Information Technology

Mobile Computing

Module: Snooping TCP

Learning Objective

- Understand need for optimized TCP in wireless networks
- Understand limitations of I-TCP
- Snooping protocol and its design in order to remove limitations of I-TCP
- Advantages and limitations of Snooping TCP

Introduction

The wireless communication is characterized by followingproperties:

1) Limited bandwidth
2) High latency rate
3) High bit error rate
4) Temporary disconnections
5) User Mobility and handoffs

All these factors affect the protocols for wireless communication. There have been attempts to modify the existing protocols in wired networks to comply with wireless environment. Like MACA for data link layer to replace CSMA/CD and Mobile IP as a substitute for IP in network layer. To support mobility, protocols in higher layers like TCP in transport layer also needs to be modified or some alternate protocols need to be proposed. In this module we will understand the performance of transport layer protocols in wireless communication scenario and study a protocol called Snooping TCP which is adaptedas per characteristics of wireless communications.

Need for optimized transport layer protocols

Standard TCP is a well-established transport layer protocol for wired links and fixed hosts. TCP provides reliable transmission by retransmission on time-out and handles end to end delays and packet losses efficiently. Assuming that thebit error rate over wired links is low, TCP assumes congestion to be the only cause of packet loss and reacts by reducing the window size before retransmissionof packets. This mechanism is known as **slow start**. The scheme works well in wired networks but in wireless networks, high errorrate of links, intermittent connectivity, improper hand offs are the other reasons for packet loss. In such a situation, if TCP goes into slow-start, it will result in reduction of bandwidth utilization, poor throughput and high delay hence the performance will be degraded. To handle this, lots of research has been going on to improve the performance of TCP over wireless links. All of the researches believe that TCP is the only appropriate model for wireless networks since many network applications are built on top of TCP therefore it is not possible to change the entire protocol. Hence it is necessary to propose optimized versions of standard TCP maintaining its performance. The optimized versions should not tend to make changes on fixed hosts which mean that it should not be aware of the errors on the wireless link.Many TCP protocols for wireless networks have been proposed, one of them is I-TCP. In this module, the design and functioning of snoop protocol and how it overcomes the limitations of I-TCP has been described.

Limitation of I-TCP

In I-TCP, the foreign agent or router or the base station splits the TCP connection into 2 parts. Between fixed computer and base station, standard TCP is used and between base station and wireless host,optimized protocol specific to wireless links is used. The limitations of this scheme are:

- **Loss of end-to-end semantics of TCP**: The acknowledgements are given by the foreign agent as soon as it receives the packets .The acknowledgements are received by the senderwhich makes it understand that the packet has been received even before the receiver gets it.
- **Centralized Proxy**: The base station or the foreign agent acts as a proxy forwarding the packets in both the directions therefore whole scheme fails if foreign agent is crashed
- **Security Threat:**The foreign agent acting as a proxy receives all the packets so it should be a trusted entity

Snooping TCP

The Snooping TCP was proposed by Balakrishnaet. al. in 1995.This approach is designed in such a way so as to overcome the end-to-end semantics loss in I-TCP. Snooping TCP offers a transparent design which leave the end-end connection of TCP intact. Basic idea is to buffer packets close to mobile host and perform local retransmission in case of packet loss.The scheme works as follows:

- Foreign agent buffers the packet until it receives acknowledgement from the mobile host.
- Foreign agent snoops the packet flow and acknowledgement in both the directions.

- If the foreign agent does not receive acknowledgement from the mobile host or receives duplicate acknowledgements, it assumes either the packet or the acknowledgement is lost
- Foreign agent directly retransmits the packet from its buffer.
- Foreign agent also maintains its own timer for retransmission of buffered packet in case it is lost on wireless link
- If the foreign agent crashes, a timeout at fixed host will work and cause retransmissionand the scheme falls to standard TCP.The foreign agent in contrast to forwarding the packets as in case of I-TCP, just buffers the packets intended for mobile host
- To maintain transparency foreign agent does not acknowledge the packet to the fixed host(END-TO-END Semantics is maintained)

