Approaches to defend against DDoS attacks in mobile ad hoc networks

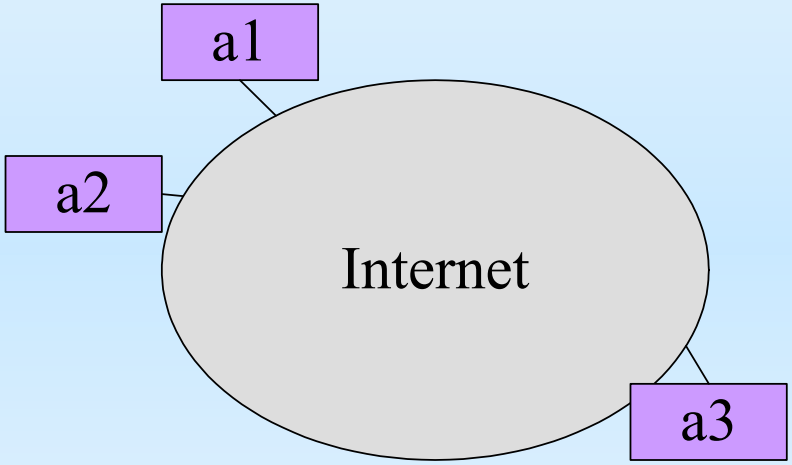
Gu, Qijun Liu, Peng Chu, Chao-Hsien
School of Information Sciences and Technology
The Pennsylvania State University
University Park, PA 16802

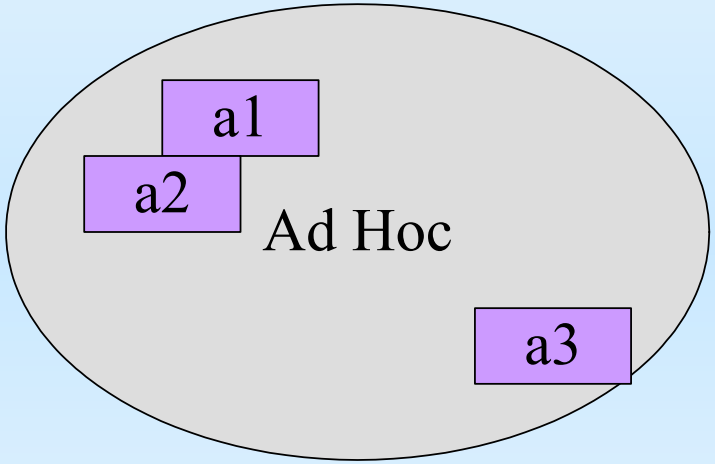
Abstract

Experiences of distributed denial-of-service (DDoS) attacks in the Internet motivate us to investigate new attack aspects and new defense technologies. First, we studied the unique properties of two types of area-congestion-based DDoS attacks in ad hoc networks, which are obviously different from attacks in the Internet in term of attack impact. We also identified some DoS attack approaches, with which attackers follow all protocols instead breaking into them, and hide their traces. Finally, we proposed a system of several approaches to defend with such attacks. Although the system is not perfect at this stage, it does provide efficient and secure countermeasures.

Introduction

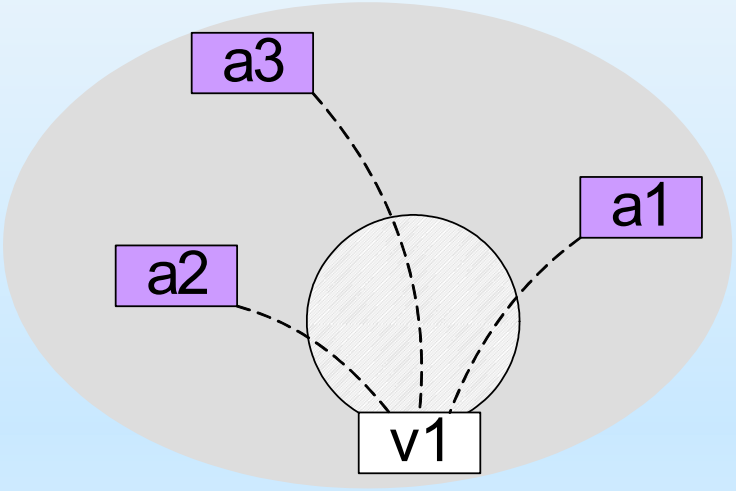
Structure difference: Internet vs. Ad hoc



