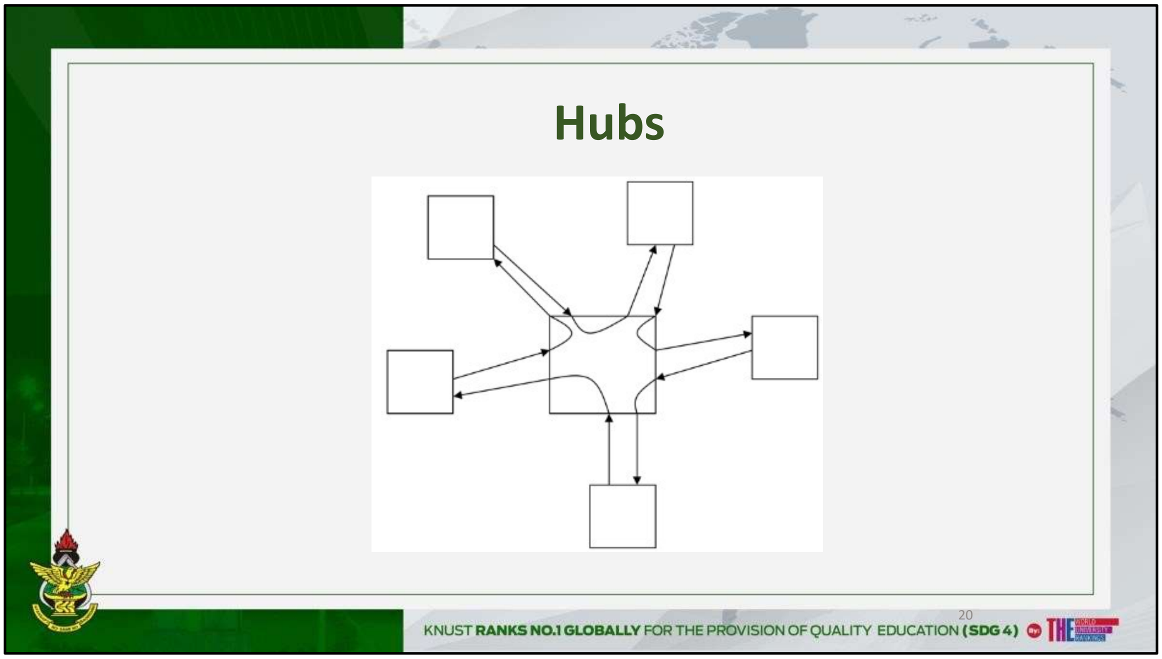



In this configuration the central node (HUB) is “passive”.

Logically, hub networks can be of bus or ring topologies.

- With passive power splitting the hub is equivalent to a bus.
- With collapsed wiring, as above, it is equivalent to a ring.

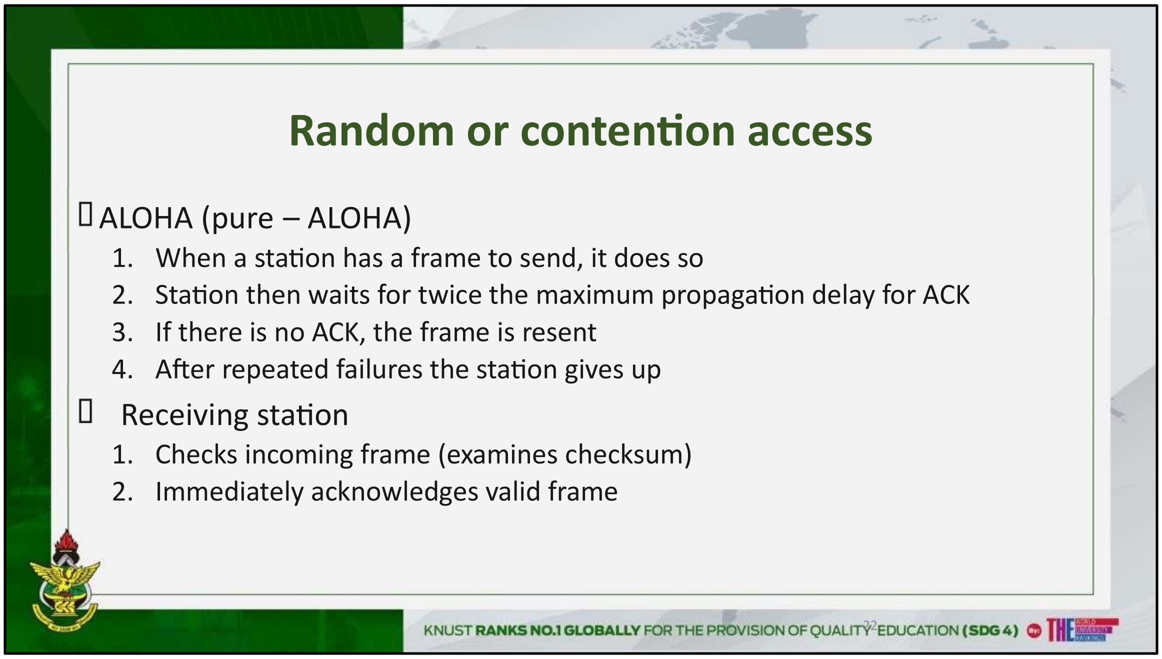
In reality, it is usually the case that the hub will contain repeater electronics, enabling longer link distances to the attached devices, and more of them.


