RGPVNOTES.IN

Program : **B.Tech**

Subject Name: **Wireless and Mobile Computing**

Subject Code: **IT-602**

Semester: **6th**

Unit 4:

Mobile IP: A standard that allows users with mobile devices whose IP addresses are associated with one network to stay connected when moving to a network with a different IP address.
When a user leaves the network with which his device is associated (home network) and enters the domain of a foreign network, the foreign network uses the Mobile IP protocol to inform the home network of a care-of address to which all packets for the user's device should be sent.
Mobile IP is used in wireless WAN environments where users need to carry their mobile devices across multiple LANs with different IP addresses.
A common example to explain Mobile IP is, if someone moves his residence from one location to another. Person moves from Indore to Bhopal. Person drops off new mailing address to Bhopal post office. Bhopal post office notifies Indore post office of new mailing address. When Indore post office receives mail for person it knows to forward mail to person's Bhopal address

DHCP (Dynamic host configuration protocol)
The dynamic host configuration protocol) is used to simplify the installation and maintenance of networked computers. If a new computer is connected to a network, DHCP can provide it with all the necessary information for full system integration into the network, e.g., addresses of a DNS server and the default router, the subnet mask, the domain name, and an IP address. DHCP is based on a client/server model. DHCP clients send a request to a server (DHCPDISCOVER in the example) to which the server responds. A client sends requests using MAC broadcasts to reach all devices in the LAN. A DHCP relay might be needed to forward requests across inter-working units to a DHCP server. The dynamic host con figuration protocol is mainly used to simplify the installation and maintenance of networked computers. If a new computer is connected to a network, DHCP can provide it with all the necessary information for full system integration in to the network, e.g., addresses of a DNS server an d the default router, the subnet m ask, the domain n am e, an d an IP address. Providing an IP address, makes DHCP very attractive for mobile IP as a source of care-of-addresses.
DHCP is based on a client/ server model. DHCP clients send a request to a server (DHCPDISCOVER in the example) to which the server responds. A client sends requests u sin g MAC broadcasts to reach all devices in the LAN. A DHCP relay might be needed to forward requests across inter-working units to a DHCP server.)

Characteristics of Ad Hoc Networks
The MANET working group has defined some unique properties of ad hoc networks. The properties does not directly relate to performance.
In a manner, they affect performance, since they greatly affect on the design of ad hoc routing protocols. The following characteristics of Ad-hoc networks are defined:
1. Dynamic topologies
Nodes can move arbitrarily with respect to other nodes in the network.
2. Bandwidth-constrained
Nodes in an ad hoc network are mobile. Thus, they are using radio links that have far lower capacity than hardwired links could use.
3. Energy constrained operation
Mobile nodes are likely to rely on batteries. That is why the primary design criteria may sometimes be energy conservation.
4. Limited physical security
The radio networks are vulnerable to physical security threats compared to fixed networks. The possibility of eavesdropping, spoofing and DoS attacks is higher. Existing link security techniques can be applied. However, a single point failure in an ad hoc network is not as crucial as in more centralized networks.

Performance Issues in Ad Hoc Networks

To judge the merit of a routing protocol, one needs metrics which both qualitative and quantitative to measure its suitability and performance. These metrics should be independent of any given routing protocol.

Qualitative properties of MANET routing protocols:

