SCTP, TCP-MH and DCCP Networking Protocols and its Comparison

Miral J Patel[1] Hasmukh P Koringa[2]
[1]Assistant Professor, EC dept., Government Engineering College Rajkot
[2]Assistant Professor, EC dept., Government Engineering College Rajkot

Abstract : TCP/IP protocols were designed at 1970s-1980s and during that time computer were single-homed. Nowadays there is more and more need for the mobility, so new protocols are needed for the mobility and multi homing. As we described in this paper that mobility and multi homing can be implemented at the transport layer by new various protocol like Stream Control Transmission Protocol(SCTP),TCP Multi Home Options(TCP-MH) and Datagram Congestion Control Protocol(DCCP).

IndexTerms - **DCCP, SCTP, TCPMH, UDP, Multihoming.**

I. INTRODUCTION

In telecommunication area the term mobility are used to denote the phenomenon where an entity moves while keeping its communication context active [1].We assumed that there are a number of mobile nodes that attach to a relatively fixed network. We assumed that network layer address prefixes are determined by the network. Network topology determines the routing related portion of the IP layer addresses. From this assumption it can be know that for the large network, it is important to keep the routing table sizes manageable for keeping the routing prefixes consistent with the network topology. All this addresses are globally routable.

As a consequences of these assumption, In a mobile network when nodes moves, its network layer address necessarily changes. As IP addresses of the host changes there should be possibility of sending new IP address to the other part of communication. Also communication should not be interrupt. Furthermore the IP address should be sent securely which can not lead unauthorized traffic and denial-of-service attacks. Mobility can be implemented in different layers of protocol stack. For example Mobile IP works in network layer[2]. For the transport layer there are few protocols which supports mobility like SCTP,TCP-MH,DCCP. The main advantage of choosing the transport layer for providing mobility is than the network layer remain untouched and still allow roaming between networks[2]. In MIP(Mobile IP) a special device is need to maintain states and location of the mobile host. Usually router is used for this purpose but it should maintain a table with host locations and states. Also all data is sent to home agent and home agent redirect packets to mobile node. This cause extra traffic and complexities. If mobility is implemented at the transport layer, location management is done at the ends and no any special devices are need. Multi homing is an ability for a single endpoint to support multiple IP address[2].

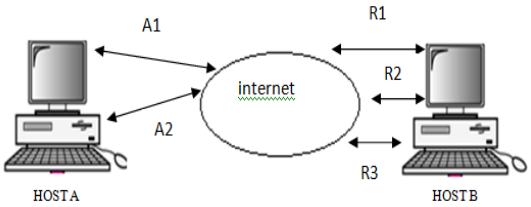

Fig 1. Multihoming

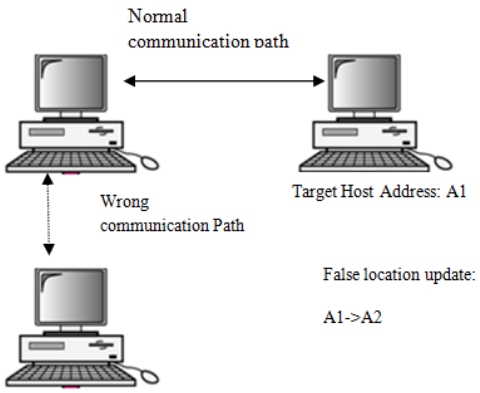

Fig 2.Stealing Attack

II. MULTIHOMING

Multi-homing refers to a situation where an end-point has several parallel communication paths that it can use [2]. Usually multihoming is a result of either the host having several network interfaces (end-host multi-homing) or due to a network between the host and the rest of the network having redundant paths. From our theoretical point of view, a multi homed endhost is a node that has two or more points-of-attachment with the rest of the network. This is illustrated in Figure 1.This situation can be characterized as the node being reachable through several topological paths; the node is simultaneously present at several topological locations. As a consequence, it also has several network layer addresses, each of which reflects one of the topological locations. In the general case, the addresses are completely independent of each other.