The topology of LANs means that no routing is required and that there may be a shared transmission facility. This gives rise to particular access methods.

With FIXED ASSIGNMENT, channels are allocated on a static basis.
RANDOM/CONTENTION ACCESS methods allow the entire b/w to be accessed randomly or contended for. Collisions between transmitted packets can occur.
SCHEDULED ACCESS methods may be *centrally controlled with the controller allocating time or* b/w according to demand. *Distributed control is usually preferred for LANs as it increases* reliability and can improve performance.
ADAPTIVE STRATEGIES change the access technique according to the demands placed on the network.

Purely fixed assignment techniques tend not to be used in LANs. FDMA and TDMA are used in satellite links, although newer systems tend to incorporate some demand assignment. CDMA is used in satellite/military links where secure communications is desired. As it is robust to interference it is also being adopted in digital cellular networks.

In LANs, distances are short, so stations can monitor and react to changes in demand very quickly. The traffic is also very 'bursty' for which fixed assignment is not suitable. Other access techniques are preferred: random access in which stations contend for use of the channel; and scheduled access in which access is controlled and assigned according to demand.



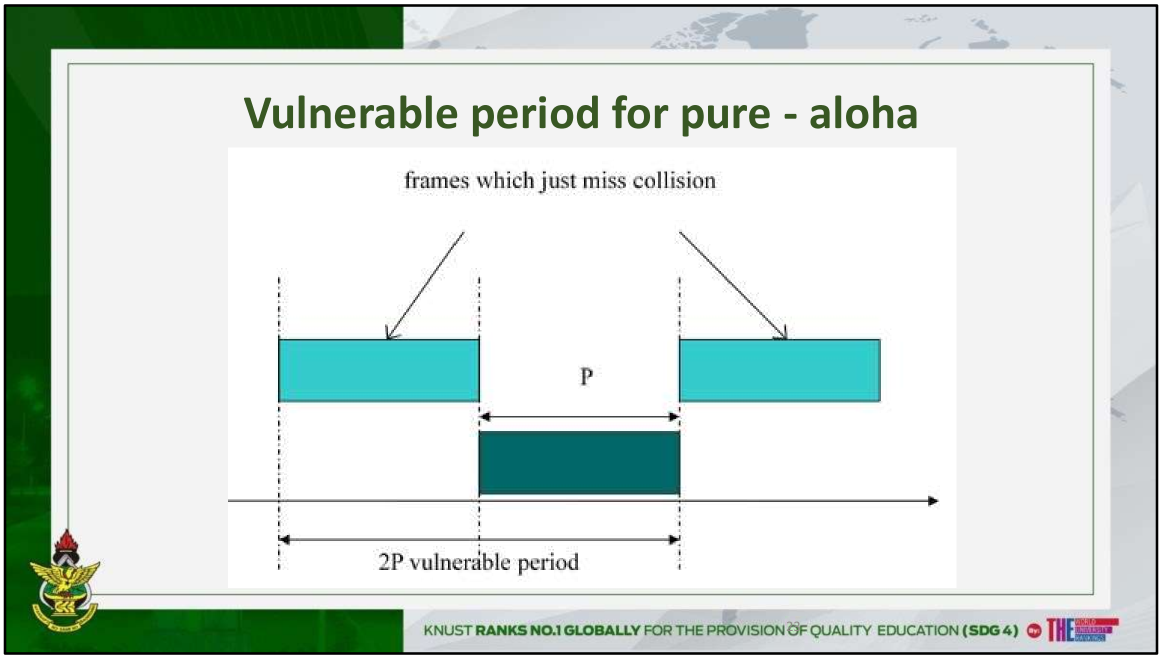

The ALOHA protocol was developed c.1970 for a packet-radio broadcast network at the University of Hawaii - although this was not strictly a LAN the concept is applicable to local networking. It is a very simple, purely random access protocol.