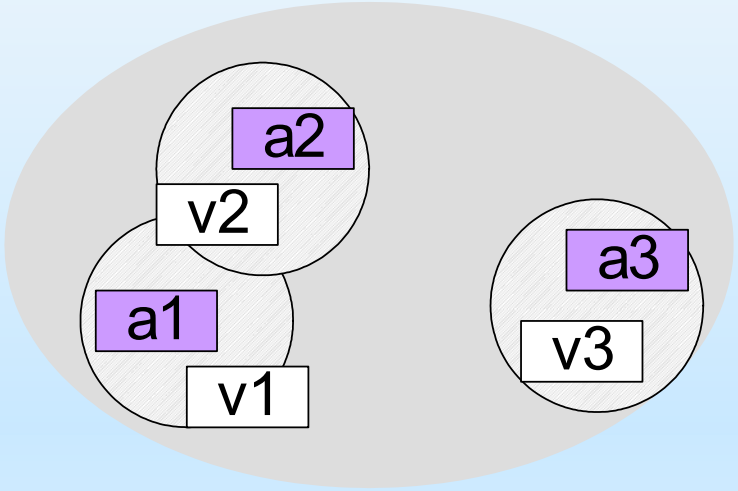


	Internet	Ad hoc	Attackers
Nodes	External	Internal	Insiders
Routers	Trustable	Untrustable	Insiders
Links	Separated	Open and shared	Insiders
Positions	Static	Mobile	Insiders

Attack properties



Remote topology



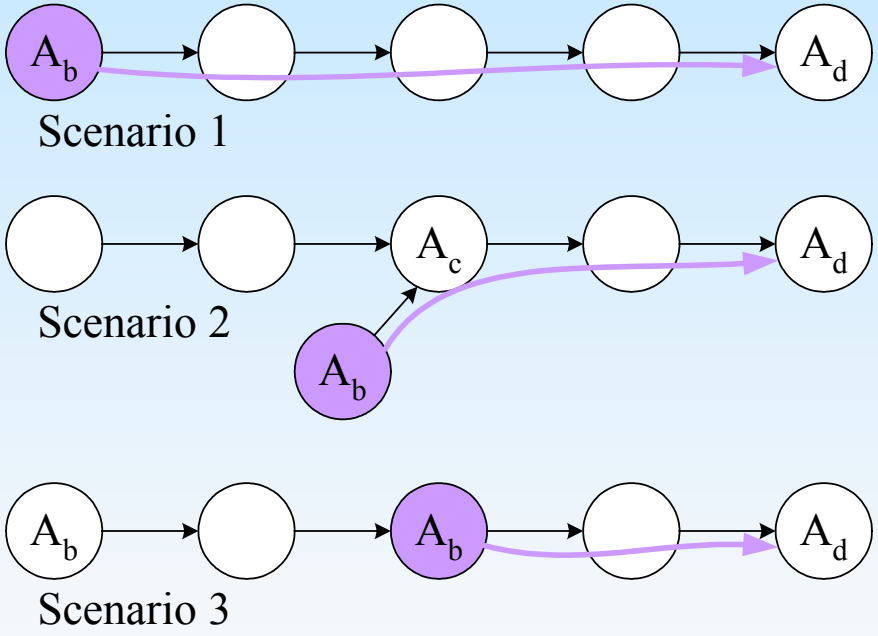
Local topology

Congestion-based: attackers congest the network-wide traffic
Area-oriented: attackers affect all nearby links
Indirect: attackers congest non-target to block the target
Volatile: even attackers don't know what are congested
Coordinated: attackers have friends

