. An automatic address resolution has been presented in Ref.[27] by Carter *et al*., which moves address resolution into the routing protocol along with neighbor discovery to correct the problem.

Obviously, an efficient manycast requests routing protocol to support.

3.5 Service quality

In mobile Ad hoc networks, the scarce bandwidth, highly dynamic topology and unreliable physical transmission media obviously restrict the routing protocol design and implementation. Furthermore, the set of applications for MANETs is diverse, ranging from small and static networks that are constrained by power sources to large-scale, mobile, and highly dynamic networks. Thus it is unlikely that a single routing protocol will be optimal for all scenarios. A good protocol should execute efficiently in accord with the characteristics of networks. Because manycast mechanism is likely integrated with the routing protocols, the quality of manycast is related not only to performance metrics about routing, but also performance of service.

Reliability

The current Internet protocol provides a best-effort data delivery. The manycast mechanism attempts to reach ***k*** servers without any guarantee to contact exactly ***k*** servers. However, most of today's popular applications and the control message dissemination of existing protocols require reliable delivery capabilities. Thus, applications using manycast for data delivery with reliability needs must rely on additional approaches to achieve the end-to-end transactions.

Control overhead

Lower control overhead means lower power consumption, this is very important to Ad hoc networks. Mehran Abolhasan points out that the control traffic overhead of proactive routing protocols is usually high, the control traffic overhead of hybrid routing protocols is medium, and the overhead for reactive routing protocols is lower. With proactive routing protocols, a considerable amount of bandwidth is consumed by routing update messages, while the hybrid routing protocol only update routing messages inside each zone or between gateways, the reactive routing protocols do not require any update message at all. However, proactive routing protocols have an advantage of instant availability of route and are very suitable to small networks of less mobility. When designing and implementing manycast mechanism, the characteristics of the corresponding network and routing protocol should be considered.

Delay level

In order to support real time applications, the wireless network needs to provide bandwidth reservation. This means one needs to know not only the minimum delay path to the destination, but also the bandwidth available on it. In addition to bandwidth, the network congestion should also be considered. The QoS routing in a mobile network is a major challenge due to the dynamics of mobility and traffic patterns, because most of the routing protocols proposed determine routing by the minimum hops. Even if the network can support routing with QoS, the problems about queuing effect and reverse broadcast storm (discussed in the last section) existing in manycast have to be solved.

Service quality

For the network layer manycast, QoS routing can determine the client-to-server route by using different metrics, such as minimum hops, shortest path, least delay etc., specified by the client. But it is still difficult for the client to send the request to the servers with the best process ability, since the network layer does not know any

service information about the above applications, such as server load or service availability. There should be a need to develop a special approach for the network layer to get application level knowledge, and to improve the network level performance of the manycast delivery and the quality of the service.

4 Manycast Mechanisms

In a manycast transaction, a single client requests service from many servers whose locations are not known a priori, and identified by a multicast-like address, some of them respond to that client.

There are some successful applications using application-layer manycast scheme (see Section 2) and many research activities on network-layer manycast routing. In this section, we first briefly review several typical applications and then investigate the manycast routing mechanisms.

4.1 Application layer manycast

The simplest way to implement manycast is to implement it in the application layer using unicast or multicast to contact multiple servers. There are some successful applications based on manycast .

NTPv4 has introduced a new automatic discovery and configuration paradigm by using manycast. A manycast client rambles on a nearby neighborhood to find cooperating manycast servers, validate them using cryptographic means and evaluate their time values with respect to other servers. Each manycast client associates with a number of nearby manycast servers, and meanwhile automatically reconfigures the number of servers. Clients locate servers by performing an expanding ring search over the IP multicast tree, named Scoped-Multicast detailed in Section 4.2. The NTP mechanism belongs to an application layer manycast.

Public Key Infrastructure is an infrastructure for managing digital certificates. The most important component of PKI is the CA. MOCA, proposed by S.Yi and R.Kravets in Ref.[8], uses threshold cryptography to distribute the CA's private key among many nodes that collectively act as the CA for the network. It is essentially a special-purpose manycast by unicast communication.

