PATTERNS IN NETWORK ARCHITECTURE:

NEW PROPOSALS FOR SECURITY

NAMES

MANY PROPOSALS HAVE A SEPARATION OF IDENTIFIERS AND LOCATORS

which is good for mobility

which must be routable

PROPOSAL	IDENTIFIERS	LOCATORS
ILNP+IPv6	lower 64 bits of address	all 128 bits of address
AIP	Endpoint Identifier (EID)	[AD, EID], where AD is an Administrative Domain
MobilityFirst	Globally Unique Identifier (GUID)	[NA, GUID], where NA is a Network Address
NUTSS	(user, domain, service) triple	IP addresses

NAMES

MANY PROPOSALS with A SEPARATION OF IDENTIFIERS AND LOCATORS

also have LOCATOR = NETWORK + IDENTIFIER

PROPOSAL	IDENTIFIERS	LOCATORS
ILNP+IPv6	lower 64 bits of address	all 128 bits of address
AIP	Endpoint Identifier (EID)	[AD, EID], where AD is an Administrative Domain
MobilityFirst	Globally Unique Identifier (GUID)	[NA, GUID], where NA is a Network Address

this is convenient, but comes with some cost:

- addressing inside a network must be “flat”, because addresses are not chosen by the network
- there is a risk of collisions, unlimited identifier minting

SELF-CERTIFYING IDENTIFIERS

MANY PROPOSALS with A SEPARATION OF IDENTIFIERS AND LOCATORS

also have LOCATOR = NETWORK + IDENTIFIER

and SELF-CERTIFYING IDENTIFIERS

these designs have already paid the cost of flat identifiers

PROPOSAL	IDENTIFIERS	LOCATORS
AIP	Endpoint Identifier (EID)	[AD, EID], where AD is an Administrative Domain
MobilityFirst	Globally Unique Identifier (GUID)	[NA, GUID], where NA is a Network Address

identifiers are hashes of public keys

public key needs to be 2K bits

AIP EID is 160 bits

with a challenge/response, anyone can check that a node is using its own identifier

there is no need to rely on a trusted global authority

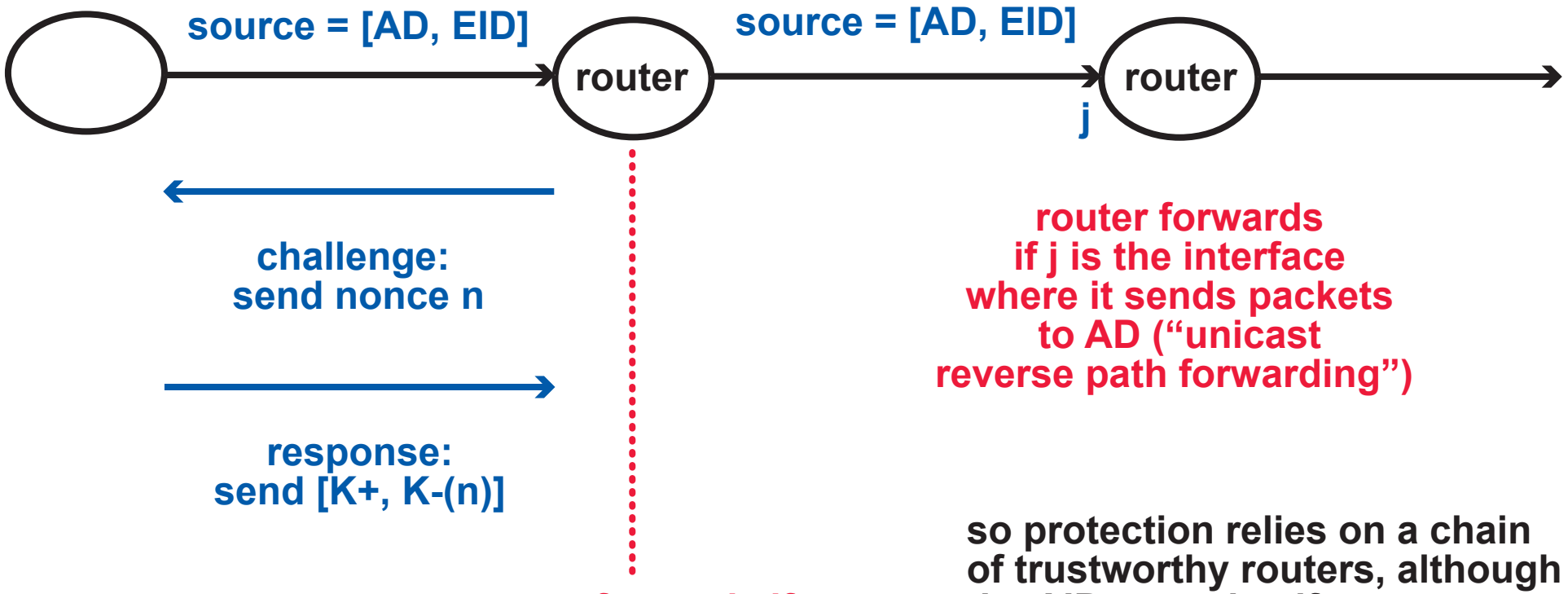
network names are also self-certifying, for secure routing

