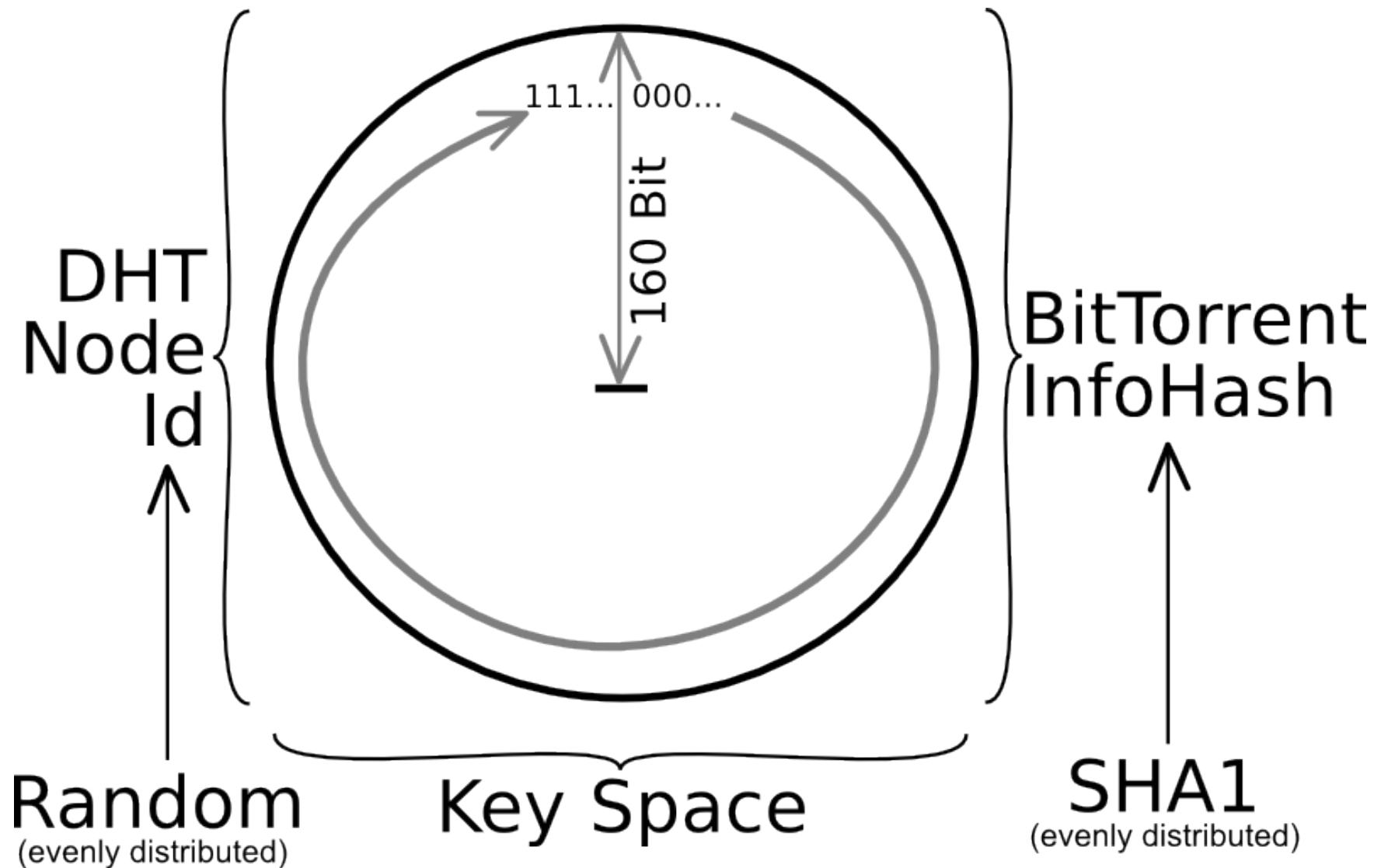


Sybil Attack & DDoS with the BitTorrent DHT

<<</>>

Kademlia DHT stores Resource Locations



Problem 1

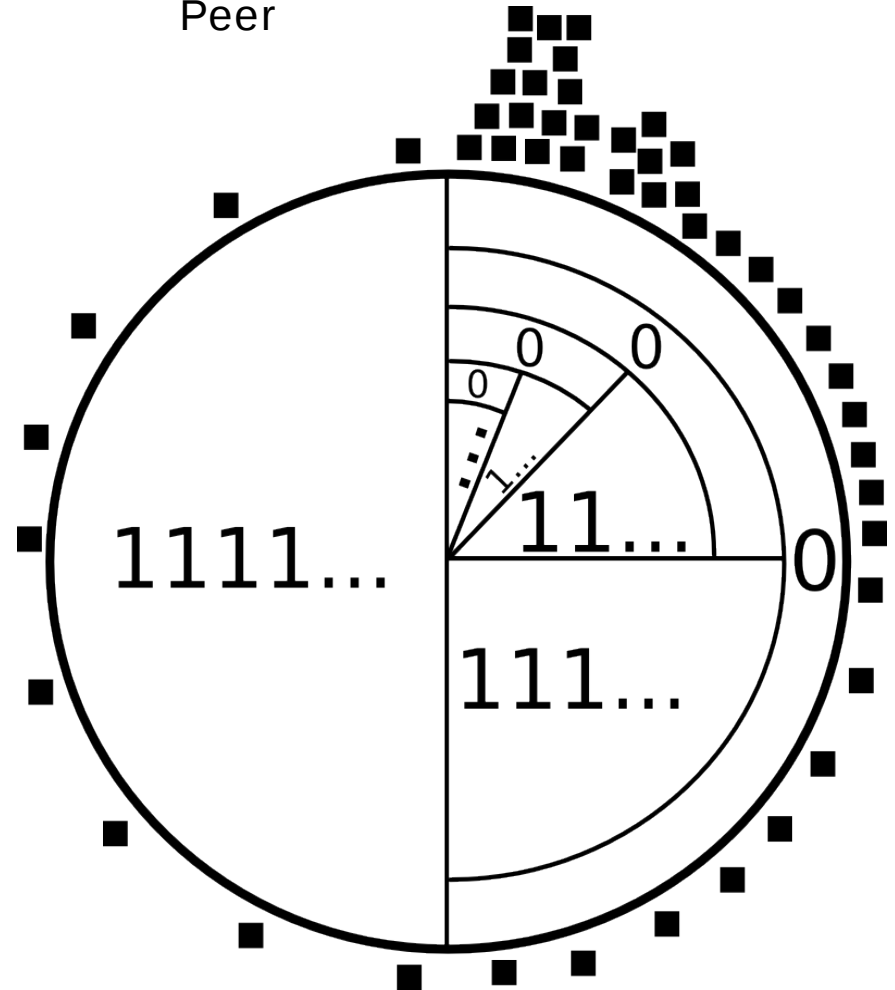
- **DHT Node Id** isn't verifiably **random**
- No Trust Model
- **Anybody** may grab a bit of keyspace to **modify/suppress tracker data** for a specific BitTorrent InfoHash
 - Intellectual Property owners
 - DHT abusers

DHT Node Communication

- **UDP** packets (*KRPC*):
 - ping (determining reachability → bad/good node)
 - find_node (finding neighbors)
 - get_peers (get tracker data)
 - announce_peer (add tracker data)