Internet Indirection Infrastructure (I3)[28] proposes an overlay-based Infrastructure that offers a rendezvous-based communication abstraction. Instead of explicitly sending a packet to a destination, each packet is associated with an identifier; which is then used by the receiver to obtain delivery of the packet. Such indirection concept separates the act of sending from the act of receiving, and provides efficient support to a wide variety of fundamental communication services like multicast, anycast, manycast etc. I3 is an overlay network which consists of a set of servers that store triggers and forward packets (using IP) between I3 nodes and to end-system. Identifiers and triggers have meaning only in this overlay network. Figure 1 illustrates manycast in I3 (Reproduction based on Fig.2c in Ref.[28]). The dashed directional lines represent triggers and solid directional lines indicate the data transmissions.

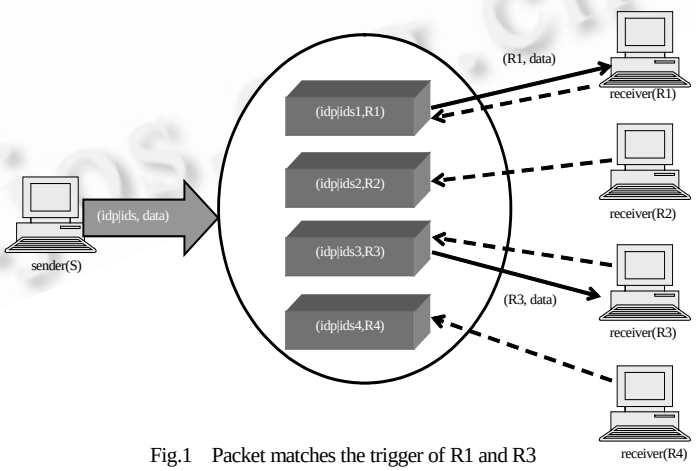

Fig.1 Packet matches the trigger of R1 and R3

When applications or approaches all provide manycast routing in application layer, because of lack of the complete network knowledge, the inability of controlling exact transmission, and the rapid topology change,

application layer manycast can not reduce the traffic and is less efficient than network layer manycast

4.2 Network layer manycast

Application layer manycast is the simplest way to implement manycast, for there is no need of knowing any network topology changes. However, there are two issues: scalability and overhead. Ad hoc networks are self-organized networks without any centralized structure. For manycast communication in which one client contacts to ***k*** servers, the client must know the addresses of ***k*** servers. Thus how to discover servers becomes more complex. Moreover, each transmission in MANET requires route discovery for each server, which results in considerable overhead.

Now we concentrate on network routing mechanisms for supporting manycast delivery. In MANET all network components can be mobile. There is no real distinction between a host and a router like the Internet, since all nodes can be sources as well as forwarders of traffic. Thus, the routing protocol in MANET is very different from the protocol having been deployed in current infrastructure networks. There have been many MANET routing protocols proposed in the last decade. They can be classified as proactive, reactive, and hybrid protocoal. The proactive protocols are global routing protocols, maintaining network connectivity proactively, while the reactive protocols reduce the impact of frequent topology changes by acquiring route on demand. The hybrid routing protocols employ both reactive and proactive properties by maintaining intra-zone information proactively and inter-zone information reactively.

In the interest of discussion, we suppose that the total members in a group is ***m*** and the number of responses desired is ***k***. Manycast attempts to reach ***k*** servers in the group. If at least ***k*** distinct servers' responses come back to the requester, we say the request is satisfied. We also suppose the routing protocol mentioned next is on-demand exception specification.

Flood

Flooding is a very simple but reliable method to delivery packet in dynamic mobile networks, similar to broadcast in wired networks. A simple flooding performs comparatively well and shows promise as a foundation for more specialized protocols for highly dynamic MANET[29]. For a manycast request, the routing protocol floods the request as route discovery, so all intermediate nodes can set up a route state just as they react to a route request. Then responses are returned to the requesting source along the return path by unicast without any additional discovery process. Figure 2 indicates an example of flooding. The shaded circles are servers, the shaded squares are the clients, and the dashed lines between nodes indicate connectivity. The thick lightly shaded lines represent request transmission, while the narrow dark directional lines represent the response back to the client. All the figures from Fig.2 to Fig.6 are reproductions based on Refs.[23].