FINDING AND MOBILITY

PROPOSAL	MAP FROM HUMAN-READABLE NAME TO IDENTIFIER		MAP FROM IDENTIFIER TO LOCATOR
ILNP+IPv6	DNS		DNS
AIP	DNS	*when a host is mobile, it updates its locator in DNS; because identifier is self-certifying, DNS can trust update*	DNS
MobilityFirst	GNS (a bigger DNS, which is necessary because every host will have a GUID)	*GNS should also benefit from self-certifying location update*	GNS
NUTSS	identifiers are human-readable	for name-routed signaling DNS finds P-box of domain, which routes to endpoint; if name-routed signaling is successful, it supplies locator	

PROTECTION AGAINST SOURCE SPOOFING

ONLY AIP EXPLAINS IT, ALTHOUGH MobilityFirst HAS THE RIGHT KIND OF NAMES



so protection relies on a chain of trustworthy routers, although the AIP paper itself says you can't trust other networks' routers to be diligent in this way (?)

alternatively, any node can repeat the challenge/response

PROTECTION AGAINST DENIAL OF SERVICE

MUST FILTER OUT BAD TRAFFIC

MUST RECOGNIZE BAD TRAFFIC WITH LITTLE EFFORT

because otherwise the attacker has already won

note, however, that there can be stages of defense, e.g., IDS diagnoses suspicious sources, which are then blocked

THIS REQUIRES A . . .

however, a firewall cannot be configured with flat identifiers!

simply because there is no aggregation, so the scheme is not scalable

this is an opinion from the NUTSS paper, but I don't see anything wrong with it

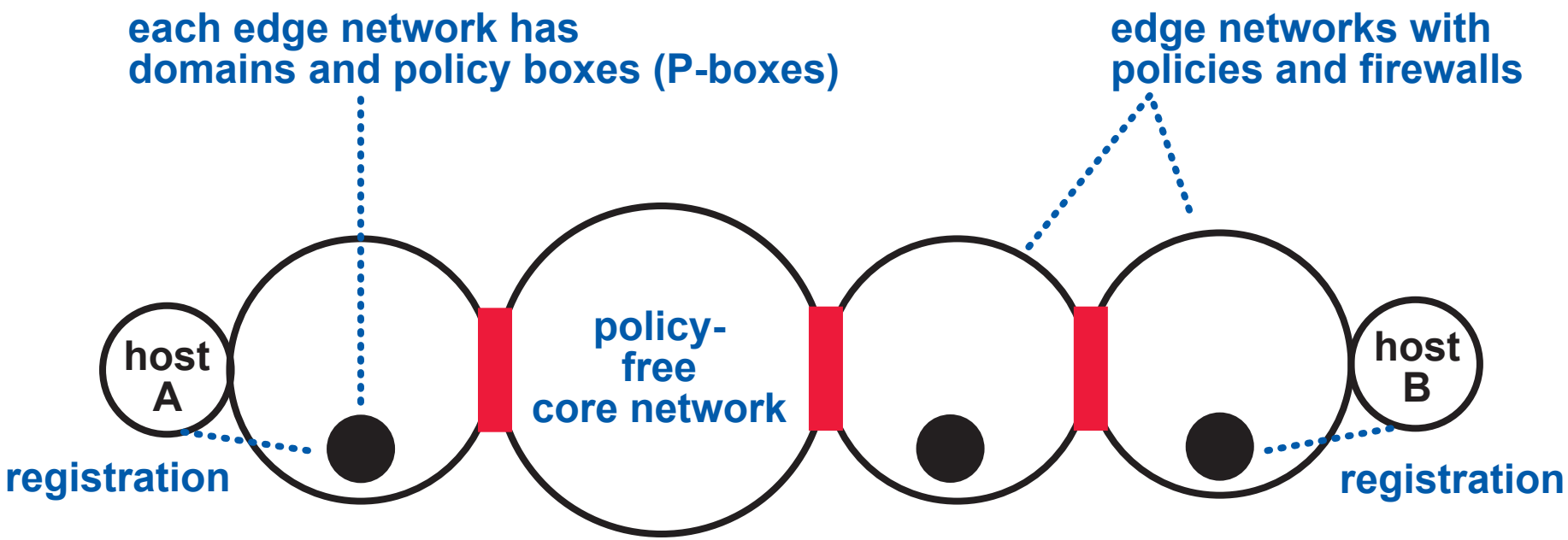
AIP and MobilityFirst papers do not mention firewalls