Attack approaches

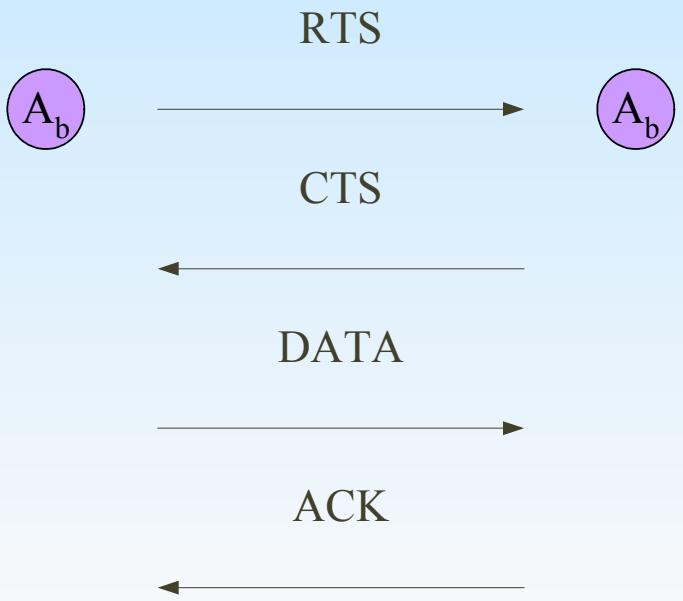
In forwarding

Flooding and injection: an attacker asks a router to forward packets in a route established securely by another source.

