

Protecting IPv6 AODV against impersonation attacks

Claude Castelluccia (INRIA)

Gabriel Montenegro (SUNLabs Europe)

June 2002

Problem Statement

- *Source-initiated On-Demand Driven Ad-Hoc Routing Protocols* (such as AODV, DSR,...) create routes only when desired by the source node...
- When a node (S) requires a route to a destination (D), it initiates a *route (or path) discovery process*.
- In AODV:
 - the source S broadcasts a RREQ for D
 - intermediate routers record the neighbor from which the RREQ is received- establishing a reverse path i.e. a path to S
 - the source or an intermediate node with a fresh enough route responds by unicasting a route reply (RREP) back to the S.
 - intermediate routers updates their forwarding table for D.
 - a bidirectional path is created!

Impersonation Attack

- The route discovery process is subject to the impersonation (redirection) attack:
 - anyone can send a RREQ on behalf of S and redirect S ' traffic.
 - anyone can reply to a RREQ with a fake RREP and hijack D 's traffic!
- How to solve this problem?
 - A host S that sends a RREQ MUST prove that it owns its address
 - ... S signs its RREQ and P signs its RREP (as suggested in [SAODV])....this requires that only S can issue a RREP (see slide 8)

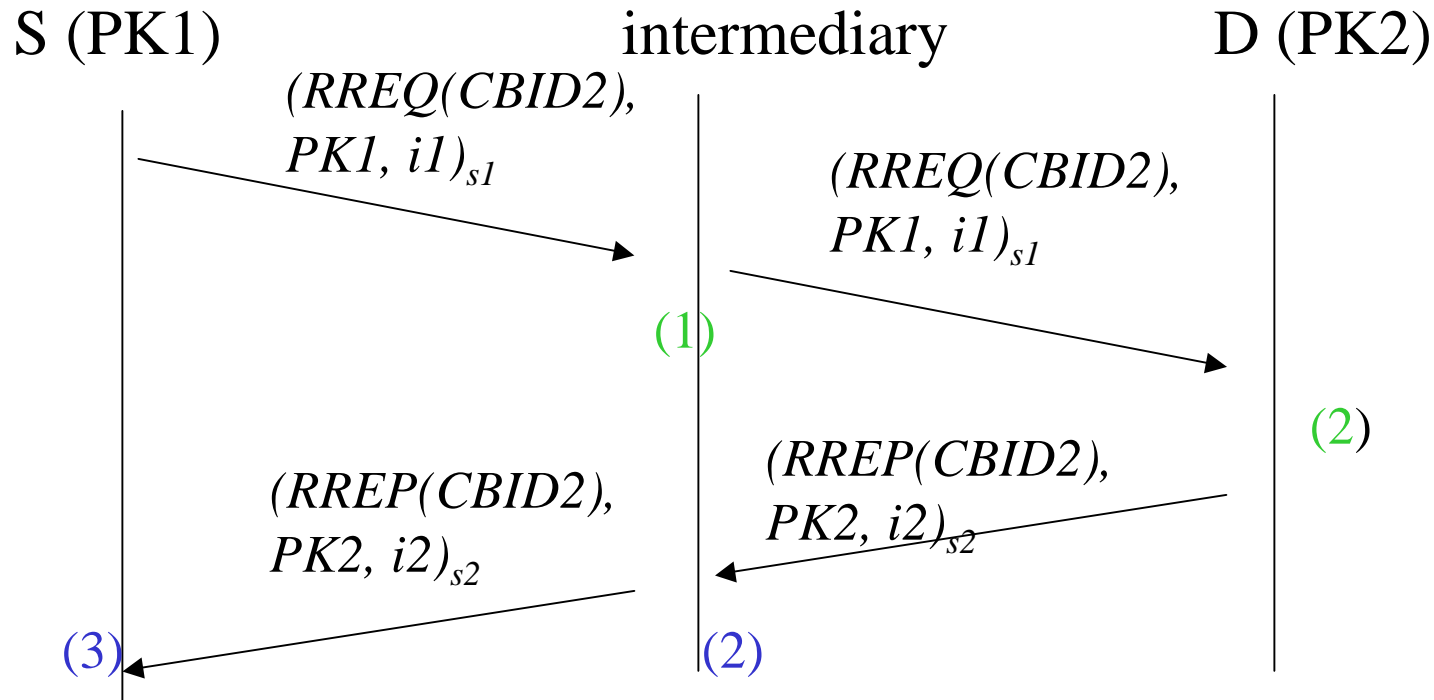
Our Proposal

- But How does D verify S 's signature on the RREQ? [Or, inversely, for S to verify D's signature on the RREP?]
 - i.e how do we bind the PK to the address
 - relying on a CA is not practical in a MANET env.!!
- We propose to avoid a CA by binding the hosts' addresses or identifiers to their public key .i.e. by using *Crypto-based ID's* (**CBID's**).
- IPv6 (unicast) address format:
 - prefix (64 bits) + HostID (64 bits) = 128 bits
 - IPv6 CBA: HostID = hmac-64(imprint, sha1(PK))
 - PK : public key
 - imprint: a 64-bit field (0's if not specified)
- CBI = hmac-128(imprint, sha1(PK))

Our Proposal (cont.)