AIP paper says that a victim can send a shutoff message to an attacker, . . .

. . . on which a smart NIC will stop the attack, . . .

. . . which does not sound very reassuring

PROTECTION AGAINST DENIAL OF SERVICE IN NUTSS 1

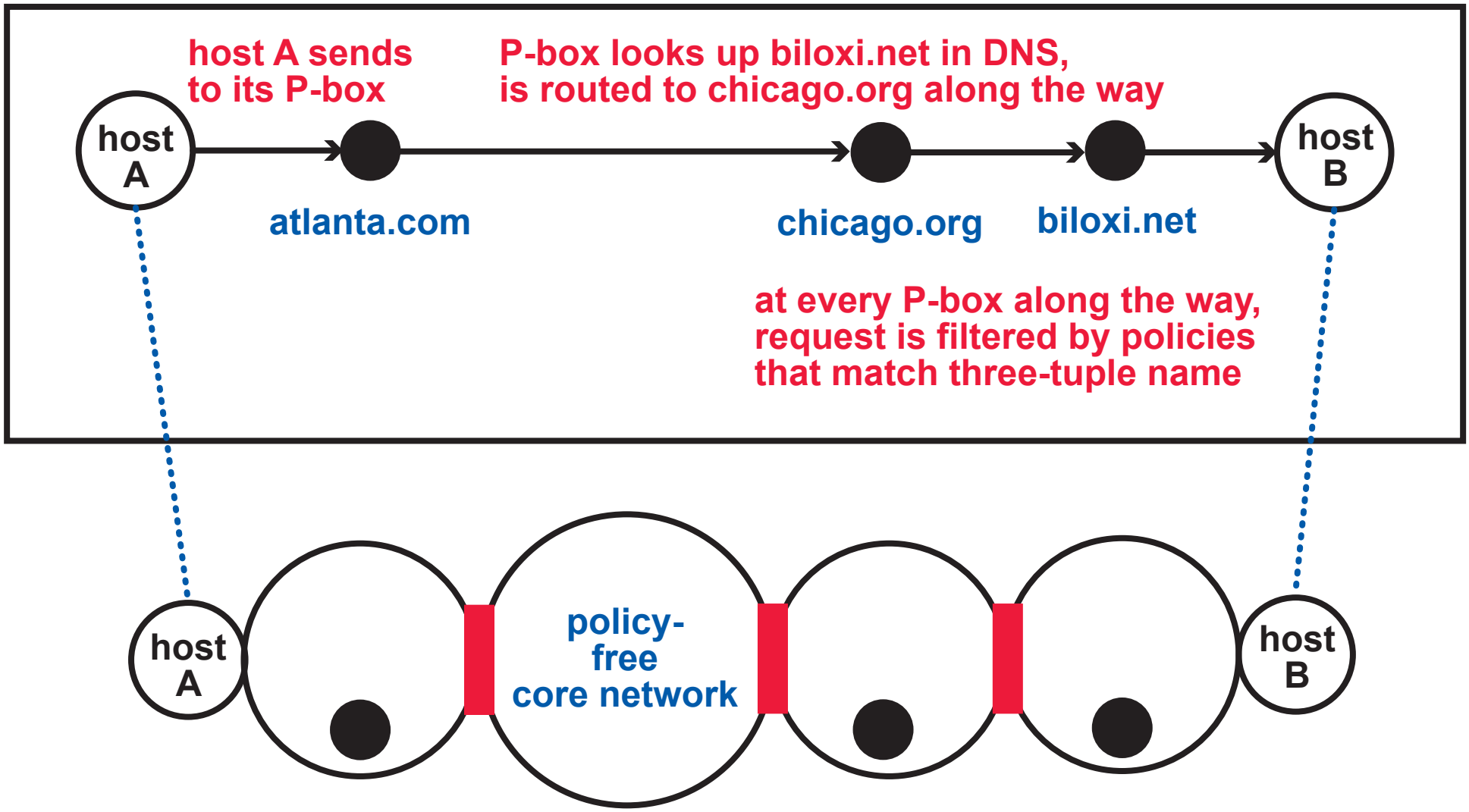


(A, atlanta.com, service) wishes to connect to (B, biloxi.net, service)

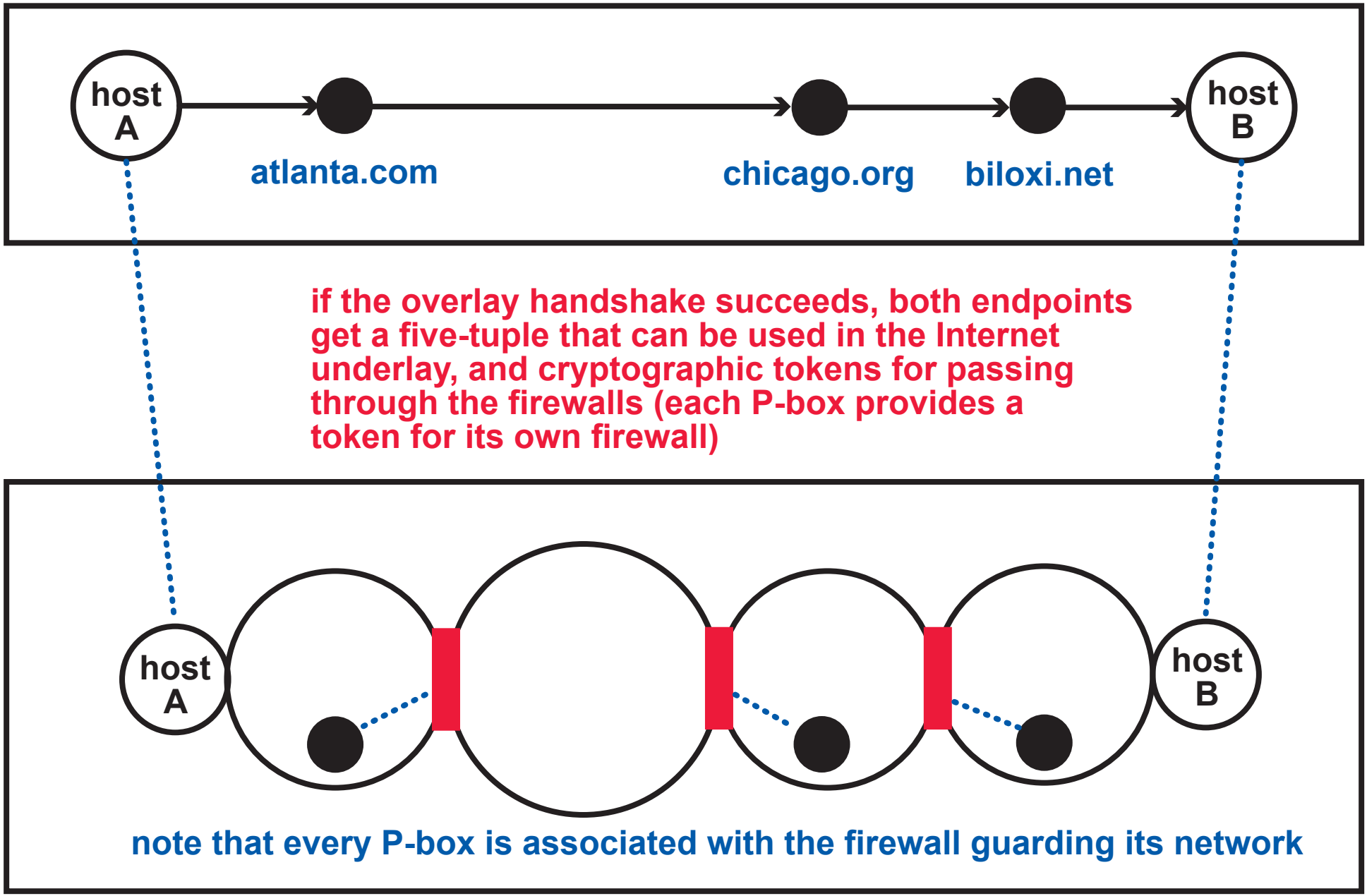
PROTECTION AGAINST DENIAL OF SERVICE IN NUTSS 2