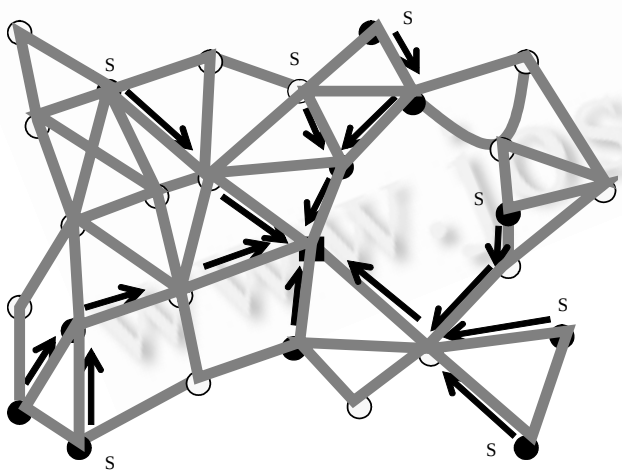

Fig.2 Network wide flooding can find all the servers

Scoped-flooding adds some intelligence on the basis of pure flooding. “Scoped” means that the flooding is restricted with a limited scope. Casey Carter presents the definition of scoped-flood: it floods the request packet within the smallest TTL-limited scope that covers at least ***k*** servers. The discovery phase of scoped-flood is identical to flood. When the routing protocol propagates manycast requests, the reverse route is established. The client uses the routing state to find the ***k*** servers within the scope.

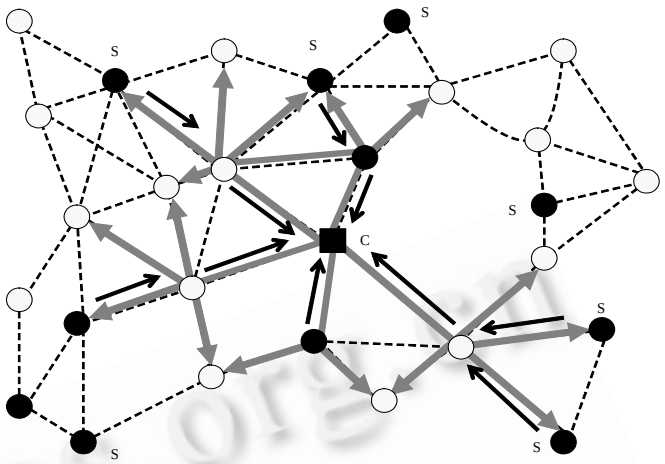

Fig.3 Scoped-flooding with TTL=2 can find 7servers

Expanding ring search is also an approach on the basis of flooding which incrementally explores one’s neighborhood in search of ***k*** servers. The idea is simply flooding with packets of TTL 1, 2, 3, and so on until ***k*** servers are contacted. Initially the number of cached servers is zero, the manycast request’s TTL is 1. After the first flooding, if the number of routes to server founded is less than ***k***, the client does not reach ***k*** servers. The next flooding is carried out with TTL 2, and so on until the client reaches ***k*** servers.

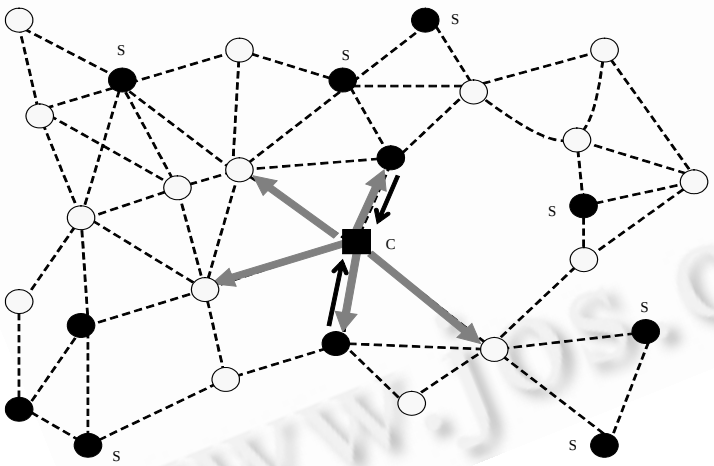

Fig.4 Expanding ring search: first search can find 2 servers; second search can find 7 same as Fig.3

