Multicast Data Source Authentication Ideas

Atul Sharma

Nokia, Inc.

Multicast Data Source Authentication

- Need to authenticate a particular member as the sender over and above group authentication (someone in the group sent it). Should not allow a member to spoof the identity of another member.

- Can digitally sign each packet ➔ expensive in computation time and space requirements.

- Goal: How to provide Data Source Authentication, without digitally signing every packet?

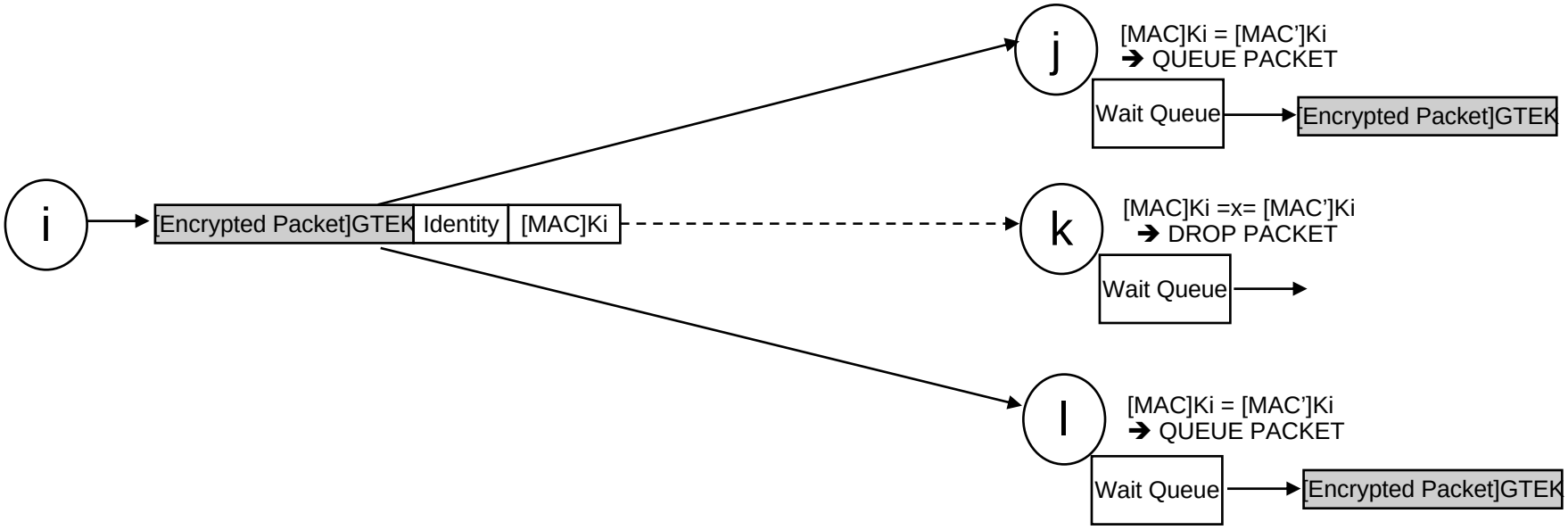
- These ideas shall be presented:
  - Recall Packet Scheme
  - Rogue Member Detection
  - Delegated Authentication Scheme
  - Delegated TESLA

Recall Packet Scheme

- Each member has a symmetric key (known to every other member) to be used to authenticate (calculate MAC) the packet.
- GTEK or another symmetric key of the member could be used to encrypt the packet.
- Each member has a public-private key pair to digitally sign the recall packet.
- The identity of the sending member is included in the composed packet:

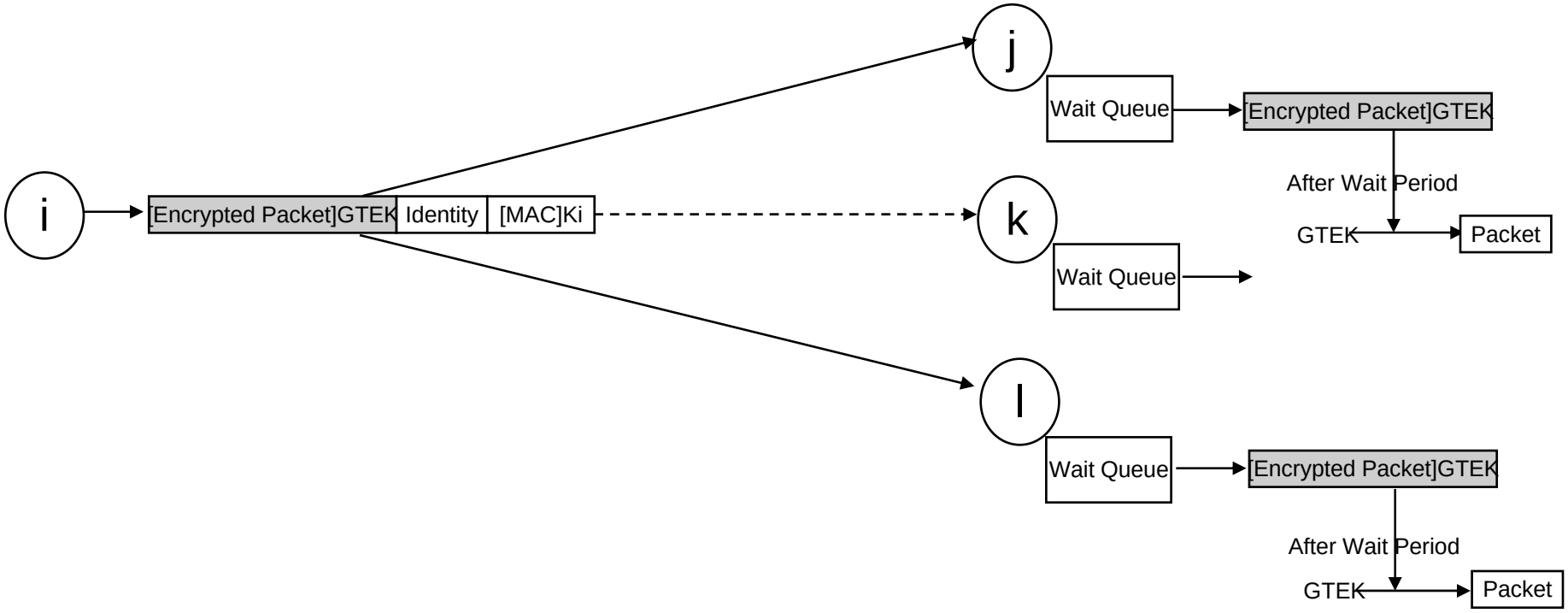
Recall Packet Scheme - II

- The Composed packet is multicast by the sending member.
- Each receiving member looks at the identity in the packet; uses the symmetric key associated with the identity to authenticate the MAC attached to the composed packet.
- The authenticated (still encrypted) packet is put in a wait queue for some wait period.