- Distributed operation: This is an essential property, but it should be stated nonetheless.
- Loop-freedom: It is not required for certain quantitative measures (i.e. performance criteria), but generally desirable to avoid problems such as worst-case phenomena, e.g. a small fraction of packets spinning around in the network for arbitrary time periods. Ad hoc solutions such as TTL values can bound the problem, but a more structured and well-formed approach is generally desirable as it usually leads to better overall performance.
- Demand-based operation: Instead of assuming an uniform traffic distribution within the network (and maintaining routing between all nodes at all times), let the routing algorithm adapt to the traffic pattern on a demand or need basis. If this is done intelligently, it can utilize network energy and bandwidth resources more efficiently, at the cost of increased route discovery delay.
- Proactive operation: The flip-side of demand-based operation. In certain contexts, the additional latency demand-based operation incurs may be unacceptable. If bandwidth and energy resources permit, proactive operation is desirable in these contexts.
- Security: Without some form of network-level or link-layer security, a MANET routing protocol is vulnerable to many forms of attack. It may be relatively simple to snoop network traffic, replay transmissions, manipulate packet headers, and redirect routing messages, within a wireless network without appropriate security provisions. While these concerns exist within wired infrastructures and routing protocols as well, maintaining the "physical" security of the transmission media is harder in practice with MANETs. Sufficient security protection to prohibit disruption of modification of protocol operation is desired.
- Sleep period operation: As a result of energy conservation, or some other need to be inactive, nodes of a MANET may stop transmitting and/or receiving (even receiving requires power) for arbitrary time periods. A routing protocol should be able to accommodate such sleep periods without overly adverse consequences. This property may require close coupling with the link-layer protocol through a standardized interface.
- Unidirectional link support: Bidirectional links are typically assumed in the design of routing algorithms, and many algorithms are incapable of functioning properly over unidirectional links. Nevertheless, unidirectional links can and do occur in wireless networks. Oftentimes, a sufficient number of duplex links exist so that usage of unidirectional links is of limited added value.However, in situations where a pair of unidirectional links (in opposite directions) form the only bidirectional connection between two ad hoc regions, the ability to make use of them is valuable.
- End-to-end data throughput and delay: Statistical measures of data routing performance (e.g., means, variances, distributions) are important. These are the measures of a routing policy's effectiveness i.e.., how well it does its jobas measured from theexternal perspective of other policies that make use of routing.
- Route Acquisition Time: A particular form of external end-to-end delay measurementof particular concern with "on demand" routing algorithms which is the time required to establish route(s) when requested.
- Percentage Out-of-Order Delivery: An external measure of connectionless routing performance of particular interest to transport layer protocols such as TCP which prefer in-order delivery.
- Efficiency: If data routing effectiveness is the external measure of a policy's performance, efficiency is the internal measure of its effectiveness. To achieve a given level of data routing performance, two different policies can expend differing amounts of overhead, depending on their internal efficiency. If control and data traffic must share the same channel, and the channel's capacity is limited, then excessive control traffic often impacts data routing

performance. It is useful to track several ratios that illuminate the internal efficiency of a protocol in doing its job (there may be others that the authors have not considered).

- Average number of data bits transmitted/data bit delivered: This can be thought of as a measure of the bit efficiency of delivering data within the network. Indirectly, it also gives the average hop count taken by data packets.
- Average number of control bits transmitted/data bit delivered: This measures the bit efficiency of the protocol in expending control overhead to delivery data. Note that this should include not only the bits in the routing control packets, but also the bits in the header of the data packets. In other words, anything that is not data is control overhead, and should be counted in the control portion of the algorithm.
- Average number of control and data packets transmitted/data packet delivered: Rather than measuring pure algorithmic efficiency in terms of bit count, this measure tries to capture a protocol's channel access efficiency, as the cost of channel access is high in contention-based link layers .
- In networking context, the essential parameters that should be varied include:
- Network size: Measured in the number of nodes.
- Network connectivity: The average degree of a node (i.e. the average number of neighbors of a node).
- Topological rate of change: The speed with which a network's topology is changing
- Link capacity: Effective link speed measured in bits/second, after accounting for losses due tomultiple access, coding, framing, etc.
- Fraction of unidirectional links: How effectively does a protocol perform as a function of the presence of unidirectional links?
- Traffic patterns: How effective is a protocol in adapting to non-uniform or bursty traffic patterns?
- Mobility: When and under what circumstances, is temporal and spatial topological correlation relevant to the performance of a routing protocol?

Routing In Mobile Host

wireless networks with infrastructure support a base station always reaches all mobile nodes, this is not always the case in an ad-hoc network. A destination node might be out of range of a source node transmitting packets. Routing is needed to find a path between source and destination and to forward the packets appropriately. In wireless networks using an infrastructure, cells have been defined. Within a cell, the base station can reach all mobile nodes without routing via a broadcast. In the case of ad-hoc networks, each node must be able to forward data for other nodes.

These are the basic algorithms for routing in mobile host.

- Link state: In link-state, routing each router first obtains a view of the complete topology of the network with a cost for each link and then computes the shortest path to every other router by using, for instance, Dijkstra's algorithm.
- Distance vector: In distance vector, every node only monitors the cost of its outgoing links and periodically broadcasts an estimation of the shortest distance to every other node in the network. The receiving nodes then use this information to recalculate the routing tables.
- Source routing: In source, routing each packet carries the complete path it has to follow around the network, which requires great overhead if the route has many hops. Given that the routing decision is made at the source, it is easy to avoid routing loops.

Wireless Sensor Network

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. A WSN system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes. The selection of wireless protocol depends on the application requirements. Some of the available standards include 2.4

GHz radios based on either IEEE 802.15.4 or IEEE 802.11 (Wi-Fi) standards or proprietary radios, which are usually 900 MHz.