We call the *scoped-flooding* as static scoped-flood and *expanding ring search* dynamic or iterative scoped-flooding, because the former has the definite TTL while the later has various TTL for every flooding. When the servers are spread sparsely and the chosen TTL is small, it will be quite likely that the *scoped-flooding* can not reach ***k*** servers. That will result in another scoped-flooding with larger TTL to discovery desired ***k*** servers. On the other hand, if service requires a larger ***k*** and servers are deployed uniformly throughout the network, then *expanding ring search* may employ multiple scoped-flooding (with TTL1,2,3…) before finding ***k*** servers. Both authors of Refs.[23] have respectively simulated the algorithm, but the conclusions are not very consistent. For the sake of accurately evaluating performance of different approaches, further research has to be taken, especially on evaluating metric and methods.

Multicast

Multicasting delivery schemes have been widely deployed in the Internet to support network applications, such as VOD, video conferences, teleconference etc. In recent years, many multicast protocols have been proposed specifically for MANETs (e.g., SMB, CAMP, ODMRP, MAODV, AMRoute, AMRIS, BEMRP, MCEDER, and LAM). These protocols all follow the traditional multicast approaches, i.e., distributed group membership management and distributed multicast routing state maintenance. Any approach using such multicast routing to perform manycast delivery can take advantage of the multicast tree. Although maintaining the multicast tree may produce additional overhead, especially in high mobility networks, this approach has lower overhead than flooding, because the multicast request is propagated following the multicast tree. Nevertheless there is still a space to improve the efficiency of this approach.

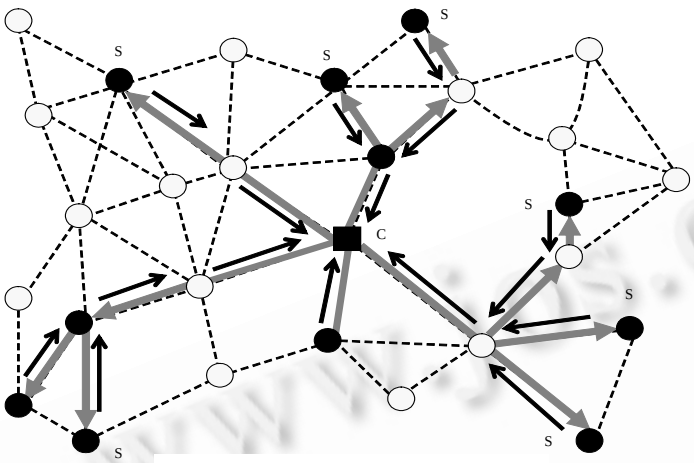

Fig.5 Multicasting can find all the servers

Scoped-multicasingt is evolved from traditional multicast, putting limits on the scope of propagating request by TTL to reduce the strain on network, much similar to scoped-flooding. There is still a problem about the multicast tree. Limiting the scope of transmission, the multicast tree must be pruned on the basis of current TTL, but these pruned branches must rejoint the tree so as to perform next multicast operation with increased TTL, in case of this request not reaching ***k*** servers. According to the knowledge of the author, no current manycast routing protocol has this automatic resume-tree capability. Scoped operations are more selective than infinite scope operations. Withering flood or multicast may be dependent on the tradeoff between the overhead of tree maintenance proactively and the network load by simply flooding.