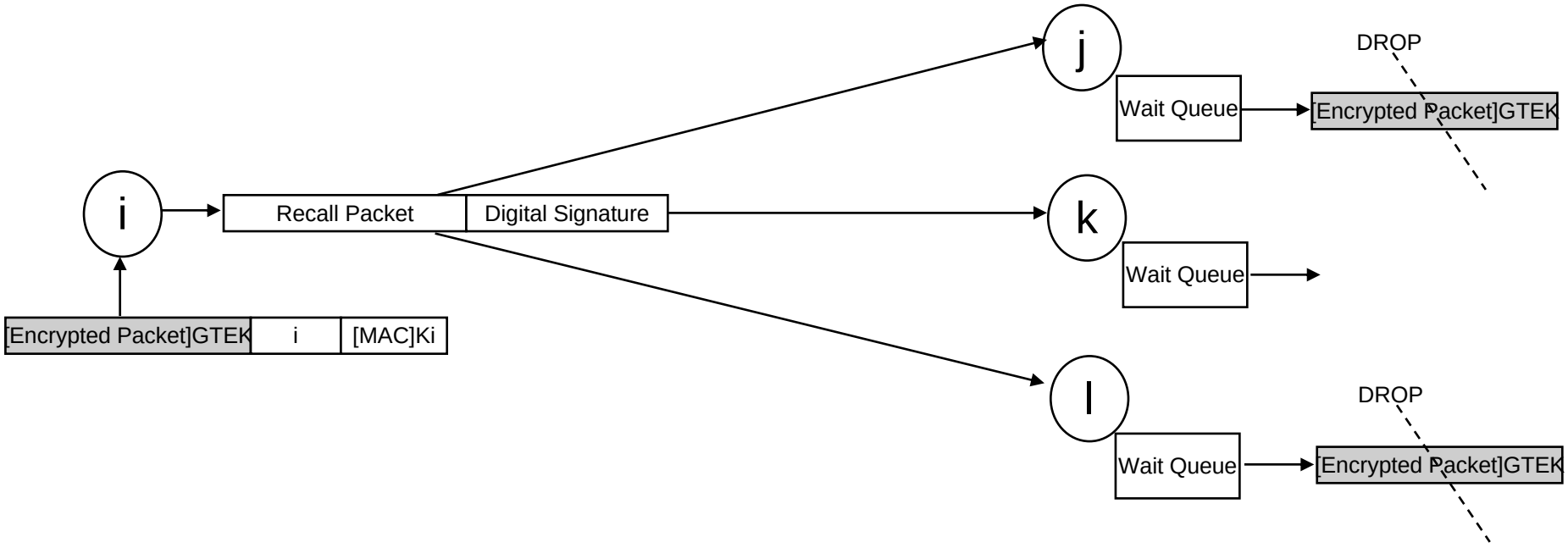
Recall Packet Scheme - III

- If in the wait period, no recall packet is received, the packet is dequeued, decrypted and accepted. If a recall packet corresponding to the packet in the wait queue is received prior to the expiry of wait period, the packet is dropped.



Recall Packet Scheme - IV

- If member “i” receives a packet seemingly coming from member “i”, it digitally signs a recall packet with its private key of the public-private key pair and multicasts to the group. The recall packet can use the IP identification of the original packet in identifying the packet to be recalled.
- The recall packet may be an ICMP packet with a new type and code.



Problems with Recall Packet Scheme

- Vulnerable to packet losses. What if the recall packet gets lost?
  - ➔Institute some kind of handshake to ensure delivery of Recall Packet?
  - ➔Any Other suggestions?
- Vulnerable to Denial of Service from a rogue member, spoofing packets, keeping the whole group busy with processing of Recall Packets.
  - ➔Develop some Rogue member identification scheme?