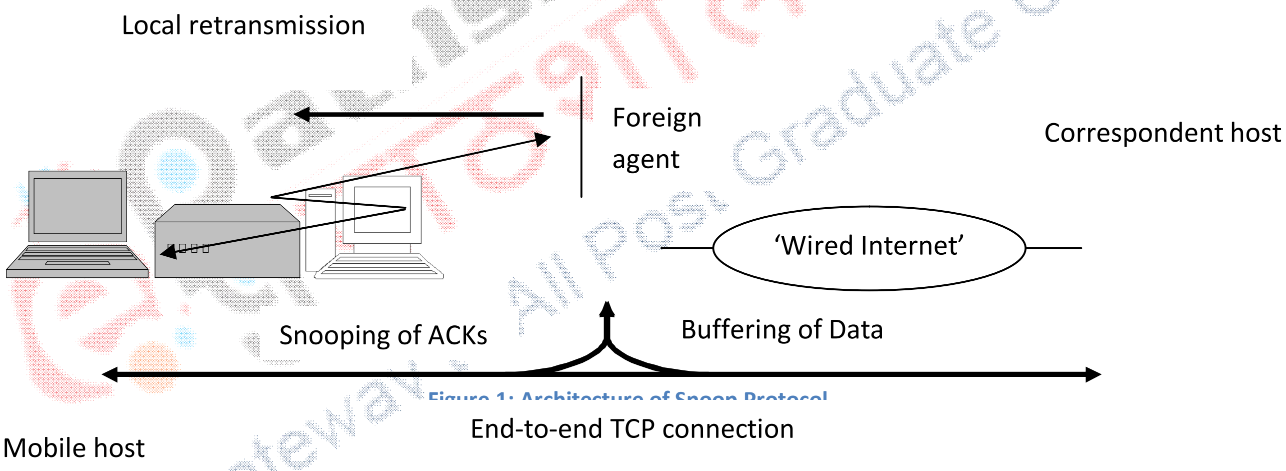

Figure 1: Architecture of Snoop Protocol

Design of Snoop Protocol

The snoop protocol is implemented as follows:

- The TCP connection on the wired link between foreign agent and fixed host is standard TCP
- The TCP connection on the wireless link between foreign agent and mobile host is optimized TCP
- The foreign agent snoops the flow of packets and acknowledgements and caches the packets towards the mobile host

- The scheme suggests some changes on the routing code of the foreign agent when there is packet flow from fixed host to the mobile host
- For data transfer from mobile host to fixed host additional mechanisms at mobile hosts are required
- No changes are required at the fixed host

Additional mechanisms required to implement Snoop Protocol

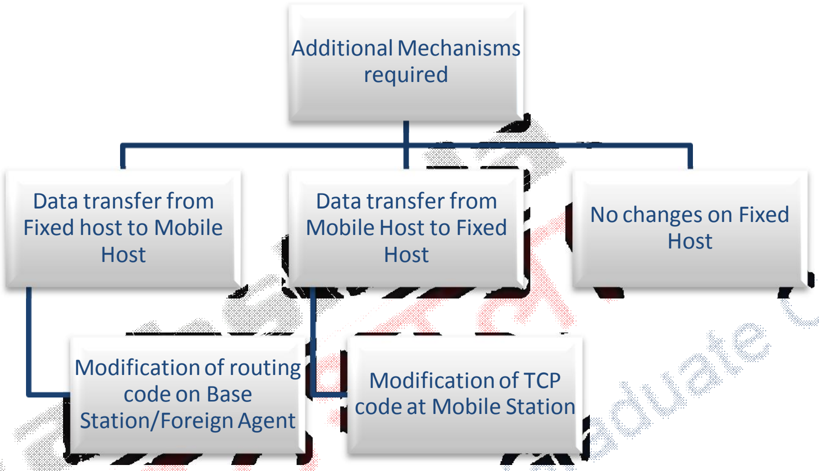
Additional Mechanisms required
Data transfer from Fixed host to Mobile Host
Data transfer from Mobile Host to Fixed Host
No changes on Fixed Host
Modification of routing code on Base Station/Foreign Agent
Modification of TCP code at Mobile Station

Figure 2: Additional mechanisms required by Snoop Module

Data transfer from fixed host to mobile host

The change in the routing code of (BS)is additionof snoopingmodule. The function of module is to monitor the packets passing through the connection in both the direction.The snoop module caches TCP packets sent from fixed host (FH) that are not acknowledged by mobile host (MH)i.e. the packets are cached until they are acknowledged by mobile host. The snooping module keeps track of the entire acknowledgement sent from the mobile host. If a packet loss is detected by the Base Station (BS) either by arrivals of duplicate acknowledgement or by local timeout,snoop module retransmits the lost packets to mobile host(MH) which has been cached.

