Technische Universität München
Lehrstuhl Informatik VIII
Prof. Dr.-Ing. Georg Carle
Christian Grothoff, Ph.D.
Stephan M. Günther, M.Sc.

Master Course Computer Networks

Homework 5
(submission until January 21 into INBOX located in front of 03.05.052)

Note: Subproblems marked by * can be solved without preceding results.

Middleboxes Processing of packets

Given a network protected by a stateful firewall with two network interfaces, an internal and an external one. The firewall operates between two zones: green (the internal one) and red (the external one). It should allow incoming packets that are related to an already established state, as well as incoming packets that match user-defined policies. If packets are not related to an established state and if no policy exists, packets should be dropped.

a)* What means the termin *stateful* firewall?

Decisions made by the firewall not only depend on the current packet but also on traffic history.

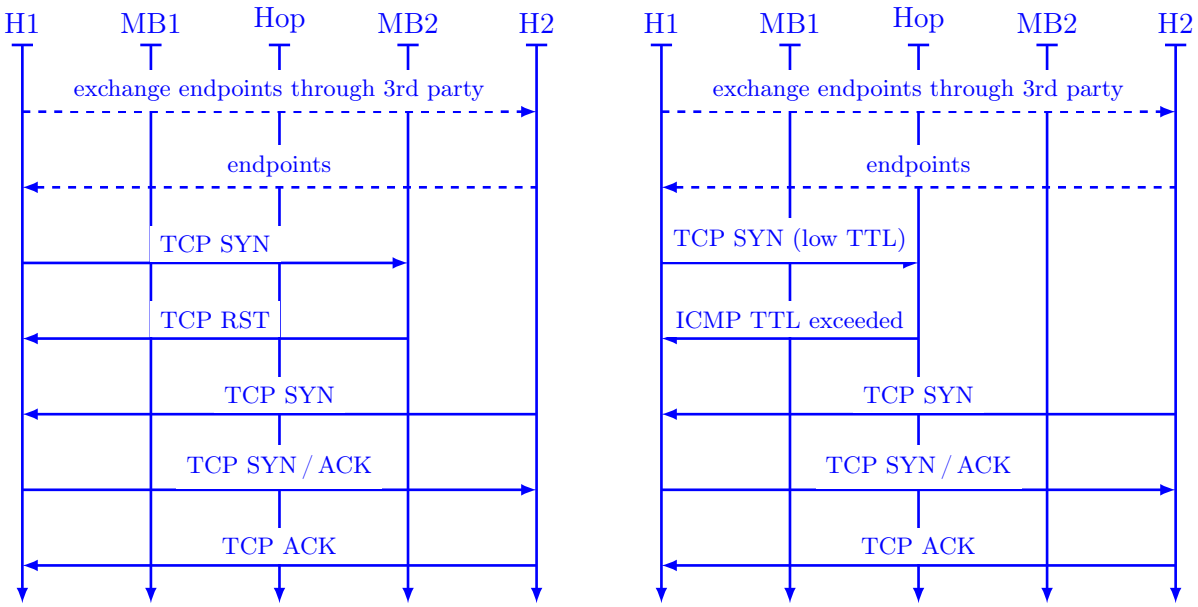
b) Describe the operation for incoming packets of a stateful firewall using the Processing Model as presented in the lecture.

Path	Event	Processing
In	`E(A,red,p)`	`receive(p) && TE(getState,p)`
Proc	`E(getState)`	`TE(DB.(RELATED or UNKNOWN))`
	`E(Sstate.RELATED)`	`TE(FW,green,p)`
	`E(State.UNKNOWN)`	`TE(getPolicy,p)`
	`E(getPolicy)`	`TE(policy.(allow or deny))`
	`E(policy.allow)`	`TE(FW,green,p)`
	`E(policy.deny)`	`DROP(p)`
Output	`E(FW, green)`	`send(p)`

Figure 1 shows two variants of TCP hole punching.

c)* Explain both variants and think of possible scenarios that might happen depending on the behavior of the middleboxes involved, e.g. packet 1 causes packet 2, which might or might not cause event x.

For the first version, the initial hole punching packet (TCP SYN) is sent from H1 towards H2, thus creating a hole at MB1. However, the TCP-SYN packet causes MB2 to send a TCP-RST as a reply, which could be a problem regarding the state of MB1. To prevent such TCP-RST packets the second variant (as depicted on the right hand side) sets the TTL field of the IP header to a value that the packet does not reach MB2. A possible ICMP TTL Exceeded message as generated by an intermediate hop might not close the state at MB1.



(a) Variant 1 (b) Variant 2

Figure 1: TCP hole punching, H = Host, MB = Middlebox.

d)* What are the general prerequisites for TCP hole punching?
Note: Please refer to the information model as presented in the lecture and follow the example for UDP hole punching when giving your answer.

In general, two things have to be considered:

1. Endpoint predictability as with UDP (see slides)
2. Prevent state from being closed by accident

For 2) the relevant fields in the information model are NoStatePolicy and StateRemovePolicy of the filtering element.

Delay in packet networks

Consider the wireless setup in Figure 2. Nodes i and j represent wireless computers like notebooks operating in ad-hoc mode, i. e., there is not access point. We assume that frames are sent at a constant rate r. However, due to media access control procedures there must be an average[1] idle time of Δt between any two frames. The MTU on the wireless link is denoted by l and the additional header information added by layers 2 and 1 is denoted by l_h. Further, the distance between i and j is given by d and the signal propagation of electromagnetic waves is approximately c (speed of light).

a)* Give a precise definition of MTU.