Small group multicasting may be an alternative approach for manycast. Small group multicast can support a very large number of small multicast sessions, whereas the existing multicast schemes support a limited number of very large multicast sessions. DCM[30], based on an extension of the centre-based tree approach, uses several core routers and a special protocol between them to scale well with the number of multicast groups by (1) avoiding multicast group state information in backbone routers, (2) avoiding triangular routing across expensive backbone links. Explicit Multicast (Xcast)[31] and DDM[32] give sources knowledge of group membership and explicitly encode the list of destinations in the data packets. That is, differentially encoded, variable length destination headers are inserted in data packets which are used in

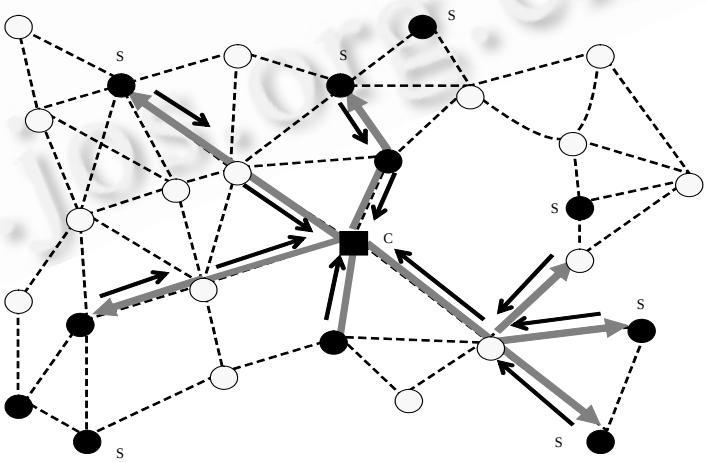

Fig.6 Scoped-multicast: find 7 servers

combination with unicast routing tables to forward multicast packets towards multicast receivers. The protocol is best suited for applications with small multicast groups in dynamic MANET environment. It is very obvious that the objective of small group multicast is adaptable for manycast. Figure 7 illustrates a concept of using small group multicast for manycast delivery. Client sends two packets by two different interfaces respectively, and contacts to three servers.

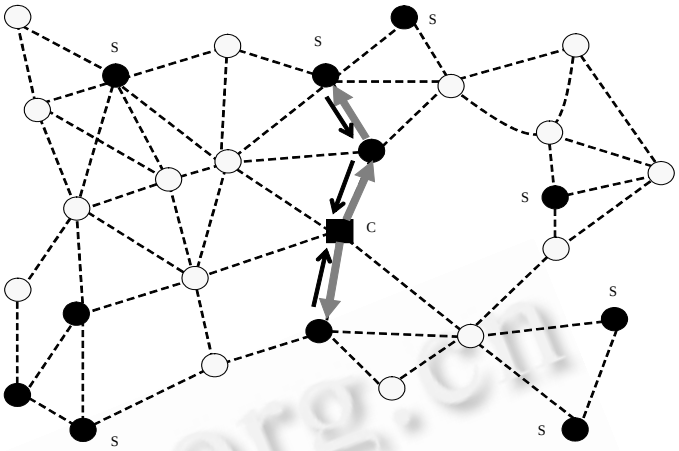

Fig.7 An example of using small group multicast

Manycast tree

William Strathearn and Chiranjeeb Buragohain created a group-shared multicast tree maintained by all the servers. When any server receives a message, it forwards that message to ***k*** other servers. The algorithm comprises of two important phases: multicast tree formation/maintenance, and data forwarding. To create a tree containing all the servers, a rendezvous point (RP) is assigned a well known address. To join the tree, servers send a joint request to RP. Then RP or a server which is already in the tree sends back a reply message and considers the requesting servers being its children. The tree is maintained by a neighbor list on every node belonging to the tree. All neighbor lists reflect the relationship between parents and its children in the tree. Like normal multicast trees for Ad hoc networks, however, the *manycast tree* suffer from the high mobility of both network topology and nodes, which means any tree constructed can not be stable for long. Therefore, the algorithm associates a soft state with the neighbor list on every tree node to keep up-to-date of the tree. Every server periodically sends a request massage towards the RP and refreshes the neighbor entry in a neighbor list, the neighbor replying to the request may be RP or other servers. Figure 8 is an example of a multicast tree. The lightly shaded lines indicate the multicast tree and the dark directional lines indicate the nearest server from the clients.