The snoop module has twoproceduresSnoopData and Snoop acknowledge. Snoop data process and cache packets towardsmobile host and Snoop acknowledge process acknowledgements coming from mobile host (MH) and drive local retransmission.

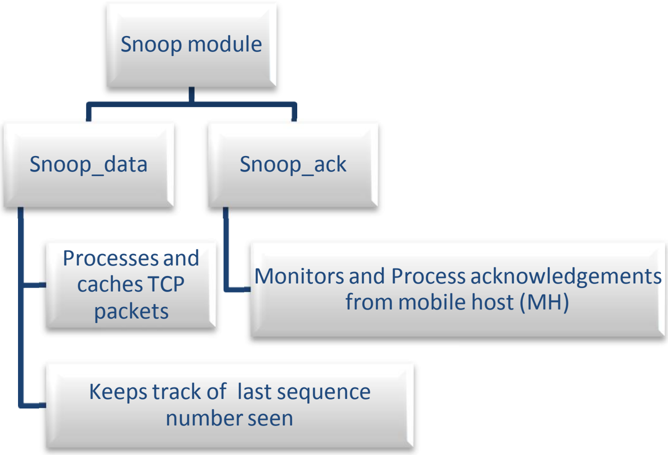
Snoop module
Snoop_data
Snoop_ack
Processes and caches TCP packets
Monitors and Process acknowledgements from mobile host (MH)
Keeps track of last sequence number seen

Figure 3: the procedures of Snoop Module

Snoop data (): This module processes packets arriving from the fixed host. A TCP packet is uniquely identified by the sequence number of its first byte of data and size. The BS/AP keeps track of past sequence number seen for connection. Appropriate actions are performed by this module depending on sequence number of the packet and status of the cache. The packets arriving at the Base Station (BS) from the fixed computer are one of the three types mentioned below:

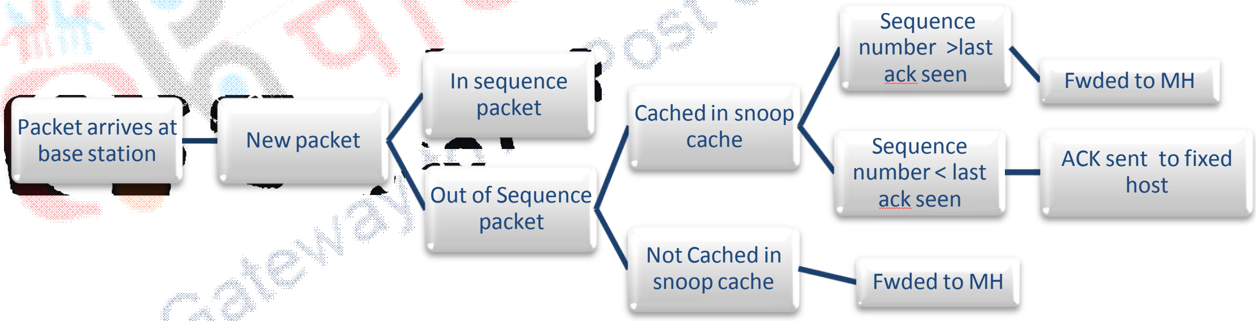
Packet arrives at base station
New packet
In sequence packet
Out of Sequence packet
Cached in snoop cache
Not Cached in snoop cache
Sequence number >last ack seen
Sequence number < last ack seen
Fwded to MH
ACK sent to fixed host
Fwded to MH

Figure 4: Types of packets arriving at base station and action taken accordingly

In sequence Packet: The packet arrivesin the normal in sequence. The packet is added to snoop cache and forwarded to the mobile host (MH). A time stamp is placed on one packet per transmitted window in order to estimate the round trip time of wireless link.

Out of sequence Packet: A packet whose sequence number is out-of-order. There is possibility that this packet has been cached or not been cached.

Out of sequence Packet that has been cached: This happens when dropped packet causes timeouts at the sender. Packet after TCP sender fast retransmission arrives at the sender. The base Station (BS) now sees whether this packet is greater or less than the last acknowledged packet and different actions are taken accordingly.