The receiving station checks incoming frames for errors - if the frame is valid it is immediately acknowledged.

There are two main reasons for invalid frames :

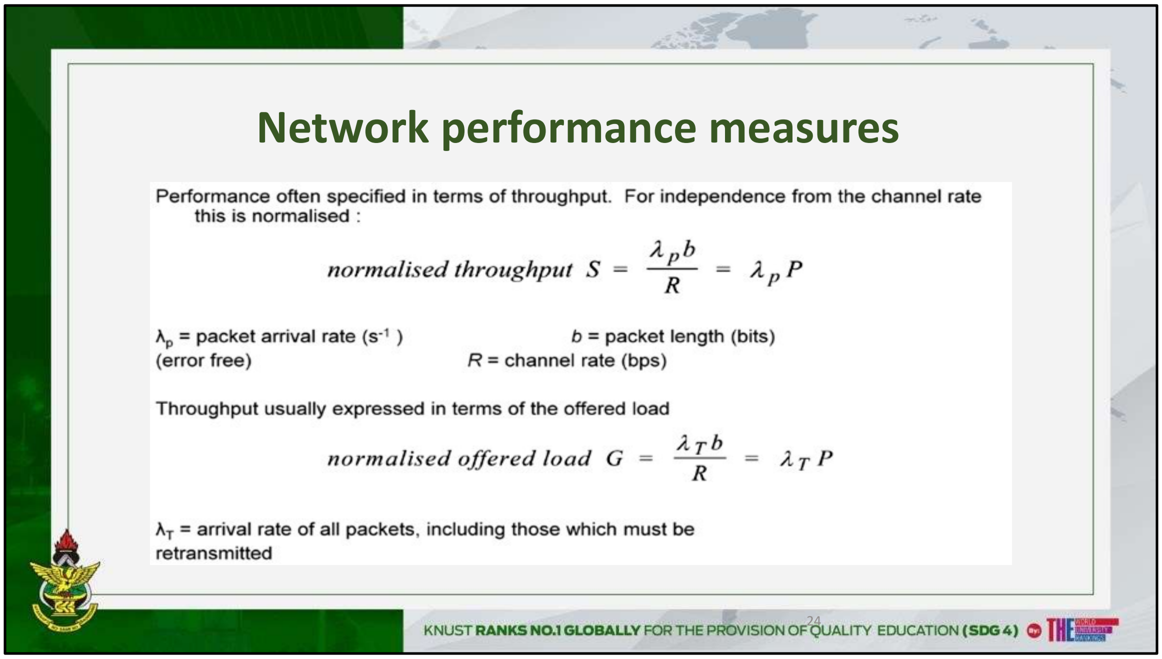
1. channel noise
2. another transmission occurred at the same time- the frames interfered and were corrupted.

In looking at access protocols, the second reason is of prime interest.




In pure-ALOHA a packet will be successfully transmitted if no other frames are transmitted *P* seconds before or after it, where *P is the packet transmission time.*

This gives a *vulnerable period of 2P.*




Network performance is often specified in terms of the throughput, which is a measure in bps of the *successful traffic being transmitted between stations. To make the analysis of performance* independent of channel rate, normalised throughput is used.

Throughput is expressed in terms of the offered load, which can be normalised in a similar manner.

Note that whereas the normalised throughput is limited to values $0 < S < 1$, *the offered load can* become arbitrarily large as the number of packets requiring retransmission builds up ($0 < G < \infty$).

# Performance of pure - aloha

We can say that throughput = offered load x prob. of transmissions being successful

So,

$S = G\,p_0(2P)$, where $p_0(2P)$ is the probability of there being no other transmissions in the vulnerable period 2P.

