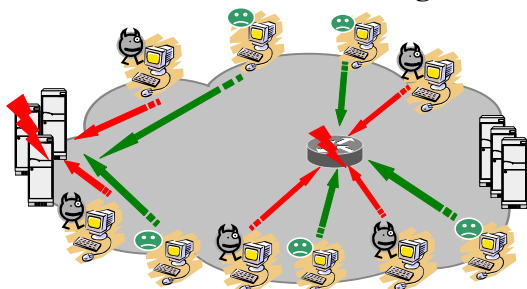




## 1 Context

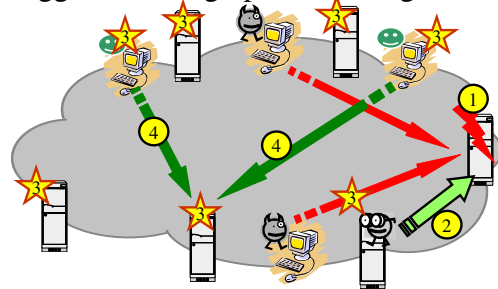
Maintaining Quality of Service Guarantees under DoS Attacks is a Challenge.



- DoS attack packets deplete resources (e.g., router buffers, server CPU time or memory structures).
- The general DoS problem is to distinguish attack packets from legitimate packets.
- Distributed DoS (DDoS) attacks exploit software vulnerabilities to capture "zombies" or "agents" and use them as attacking machines on behalf of the real attacker.
- As "agents" can be "insiders", things are even more challenging.

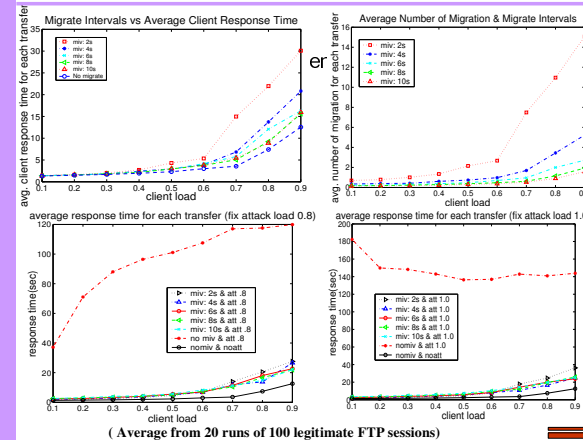
## 3 Reactive Roaming

A proactively roaming Health Monitor triggers roaming upon detecting an attack.



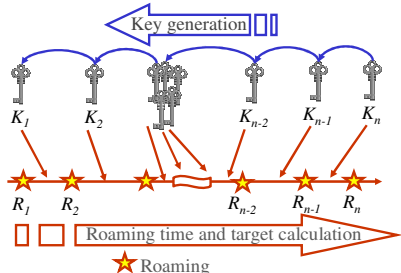
- After detecting an attack, the health monitor sends a roaming trigger to all servers and legitimate clients. Using their key chains, legitimate clients can switch to the new server.
- After roaming, either proactively or reactively, the old server is forced to flush its state and reload its system software to avoid Trojan horses.

## 5 No Attack: Low Overhead Attack: Substantial Gain



## 2 Secure Proactive Roaming

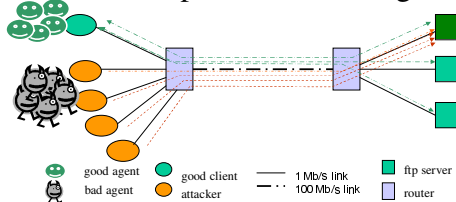
Service migrates within a pool of replicas and **only** legitimate clients can follow it. Proactive roaming is time-triggered.



- Key Generation:  $K_i = H(K)$ , for  $1 < i < n$  and  $H(\cdot)$  is a one-way hash function.
- Roaming Trigger:  $R_i, R_j = MSB_{2^m}(G(K_i))$ ,  $2^m = \max(R_i, R_j)$  for  $1 < i < n$  and  $MSB$  are the most significant bits of  $x$ .
- Roaming Target: Servers  $[MSB_{2^m}(G(K_i))]$ , where Servers is the list of  $N$  servers.

## 4 Proactive Roaming Simulation

We built a simple file transfer service which utilizes proactive roaming in NS2.



- Network topology as shown above.
- File requests of 1Mb each.
- Attackers bombard the server with requests for files.
- We simulated one type of attacks in which the attackers attack only one server.

## 6 Conclusions

- Replication provides Fault Tolerance.
- Server Roaming augments Replication with DoS attack tolerance.
- Secure Proactive Roaming is a promising direction for providing sustained QoS level in the presence of (undetected) DoS attacks.

## Future Work

- More complex attack models.
- Formal proof of the mechanism's security.
- Analytical study using Markov Chains and/or Game theoretic Models.