- If the sequence number is greater than last acknowledged packet it would mean that the packet didn't reach the mobile host (MH) earlier and hence it is forwarded.
- If the sequence number is less than the previously acknowledge, it is assumed that packet is received by mobile host (MH).One thing to do is to discard the packet but it is not a wise thing to do because the acknowledgement from mobile host (MH) to fixed host (FH) might have lost due to congestion a TCP acknowledgement correspondence to last acknowledgement seen at base station (BS) is generated with source address and port number of the mobile and sent to fixed host (FH).

Out of sequence Packet that has NOT been cached: This case happens when packet was lost due to congestion or it is delivered out of order by the network. This packet is forwarded to the mobile host and on additional information regarding packet retransmitted by sender is associated at base station (BS).

Snoop Acknowledge (): This module monitors and processes the acknowledgement sent by mobile host (MH) and different types of actions are performed depending on type and number of acknowledgements received.

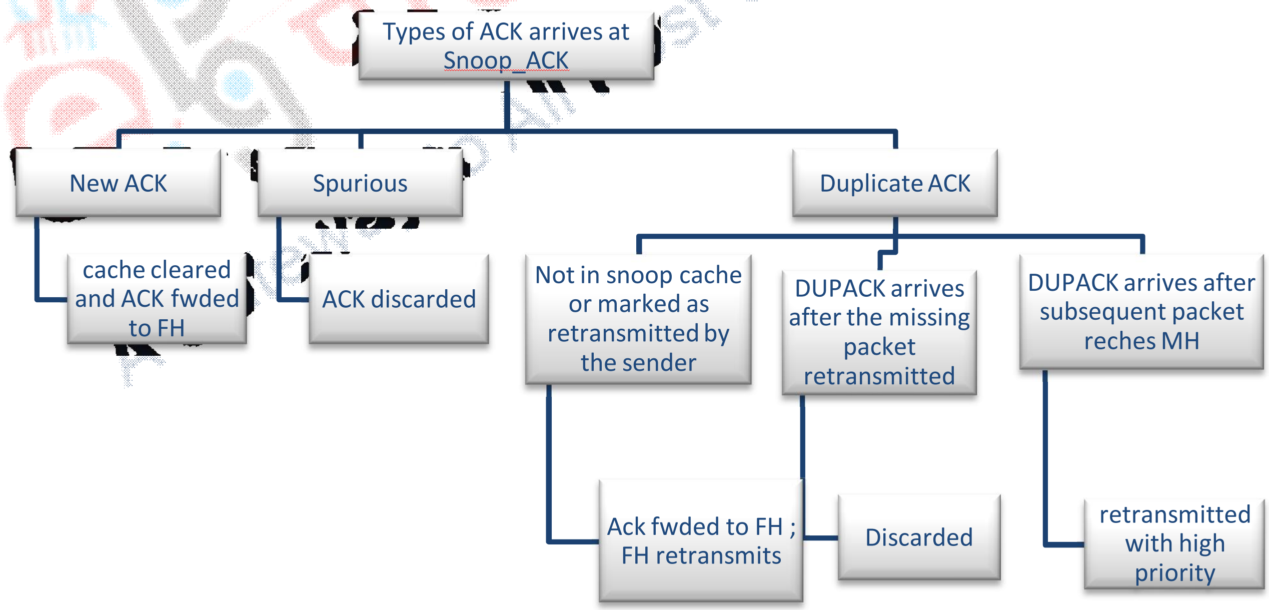
Types of ACK arrives at Snoop_ACK
New ACK
Spurious
Duplicate ACK
cache cleared and ACK fwded to FH
ACK discarded
Not in snoop cache or marked as retransmitted by the sender
DUPACK arrives after the missing packet retransmitted
DUPACK arrives after subsequent packet reches MH
Ack fwded to FH ; FH retransmits
Discarded
retransmitted with high priority

Figure 5: Types of acknowledgements received and action taken

- **New acknowledgement**: Indicates that the packet is received at the mobiles host indicating the link is error free. The packet sequence number arriving at the receiver will be increased.

On receiving this acknowledgement, the snoop cache is cleaned and all the packets which are acknowledged are freed. The acknowledge packet is forwarded to the fixed host.