The main benefit of the multi homed systems are: when one path fails, another interface can be used for data delivery without interruption, that means "tolerance against physical network failures".

III. SECURITY ISSUES IN MOBILITY AND MULTIHOMIG

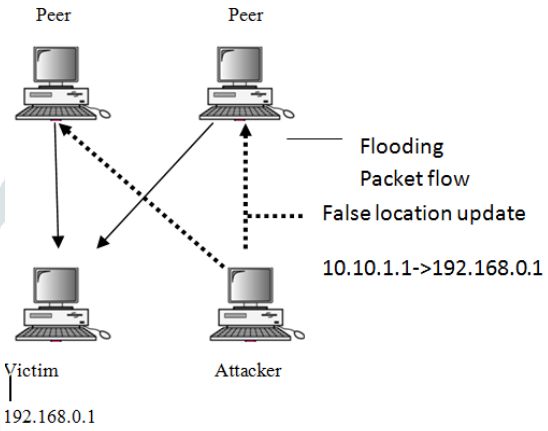

Fig 3. Flooding attack

There are two main security problems in Mobility and Multihoming - address stealing and address flooding [1]. Address stealing is an attack when attacker simulates a situation when endpoint thinks that attacker's address is new address of its peer described in Fig 2 . The address stealing attack is available when endpoint is not able to "verify that sender of the update was earlier at the target address" [1].The flooding attack is an attack when attacker sends location update to several peers. The new address is victim's address. Peers start to send unwanted traffic to victim Fig 3. This happens when endpoint is not able to verify that the host at new address is the host that sent location update.

IV TRANSPORT LAYER PROTOCOL UDP AND TCP

There are well known and widely used transport protocols (TCP and UDP). Why new protocols should be used? The main issue here is that old protocols do not support features like multihoming and mobility. But also there are some other problems.

UDP: UDP is unreliable connectionless message oriented transport protocol, so ordered delivery, loss recovery and duplicate detection are not supported by this protocol. UDP also lacks some other features such as congestion control and flow control algorithm. Also another problem is that firewalls and NAT's do not always pass UDP traffics.

TCP: TCP is reliable connection-oriented transport protocol that supports congestion control - so it is a very complex protocol and because of that too "heavy" for some applications (TCP headers are too long). As TCP provides ordered delivery, it can cause delays in delivery. In mobile world the main problem is security. TCP and UDP are not secure enough

V STREAM CONTROL TRANSMISSION PROTOCOL

SCTP combines the best features of UDP and TCP[3]. SCTP is reliable message-oriented transport protocol. SCTP supports multi-streaming and multi-homing, provides congestion control and flow control mechanism. SCTP is more secure than TCP, it is resistant to denial-of-service attacks. SCTP provides partially ordered data delivery (data is sequenced within one stream)[2].

A. Multi homing:

To setup the SCTP connection between two end,first INIT chunk (initiation chunk) is the sent by an end point to establish an association. The packet which carries this chunk cannot carry data chunk and control chunk. INIT chunk also contains different IP addresses of host if it is multi homed. INIT-ACK chunk communication peer sends all its IP addresses. Endpoint could have one IP address, then source address of the INIT chunk is considered as IP address of the peer. "Transmission path" set is formed based on the information in INIT and INIT-ACK chunks. "Transmission path" - is path from STCP instance to one of the IP address of the peer.

To monitor all transmission paths, host sends HEARTBEAT chunks over all paths that are not currently used in data communication. HEARTBEAT chunk should be acknowledged by HEARTBEAT-ACK chunk. There is a counter that counts unacknowledged HEARTBEAT chunks.

When it reaches the certain predefined number, destination address is considered to be unreachable. Another way of detecting unreachable destination is to count unacknowledged data chunks. For data packets transfer one transmission path is selected to be primary. If it fails, alternative transmission path will be used to continue communication.

Although SCTP supports multihoming, it does not support load sharing[2]. It can only select another Communication path if one is not available.