Transport Layer

Supporting mobility only on lower layers up to the network layer is not enough to provide mobility support for applications. Most applications rely on a transport layer, such as TCP (transmission control protocol) or UDP (user datagram protocol) in the case of the internet. Two functions of the transport layer in the internet. Two functions of the transport layer in the internet are check summing over user data and multiplexing/ de-multiplexing of data from/to applications.

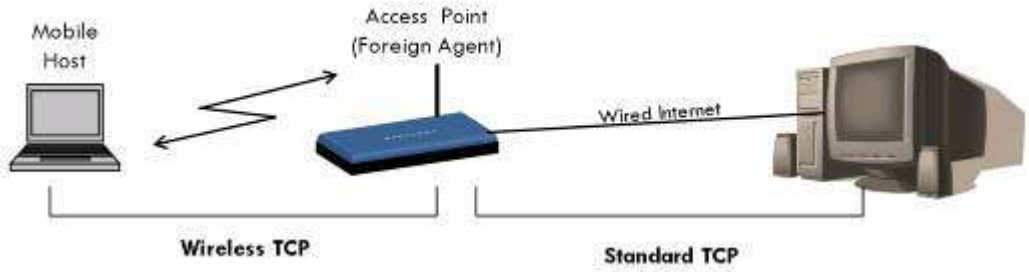

Figure 24: Indirect TCP segments a TCP connection into two parts

The above figure shows a mobile host connected via a wireless link to an access point (AP). Also access node is connected to the internet via the wired Internet. Standard TCP is used to connect to the AP from fixed computer. No computer over the internet recognizes any change to the TCP. The Access point acts as a proxy of mobile host and terminates the TCP connection. Therefore, the fixed computer now sees the AP as mobile host; on other hand, the mobile host sees AP as the fixed computer. In between the AP and the mobile host, a special TCP adapted to wireless links is used. A change is TCP is not needed as even as unchanged TCP produces the same round trip time. Such segmentation methods can be used is connection between mobile node and correspondent host when host is at the FA. Therefore, during handover, control transfers from one FA to another FA in the nearby cell.

Advantages of I-TCP:

- I-TCP does not require any changes in TCP protocol as used by the different hosts in network.
- Because of a strict partition between the two connections, transmission error on the wireless link will not propagate to the wired link. Therefore, flow will always be in a sequence.
- The delay between the FA and Mobile host is small and if optimized properly, precise time-outs can be used to carry out retransmission of lost packets.
- Different solutions can be implemented ad tested between the FA and mobile host without jeopardizing the stability of the internet.
- With two partitions, we can use a different transport layer protocol in the second half with the FA acting as a translator.

Disadvantages of I-TCP:

- The end-to-end connection for which TCP has been designed will fail if the Foreign Agent (FA) crashes.
- The foreign agent (FA) must be a trusted entity as the TCP connections end at this point.
- Increased handover may latency may be much more problematic. (During handover from old FA to new FA, some delay will occur. During this period, some extra data will come at old FA. This data also needs to be send)

Snoop-TCP

One of the main feature of I-TCP also goes on to become its major disadvantage i.e. segmentation of TCP.

To overcome it but also to provide enhanced feature a new TCP was designed which worked completely transparent and also left the TCP end-to-end connection intact. The new idea for making an enhancement is to buffer the data close to the mobile host to perform fast local retransmission in case of packet loss. A good place to carry out this enhancement is at the foreign agent (FA).

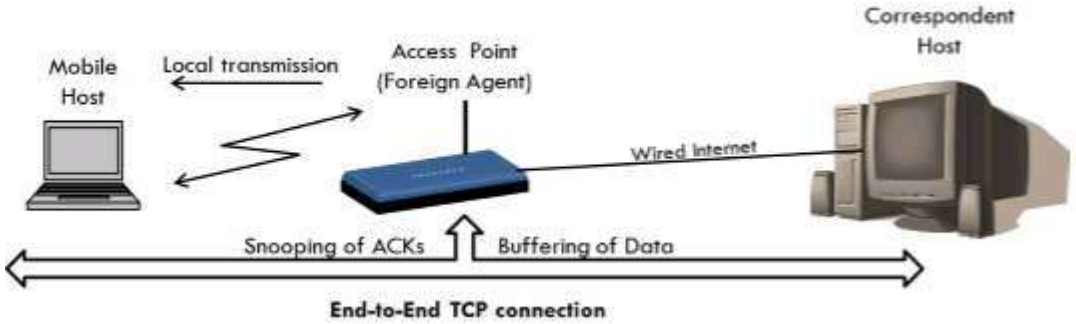

Figure 25: Snooping TCP as a transparent TCP extension

Method for Snoop-TCP

The foreign agent instead of terminating all packet with destination mobile host, it buffers (i.e. temporarily stores all these packets). It also 'snoops' each packet flowing in both the directions for reading acknowledgements. Buffering towards the mobile host is carried out so that a retransmission can be done in case of missing acknowledgements. The FA buffers every packet until an acknowledgement is received from the mobile host. If the foreign agent does not receive an acknowledgement within the stipulated time, the packet or the acknowledgement has been lost. In such a situation, the FA can directly retransmit the packet without waiting for the correspondent host.

