A SURVEY OF CONNECTIONLESS NETWORK SERVICE PROTOCOLS FOR MOBILE AD HOC NETWORKS

MANIYAR SHIRAZ AHMED[1], DR. SYED ABDUL SATTAR[2], FAZEELATUNNISA[3]

[1] Lecturer, Department of Computer Science & Information Systems,
Najran University, Najran, Saudi Arabia,

[2]Professor and Dean of Academics

[3]Lecturer, Department of Computer Science & Information Systems,
Najran University, Najran, Saudi Arabia

Abstract:

A Mobile Ad Hoc Network (MANET) is a network that changes locations and configure itself on the fly. It means MANETs are used where the infrastructure is not available such as military or police exercises, disaster relief operations and urgent business meetings. The stipulation of connectionless network service (CLNS) is much more demanding in mobile ad hoc networks. A lot of research have been done so as to provide CLNS by designing various MANET protocols. However, efficient performance evaluations and relative analysis of these protocols in a common pragmatic environment have been performed only in a limited manner. In this survey the relative features, functions and reliability of each CLNS protocols are studied and discussed.

Keywords: CLNS, MANETS, Reliability

Introduction:

Recent advancements such as Bluetooth introduced a new type of wireless systems known as mobile ad hoc networks. Mobile ad hoc networks or "short live" networks operate in the absence of fixed infrastructure. They offer quick and easy network deployment in situations where it is not possible otherwise. Ad hoc is a Latin word, which means "for this or for this only" Mobile ad hoc network is an autonomous system of mobile nodes connected by wireless links; each node operates as an end system and a router for all other nodes in the network.

Ad Hoc networks can provide communication for civilian applications, such as message exchanges among business meeting, medical and security personnel involved in rescue missions. These applications rely only on connectionless services because of no infrastructure available.

Connectionless network service provides network layer services to the transport layer. When support is provided for CLNS, routing uses routing protocols to exchange routing information. CLNS does not perform connection setup or termination because paths are determined independently for each packet that is transmitted through a network. In addition, CLNS provides best effort delivery, which means that no guarantee exists that data will not be lost, corrupted, disordered, or duplicated. CLNS relies on transport layer protocols to perform error detection and correction.

Following this, we recap the operation, key features & functions and major protocols in selecting a connectionless network service. We

focus on journal articles and peer-reviewed conferences, thereby hopefully extracting the most useful and important rift of the candidate solutions.

(I) Issues need to be considered while providing CLNS:

Connectionless network service refers to communication between two network end points in which messages can be sent from one end point to another without prior arrangement.

CLNS are:

- Stateless having no previously defined protocol
- Easily accessible.

But the CLNS is not ensured that the recipient is available to receive the data. The Data has to be resent several times. It's hard to filter malicious packets using firewalls. No acknowledgement will be given during the data transfer. The main advantage of using CLNS is that it is mainly used in "real time" applications where data sending is more important.

CLNS is a type of network service at the layer 3 of the OSI model. This service does not have the reliability of the connection-oriented method, but it is useful for periodic burst transfers. Neither system must maintain state information for the systems that they send transmission to or receive transmission from. LANs operate as connectionless systems. A computer attached to a network can start transmitting frames as soon as it has access to the network. It does not need to set up a connection with the destination system ahead of time. However, a transport-level protocol such as TCP may set up a connection-oriented session when necessary. Contrast this with Connectionless service, which does not require establishing a session and a virtual circuit[1]. This can be found in the network layer or transport layer, depending on the protocol. You can think of a connectionless protocol as being akin to mailing a post card. You send it and hope that the receiver gets it.

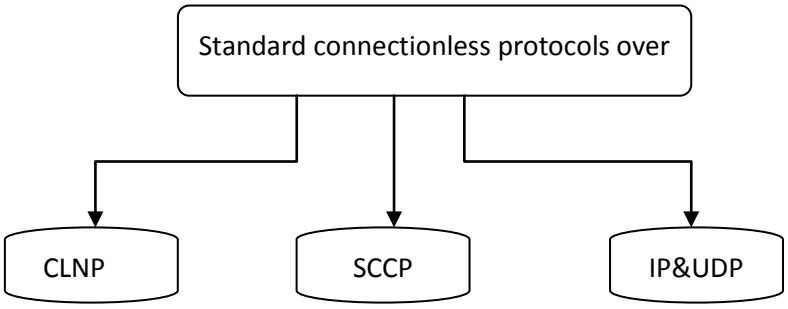
Features of a connectionless service :

- Packets do not need to arrive in a specific order
- Reassembly of any packet broken into fragments during transmission must be in proper order
- No time is used in creating a session
- No Acknowledgement is required.

The largest connectionless network in use today is the Internet.

4. Protocols providing CLNS

Protocol classification



(a) Connectionless network protocol (CLNP):

CLNP, is a Public Data Network protocol that provides the connectionless mode network service.