B. Mobility:

There is a SCTP extension for dynamic addition of IP address [9]. With this extension it is possible to add dynamically new peer IP addresses and create new transmission paths. So when a host is moving, it receives a new IP address and a new transmission path is created, therefore data transfer will not be interrupted. Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration Internet-draft [9] defines two new chunks that are needed to support mobility. These chunks are:

ASCONF - Address Configuration Change Chunk

ASCONF-ACK - Address Configuration Acknowledgment Chunk

Also six new parameters types are defined for adding and deleting new IP addresses, setting up primary address and some others. The most important types are:

0xC004 - Set Primary Address

0xC001 - Add IP Address

0xC002 - Delete IP Address

To add new IP address, the peer should send ASCONF chunk of 0xC001 type, which should be acknowledged by ASCONF-ACK chunk. This solution provides mobility of only one endpoint.

C. Other Features:

1) Multistreaming:

SCTP has several streams within a connection and messages are sequenced in the stream independent from other streams, so if message of one stream is lost, it does not affect to the delivery in the other streams. Consequently it is reducing the risk of blocking what happens with TCP as it has only one stream and in-order delivery feature.

2) Congestion Control:

Congestion happens when a router receives much more packets than it can forward and a big packet queue appears. Congestion control is process of detecting of congestion events and preventing sending packets to congested region, decreasing sending rate or taking other actions helping to resolve congestion. SCTP uses the same congestion control mechanism as TCP - rate-adaptive window-based congestion control scheme with small differences [10][11] .

3) Security:

SCTP has four-way handshake for connection establishing

1. Client (or active side) sends INIT chunk to Server

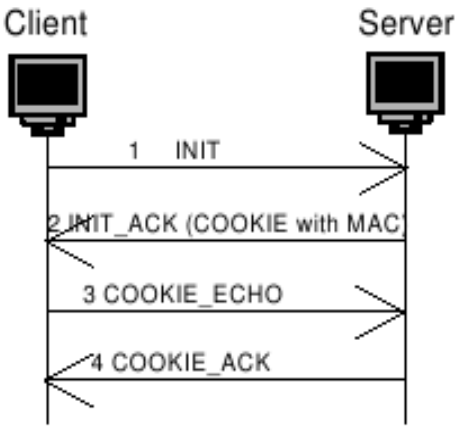

Fig 4: Four-Way Handshake for connection establishing in SCTP

2. Server replies with INIT-ACK chunk containing COOKIE with a Message Authentication Code (MAC). Cookie also contains transmission control block, cookie generation time, cookie expiration time.
3. Client sends back a copy of COOKIE in COOKIE-ECHO chunk.
4. Server calculates new MAC based on transmission control block from COOKIE-ECHO and compares it with MAC that it sent to client earlier and sends COOKIE- ACK chunk.

Protection against the flooding attack and the address stealing attack is done by sending MAC in INIT- ACK chunk and verifying it in COOKIE-ECHO. Addition and Deletion of IP Addresses using SCTP Dynamic Address Reconfigurations provide more opportunities for connection hijacking.

VI TCP MULTI HOME OPTIONS

There is an Internet-draft [8] proposing another way of solving multihoming problem. TCP-MH maintains access lines associated with different addresses in one TCP session and if one access line goes down, it can switch to other access line.

If host is able to use MH options it should send MH-permitted option during connection establishing (in SYN packet). If other side accepts it and after connection is established, the peers can start using MH options. Hosts should exchange their IP addresses using MH-Add-IPv4 or MH-Add-IPv6 options. After receiving MH-Add option endpoint should register new transmission paths based on the address mentioned in option. There are MH-Delete-IPv4 and MH-Delete-IPv6 options for deleting address, although due to security reasons endpoint should not delete path right away after receiving MH-Delete option. The following sequence describe the packets flow between endpoints.

1. Client (or active side) sends a SYN packet containing MH Permitted option.
2. Server replies with a SYN-ACK packet containing MH Permitted option.
3. Client sends ACK packet, now connection is established in client side.
4. Server receives ACK packet, now connection is established in server side also.
5. Now Client sends DATA with MH-Add-IPv4 option included. Option contains another IP address of client.
6. Server accepts MH-Add-IPv4 option and sends MH Ack option.
7. Client wants to add another IP address (IPv6) and sends DATA with MH-Add-IPv6 option included.
8. Server accepts MH-Add-IPv6 option and sends MHAck option.
9. After that peers communicate in normal mode.
10. If communication is lost, server switches to the other address.