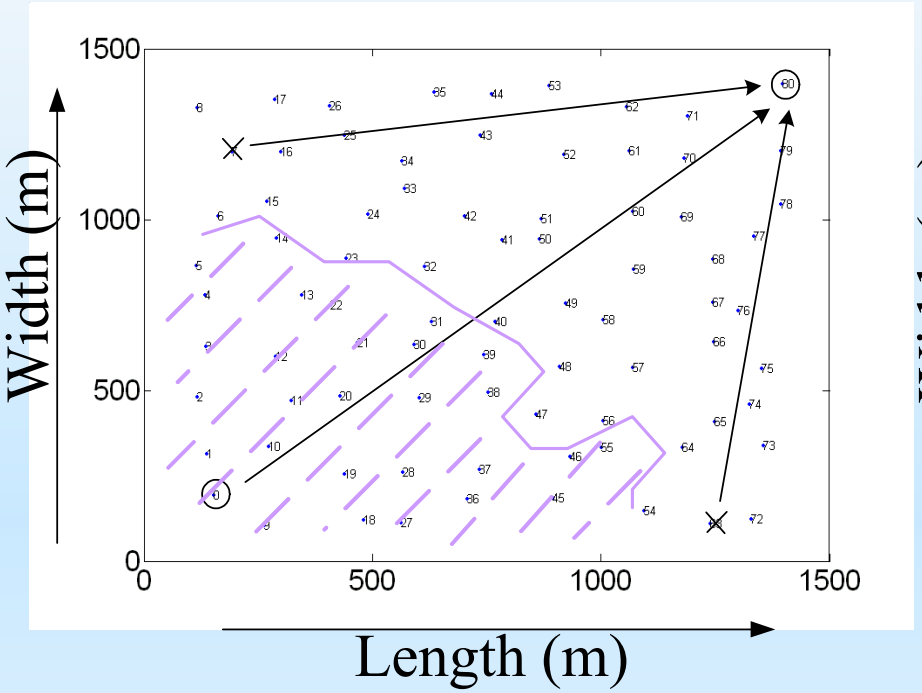


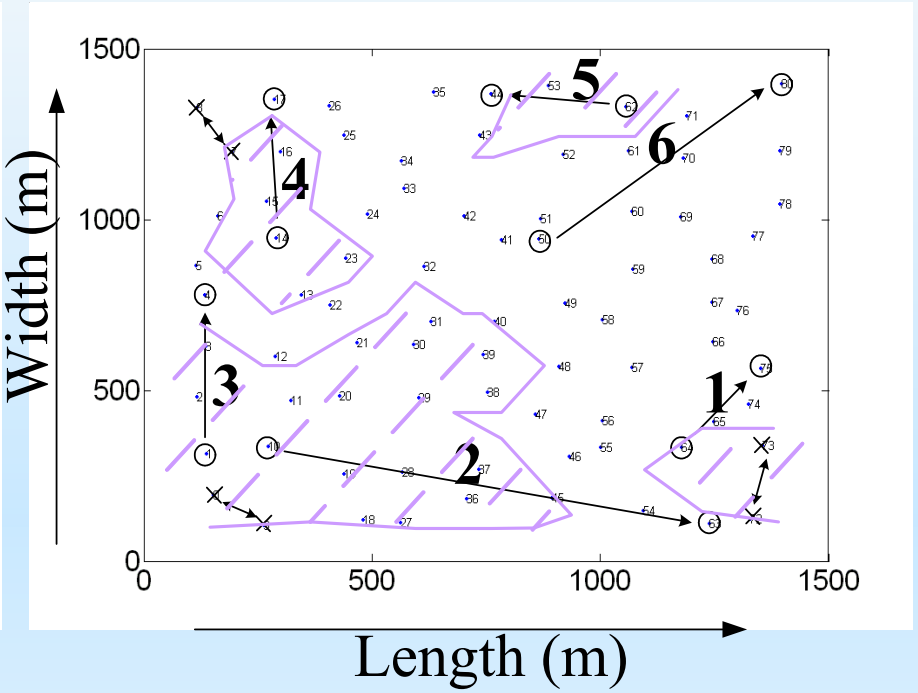
In MAC/DCF

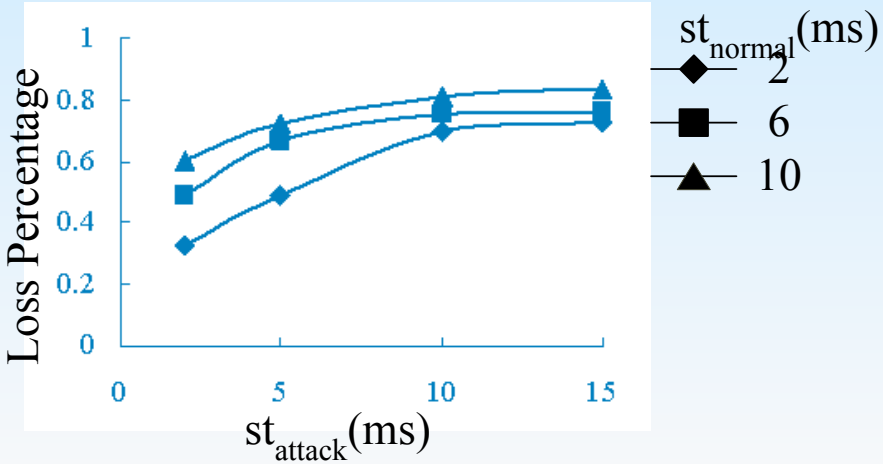
Deceiving and tricks: an attacker forges MAC packets with false duration, or smartly select certain traffic patterns.