Assuming that packet arrivals are independent with a mean arrival rate $\lambda_T$, the probability of $k$ arrivals in a time $t$ is Poisson-distributed :

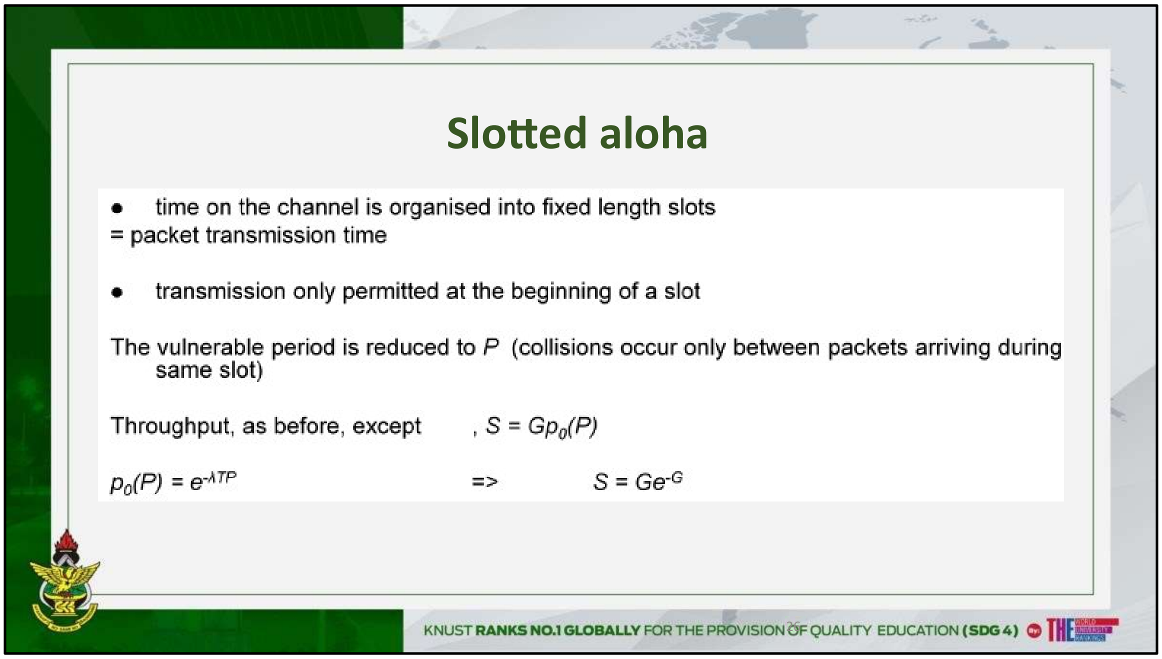
$$p_k(t) = (\lambda_T t)^k \frac{e^{-\lambda_T t}}{k!}$$