TCP-MH does not support all forms of mobility,it is assume only the situation when host is non-mobile and has several IP addresses (multi-homed).

A. Security

TCP-MH does not provide any additional protection against connection hijacking, man-in-the-middle and other types of attacks. Regarding flooding attack TCP-MH options also does not add any improvement or degradation. For address stealing (or redirection attack) offer to use Return Routability Test [4].

VII DATAGRAM CONGESTION CONTROL PROTOCOL

DCCP protocol is one more transport protocol that should be used by applications that need flow-based semantics of TCP, but don't need "in-order delivery and reliability semantics" [6] and also for those that don't need multistreaming feature of SCTP. Among others DCCP has the following features:

- unreliable flow of datagrams, with acknowledgements
- reliable handshake for connection setup and teardown
- reliable negotiation of options [6].

A Mobility

DCCP provides primitive support for multi homing and mobility via a mechanism for transferring a connection endpoint from one address to another [6]. DCCP supports mobility of only one end point, the other one should remain stationary. Before the moving endpoint must notify other peer about it (using Mobility Capable Feature) and once it gets new IP address it must send DCCP-Move packet containing its new Address to stationary peer. Upon the receiving DCCP-Move packet stationary endpoint changes its connection state and starts using new address of moving peer.

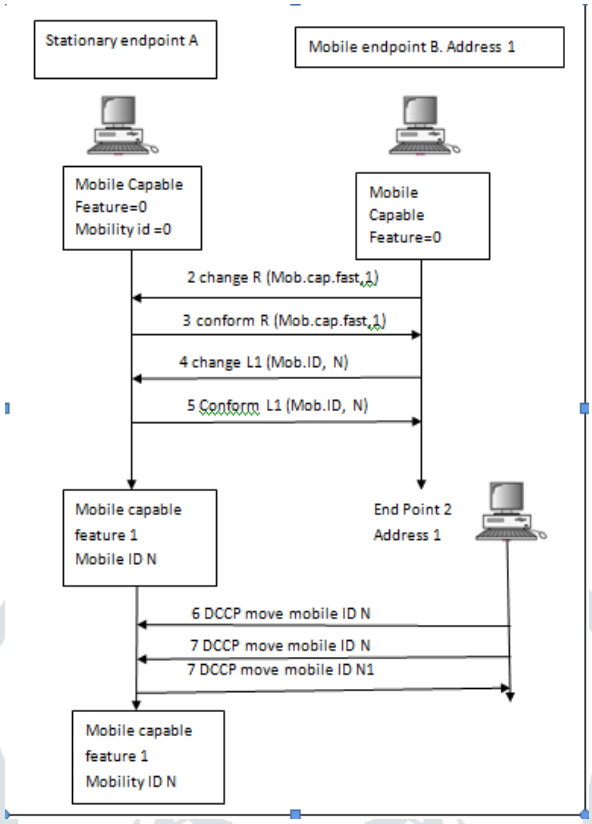

Fig 5 Packet Flow between End Points

The diagram on Fig.5 illustrates the packets flow between endpoints:
1. When communication starts Mobility Capable feature and Mobility ID have zero value in both endpoints.
2. Then mobile endpoint (B on diagram) sends "Change R" option with value "1" for Mobility Capable Feature. In DCCP "Change R" means that endpoint B wants negotiate some feature (in our case Mobility Capable Feature) for remote endpoint A. There is also "Change L" option for the situation when endpoint wants to negotiate feature for itself.
3. Endpoint A confirms feature value by sending "Conform R" option.
4. After that endpoint A sends a value for Mobility ID feature, that will be used by endpoints to identify connection. The value of Mobility ID feature is selected randomly for security reasons, also new value should be chosen after each move of mobile endpoint (can be also done more frequently). Zero value cannot be used in DCCP-Move packets, such packets should be discarded.
5. Endpoint B confirms value of Mobility ID feature by sending "Conform L" option.
6. After mobile endpoint (endpoint B on diagram) has moved or changed port, it sends DCCP-Move packet containing Mobility ID value that was chosen for connection identification.
7. Endpoint B should send DCCP-Move packets until it gets DCCP-Sync packet.
8. Endpoint A gets new address and port of B from the received DCCP-Move packet. Then Endpoint A sends DCCP-Sync message containing new value for Mobility ID feature and conforming B's move.