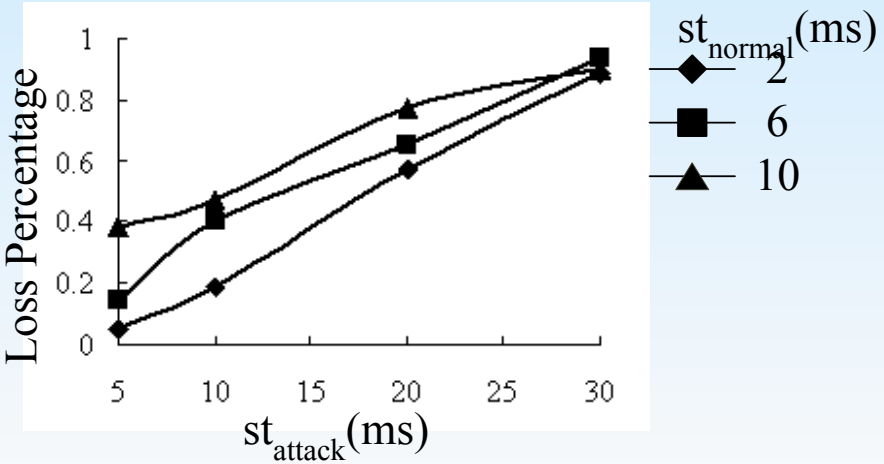


Attack Impacts



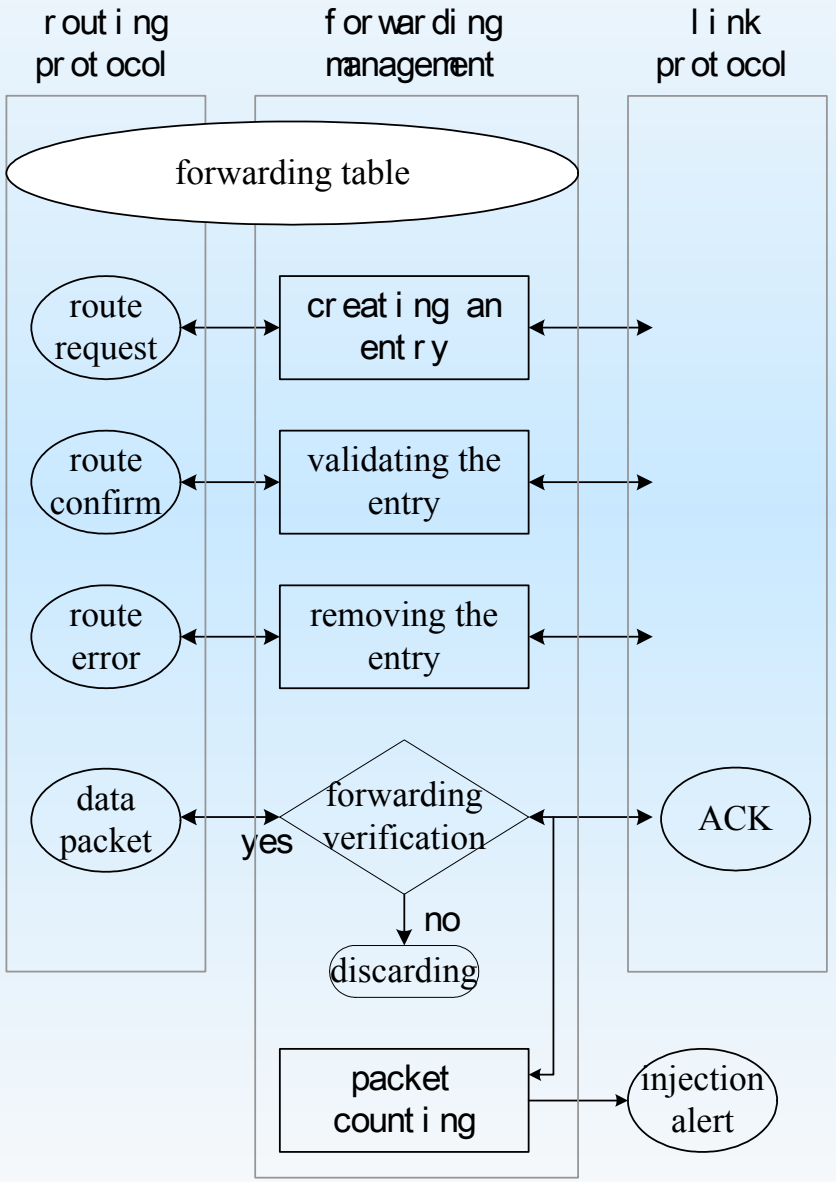






Defense framework

The defense system (right) is to address security problems identified in the forwarding part. It runs between routing and link layers, and gets supportive information from them. For the MAC problem, it is needed to physically shut down the bad nodes, and more work is deserved. The proposed system is composed of three parts (below): source address control, packet counting and detection, and forwarding authentication.