- **Spurious acknowledgement**:This is anacknowledgement forthe packet with sequence number less than the last seen acknowledgement. This acknowledgement is discarded.
- **Duplicate acknowledge:**The acknowledgement is same as the previous one receipt packet indicates that the next packet in sequence with the duplicate acknowledge has not seen received by the mobile host (HS). But some subsequent packets might have been received because a duplicate acknowledgement is generated for every TCP segment received out of sequence. When the base host (BH) of foreign agent (FA) notices duplicate acknowledge it takes action depending on the snoop cache state and type of acknowledgement.
    - If the packet is not in cache the duplicate acknowledgement is forwarded to the fixed host (FH) because now it should be resent from the fixed computers.
    - If the packet is marked as sender retransmitted packet, then also it is forwarded to the fixed host (FH) because on number of duplicate acknowledgements it receives when it retransmits a packet.
    - When the missing packet is already being retransmitted when the first DUPLICATE ACKNOWLEDGE arrived so this is discarded.
    - When the first duplicate acknowledgement of the packet arrives after the subsequent packet in the stream reaches mobile host (MH). Now for every successive packet in the window, a duplicate acknowledgement should be generated so to minimize the number of duplicate acknowledgements the lost packet should be transmitted as soon as possible. This packet should be retransmitted with a higher priority than other packets. To implement this, two queues of retransmitting packets are maintained one for high priority packets and other for normal packets Retransmission using fast queue also improves the performance. The approachof maintaining two queues is helpful when there are low or medium error rates because when the error rate is high; all the packets are required to be retransmitted again therefore there is no need to maintain 2 queues. But when bit rates are lower or medium, fast queue enables the lost packets to be retransmitted soon hence increasing the performance.

Data Transfer from a mobile host

The proposed protocol suggests a modification at TCP code at the mobile host also. This is necessary because the modification made at the base because when the transfer is from mobile host to the fixed host (FH) and a packet is lost, it cannot be found whether it is on wireless link or due to congestion.In the proposed protocol, track of lost packets is kept as well as NACKS are generated for these lost packets back to the mobile. This is helpful when there are several packet losses in a single transmission window which may be due to high interference or when strength or quality of signal is low. On receiving the NACK, the mobile host retransmits the missing packet immediately. This retransmitted packet would arrive out of sequence at the fixed host hence they should be rerecorded at the fixed host.

Handoffs

In case of handoffs, the new base station (BS) should perform the task of snooping so the new base station (BS) should prepare their snoop cache for the mobile host. This is the transition state called “buffering” state and the base station (BS) cannot snoop onto the acknowledgements. As soon as hand off occurs, snoop cache is synchronized to the new base station (BS) and the process continues.

Advantages

1. **End-to-end semantics is preserved**: The FA does not acknowledge the packet. Even if the foreign agent (FA) or base station (BS) crashes, the approach automatically fall into standard TCP
2. **No Modifications at Fixed Host**:The fixed computer TCP does not require any modifications. Most of the modifications are at foreign agent (FA) / base station (BS) and some on mobile host.
3. **No packet loss during handovers**: In case of handovers, if there is some data not transferred to the new foreign agent, there will be a time-out at fixed host triggering retransmission of packet, following mobile IP, to a new COA.If the new base station does not comply with scheme, approach will fall back to standard TCP.

Disadvantages

1. If the packet is lost or delayed during the retransmission from buffer of the foreign agent, due to error on wireless link, time-out will occur at fixed host (FH).Therefore problems on wireless link are not isolated.
2. The wireless links offers very high delay as compared to wired link almost by a factor of 10. In this case the timers in foreign agent (FA) and fixed host are almost equal and approach is almost ineffective.
3. Use of NAK between foreign agent and mobile host assumes additional mechanism on the mobile host.
4. Snooping and buffering won’t be applicable if there is end-end encryption between fixed host and mobile host. As per RFC 2406 in IP encapsulation security payload TCP protocol header are encrypted and the snooping on sequence numbers won’t be possible.
5. Retransmission from foreign agent (FA)/ base station (BS) may not work because many schemes prevent replay attacks and retransmission may be interpreted as replay.

Therefore snooping protocol is used only when encryption is used above transport layers.

6. Architecture of snooping protocol to overcome limitations of I- TCP.
7. Functioning Snoop-module at base station (BS)/ foreign agent (FA).