Aim of CLNP:

CLNP performs two services: breaking data into packets and addressing packets across networks. It is known as a "datagram" service, which refers to the process of splitting up data into chunks for transmission and adding a header to it. The addressing responsibilities of

the protocol follow the Network Service Access Point (NSAP) protocol[6].

Functions of CLNP:

CLNP is the equivalent to the Internet Protocol definition of the TCP/IP (Transmission Control Protocol/Internet Protocol) stack. "Connectionless" systems simply send out data to an address without checking whether the data actually arrived. Connectionless Network Protocol (CLNP)[10] is an ISO network layer datagram protocol. CLNP provides the Connectionless-mode Network Service. CLNP is intended for use in the Sub network Independent Convergence Protocol (SNICP) role, which operates to construct the OSI Network Service over a defined set of underlying services, performing functions necessary to support the uniform appearance of the OSI Connectionless-mode Network Service over a homogeneous or heterogeneous set of interconnected sub networks[7].

CLNP uses Network service access point (NSAP) addresses and titles to identify network devices. The Source Address and Destination Address parameters are OSI Network Service Access Point Addresses (NSAP address). A network-entity title is an identifier for a network-entity in an end-system or intermediate-system. Network-entity titles are allocated from the same name space as NSAP addresses, and the determination of whether an address is an NSAP address or a network-entity title depends on the context in which the address is interpreted. CLNP (Connectionless Network Protocol) provides the same maximum datagram size as IP, and for those circumstances where datagrams may need to traverse a network whose maximum packet size is smaller than the size of the datagram, CLNP (Connectionless Network Protocol) provides mechanisms for fragmentation (data unit identification, fragment/total length and offset). Like IP, a checksum computed on the CLNP header provides a verification that the information used in processing the CLNP datagram has been transmitted correctly, and a lifetime control mechanism ("Time to Live") imposes a limit on the amount of time a datagram is allowed to remain in the Internet system.

CLNP has the following PDU(protocol data unit) structure:

Header part	**Address part**	**Segmentation part**	**Option part**	**data**

Header part

8	**16**	**24**	**24**	**35**	**40**	**56**	**72bit**
NLP ID	Length ID	Version	Life time	Flags	Type	Seg. Length	Check sum

NLP ID - Network Layer Protocol Identifier. The value of this field is set to binary 1000 0001 to identify this Network Layer protocol as ISO 8473, Protocol for Providing the Connectionless- mode Network Service and the value of this field is set to binary 0000 0000 to identify the Inactive Network Layer protocol subset.

- Length ID - Length Indicator is the length in octets of the header
- Version - Version/Protocol Id Extension identifies the standard Version of ISO 8473
- Lifetime - PDU Lifetime representing the remaining lifetime of the PDU, in units of 500 milliseconds.
- Flags - three flags: segmentation permitted, more segments, error report
- Type - The Type code field identifies the type of the protocol data unit, which could be data PDU or Error Report PDU

- Seg. Length - The Segment Length field specifies the entire length, in octets, of the Derived PDU, including both header and data (if present).
- Checksum - The checksum is computed on the entire PDU header.

Address Part

It contains information of destination and source addresses, which are defined in OSI 8348/AD2 with variable length.

Segmentation Part

If the Segmentation Permitted Flag in the Fixed Part of the PDU Header[2] (Octet 4, Bit 8) is set to one, the segmentation part of the header, illustrated in Figure 6, must be present: If the Segmentation Permitted flag is set to zero, the non-segmenting protocol subset is in use.

Option Part

The options part is used to convey optional parameters.

Data Part

The Data part of the PDU is structured as an ordered multiple of octets.

(b) Signaling connection control part (Sccp):

Signaling Connection Control Part (SCCP), is a Signaling System 7 protocol that provides the connectionless mode network service as described in ITU-T Recommendation X.213. Signaling Connection Control Part (SCCP), a routing protocol in SS7 protocol suite in layer 4, provides end-to-end routing for TCAP messages to their proper database and relies on the services of MTP for basic routing and error detection. SCCP provides connectionless and connection-oriented network services above MTP Level 3.

SCCP allows routing using a Point Code and Subsystem number or a Global Title. A Point Code is used to address a particular node on the network, whereas a Subsystem number addresses a specific application available on that node. SCCP employs a process called Global Title Translation to determine Point Codes from Global Titles so as to instruct MTP on where to route messages.