$$\therefore\ p_0(2P) = e^{-\lambda_T 2P}$$

As $G = \lambda_T P$, this gives the throughput,

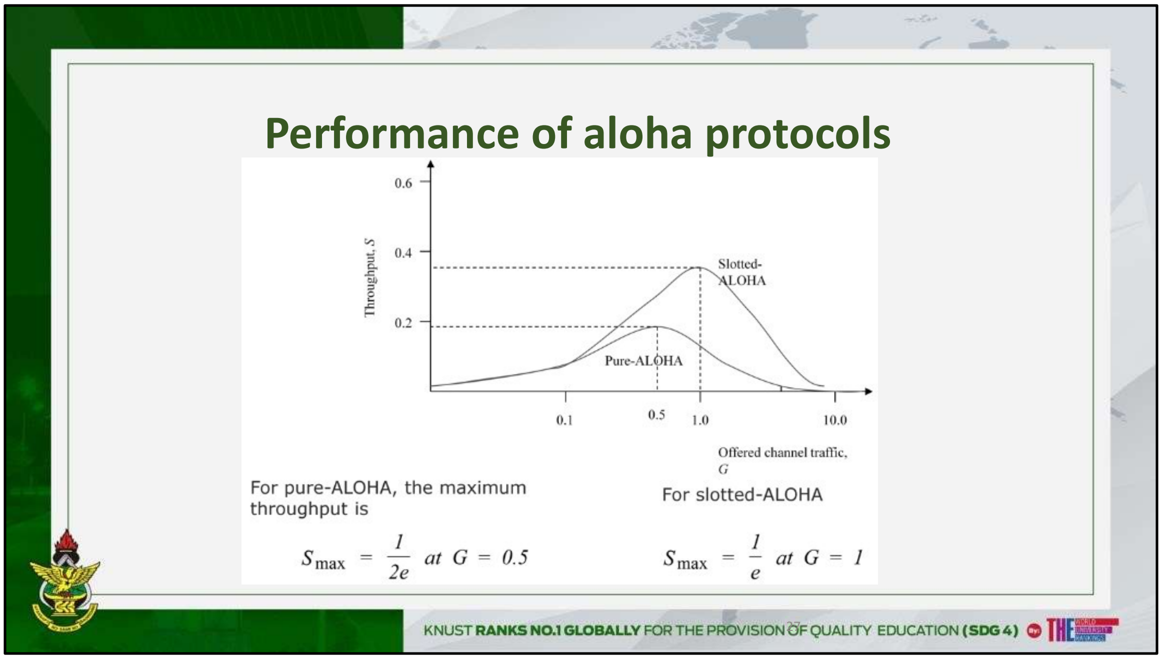
$$S = G\,e^{-2G}$$

KNUST **RANKS NO.1 GLOBALLY** FOR THE PROVISION OF QUALITY EDUCATION **(SDG 4)** By: THE



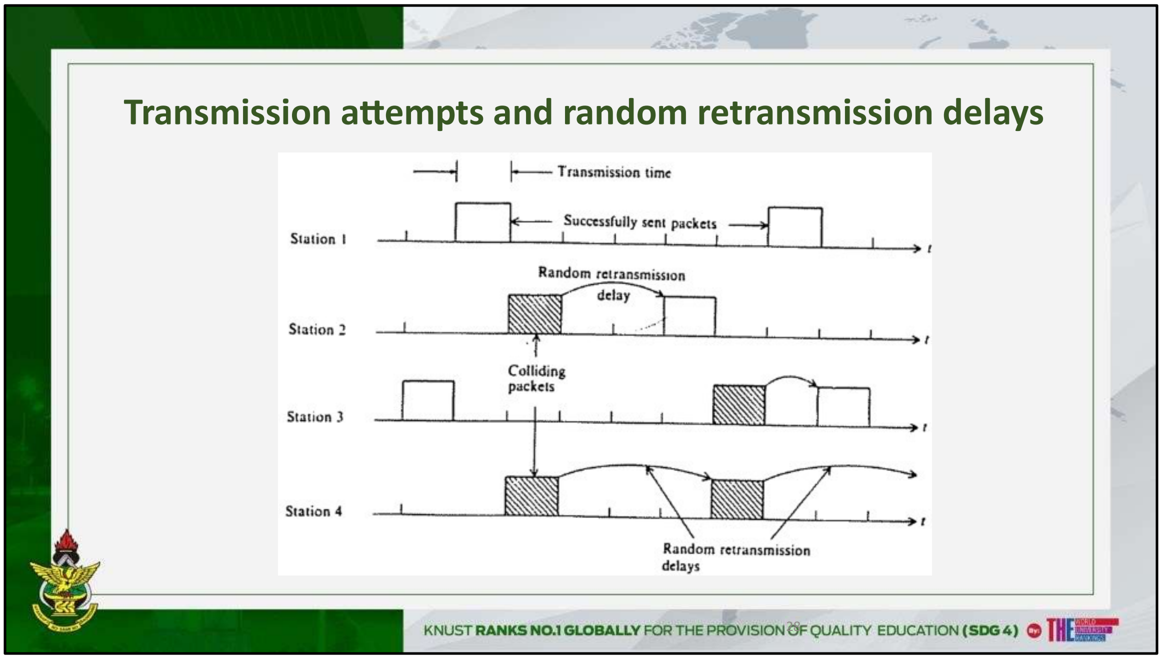

To increase efficiency the slotted-ALOHA scheme was developed.
Channel time is divided up into fixed-length slots which are equal in duration to the packet transmission time; a central clock is required to synchronise all stations.

Transmission is only permitted at the beginning of a slot, so packets arriving during a slot are held
until the beginning of the next slot. This has the effect of reducing the vulnerable period to *P, and* increasing the throughput.