Advantages of Snoop-TCP:

- The original TCP sematic i.e. end-to-end connection is preserved.
- The correspondent node need not be changed as all the new enhancements are made in the FA.
- During handover form on cell to another, there is no need to transfer the previous incoming data (as in I-TCP).
- In handover, the next foreign Agent (FA) need not use the same enhancements used here i.e. follow Snoop-TCP method.

Disadvantages of Snoop-TCP:

- If any encryption is applied at both ends, the snooping and buffering process would be a waste of time as no data can be read by FA.
- Does not fully isolate wireless link error from the fixed network (e.g. problems like congestion and interference may cause a delay in retransmission).
- The Mobile host needs to be modified to handle the NACK signals (No Acknowledgement) for reverse traffic (i.e. from MH to Sender)

Mobile TCP:

The M-TCP splits up the connection into two parts:
An unmodified TCP is used on the Standard host-Supervisory Host section
An optimized TCP is used on the Supervisory Host- Mobile Host section.
The Supervisory Host (SH) adorns the same role as the proxy (Foreign Agent) in I-TCP. The SH is responsible for exchanging data to both the Standard host and the Mobile host.
Here in this approach, we assume that the error bit rate is less as compared to other wireless links. So if any packet is lost, the retransmission has to occur from the original sender and not by the SH. (This also maintains the end-to-end TCP semantic). The SH monitors the ACKs (ACK means acknowledgement) being sent by the MH. If for a long period ACKs have not been received, then the SH assumes that the MH has been disconnected (maybe due to failure or moved out of range, etc...). If so the SH chokes the sender by setting its window size to 0. Because of this the sender goes into persistent mode i.e. the sender's state will not change no matter how long the receiver is disconnected.

This means that the sender will not try to retransmit the data. Now when the SH detects a connectivity established again with the MH (the old SH or new SH if handover), the window of the sender is restored to original value.

Advantages:

- Maintains the TCP end-to-end semantics. (No failed packet retransmission is done by the SH. All job handled by original sender)
- Does not require the change in the sender's TCP.
- If MH disconnected, it doesn't waste time in useless transmissions and shrinks the window size to 0.
- No need to send old buffer data to new SH in case of handover (as in I-TCP).

Disadvantages:

- M-TCP assumes low bit error which is not always true. So, any packet loss due to bit-errors occurring, then its propagated to the sender.
- Modifications are required for the MH protocol software.

Transmission/time-out freezing

In some cases mobile hosts can be disconnected for a longer time therefore no packet exchange possible, e.g., in a tunnel, disconnection due to overloaded cells or mux with higher priority traffic TCP disconnects after time-out completely called freezing.

TCP freezing

MAC layer is often able to detect interruption in advance and MAC can inform TCP layer of upcoming loss of connection then TCP stops sending, but does now not assume a congested link after that MAC layer signals again if reconnected

Advantage

This scheme is independent of data

Disadvantage

TCP on mobile host has to be changed, this mechanism depends on MAC layer

Selective retransmission

TCP acknowledgements are often cumulative. ACK n acknowledges correct and in-sequence receipt of packets up to n and if single packets are missing quite often a whole packet sequence beginning at the gap has to be retransmitted (go-back-n) thus wasting bandwidth

Selective retransmission gives a solution

The RFC2018 allows for acknowledgements of single packets, not only acknowledgements of in-sequence packet streams without gaps and now sender can now retransmit only the missing packets

Advantage

It provides much higher efficiency

Disadvantage

It is very complex

Transaction oriented TCP

TCP has the folowing phases

For connection setup, data transmission, connection release the TCP uses 3-way-handshake therefore needs 3 packets for setup and release, respectively thus, even short messages need a minimum of 7 packets, it results in overhead.

