



# Delay-Tolerant Security Key Agreement (DTKA)

Scott Burleigh  
Jet Propulsion Laboratory  
California Institute of Technology

31 May 2013

This research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration. (c) 2013 California Institute of Technology. Government sponsorship acknowledged.



# Security and Key Exchange

---

- In the Internet:
  - Security keys can be – and are – established by negotiation.
    - Internet Key Exchange (IKE): a 4-message initialization exchange (2 round trips) in IKEv2.
    - Transport Layer Security (TLS): 13 messages (2 round trips) to initialize a session.
  - A public key and its authenticating certificate can be obtained by querying the owner of the key (e.g., a server) before beginning secured communication.
- In DTN:
  - Security keys can't be negotiated: the communication opportunity might end before initialization has completed.
  - Public keys and certificates can't be obtained by query: the communication opportunity might end before the key is disclosed.



# Key Management in DTN (1 of 5)

---

- A single-use symmetric key – generated by the sender, encrypted in the receiver’s public key, and used to encrypt the payload – can be attached to each bundle. “Session keys” are possible but not necessary.
- Public keys can also be used for computing and verifying integrity signatures:
  - A hash of the bundle is encrypted in the sender’s private key.
  - Hash decryption in the sender’s public key proves authenticity.
- All nodes can generate their own public/private key pairs.
- Asserted public keys can have associated intervals of validity, after which they are automatically revoked.



# Key Management in DTN (2 of 5)

---

- Public keys can be asynchronously asserted by their owners, e.g., by multicast. No need to query for them.
- **But** nodes can't simply assert public keys to one another: there would be no assurance that a public key asserted for a given node was authentic.
- Suppose a node is physically compromised, to the point at which its current private key is exposed to the attacker.
  - The attacker can now decrypt all confidential information transmitted to this node.
  - The attacker can also induce the node to announce a new public key – paired with a private key that is known to the attacker, and certified in the node's current private key – to the network at any time.



# Key Management in DTN (3 of 5)

---

- The network's only defense against such an assault is to “revoke” the current public key of the compromised node.  
But:
  - Which node can be trusted to issue such a revocation? (Inauthentic key revocations could seriously damage the network.)
  - In order to reinstate the compromised node following its recovery, it would be necessary to once again issue a new public key for that node. But which node can be trusted to issue that reinstatement key? (If the node itself were authorized to issue such a key then the node could reinstate itself while still under the control of the attacker.)



# Key Management in DTN (4 of 5)

---

- Moreover, when new nodes are instantiated, if their initial public keys are self-generated and self-certified then the nodes receiving those keys have no way of knowing whether or not they are authentic and whether the nodes themselves are trustworthy.
- In short, the missing component to DTN security key administration is a central key authority that can be trusted to issue and revoke the public keys of all nodes in the network.
- But the design of such a central key authority must be approached with care...