No Peer Knows All Other Peers

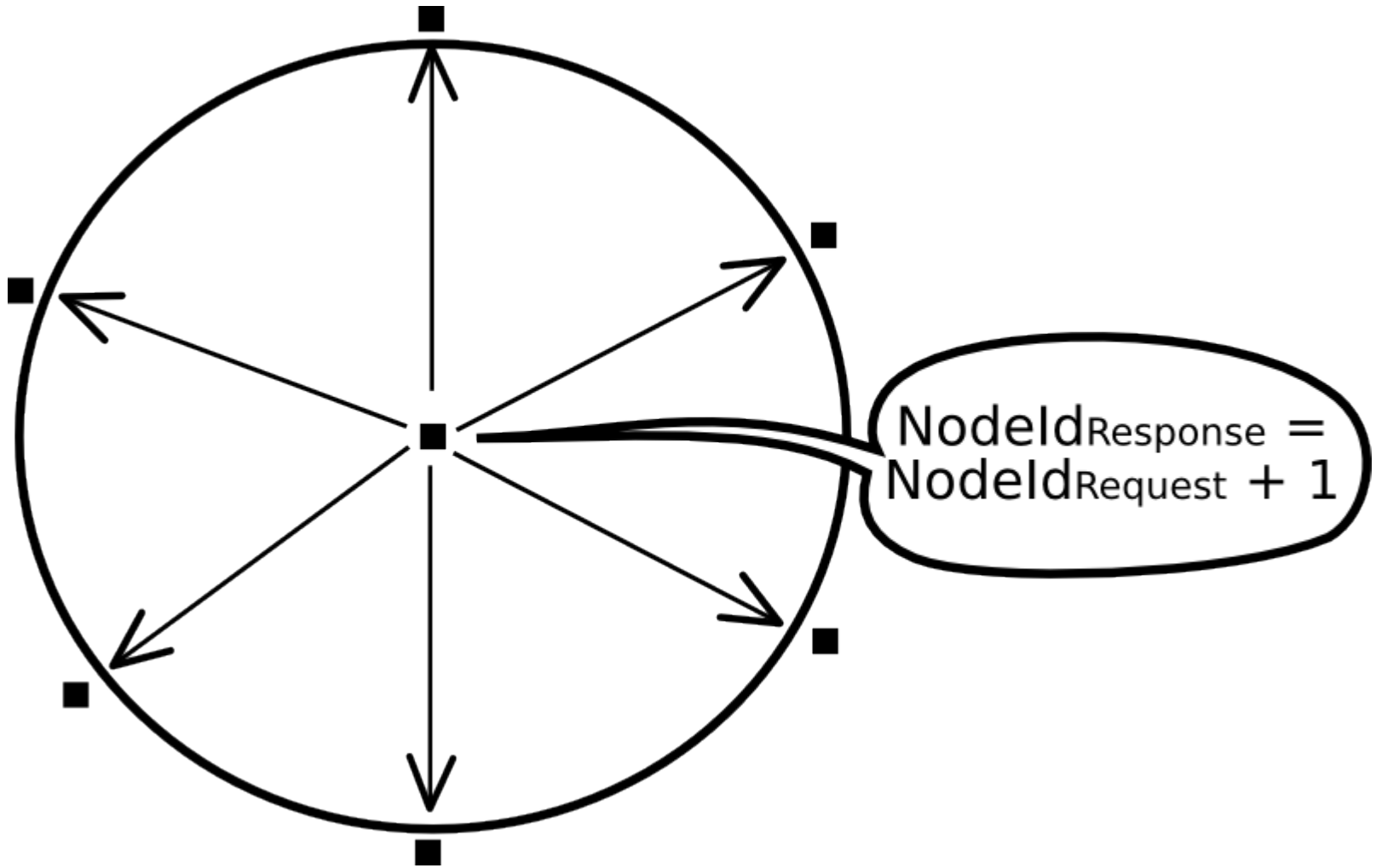
- Distance = $\text{NodeId}_{\text{Mine}} \oplus \text{NodeId}_{\text{Peer}}$
- 8-Buckets: eight peers per distance order
- Far, far away: keep stable peers
- Allow network growth: quickly accept peers close to me