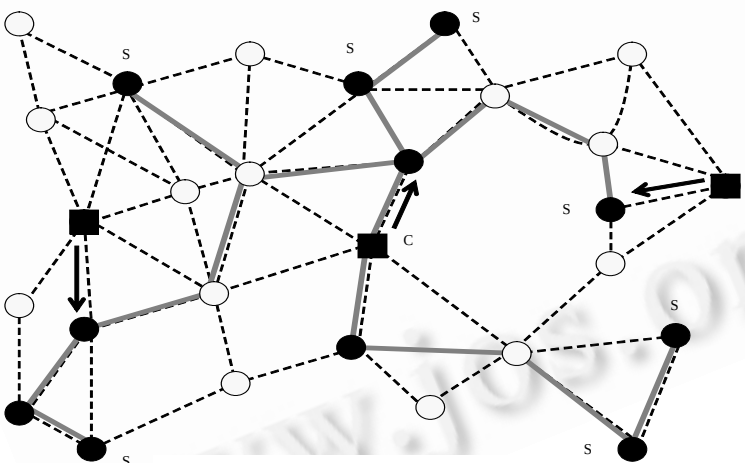

Fig.8 Multicast tree is composed by all servers and thick lightly shaded lines

As long as the multicast tree is up to date and a packet reaches at least one server, the packet can be efficiently transmitted to other servers by following the tree. Expanding ring search mentioned above would be the best candidate approach for delivery of the packet to any server. To reduce the network load, *manycast tree* puts a special field to specify how many servers this packet to be delivered, the field being initially set to ***k***. When the packet is forwarded by a server with ***p*** neighbors, the field is updated by subtracting ***p***, which enables the data packet to reach ***k*+1** servers. Because the efficiency of a packet forwarding depends on the tree, *manycast tree* is more adaptable to

low mobility, high request rate application scenarios.

4.3 Improving manycast

With the feasibility issues of manycast addressed and some candidate approaches investigated, we can further discuss how to improve the performance of manycast by referencing other research results in related routing areas.

Overlay network routing

Some distributed services have some requirements about billing, security, etc. Distributed membership management may be more difficult due to the lack of admission control. Without the support for end-to-end signaling between sources and receivers, security management may rely on external mechanisms, and billing management becomes more complicated because the sources (information owners) have no control and knowledge over how and to whom their data is distributed. Miguel Castro et al proposed a proximity-aware peer-to-peer overlay network for decentralized, lightweight group maintenance and implemented a scalable application-level anycast system[33]. The approach uses Scribe[34] to manage groups and maintain a spanning tree connecting the members of each group. The spanning trees are used to deliver messages efficiently to a nearby group member with low delay and link stress.

The authors of Ref.[33] think that their overlay approach can support manycast communication scheme. The message can be sent to several group members by continuing the anycast until the message has been delivered to the desired number of members, and tracking the number of recipients in the message. The manycast primitives provided by them can be secured from malicious participating nodes in the overlay network, which is done by extending the secure routing in Pastry[35].

QoS routing

In addition to security, the quality of manycast delivery process is another measure. In Refs[23], the quality is defined as reliability, the expectation that any given request will receive at least k responses. Any application that needs to improve its service reliability may contact $K>k$ servers to increase the likelihood that at least k servers respond successfully. At the same time, the author thinks the quality of manycast routing is also related to aforementioned applications. For real time streaming applications, the QoS on the service data direction is more important than that on the request direction. For this feature, my colleagues and I propose a reverse QoS routing algorithm[36], which uses reverse dynamic distance from servers to the source of the requesting message as one of performance metrics. The service load of servers is also taken into account. These two special metrics can guarantee the reverse streaming data transmission and balance the server load to some extent.

Backbone routing

Minimum service response delay is essential for network applications. Mehran Abolhasan concludes that the delay level of reactive routing protocols is higher than that of proactive routing protocols[37]. For some small Ad hoc networks with less mobility, the backbone routing may be the best alternative. The virtual dynamic backbone protocol has been proposed in Refs[38], which constructs a backbone from a subset of the nodes in the network. The backbone nodes are connected to each other via other backbone nodes, and the non backbone nodes are neighbors of a backbone node. The protocol consists of three phases: backbone selection process, backbone connection process and backbone maintenance process. Relatively stable and high degree nodes will be prior to backbone nodes. If above phases force all members of a manycast group to be the backbone nodes in constructing and maintaining a connected backbone, the performance of manycast will be improved on the benefit of reducing response time for locating services.