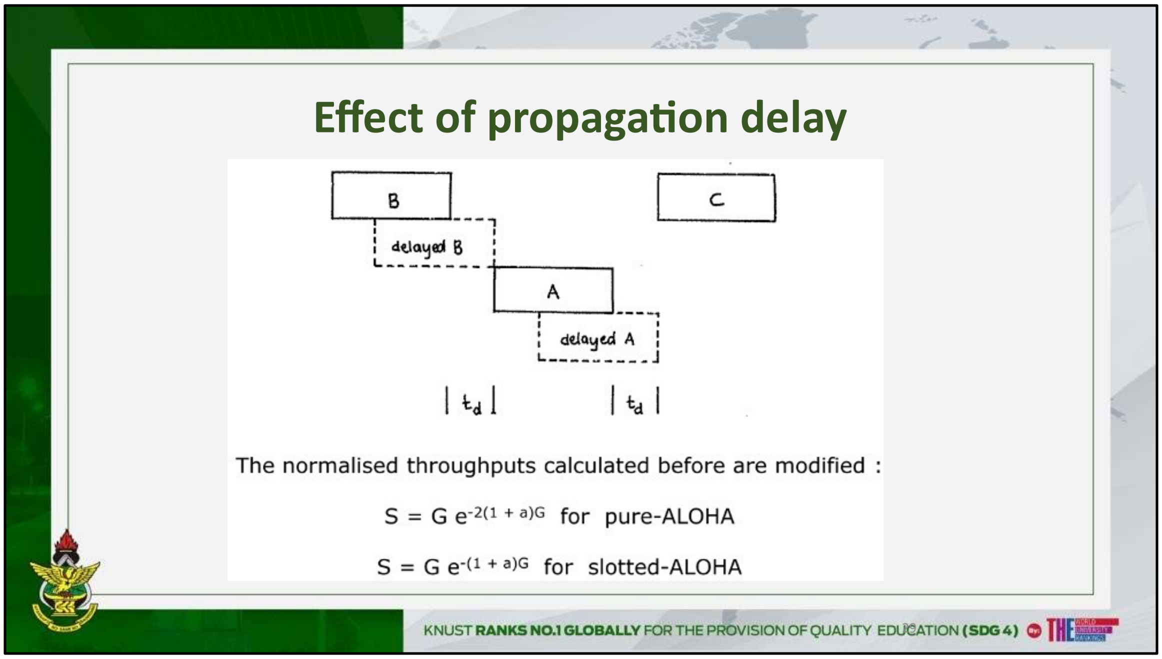



A major problem for both pure- and slotted-ALOHA (and for random / contention access schemes generally) is INSTABILITY.

At high offered traffic the throughput actually *decreases, due to increased collisions. The number* of retransmissions required will therefore increase and increase the offered traffic still further.