The MTU is the maximum size of the layer 2 SDU, e.g. an IP packet including its IP header that is passed down to the MAC layer.

b) Derive the total time t it takes node i to transmit a *single* frame to node j (including headers, without the idle time Δ_t).

[1]The idle time contains a random component for collision avoidance. You don't have to care about that, just use the average here.

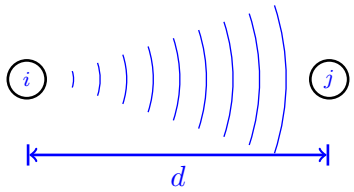


Figure 2: Sample network

$$t = \frac{d}{c} + \frac{l + l_h}{r}$$

c) The expression derived in (b) consists of two components. Discuss which of these terms primarily accounts for the transmission time.

Assume something like 10 m and a MTU of 1500 Byte, the serialization delay is three order of magnitude larger than the propagation delay.

From now on you may disregard the smaller term but remember the idle time Δt before each frame.

d) Derive the transmission time T of a data block of s Byte, which is fragmented into multiple frames if s exceeds the MTU.

$$T(r, s) = \left\lceil \frac{s}{l} \right\rceil \cdot \left(\frac{l_h}{r} + \Delta t \right) + \frac{s}{r}$$

e) Derive the effective average transmit rate r_{eff}, assuming that no collisions occur. (You do not have to consider acknowledgements that might be sent by j, just give a term for the transmit rate of i.)

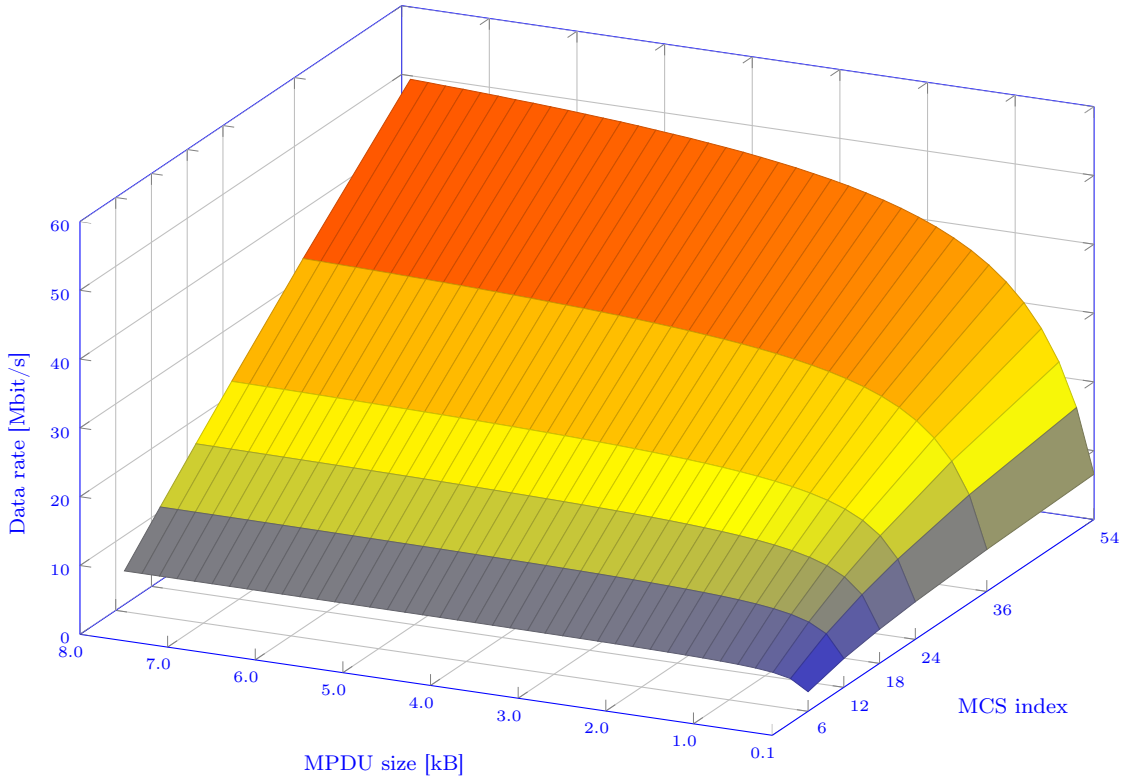
$$r_{eff} = \frac{T(s, r)}{s} \quad \text{for } s \text{ sufficiently large.}$$

Now assume $\Delta t = 101.5\,\mu$s, which is an approximation for IEEE 802.11a/g networks. Further, consider the cooresponding gross data rates of $r \in \{6, 12, 18, 24, 36, 54\}$ Mbit/s.

f) Use a CAS and plot r_{eff} depending on r and a series of meaningful values for l (for IEEE 802.11a $l_{\max}$ is somewhere around 2200 Byte, $l_h = 34$ Byte is fine).

g) What is wrong with IEEE 802.11a/g? Suggest possible fixes (except for removing Δt).

The interframe spaces have a significant impact on effective transmit rates that increases with the gross transmit rate.
Frames may be aggregated to jumbo frames (done with IEEE 802.11n) or consecutive frames may sent in blocks with a short interframe gap than Δt (also done with IEEE 802.11n).


Data rate [Mbit/s]
60
50
40
30
20
10
0
8.0
7.0
6.0
5.0
4.0
3.0
2.0
1.0
0.1
MPDU size [kB]
6
12
18
24
36
54
MCS index