5 Summary

This paper presents some applications of manycast. We have surveyed some problems faced by manycast. Some different approaches are reviewed from application layer manycast to network layer manycast. Candidate techniques for improving manycast performance have been proposed. Our goal is to show all aspects involved in designing, implementing manycast mechanism, and deploying related distributed services atop on it in MANETs as possible as we can. Future research will be continued, focusing on exploring the various methods integrated to three classes routing protocol, standardizing the evaluation metric, and applying the features of manycast to generate new services and applications.

Acknowledgement The first author acknowledges the support of HKUST that enabled her to carry out this research.

References:

[1] Agrawal DP, Zeng QZ. Introduction to wireless and mobile systems. Beijing: Higher Education Press, 2003.

[2] Kozat UC, Tassiulas L. Network layer support for service discovery in mobile Ad hoc networks. In: Proc. of the IEEE INFOCOM 2003. 2003. 1965−1975.

[3] Partridge C, Mendez T, Milliken W. Host anycasting service. RFC 1546, 1993. http://www.faqs.org/rfcs/rfc1546.html

[4] Deering S. Host extensions for IP multicasting. Request for Comments (Standard) RFC 1112, Internet Engineering Task Force, 1989.

[5] Mills DL. The network time protocol (NTP) distribution. Department of EE/CIS, the University of Delaware http://www.eecis.udel.edu/mills/ntp/html/

[6] Wu T, Malkin M, Boneh D. Building intrusion tolerant applications. In: Proc. of the 8th USENIX Security Symp.1999. 79−91.

[7] Seung Yi, Kravets, R. Key management for heterogeneous Ad hoc wireless networks. In: Proc. of the 10th IEEE Int'l Conf. on Network Protocols. Paris, 2002. 202−203.

[8] Zhou LD, Schneider FB, van Renesse R. COCA: A secure distributed on-line certification authority. ACM Trans. on Computer Systems, 2002,20(4):329−368.

[9] Yi S, Kravets R. MOCA: Mobile certificate authority for wireless Ad hoc networks. In: Proc. of the 2nd Annual PKI Research Workshop (PKI03). Gaithersburg, 2003.

[10] Weber S, Cheng L. A survey of anycast in IPv6 networks. IEEE Communication Magazine, 2004,42:127−132.

[11] Wu J, Zitterbart M. Service awareness and its challenges in mobile Ad hoc networks. In: Workshop on Computer Science 2001: Mobile Communication over Wireless LAN: Research and Applications. 2001.

[12] Ohmori S. The future generations of mobile communications based on broadband access technologies. IEEE Communication Magazine, 2000,38:134−142.

[13] Perkins CE. IP mobility support. RFC2002, 1996, Updated by RFC2290. http://www.faqs.org/rfcs/rfc2002.html

[14] Pan Asia Networking. Wireless Internet Post Office. http://genie.iitd.ernet.in/wipo/routing-protocols.html

[15] Jonsson U, Alriksson F, Larsson T, Johansson P, Maguire G Jr. MIPMANET-Mobile IP for mobile Ad hoc networks. In: Proc. of the IEEE/ACM Workshop on Mobile and Ad hoc Networking and Computing. Boston, 1999. 75−85.

[16] Sun Y, Belding-Royer EM, Perkins CE. Internet connectivity for Ad hoc mobile networks. Int'l Journal of Wireless Information Networks Special Issue on "Mobile Ad hoc Networks (MANETs): Standards, Research, Applications". 2002,9(2).

[17] Broch J, Maltz D, Johnson D. Supporting hierarchy and heterogeneous interfaces in multi-hop wireless Ad hoc networks. In: Proc. of the Workshop on Mobile Computing Held in Conjunction with the Int'l Symp. on Parallel Architectures, Algorithms, and Networks. Perth, 1999. 370−375.

[18] Wakikawa R, Malinen JT, Perkins CE, Nilsson A, Tuominen AJ. Global connectivity for IPv6 mobile Ad hoc networks. Internet Engineering Task Force. Internet Draft, 2002.