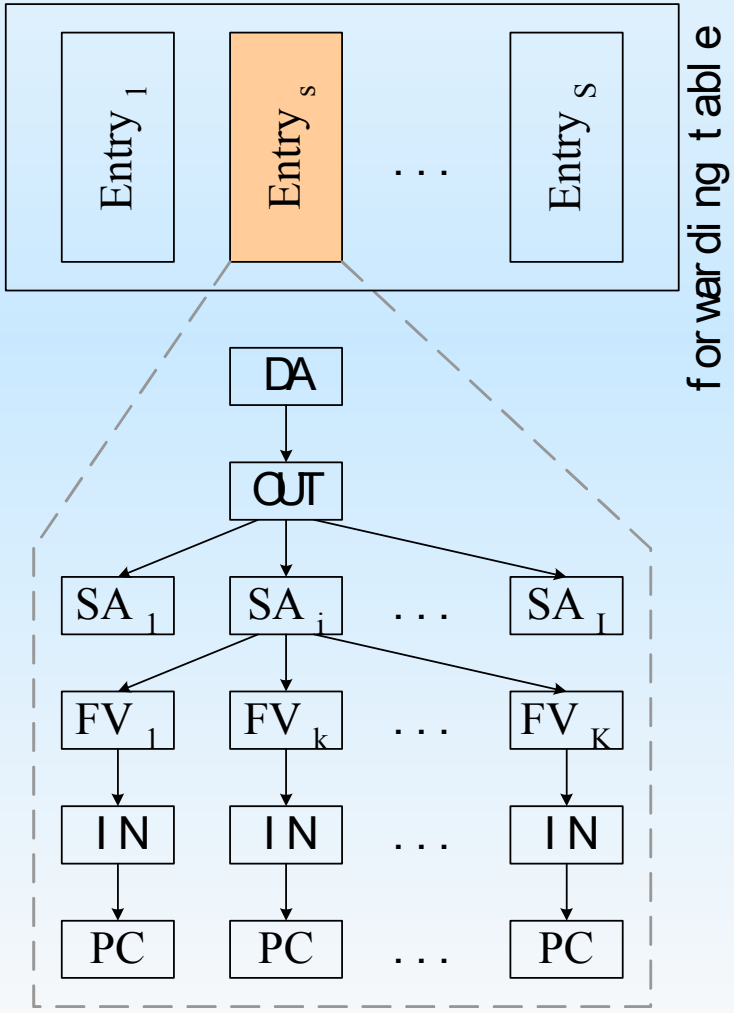


Source address control

A forwarding table is composed of multiple tree-like forwarding entries and can be considered as an extended structure of a traditional forwarding table.

To deal with complex and dynamic situations in ad hoc neworks, such as multicast, multipath, broken route, etc, and facilitate fast forwarding and other security mechanism, a forwarding entry consists of source address, destination address, previous hop, next hop, flow hash and counting fields in a tree structure.