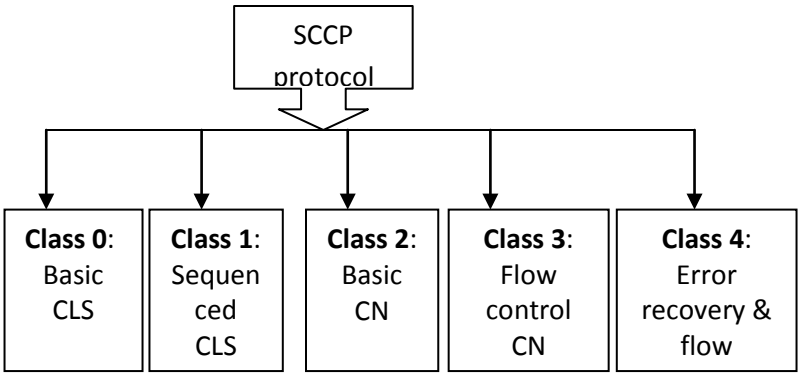
SCCP[10] messages contains 3 parameters which describe the type of addressing used, and how the message should be routed:

SCCP message parameters:

(i) Address Indicator
(ii) Global title indicator
(iii) Routing indicator
(iv) Address Indicator Coding

SCCP Protocol classes:

SCCP provides 5 classes of protocol to its applications:



***CLS – Connectionless**

***CN – Connection Oriented**

Class 0: Basic connectionless

The SCCP Class 0 protocol class is the most basic of the SCCP protocol classes. Network Service Data Units passed by higher layers to the SCCP in the originating node are delivered by the SCCP to higher layers in the destination node. They are transferred independently of each other. Therefore, they may be delivered to the SCCP user out-of-sequence. Thus, this protocol class corresponds to a pure connectionless network service. As a connectionless protocol, no network connection is established between the sender and the receiver.

Class 1: Sequenced connectionless

SCCP Class 1 builds on the capabilities of Class 0, with the addition of a sequence control parameter in the NSDU which allows the SCCP User to instruct the SCCP that a given stream of messages should be delivered in sequence. Therefore, Protocol Class 1 corresponds to an enhanced connectionless protocol with assurances of in-sequence delivery.

Class 2: Basic connection-oriented

SCCP Class 2 provides the facilities of Class 1, but also allows for an entity to establish a two-way dialog with another entity using SCCP.

Class 3: Flow control connection oriented

Class 3 service builds upon Class 2, but also allows for expedited (urgent) messages to be sent and received, and for errors in sequencing (segment re-assembly) to be detected and for SCCP to restart a connection.

Class 4: **Error recovery and flow control connection oriented**

Class 4 service is never used in real time.Signaling Connection Control Part provides reliable delivery of packets between end stations in a telephone network. SCCP makes it possible to address a message to a specific type of device, such as a conventional telephone set, cell phone set, VoIP end station, fax machine, or computer. SCCP maintains the correct sequencing of packets, even during times of high network traffic or partial network failure. SCCP is used as the transport layer for services such as 800/888/877 (free-phone) numbers, phone cards (calling cards) and roaming in cellular networks.

Protocol Structure

SCCP messages are contained within the Signaling Information Field (SIF) of an MSU. There are two formats for the SCCP messages: one is defined by ANSI[3] and the other is defined by ITU-T.[10]

SCCP Header Structure

Routing table

Offset	Service Information Octet		
0	Service field	Service Indicator	
1	DPC Member		
2	DPC Cluster		
3	DPC Network		
4	OPC Member		
5	OPC Cluster		
6	OPC Network		
7	3 – bits spare	Signalling Link Section	
8	Message Type		
9 . . . . N	Interpretation Varies According to Message Type Value		

Service Information Octet		
0	Service field	Service Indicator
1	DPC Low – Order Octet	
2	OPC Low-order 2-bits	DPC High-Order 6-bits
3	OPC Middle – Order Octet	
4	4-bit SLS/SLC	OPC High-Order 4-bits
5	Message Type	
6 . . . . n	Interpretation Varies According to Message Type Value	

The signaling information field(SIF) contains the routing label followed by the SCCP message header with the following structure:

Routing label
Message type
Mandatory fixed part
Mandatory variable part
Optional part

- **Routing label** - A standard routing label.
- **Message type code** - A one octet code which is mandatory for all messages. The message type code uniquely defines the function and format of each SCCP message.
- **Mandatory fixed part** - The parts that are mandatory and of fixed length for a particular message type will be contained in the mandatory fixed part.
- **Mandatory variable part** - Mandatory parameters of variable length will be included in the mandatory variable part. The name of each parameter and the order in which the pointers are sent is implicit in the message type.
- **Optional part** - The optional part consists of parameters that may or may not occur in any particular message type. Both fixed length and variable length parameters may be included. Optional parameters may be transmitted in any order. Each optional parameter will include the parameter name (one octet) and the length indicator (one octet) followed by the parameter contents.

(C) IP & UDP:

Internet Protocol and User Datagram Protocol essentially provide the connectionless mode network service as described earlier[8].