Stationary endpoint may refuse move by sending DCCP Reset option. The move can be refused because of for example address policy. If move is refused, the old address of B cannot be used; the address should be communicated again by DCCP-Move messages.

B. Security

The DCCP mobility mechanism, like DCCP in general, does not provide cryptographic security guarantees [6]. To perform address stealing attack attacker should know valid Mobility ID number. So attacker should although spoof network traffic or guess Mobility ID number. Mobile number length is increased from 64 bits to 128 bits. This will reduce the probability of guessing Mobility ID value.

VII COMPARISION OF PROTOCOLS

In the previous sections all three protocol are described. In this section all the protocols are compared not only the features of mobility and multihoming but also another features like reliability, order of delivery, security.

A. Mobility and Multihoming :

As said above, TCP-MH describes the usage of TCP-MH options only for multihoming, not mobility [4]. Other two protocols support mobility of only one endpoint.

B. Address Changing

In multihoming system when a communication link goes down how it can be automatically switch to the another address in SCTP, TCP-MH and DCCP is described here.

In SCTP if one link goes down, a new address will be selected automatically. SCTP host monitors all transmission paths by sending HEARTBEAT chunk. When counter counting unacknowledged data chunks reaches pre-defined number, alternative communication path will be selected automatically.

In TCP-MH changing of address is done in the same way - if data acknowledgement does not arrive, data is retransmitted. After several retransmissions (exact number should be predefined), endpoint automatically switches to the other address.

In DCCP automatic switching to the other path is not available as server gets new address of the endpoint only after move is completed and DCCP-Move packet is sent. Then server starts to send packets to new address and it does not have list of other client's addresses, even if movement is refused the using of old address should be communicated using DCCP-Move packet.

C. Middleboxes

Some hosts do not have public IP addresses, they have addresses that are unique only inside private network and NATs (Network Address Translators) are used for routing datagrams to and from such hosts. The problem appears when such endpoint adds its addresses into message body (e.g. into
INIT chunk in SCTP). As addresses are valid only inside private network, no any endpoints outside of that network can use those addresses. Now it is described how protocols manage with this issues and what other problems related to middleboxes can appear.
For SCTP choose the option between the following solutions to solve the problem described above:

- To use single-homed session and no any IP addresses should be included into INIT and INITACK chunks[12], then IP address of the message will be used as endpoint's address. In this case multihoming feature of SCTP is not used. For multihoming the NAT must have a public IP address for each represented internal IP address[12]. The host can preconfigure an IP address that the NAT can substitute, or, the NAT can have internal Application Layer Gateway (ALG) which will intelligently translate the IP addresses in the INIT and INIT ACK chunks [12].
- To use DNS to resolve the internal address. The host name should be put into INIT and INIT-ACK chunk and DNS should resolve it before association is setup.

In DCCP there is no such problem with NATs as in SCTP because endpoint's address is not included into packet data, and server receives new endpoint's address from the source address of DCCP-Move packet sent from new location. But there are other things that should be considered in networks with middleboxes (firewalls, NATs and others). DCCP developers list them in [6]:
In DCCP there is no such problem with NATs as in SCTP because endpoint's address is not included into packet data, and server receives new endpoint's address from the source address of DCCP-Move packet sent from new location.

First of all there is a Service Code field in DCCP-Request packet which tells to what protocol or application connection is established. It used instead of port numbers and "helps middleboxes identify the protocol used on a given connection" [6]. If endpoint tries to connect to unexpected service, middlebox can send DCCP-Reset packet with Reset Code 9 ("Bad Service Code") and close connection.