[19] Ratanchandani P, Kravets R. A hybrid approach to Internet connectivity for mobile Ad hoc networks. ACM MobiCom, 2003.

[20] Miller MJ, List WD, Vaidya NH. A hybrid network implementation to extend infrastructure reach. Technical Report, University of Illinois at Urbana-Champaign, 2003. http://www.crhc.uiuc.edu/~nhv/papers/hybrid-tech.pdf

[21] Gnutella p2p file sharing system. http://www.gnutella.com

[22] Rom´an M, Hess CK, Cerqueira R, Ranganathan A, Campbell RH, Nahrstedt K. Gaia: A middleware infrastructure to enable active spaces. IEEE Pervasive Computing, Oct-Dec 2002.

[23] Carter C, Yi S, Ratanchandani P. Manycast: Exploring the space between anycast and multicast in Ad hoc networks. In: Proc. of the MobiCom 2003. San Diego, 2003. 273−285.

[24] Shah S, Sanghi D. Host Anycast Support in IPv6. In: Proc. of the 5th Int'l Conf. Advanced Computer. 1997.

[25] Engel R, Peris V, Saha D. Using IP anycast for load distribution and server location. In: Proc. of the 3rd Global Internet MiniConf. 1998.

[26] Ni SY, Tseng YC, Chen YS, Sheu JP. The broadcast storm problem in a mobile Ad hoc network. In: Proc. of the 5th Annual Int'l Conf. on Mobile Computing and Networking (MobiCom'99). Seattle, 1999.

[27] Carter C, Yi S, Kravets R. ARP considered harmful: Manycast transactions in Ad hoc networks. In: Proc. of the IEEE Wireless Communications and Networking Conf. (WCNC). 2003. 1801−1806.

[28] Stoica I, Adkins D, Zhuang S, Shenker S, Surana S. Internet indirection infrastructure. In: Proc. of the ACM SIGCOMM. Pittsburgh, 2002.

[29] Obraczka K, Tsudik G, Viswanath K. Pushing the limits of multicast in Ad hoc networks. In: Proc. of the 21st Int'l Conf. on Distributed Computing Systems (ICDCS). 2001. 719−722.

[30] Blazevic L, Boudec JYL. Distributed core multicast (DCM): A routing protocol for many small groups with application to mobile IP telephony. Draft-blazevic-dcm-mobility-00.txt, Internet Engineering Task Force, 1999.

[31] Boivie R, Feldman N, Imai Y, Livens W, Ooms D, Paridaens O. Explicit multicast (Xcast) basic specification. Internet Draft (Work in Progress) draft-ooms-xcast-basic-spec-04.txt, Internet Engineering Task Force, 2003.

[32] Ji L, Corson MS. Explicit multicasting for mobile Ad hoc networks. Mobile Networks and Applications, 2003,(8):535−549.

[33] Castro M, Druschel P, Kermarrec AM, Rowstron A. Scalable application-level anycast for highly dynamic groups. In: Proc. of the Networked Group Communication (NGC 2003). Munich, 2003.

[34] Castro M, Druschel P, Kermarrec AM, Rowstron A. Scribe: A large-scale and decentralized application-level multicast infrastructure. IEEE Journal on Selected Areas in Communications (JSAC), 2002,20:1489−1499.

[35] Castro M, Druschel P, Ganesh A, Rowstron A, Wallach D. Secure routing for structured peer-to-peer overlay networks. In: Proc. of the 5th Usenix Symp. on Operating Systems Design and Implementation (OSDI 2002). Boston, 2002.

[36] Zhang L, Jia W, Yan W. Reverse anycast QoS routing protocol. In: Asia Pacific Advanced Network Consortium. Proc. of the 16th APAN Meetings/Advanced Network Conf. Korea, 2003.

[37] Abolhasan M, Wysocki T, Dutkiewicz E. A review of routing protocols for mobile Ad hoc networks. Ad hoc Networks, 2004, 2:1−22.

[38] Kozat UC, Kondylis G, Marina MK. Virtual dynamic backbone for mobile Ad hoc networks. In: Proc. of the IEEE Int'l Conf. on Communications. 2001. 250−255.