(A, atlanta.com, service) wishes to connect to (B, biloxi.net, service)

this request is transmitted through an overlay network



PROTECTION AGAINST DENIAL OF SERVICE IN NUTSS 3



NUTSS SUMMARY

DOS PROTECTION

- in the overlay, requests can be aggregated and filtered, with wildcards in any position of the three-tuple
- in the open Internet, firewalls can be used as usual, with some packets getting a free pass

caution:
how many valid tokens are there for a firewall to remember?

- NUTSS is far more complicated than shown here, hopefully for good reason (and it could use a much better explanation, but the details are appreciated)

SIMILAR PROPOSALS

- NEBULA uses the same approach of setting up a connection with a separate signaling path, but gives no details (not even about naming!)
- the NUTSS overlay is similar to SIP (in fact, it is implemented using SIP)

  big difference is that NUTSS signaling and data paths must be similar

  SIP is explicitly designed to have "signaling-media separation" (see the SIP trapezoid)

  so even if SIP proxies cooperated with firewalls, they could not help media packets traverse firewalls (and, in general, they cannot)

INTER-DOMAIN ROUTING

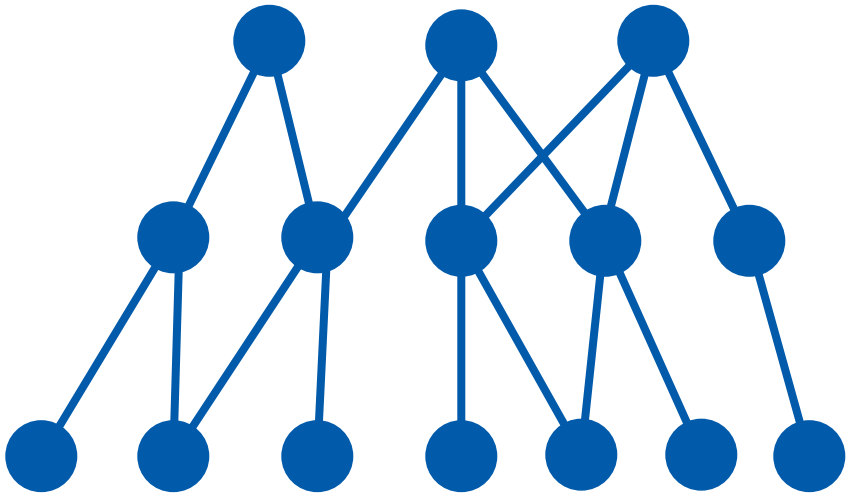
AIP, MobilityFirst, NUTSS (and probably many others) recommend routing in terms of Autonomous Domains, not IP prefixes

if the name of the AD is self-certifying, this is clearly good for routing security

inter-domain routing to ADs clearly makes sense when an AD is a topologically united subnetwork

does it also make sense for large, widespread AD?

there seems to be a notion that networks form a hierarchy, like switches in a data center



the AIP paper reports on experiments indicating that the diameter of the network will not increase, AD routing works

both AIP and MobilityFirst consider lists of AD in addresses, which reminds me of compound sessions!

NEW PROPOSALS FOR SECURITY

WHICH ONE WOULD YOU BUY?

IT MIGHT BE NICE TO USE COMPOSITION TO CREATE A VARIETY OF ALTERNATIVES