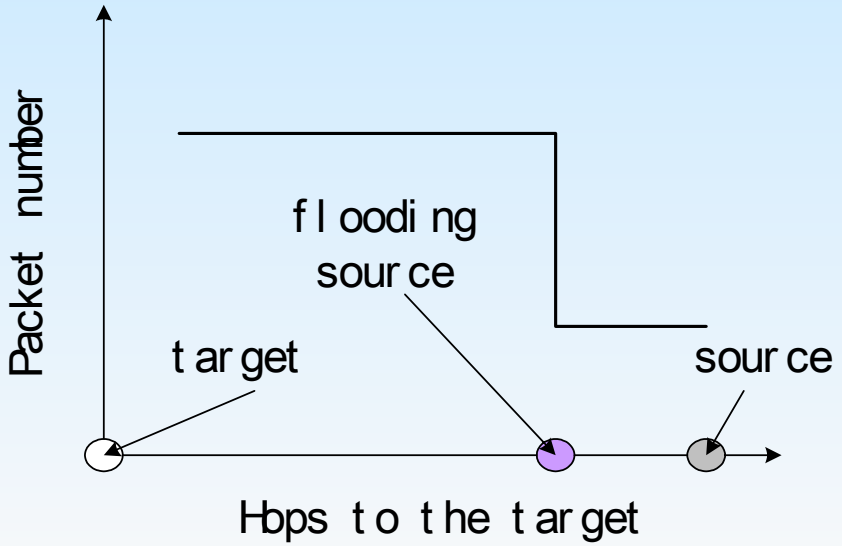
Unsolved: scenario 3 attack



Packet counting

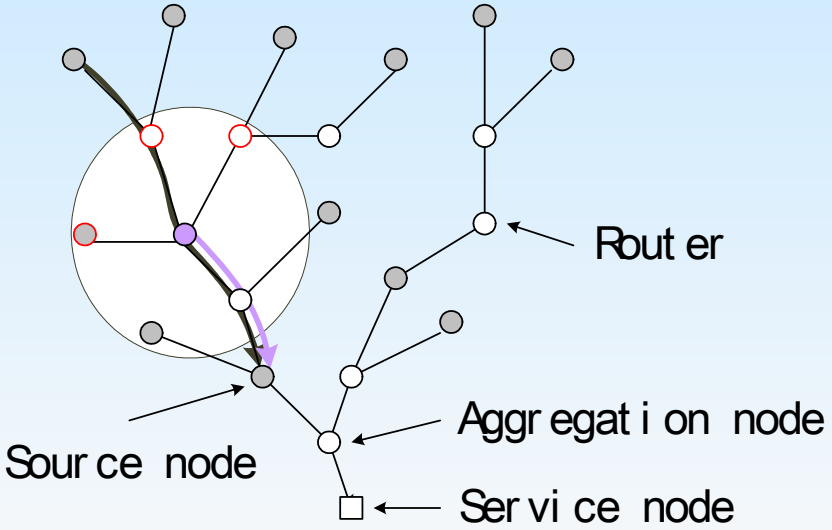
Local detection

Local data collection: audits of local communications
Anomaly analysis: a router forwards more than it should.
Local response: initiate cooperative defense action with evidence