Querying Other Nodes' Buckets

- Joining the network & “Knitting around holes”
- ```
{ "t": "aa",
 "y": "q",
 "q": "find_node",
 "a": {
 "id": "abcdefghij0123456789",
 "target": "mnopqrstuvwxyz123456"
 }
}
```

# Problem 2



# DDoS Vector 1

- Will get *many* `find_node` requests myself
- Reply with 8 (arbitrary)  
`NodeId ++ Host ++ Port` strings
- Peers will query those
- **Effect:** UDP DDoS

# DDoS Vector 2

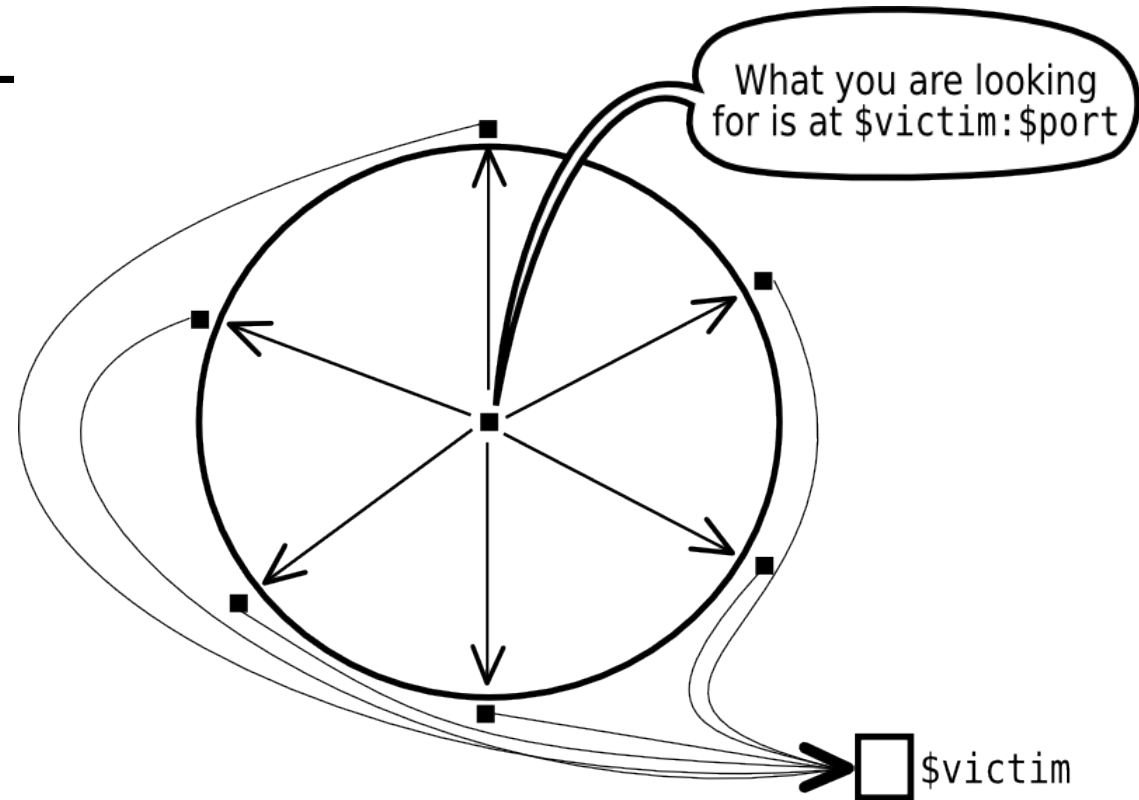
- After becoming a peer with good status
- `get_peers` queries for BitTorrent tracker data
- Replying with many (arbitrary)

`Host ++ Port strings`

- **Effect:** TCP full-open DDoS

# Many Many Packets

- KRPC replies may contain many IP ++ Port combinations
- Peers **cache** & retry for quite some time
- Characteristics of different implementations



Mail & XMPP: [astro@spaceboyz.net](mailto:astro@spaceboyz.net)  
<http://github.com/astro/hashvortex/>