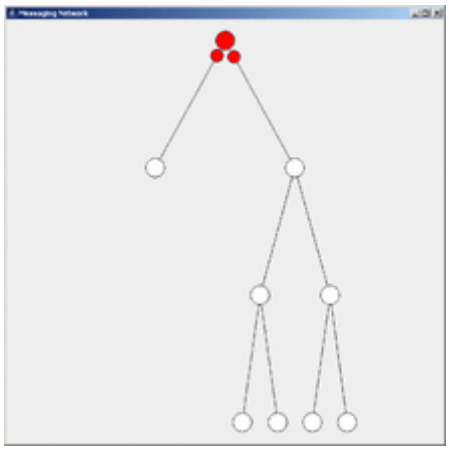
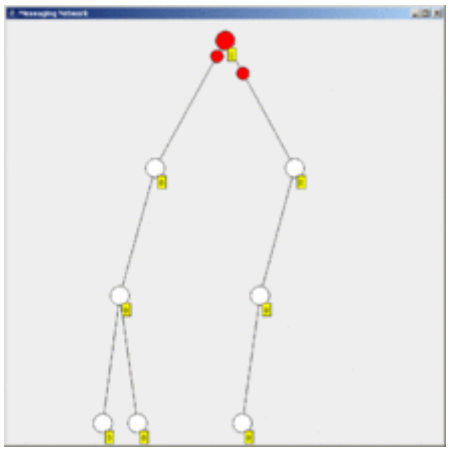
Flooding (computer networking)

Flooding is used in computer networks routing algorithm in which every incoming packet is sent through every outgoing link except the one it arrived on.[1]

Flooding is used in bridging and in systems such as Usenet and peer-to-peer file sharing and as part of some routing protocols, including OSPF, DVMRP, and those used in ad-hoc wireless networks (WANETs).[2]



Flooding algorithm



Flooding algorithm with ACK messages

Contents

Types

There are generally two types of flooding available, **uncontrolled flooding** and **controlled flooding**.

In *uncontrolled flooding* each node unconditionally distributes packets to each of its neighbors. Without conditional logic to prevent indefinite recirculation of the same packet, broadcast storms are a hazard.

Controlled flooding has its own two algorithms to make it reliable, SNCF (Sequence Number Controlled Flooding) and RPF (Reverse Path Forwarding). In SNCF, the node attaches its own address and sequence number to the packet, since every node has a memory of addresses and sequence numbers. If it receives a packet in memory, it drops it immediately while in RPF, the node will only send the packet forward. If it is received from the next node, it sends it back to the sender.

Algorithms

There are several variants of flooding algorithms. Most work roughly as follows:

1. Each node acts as both a transmitter and a receiver.

2. Each node tries to forward every message to every one of its neighbors except the source node.

This results in every message eventually being delivered to all reachable parts of the network.

Algorithms may need to be more complex than this, since, in some case, precautions have to be taken to avoid wasted duplicate deliveries and infinite loops, and to allow messages to eventually expire from the system.

Selective flooding

A variant of flooding called **selective flooding** partially addresses these issues by only sending packets to routers in the same direction. In selective flooding the routers don't send every incoming packet on every line but only on those lines which are going approximately in the right direction.

Advantages

The advantages of this method are that it is very simple to implement, if a packet can be delivered then it will (probably multiple times), and since flooding naturally utilizes every path through the network it will also use the shortest path.

Disadvantages

Flooding can be costly in terms of wasted bandwidth. While a message may only have one destination it has to be sent to every host. In the case of a ping flood or a denial of service attack, it can be harmful to the reliability of a computer network.

Messages can become duplicated in the network further increasing the load on the network as well as requiring an increase in processing complexity to disregard duplicate messages. Duplicate packets may circulate forever, unless certain precautions are taken:

- Use a hop count or a time to live (TTL) count and include it with each packet. This value should take into account the number of nodes that a packet may have to pass through on the way to its destination.
- Have each node keep track of every packet seen and only forward each packet once.
- Enforce a network topology without loops.

Examples

In Open Shortest Path First (OSPF), flooding is used for transferring updates to the topology (LSAs).

In low data rate communications, flooding can achieve fast and robust data communications in dedicated protocols such as VEmesh,[3] which operates in the Sub-1 GHz frequency band and Bluetooth mesh networking, which operates in the 2.4 GHz frequency band. Both these protocols serve as underlying technologies in the Digital Addressable Lighting Interface in use in professional and commercial lighting control.

See also

- Broadcasting (networking)

- Flood search routing
- Multicast
- Spanning Tree Protocol

References

1. Tanenbaum, Andrew S.; Wetherall, David J. (March 23, 2010). *Computer Networks* (5th ed.). Pearson Education. pp. 368–370. ISBN 978-0-13-212695-3.
2. Rahman, Ashikur; Olesinski, Wlodek; Gburzynski, Pawel (2004). "Controlled Flooding in Wireless Ad-hoc Networks" (http://www.senserf.com/pg/PAPERS/tarp1.pdf) (PDF). *International Workshop on Wireless Ad-Hoc Networks*. Edmonton, Alberta, Canada: University of Alberta, Department of Computing Science. Archived (https://web.archive.org/web/20170210205207/http://www.senserf.com/pg/PAPERS/tarp1.pdf) (PDF) from the original on February 10, 2017. Retrieved October 15, 2015.
3. virtual-extension.com

External links

- https://www.cs.cornell.edu/projects/quicksilver/ricochet.html