Transaction oriented TCP

The RFC1644, T-TCP, describes a TCP version to avoid this overhead In T-TCP the connection setup, data transfer and connection release can be combined therefore it requires only 2 or 3 packets are needed

Advantage

It is highly efficient

Disadvantage

- It requires changed TCP
- In T-TCP mobility not longer transparent

The following shows the comparison of different approaches for a "mobile" TCP

Approach	Mechanism	Advantages	Disadvantages
Indirect TCP	splits TCP connection into two connections	isolation of wireless link, simple	loss of TCP semantics, higher latency at handover
Snooping TCP	"snoops" data and acknowledgements, local retransmission	transparent for end-to-end connection, MAC integration possible	problematic with encryption, bad isolation of wireless link
M-TCP	splits TCP connection, chokes sender via window size	Maintains end-to-end semantics, handles long term and frequent disconnections	Bad isolation of wireless link, processing overhead due to bandwidth management
Fast retransmit/ fast recovery	avoids slow-start after roaming	simple and efficient	mixed layers, not transparent
Transmission/ time-out freezing	freezes TCP state at disconnect, resumes after reconnection	independent of content or encryption, works for longer interrupts	changes in TCP required, MAC dependant
Selective retransmission	retransmit only lost data	very efficient	slightly more complex receiver software, more buffer needed
Transaction oriented TCP	combine connection setup/release and data transmission	Efficient for certain applications	changes in TCP required, not transparent

Table 7: comparison of different approaches for a "mobile" TCP

Introduction to WAP

WAP stands for Wireless Application Protocol and it is a worldwide standard for providing Internet communications and advanced telephony services on digital mobile phones, pagers, personal digital assistants, and other wireless terminals

- Wireless: Lacking or not requiring a wire or wires pertaining to radio transmission.
- Application: A computer program or piece of computer software that is designed to do a specific task.
- Protocol: A set of technical rules about how information should be transmitted and received using computers.

WAP is the set of rules governing the transmission and reception of data by computer applications on or via wireless devices like mobile phones. WAP allows wireless devices to view specifically designed pages from the Internet using only plain text and very simple black-and-white pictures.

WAP is a standardized technology for cross-platform, distributed computing very similar to the Internet's combination of Hypertext Markup Language (HTML) and Hypertext Transfer Protocol (HTTP), except that it is optimized for:

- low-display capability
- low-memory
- low-bandwidth devices, such as personal digital assistants (PDAs), wireless phones, and pagers.\

WAP specifies architecture based on layers that follows the OSI model fairly closely. The WAP model, or stack as it is commonly known, is illustrated below

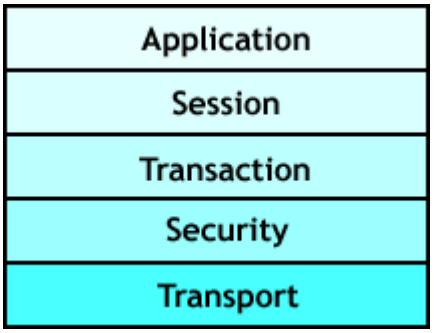

Figure 26: WAP layered architecture

Application Layer

WAP's application layer is the Wireless Application Environment (WAE). WAE directly supports WAP application development with Wireless Markup Language (WML) instead of HTML and WMLScript instead of JavaScript. WAE also includes the Wireless Telephony Application Interface (WTAI, or WTA for short) that provides a programming interface to telephones for initiating calls, sending text messages, and other networking capability.

Session Layer

WAP's session layer is the Wireless Session Protocol (WSP). WSP is the equivalent to HTTP for WAP browsers. WAP involves browsers and servers just like the Web, but HTTP was not a practical choice for WAP because of its relative inefficiency on the wire. WSP conserves precious bandwidth on wireless links; in particular, WSP works with relatively compact binary data where HTTP works mainly with text data.

Transaction, Security, and Transport Layers

There are three protocols in WAP:

- Wireless Transaction Protocol (WTP)
- Wireless Transaction Layer Security (WTLS)
- Wireless Datagram Protocol (WDP)

WTP provides transaction-level services for both reliable and unreliable transports. It prevents duplicate copies of packets from being received by a destination, and it supports retransmission, if necessary, in cases where packets are dropped. In this respect, WTP is analogous to TCP. However, WTP also differs from TCP. WTP is essentially a pared-down TCP that squeezes some extra performance from the network.

WTLS provides authentication and encryption functionality analogous to Secure Sockets Layer (SSL) in Web networking. Like SSL, WTLS is optional and used only when the content server requires it.

WDP implements an abstraction layer to lower-level network protocols; it performs functions similar to UDP. WDP is the bottom layer of the WAP stack, but it does not implement physical or data link capability. To build a complete network service, the WAP stack must be implemented on some low-level legacy interface not technically part of the model. These interfaces, called bearer services or bearers, can be IP-based or non-IP based.

RGPVNOTES.IN

We hope you find these notes useful.

You can get previous year question papers at https://qp.rgpvnotes.in .

If you have any queries or you want to submit your study notes please write us at rgpvnotes.in@gmail.com

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in