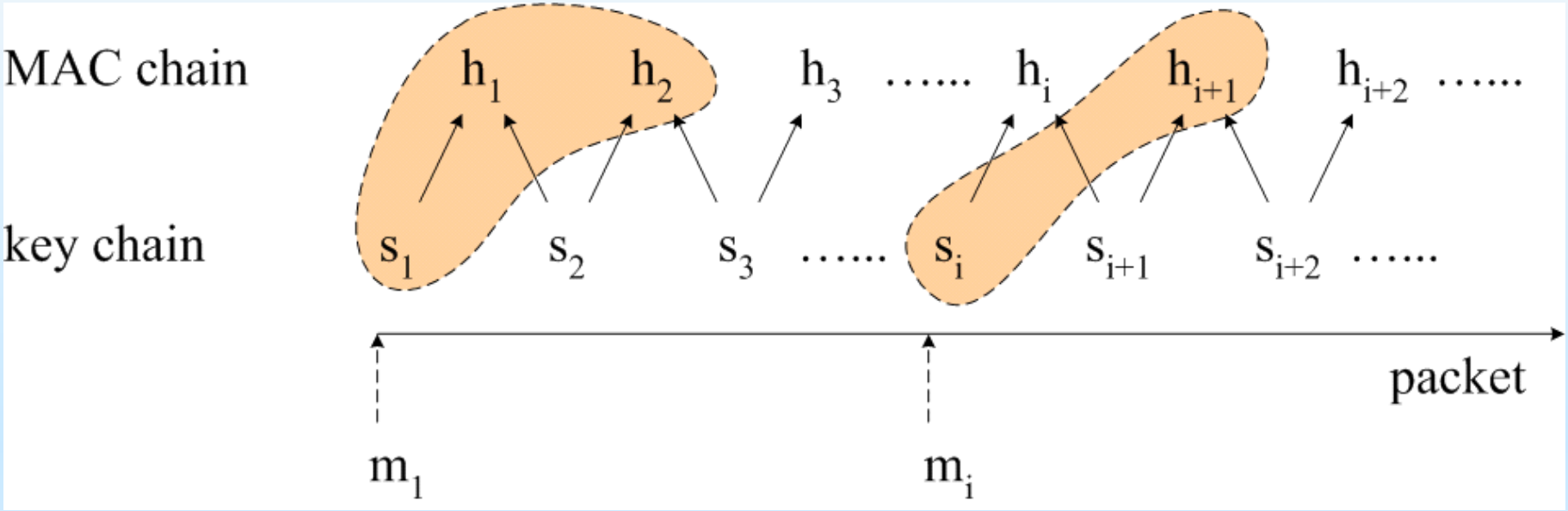


Global detection

Cooperative detection: audit exchange and decision making on majority of audits
Global defense actions: broadcast a revocation of an identified flooders.



Authentication chain



In the key chain, the source node generates keys with a pseudo random generator. Any node, except the source, cannot figure out either previous keys or future keys from the currently disclosed keys.

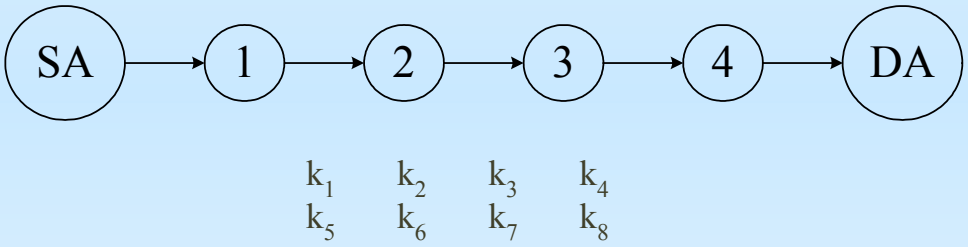
In the MAC chain, the source node computes message authentication codes (MAC) s based on the lower keys so that forwarding routers can authenticate the keys later.

Unsolved: man-in-the-middle attack to forge keys and then MACs.

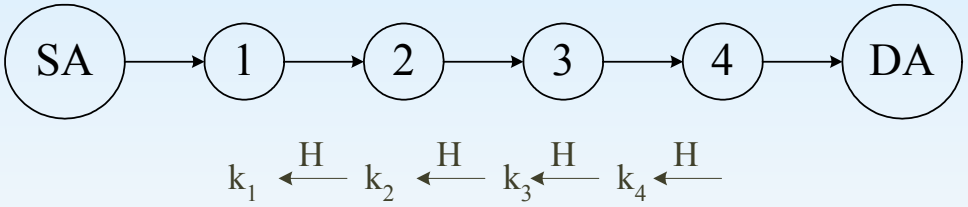
Less random keys

The unsolved man-in-the middle attack is due to the total randomness of the key chain. Two approaches can be further incorporated to address this issue.

Key inspection



One-way hash key



Conclusion and Future work

Ad hoc are still in danger with potential DoS and DDoS attacks, although many other problems have been identified and solved.

Our defense system provides intriguing security properties, such as filter useless packets injected by outsiders at the source, eliminate replay packets, detecting one inside injector collaboratively. In addition, the system works in a lightweight fashion, and is compatible with routing protocols.

The system should be extended to address situations of broken route and intermediate route reply. Implementation and evaluation of the system are needed.