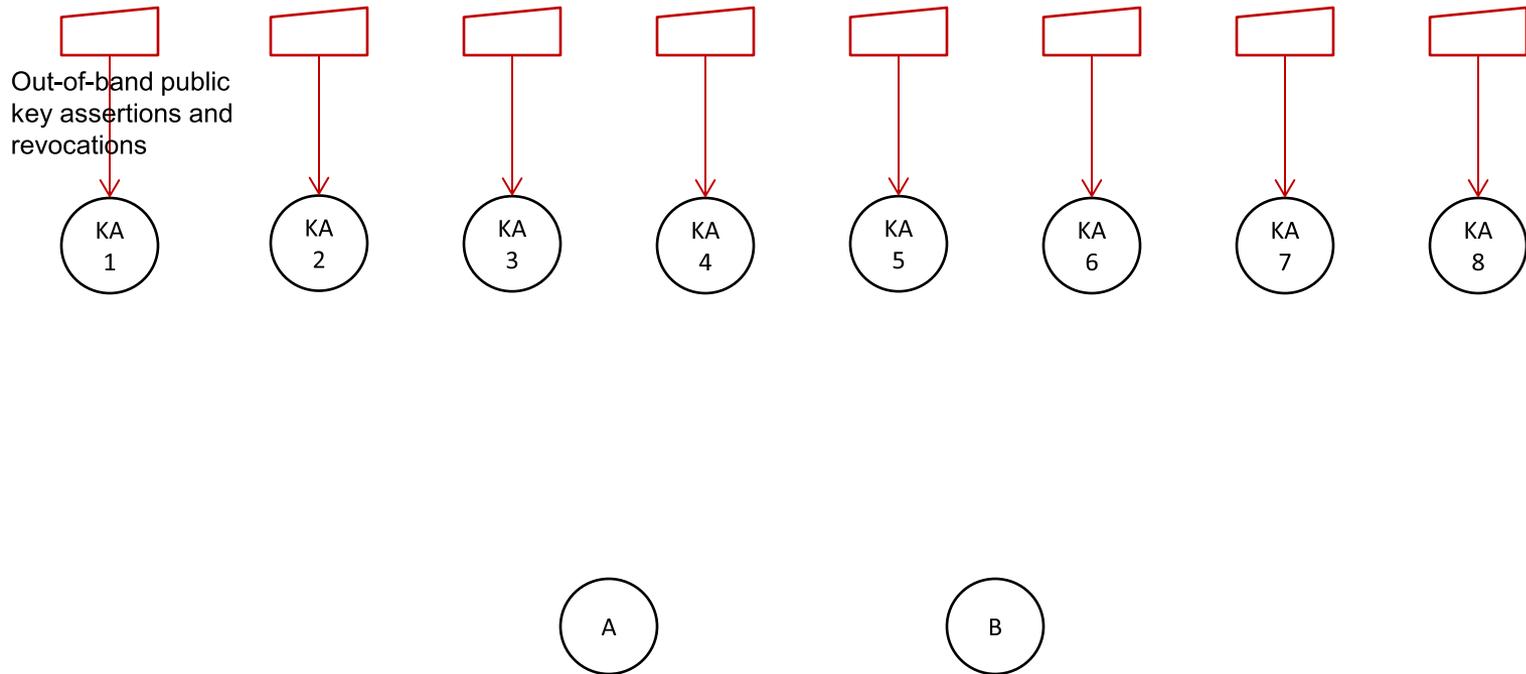
# Key Management in DTN (5 of 5)

---

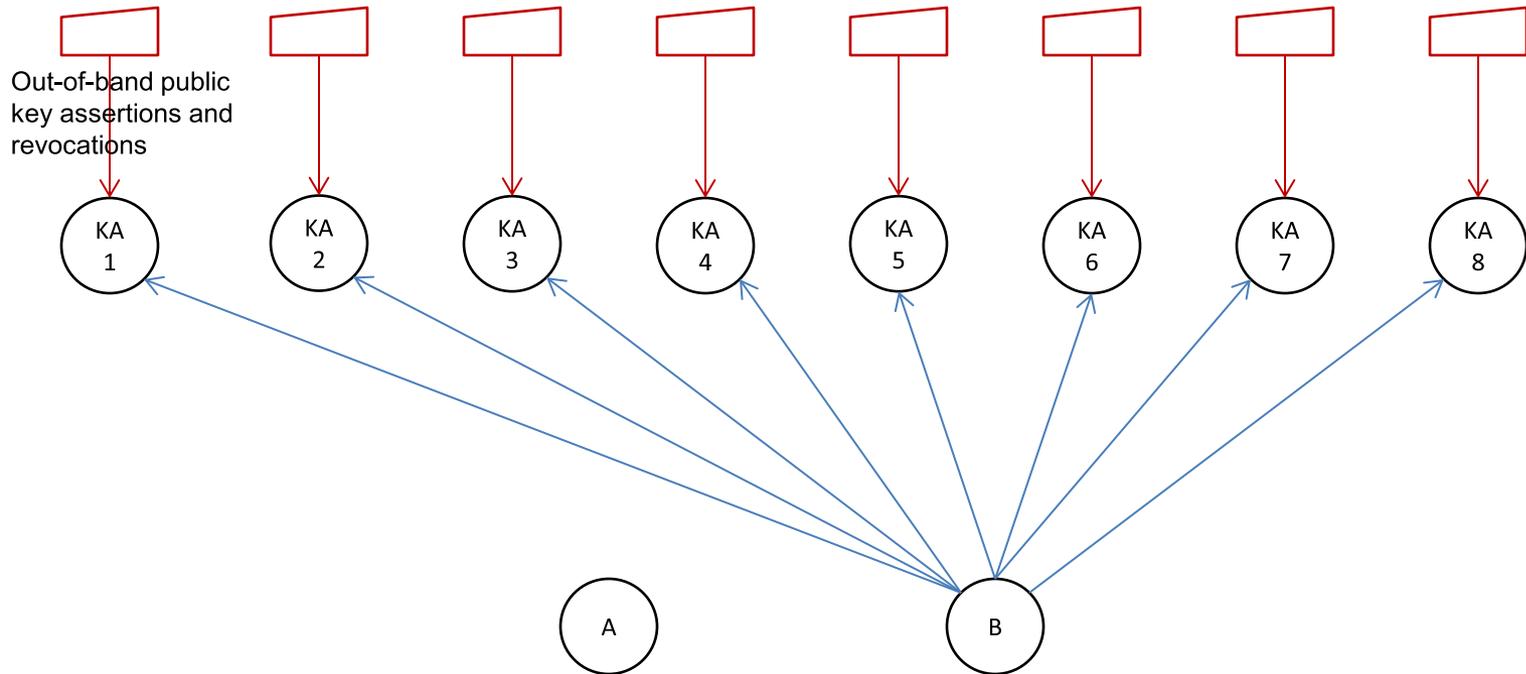
- The key authority must not be a single point of failure: loss of the trusted authority would cripple the network.
- But redundancy is not enough, because a key authority node might itself be compromised by an attacker: the distribution of bogus keys to all nodes, or the revocation of all keys, would likewise cripple the network.
  - No single key authority node can be granted unilateral key distribution authority. Key administration proclamations must be issued by agreement among multiple key authority nodes.
- Nor may any single key authority (potentially compromised) be permitted to sabotage key distribution by simply refusing to agree. What's required is agreement, not consensus.



