Digital Signature Protection of OSPF Routing Protocol

Internet Society
Symposium on
Network and Distributed System Security

February 23, 1996

Sandra Murphy
murphy@tis.com
Trusted Information Systems
Glenwood, MD 21738

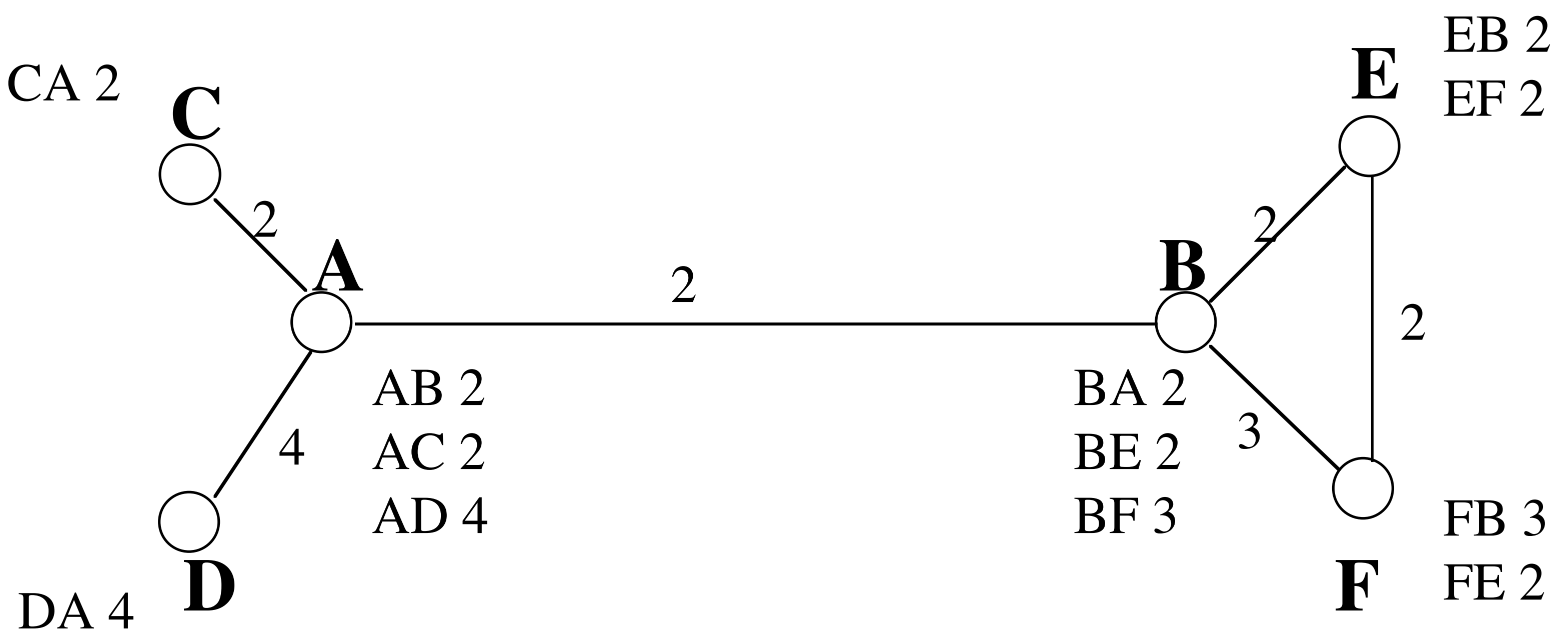
tis

Routing

- routing: distributed information distribution
- forwarding: relies on router at each hop making similar decision
- risks of bad routing information
  - sub-optimal routing
  - partition
  - congestion
  - non-delivery due to packet looping in network
  - access to transmitted data