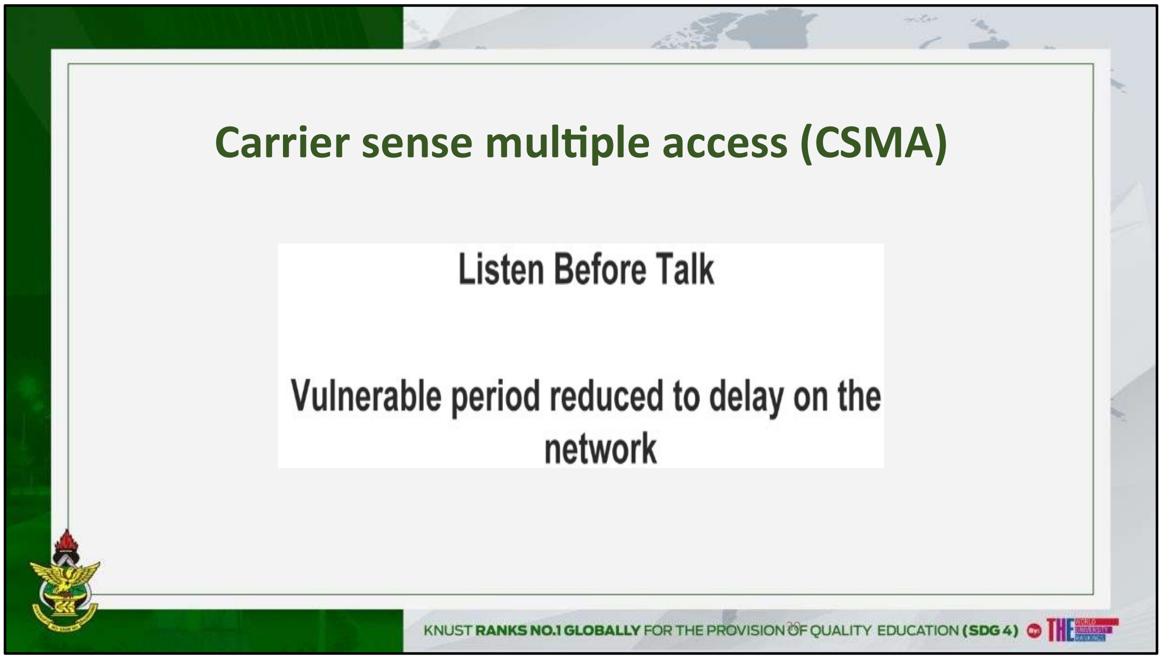

Back-off algorithms are often used. If a packet experiences a collision, the station waits a time *t,* derived from a probability distribution, before trying to retransmit. If the packet experiences a second collision then the station will wait a time 2*t, and so on. This tends to produce a more* constant throughput at higher loads, although delays may be increased at lighter loads.




The propagation delay is a very important parameter in LANs; it is typically less than the packet transmission time.

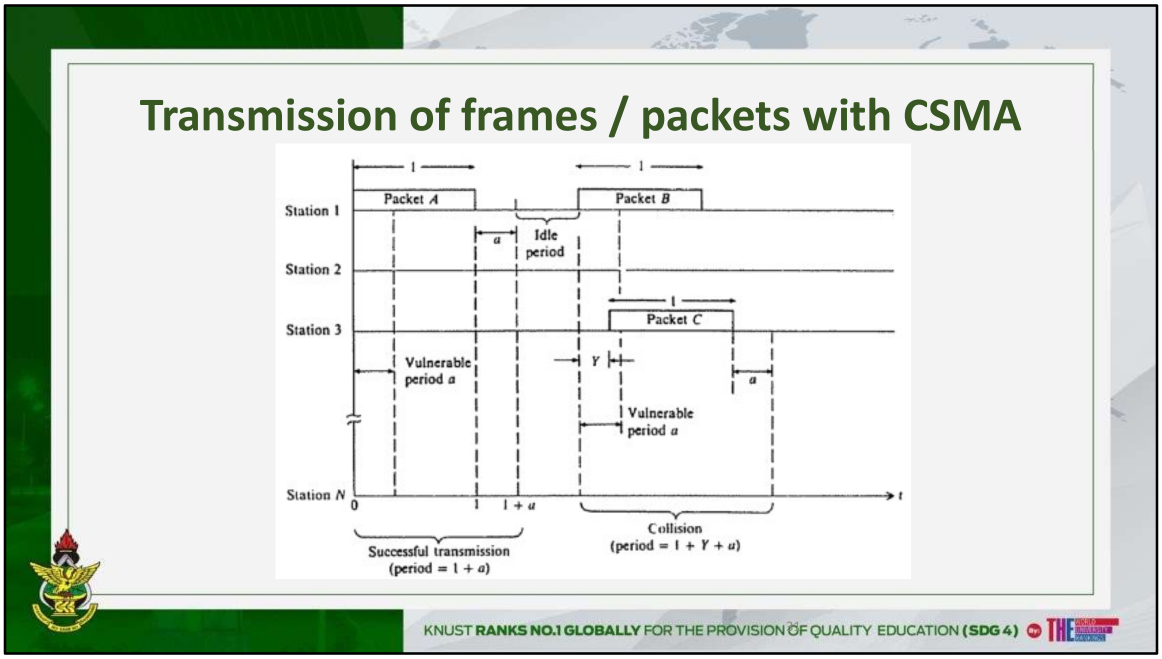
For pure-ALOHA the vulnerable period is increased to 2*P + 2td, where td is the propagation delay,* when this is taken into account.