The other thing is that Source and Destination port numbers are located in the same places in the packet as in TCP and UDP, probably middleboxes can use this feature to make implementation simpler.

Middleboxes should not change packet's sequence numbers as DCCP-Move mobility mechanism can stop working. In TCP-MH the same problem can happen as in SCTP as IP addresses are included into MH-Add/Delete packets. The TCP-MH authors say that: "Though NAT/NAPT traversal feature is not included in the present TCP-MH Options specifications, this can be solved by enhancing return routability mechanism".

D. Other Features

1) Reliability SCTP and TCP-MH are reliable protocols. DCCP provides unreliable flow of datagrams, with acknowledgements [6].
2) Order of Delivery SCTP provides in-order delivery within one stream. Unordered delivery is also supported.TCP-MH has in-order delivery. DCCP provides unordered delivery.
3) Streaming As mentioned in earlier section SCTP has multiple streams and each stream consists of messages. TCP-MH has single byte stream. DCCP is packet stream protocol.
4) Congestion Control SCTP and TCP-MH provide almost the same congestion control mechanism as SCTP took over it from TCP with some slight changes. DCCP offers strong congestion control mechanism allowing to choose between different congestion control forms.
5) Connection Setup SCTP uses 4-way handshake for connection setup. TCP-MH and DCCP use 3-way handshake for connection setup.

E. Simplicity of Implementation:

TCP-MH is quite easy to implement as it is based on existing TCP protocol, but it is not very secure (especially without SYN-COOKIE algorithm) and does not describe supporting of mobile hosts. SCTP and DCCP are new protocols. SCTP is already proposed standard, others two are only Internet drafts

VIII CONCLUSION

Here we presented how mobility and multihoming could be providing using SCTP,TCP-MH and DCCP protocols and compared them. SCTP is more investigated protocol among these three. In TCP-MH, the mobile hosts maintaining mobility of both endpoint with middle boxes. In present state SCTP is most powerful which provide mobility and multi homing with MobileIP. As other features like Streaming, order of delivery, congestion control mechanisms and other features are different for SCTP,DCCP and TCP-MH,each of them should be considered as a application point of view.

REFERENCES

1. Pekka Nikander,Jukka Ylitalo,Jorma Wall. Integrating Security,Mobility, and Multi-homing in a HIP way.Network and Distributed System security symposium,2003.
2. R. Stewart, Q. Xie Motorola. Stream Transmission Control Protocol(SCTP), IETF RFC-2960,Network Working Group,October-2000.
3. Behrouz A. Forouzan,TCP/IP Protocol Suite,Second Edition.
4. Olga Antonova, Introduction and Comparison of SCTP, TCP-MH,DCCP protocols,HUT T-110.551 Seminar on Internetworking.
5. Yong-Jin Leeand M Atiquzzaman, HTTP Transfer Latency over SCTP and TCP in Slow Start Phase ,IEEE,2007.
6. E. Kohler M. Handley,S. Floyd,Datagram Congestion Control Protocol (DCCP),RFC-4340,IETF Networking Working Group,March-2006.
7. M. Allman,S Floyd,C Partridge,Increasing TCP's Initial Window.RFC 3390,IETF Networking Working Gropu,October 2002.
8. Arifumi Matsumoto,Masahiro Kozuka,Kenji Fujikawa,Yasuo Okabe. TCP Multi-Home option, Work in progress,IETF Internet-Draft,October-2003.
9. R. Stewart,M Ramalho,Q.xie,Stream Control Transimission Protocol (SCTP) Dynamic Address Reconfiguration, Work in Progress (IETF Internet-Draft),September 2003.
10. M. Allman,V. Paxson,W.Stevens,TCP Congestion Control,RFC 3390,IETF Network working Group,April 1999.
11. M. Allman, S.Floyd,C.Partridge.Increasing TCP's Initial Window,RFC 3390,IETF Network Working Group,October 2002.
12. L.Coene. Stream Transimission Protocol Applicability Statement,RFC 3257,IETF Network Working Group,April 2002.