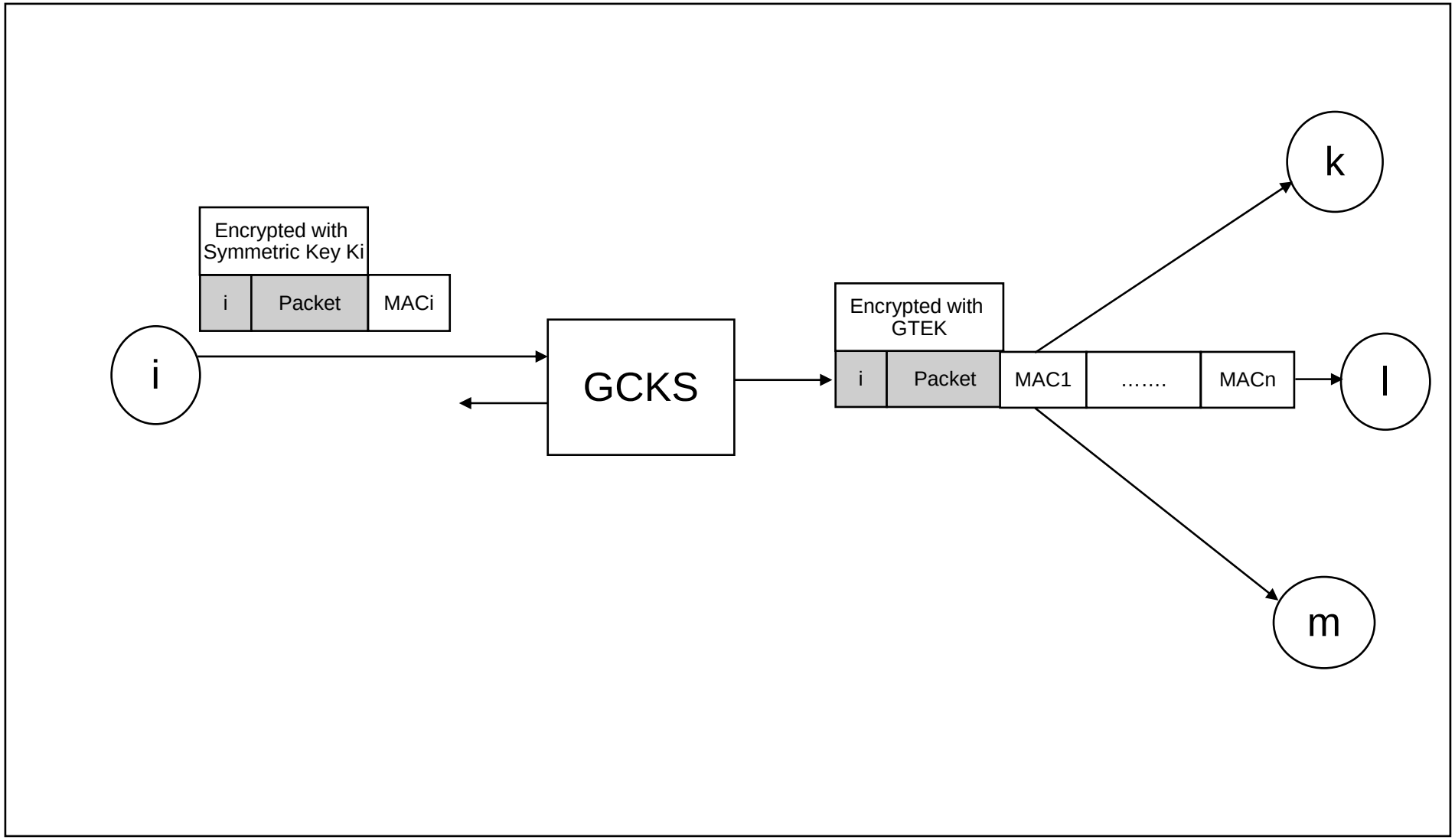
Rogue Member Detection

- Possible Solutions:
  - Based on the layer-2 addresses, IP addresses ➔ can be spoofed; not applicable always
  - Retrace the spoofed traffic ➔ Should be able to do better, as the multicast group members are known. Not easy to do (spoofed traffic has to be continuously flowing; what if multiple members behind router?)
- A new scheme to work with the mechanism just outlined:
  - Member “i” on finding that it is being spoofed instead of sending Recall Packet, initiates Rogue Member Detection. Notifies GCKS.
  - GCKS re-keys in a way that further spoofed traffic is identified as coming from the Rogue member.

Delegated Authentication Scheme - I

- Every member has a set of two symmetric keys with a centralized entity GCKS(?), which all the members trust.
- Sending member encrypts the packet with a symmetric key and authenticates the packet with a (may be another) symmetric key it shares with the central entity.
- GCKS authenticates and decrypts the packet.
- Data Source authentication between the member and GCKS is immediate, as it is between two parties. There is no man-in-the middle attack from within the group possible, as no other member in the group knows the symmetric key this member shares with the GCKS.
- GCKS puts the packet and sending member's index, encrypts it with the GTEK and authenticates by attaching a MAC for each member using the symmetric key it shares with the member. That basically means attaching N MACs with the packet for a N-member group.

Delegated Authentication Scheme - II



Problems with Delegated Authentication Scheme

- Attaching N MAC's with every packet is not going to scale well. There shall be small window for values of N, where such a scheme is going to be practical.

- GCKS can be overloaded and become a bottleneck in the secure multicast communication.
  ➔ Allow a hierarchy of GCKS's.

Delegated TESLA

- Delegated Authentication has problems. But can be a value add for other schemes like TESLA.
- TESLA assures that somebody with the time-delayed key chain is transmitting the traffic. But it is still possible for a Rogue member to launch a Denial of Service attack by transmitting phony traffic. (By instituting a group wide symmetric key MAC, we can prevent an outsider to launch a DoS attack)
- Merging Delegated Authentication with TESLA assures that GCKS authenticates the sender with the shared secret and then uses globally known time-delayed symmetric key chain scheme of TESLA to do authenticated transmission.
- Every member trusts the GCKS. GCKS verifies to the whole group that member “i” is transmitting this traffic. Use of TESLA assures that we use time-delayed symmetric key chain scheme to provide data authentication.
- There is a value-add in using Delegated Authentication with TESLA:
  - it provides another level of assurance
  - eliminates N-MAC problem.
  - prevents a Rogue member from launching a Denial of Service attack.

Future

- Solve the problems associated with each scheme:
  - Scheme(s) to identify Rogue member(s).
    - One Such Scheme presented
    - Rogue Member Detection with TESLA, how to do it?
  - A practical scheme to recover from Recall packet loss in the Recall Packet Authentication scheme.
  - A scheme to offload GCKS, so that one GCKS is not the bottleneck in the Delegated Authentication scheme.
  - Delegated TESLA
- Any of the above Working Group items?