# A Key Management Proposal for DTN



Assume  $N$  key authority (KA) nodes in the network (here  $N=8$ ). All KA nodes have all current key information for the network, as far as possible. All credible assertions of key revocation and reinstatement are provided to KAs by an out-of-band mechanism, such as a human network security analyst.



Each node generates its own public/private key pairs periodically, multicasts its public keys to all KA nodes in advance of effective time. Two types of key information messages: Node B asserts its new self-generated public key, KA<sub>x</sub> publishes bulletin of new public key assertions and revocations.



# Assertion of Public Key by Node B

---

Sign in current private key of B

Message from B

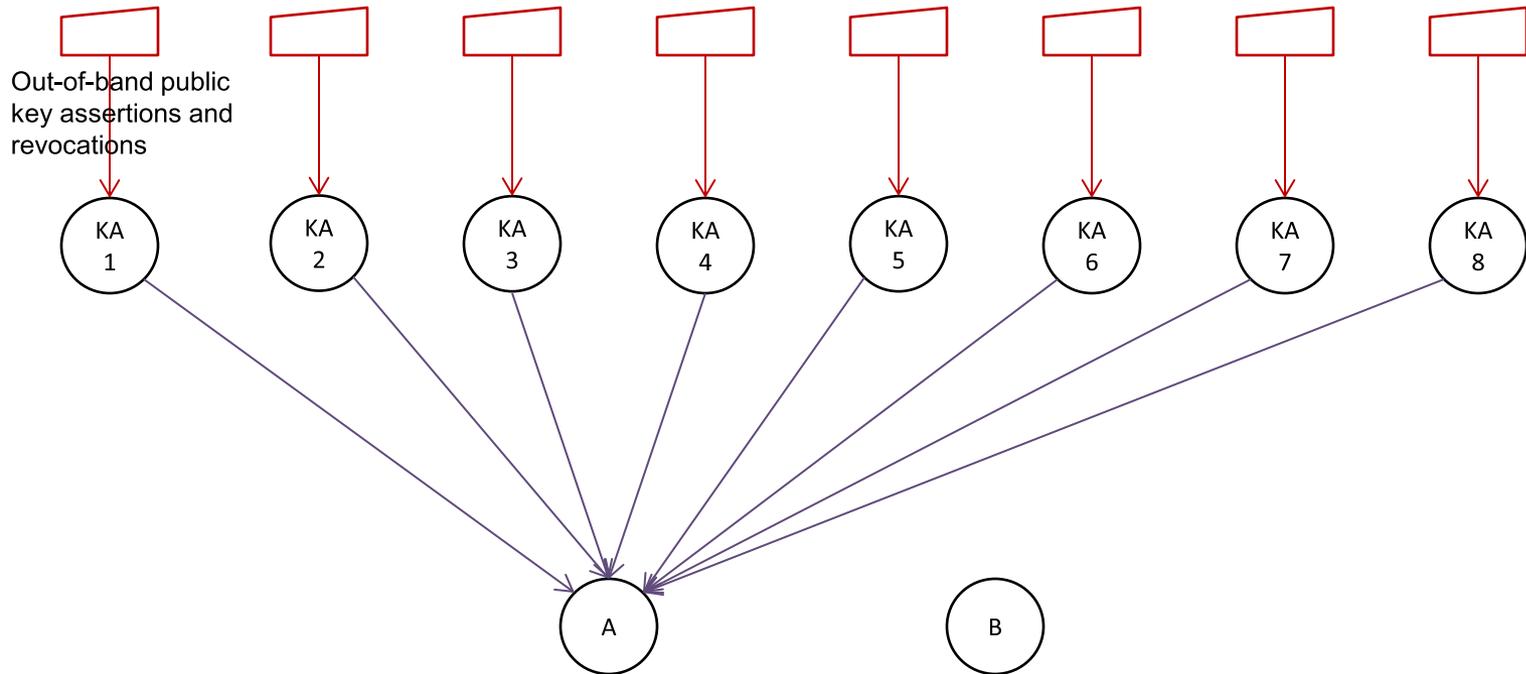


# Erasure-Coded Messages from KA

- Identical reports (associations, revocations) are generated simultaneously by all KAs, and hashes are computed for the generated reports.
- At each KA, the report is erasure-coded:  $Q + k$  code blocks are generated such that the reception of any  $Q$  different blocks will enable acquisition of the original report.
- At each KA, only a subset of the generated code blocks are transmitted. The distribution of key information relies on the acquisition of code blocks from multiple collaborating key authorities.
- Suppose  $Q=7$  and  $k=1$ , for a total of 8 blocks. Each KA then only multicasts 3 blocks:

KA	0	1	2	3	4	5	6	7
1	x	x	x					
2		x	x	x				
3			x	x	x			
4				x	x	x		
5					x	x	x	
6						x	x	x
7	x						x	x
8	x	x						x

So 24 blocks are multicast. Receiving any 7 distinct blocks will deliver the report (because  $Q = 7$ ).



Only messages with the same hash will be reassembled into the report, so if any KA is inadvertently out of agreement its report will be ignored.

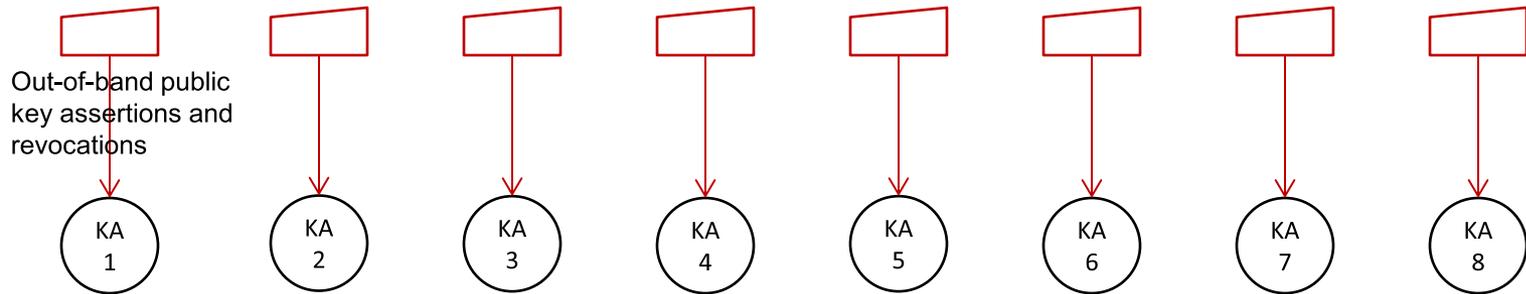


# Code Block of Report from KA

---

Sign in private key of KA<sub>x</sub>

Report hash	Code block of report
----------------	-------------------------



Asserted key information is used when its effective time range is reached.

No negotiation, no single point of failure, no single point of authority that can be compromised.