tis

Link state



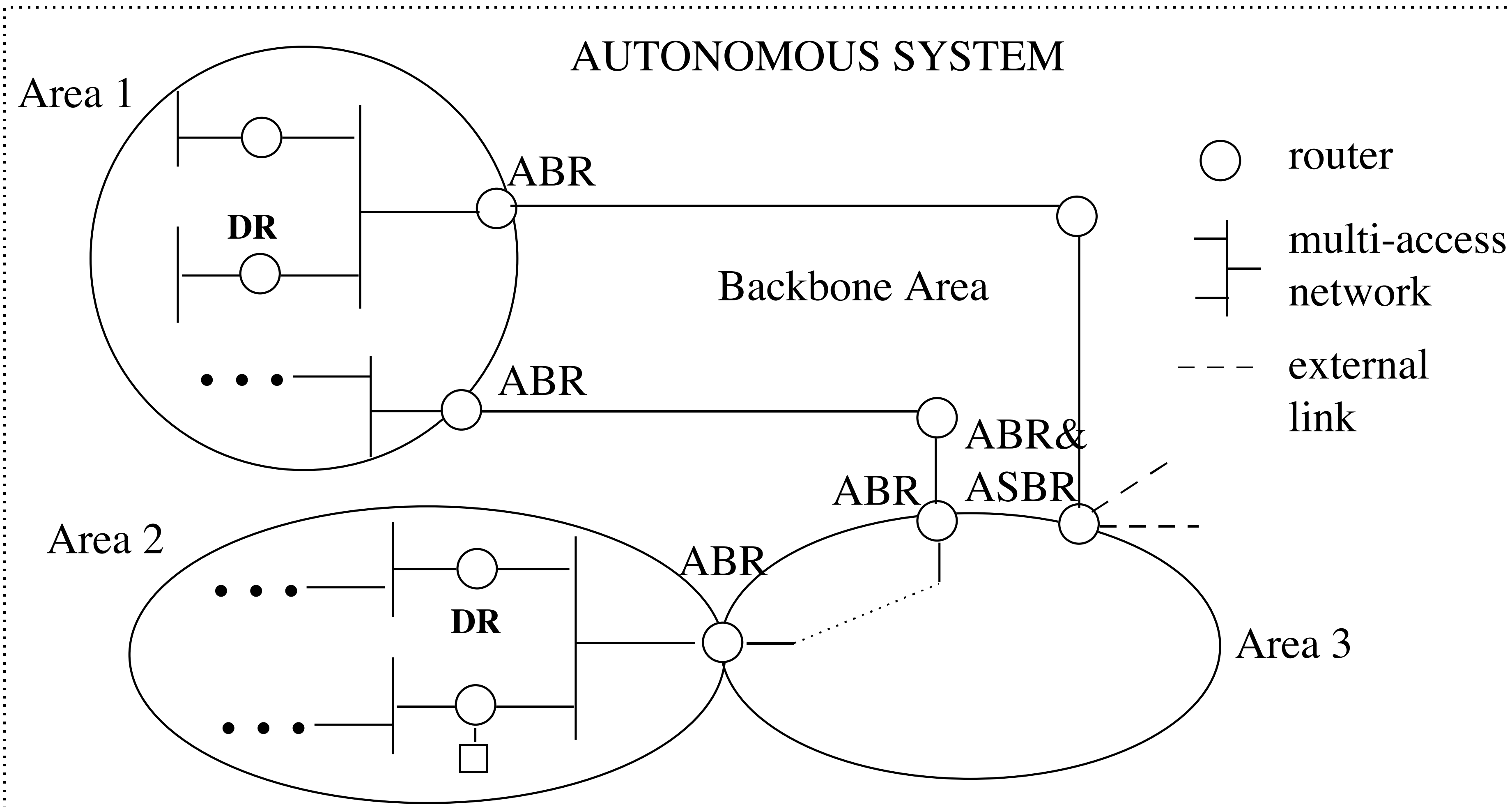
eventual database	AB 2	BA 2	CA 2	EF 2
(sane everywhere)	AC 2	BE 2	DA 4	FB 3
	AD 4	BF 3	EB 2	FE 2

Link State Properties

- each router sends info to neighbors; info eventually reaches every router in network
- each router receives info from every other router
- each router has complete topology of network on which to base decisions
- each router has same information as every other router

tis

OSPF



ABR: Area Border Router

ASBR: Autonomous System Border Router

DR: Designated Router

Behavior

- hello protocol finds neighbors, designated router
- databases exchanged to form adjacencies
- periodic re-issue of information in Link State Advertisements
- duplicate LSAs distinguished by sequence number and age
- no router knows of existence of other routers before hand

Solution

- use digital signature to protect authenticity and integrity of LSA
- sign LSA, flood as usual, verify on receipt
- use keyed MD5 to protect neighbor-neighbor protocol exchanges
- not new concept: Radia Perlman, IDPR, Crowcroft/Kumar, Finn

MAXAGE

- problem: modified everywhere, can't be included in signature
- solution: include age when age=MAXAGE
  - can still be used to flush
  - can no longer be used to expedite death-by-old-age

Key Management

- distribution:
  - query/response (i.e. send for certificates)
    - not suited for real-time behavior of routing protocol
  - in-line
    - introduce new LSA with public key, alg, router role
    - signed by Trusted Entity
- revocation:
  - independent revocation lists: not suitable for environment, e.g. Trusted Entity is not on-line
  - increasing sequence number: chosen method

Using authenticated information

- pure area: business as usual
- mixed environment area:
  - must originate signed *and* unsigned LSAs
  - to use signed information:
    - source routing
    - TOS routing: can only work within TOS connected area

Remaining vulnerabilities

- authentication vs authorization
  - ASBR: no way to check
  - ABR: each ABR could publish every ABR's info
  - internal routers: must be trusted
    - authorization for networks announced can be signed by trusted entity and included in public key LSA
  - router role (ABR, ASBR) already included in public key LSA

tis

Remaining vulnerabilities

- MAXAGE
  - speedup of aging possible but not effective or deterministic
  - could separate flush and aging mechanisms
  - but still could not allow expedite of death-by-old-age
  - speedup of aging still possible

Performance

- space: doubles (or more) size of database
- time:
  - signing is not problem, verify is
  - 180 millisec with standard software, 270 microsec optimal
  - solutions:
    - hardware: separate processor, hardware assist
    - protocol change: batch information into packages
    - operational change: verify periodically

tis

Implementation

- prototype implemented as modifications to commercial package
- prototype does not do TOS ("pure" area only)
- moving now to GateD version; TOS will be implemented

tis