- *Without loss of generality, we use the term CBID for CBI's, CBA's (which have an embedded CBI in the bottom 64 bits), or variations thereof.*
- Since CBIDs are statistically unique, a host only has to prove that it knows the private key (by signing) to prove that it owns the address or identifier...and that it is not using someone else's CBID...
- NO infrastructure required: crypto relation between address and signature...well suited to MANET environments.....
- a malicious host could only steal a CBID if:
 - 1: it can find the private key or
 - 2: it can find a public/private key pair that hashes to the target CBID
 - both are very difficult !

CBID-AODV

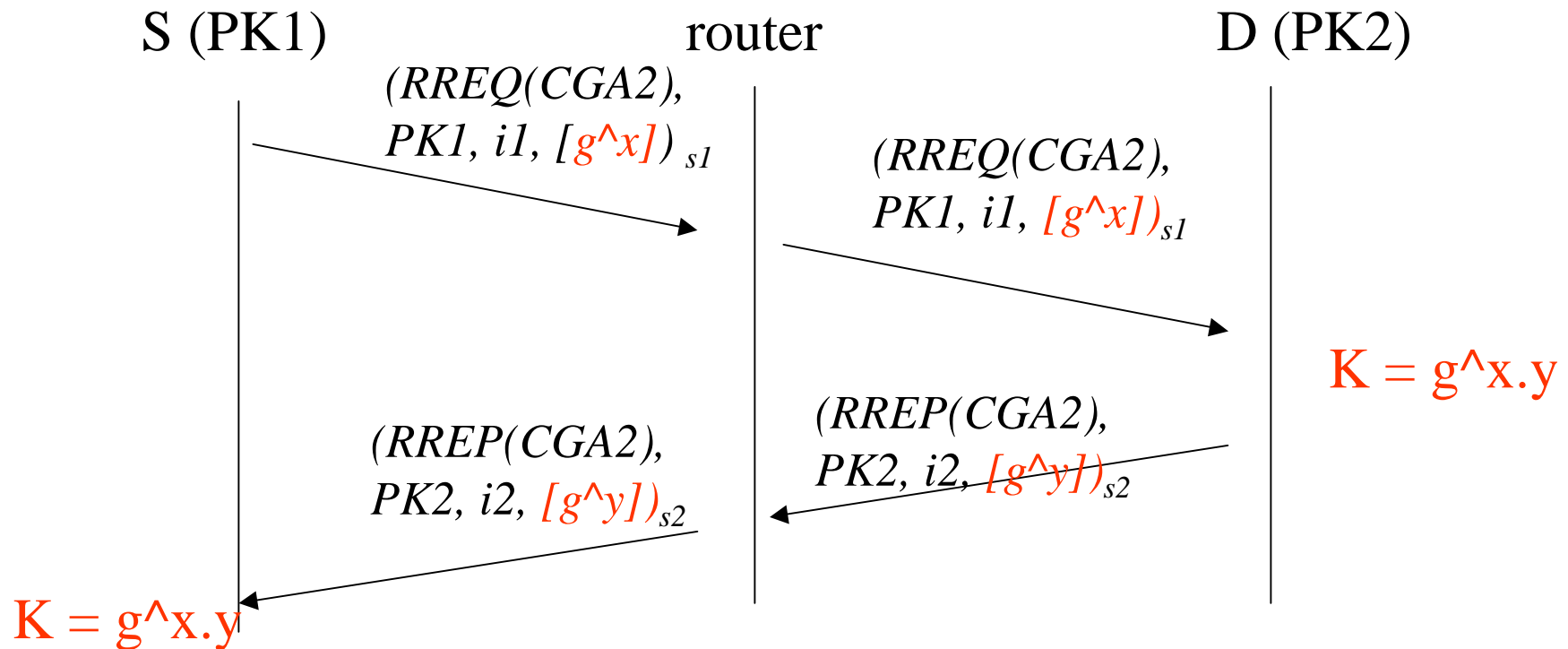


```
if (CBID2 == hmac(PK2, i2)){  
  if (signature correct) {  
    update route to D;  
  }  
}
```

```
if (CBID1 == hmac(PK1, i1)){  
  if (signature correct) {  
    update route to S; }  
}
```

CBID-AODV (2)

- Note that optionally the protocol can be extended with a DH exchange
- This allows S and D to share a secret that could be used to protect subsequent traffic...



AODV Extensions

- In our proposal only the destination is allowed to reply to a RREQ with a RREP
 - we proposed to add a D flag in the RREQ
 - when set it indicates to intermediate nodes that they must not reply to the RREQ.
- We propose RREQ and RREP signature extensions
 - that contains the signature
 - the public Key material, imprint...
 - the signature algorithm??
 - TBD...

Conclusion/Future Work

- We propose a protocol that (partially) secures AODV routing protocol without using a PKI or TTP...
- Should the routing fabric add and check signatures (or preferably MACs) of other intermediate systems?

Conclusion/Future Work (cont)

- The future work concerns efficiency
 - Our proposal requires that:
 - (in the worse case i.e. when the intermediate routers do not reject the RREP or RREQ) the source and destination perform one signature generation + verification per path discovery
 - the intermediate routers *optionally* perform 2 signature verifications...
 - How we reduce the Crypto. operation cost?
 - A low cost signature scheme is required