MANAnet ROUTER

Filter the Flood, Drain the Pain

Working defense against DDoS attacks

PURPOSE

Most approaches to DDoS defense at the victim sites cannot avoid congestion of the network upstream, and, therefore, legitimate customer packets are likely to be lost. In practice, most sites detect the packet flood, and then request that their ISP filter the bad traffic. This is a tedious manual process. MANAnet Routers are routers with additional functionality that, in cooperation with other neighboring MANAnet routers, can substantially reduce the impact of packet flooding DDoS attacks reliably, automatically, and in real-time.

Implements DDoS defense at the infrastructure level

DEVICE

The MANAnet Router makes it possible to schedule or filter packets based on more reliable data about their source addresses, thereby providing the basis for a working DDoS defense at the infrastructure level. This requires cooperation with neighboring MANAnet routers, which add path data to packets that is beyond the control of the attacker(s). The additional path information and the effort to decode path information can be handled in constant and small overhead.

All Infrastructure Owners

USERS

All Internet infrastructure owners who currently deploy traditional routers within their networks can benefit from deploying the MANAnet Router instead. The currently available Linux implementation of the MANAnet Router is not fast enough to replace high-speed, commercial routers. However, MANAnet's patent-pending technologies will be licensed to commercial router companies to provide fast routers that implement the MANAnet DDoS defense.

Infrastructure-level approach that requires no updates

BENEFITS

The MANAnet Router or its commercial counterparts have the potential to completely eliminate the threat of packet flooding DDoS attacks. The MANAnet approach has several important advantages**:**

a) An enhance path protocol that does not add significantly to latency, nor uses too much bandwidth to implement the defense.

b) The MANAnet Router does *not* rely upon "intelligent" traffic analysis to recognize known attack signatures as many competing approaches do. Instead, the router functions based on the fundamentally simple idea of "fair service."

c) No updates are required when the attackers change their methods or become more sophisticated – as they indeed will when the defenses improve. Security achieved through simplicity and elegance of design trumps "smart" approaches that invite a virtual arms race with hackers – as the virus scanning fiasco illustrates amply.

d) Cooperative MANAnet neighborhoods can be used to define a variety of new quality of service and security applications beyond DDoS defense.

5777 W. Century Blvd. ● Suite 1185 Los Angeles, CA 90045 ● www.cs3–inc.com
Phone 310.337.3013

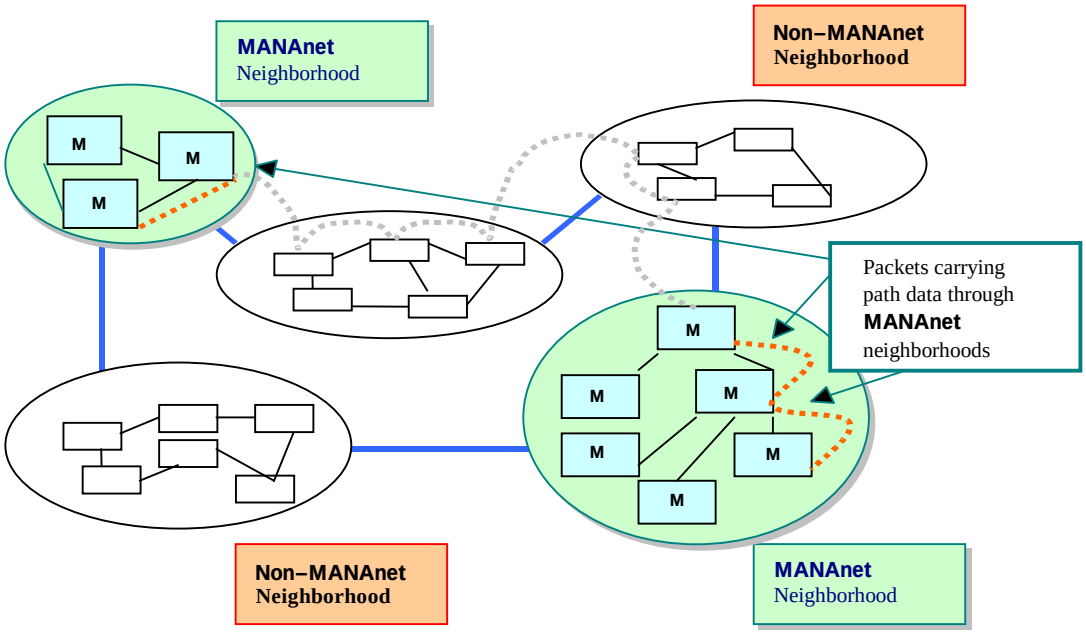
MANAnet ROUTER

How the it Works!

Uses PEIP and Fair Service Queuing

BEGIN

The MANAnet Router implements a modified form of IP called Path Enhanced IP (PEIP). Each MANAnet Router adds the place from where it got a packet to the packet before it forwards it. It really helps to have "cooperative neighborhoods" of MANAnet routers – routers that are connected to one another and are MANAnet-enabled. Within a cooperative neighborhood, one can unerringly identify the place where the packet entered the neighborhood because that data is not under the control of the DDoS attacker. Please see http://www.cs3-inc.com/sf.html for more technical details about PEIP.



In addition to PEIP, the MANAnet router includes different packet scheduling schemes that essentially eliminate the threat of DDoS attacks. For example, Places-Based Fair Queuing (PLFQ) ensures that the router metes out the bandwidth by using its knowledge of where packets come from, thereby ensuring that the attacker(s) get no more of the bandwidth than legitimate customers. These scheduling schemes within the MANAnet Router essentially frustrate the DDoS attacker by not allowing the attack to disrupt normal service – which is the basic goal of the attack. Larger neighborhoods yield the best results, although installation at smaller infrastructures will also produce tangible benefits. Please see http://www.cs3-inc.com/DDoS.html to see more technical details about the scheduling algorithms and the effectiveness of the defense in various cases where packets must pass through MANAnet and non-MANAnet infrastructure.

5777 W. Century Blvd. ● Suite 1185 Los Angeles, CA 90045 ● www.cs3–inc.com
Phone 310.337.3013