Similarly, for slotted-ALOHA, the vulnerable period is now seen to be *P + td.*
The propagation delay is usually defined in normalised form as the "*a" parameter for a LAN: a = normalised propagation delay = td/P*




CSMA made use of the fact that typically *a<<1 for LANs, so stations could be aware of packet* transmissions very quickly compared to the packet transmission time if they followed a "listen before- talk" (LBT) protocol. There are three basic protocol types, but the main element is that any station wishing to transmit listens to the medium to check if another transmission is in progress.
The *vulnerable period is effectively reduced to the delay on the network.*

As with ALOHA, the protocols can be "slotted". In this case the slot time is usually made equal to the maximum propagation delay - the vulnerable period.
Randomly distributed retransmission times are also used after collisions.

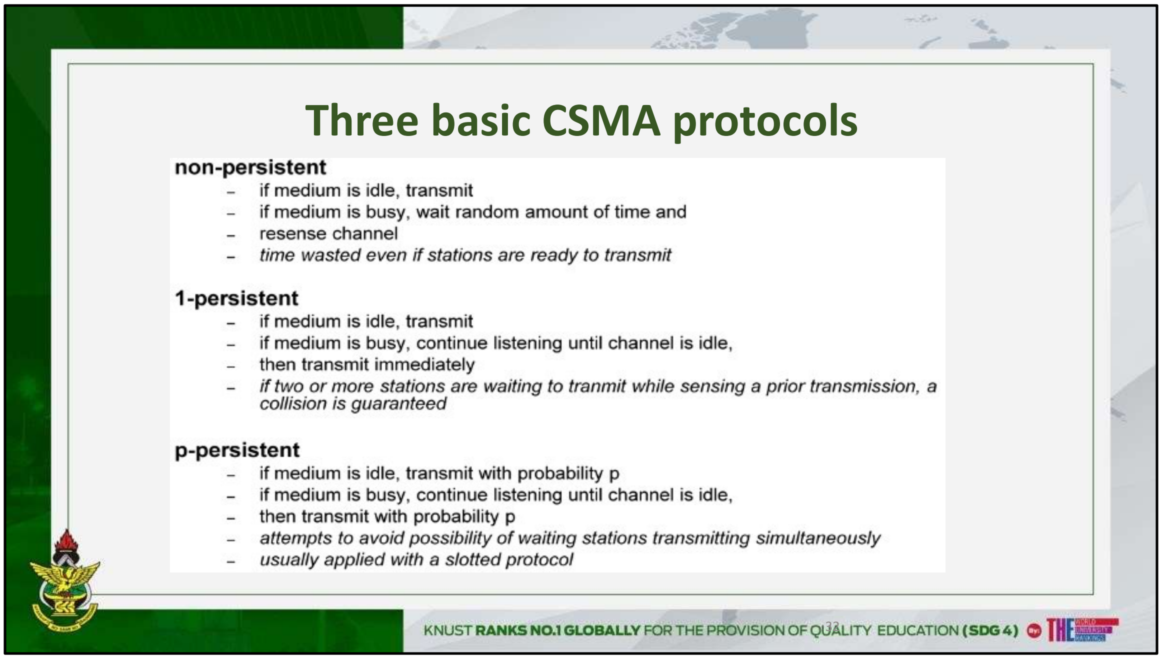



The throughput for CSMA can be defined in terms of two types of busy period, as well as the idle period.

For packet A, it can be seen that the busy period for a successful transmission = 1 + *a (with time* normalised to the packet transmission time).

For packet B, it can be seen that the busy period of an unsuccessful transmission = 1 + *a + Y, where the interval Y < a, is dependent on the packet arrival statistics, as is the idle* period.

The throughput is then
= (time spent using channel in successful transmissions) / (time spent using the channel + idle time)




With a nonpersistent protocol there is always some wasted idle time between transmissions.

A 1-persistent protocol minimises the channel idle time, but the number of collisions may be increased. If two (or more) stations are waiting to transmit while another transmission is taking place, as soon as the transmission ceases, both stations will attempt to transmit. The 1-persistent protocol can be seen as a particular case of ppersistent protocols (p = 1).

In p-persistent systems p is chosen to find a balance between the two above problems. It is usually used with a slotted scheme.  If the channel is sensed idle, the station transmits with a probability p, or defers transmission one  slot. If the deferred slot is sensed idle, again the station transmits with probability p or defers. This is repeated until the packet is transmitted or the channel is sensed busy. If the channel is sensed busy, the station acts as though a collision had occurred - it waits a time taken from a  random distribution before repeating the above procedure.

# Throughput as a function of offered load