The Internet Protocol (IP) is the principal communications protocol used for relaying datagrams (packets) across an internetwork using the Internet Protocol Suite. Responsible for routing packets across network boundaries, it is the primary protocol that establishes the Internet. Historically, IP was the connectionless datagram service in the original Transmission Control Program introduced by Vint Cerf and Bob Kahn in 1974, the other being the connection-oriented Transmission Control Protocol (TCP)[4]. The Internet Protocol Suite is therefore often referred to as TCP/IP.

The first major version of IP, now referred to as Internet Protocol Version 4 (IPv4) is the dominant protocol of the Internet, although the successor, Internet Protocol Version 6 (IPv6) is in active, growing deployment worldwide.

Services provided by IP

The Internet Protocol defines an addressing methods and structures for datagram encapsulation. Addresses identify hosts and provide a logical location service. Each packet is tagged with a header that contains the meta-data for the purpose of delivery. This process of tagging is also called encapsulation. IP is a connectionless protocol and does not need circuit setup prior to transmission.

IP Reliability

As a consequence of this design, the Internet Protocol only provides best effort delivery and its service can also be characterized as unreliable. In network architectural language it is a connection-less protocol[11]. The lack of reliability allows any of the following fault events to occur:

- Data corruption
- Lost data packets
- Duplicate arrival
- Out-of-order packet delivery; meaning, if packet 'A' is sent before packet 'B', packet 'B' may arrive before packet 'A'. Since routing is dynamic and there is no memory in the network about the path of prior packets, it is possible that the first packet sent takes a longer path to its destination.

In addition to issues of reliability[9], this dynamic nature and the diversity of the Internet and its components provide no guarantee that any particular path is actually capable of, or suitable for, performing the data transmission requested, even if the path is available and reliable.

UDP

The User Datagram Protocol (UDP) is the TCP/IP connectionless transport protocol. Connectionless transport protocols are used for multimedia applications.Networking protocols are grouped by function into a protocol stack[5]. There are several transport layer protocols available.

Features & Functions of UDP

After a connection has been established, data integrity can be managed by sequencing data packets for the same session. Without establishing a connection, these data management functions are not possible. UDP merely sends out packets at one end and receives them at the other. Whether those packets are out of sequence or have damaged or lost data is not controlled.

The purpose of UDP is to offer a lightweight alternative to TCP. Where applications perform their own data integrity checks, or have alternative connection-establishing procedures, UDP is used. UDP became popular with multimedia applications like video streaming and Internet telephony, which have separate procedures for data integrity and session management.

IV. Future challenges

MANETs are probably to expand their applications in the future communication environments. The support of CLNS will thus be an important and desirable component of MANETs. Several important research issues and open questions need to be addressed to facilitate CLNS support in MANETs. Use of location, mobility, power consumption and route availability are some of the issues that are currently being examined and need further exploration. Other challenges and open issues include robustness and security, and support for multiple levels of services in CLNS routing schemes.

V. Conclusion

In this paper, we focused on the basic concepts in CLNS routing in MANETs and the various issues that are needed to be faced during the provision of CLNS. The through overview on various CLNS routing protocols have been made. We have summarized the classifications, features and functions of these protocols. There are still many issues and challenges which have not been considered. This will be subjected to further investigations.

References:

1. Kavita Taneja, Mobile Ad hoc Networks: Challenges and Future, COIT-2007, RIMT-IET, Mandi Gobindgarh. March, 2007

2. Nishu Garg**,** MANET Security Issues, IJCSNS, VOL.9 No.8, August 2009 – 241

3. Santhi.G, A SURVEY OF QoS ROUTING PROTOCOLS FOR MOBILE AD HOC NETWORKS, CONFERENCE 26.2.2010

4. Moukhtar A.Ali, A Survey of Multicast Routing Protocols for Ad-Hoc Wireless Networks, Minufiya Journal of Electronic Engineering Research (MJEER), Vol. 17, No. 2, July 2007.

5. H. Yang, Security in Mobile Ad Hoc Networks: Challenges and Solutions, IEEE Wireless Communications, Vol.11, Issue 1, pp. 38-47, 2004

6. Shino Sara Varghese, A Survey on Anonymous Routing Protocols in MANET, International Conference on Networking VLSI & Signal Processing ICNVS'10

7. Pradeep Rai Shubha Singh, A Review of 'MANET's Security Aspects and Challenges' IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010

8. G.Vijaya Kumar, Current Research Work on Routing Protocols for MANET: A Literature Survey, (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 706-713

9. Edward W. Page, Charles K. Watt, Automated Network Management for MANETs: Challenges and Opportunities, Electronic Systems Support, LLC.

10. Wikipedia, http://en.wikipedia.org/wiki/..

11. A. K. Dwivedi, Performance of Routing Protocols for Mobile Adhoc and Wireless Sensor Networks: A Comparative Study, International Journal of Recent Trends in Engineering, Vol 2, No. 4, November 2009.