Hi^3: AN ANALYTICAL STUDY OF THE SCALABILITY

Finnish Data Processing Week (FDPW'2005)
at the Petrozavodsk State University

DMITRY G. KORZUN

InfraHIP Project
(Infrastructure for Host Identity Protocol)
by Helsinki Institute for Information Technology

May 2005

Outline

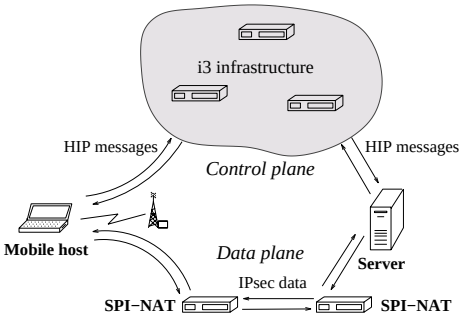
0. **What is Hi^3**
   Host Identity Protocol (HIP), Internet Indirection Infrastructure (i^3), and Hi^3 architecture.

1. **Hi^3 analysis**
   Aim, subject and assumptions.

2. **Basic Hi^3 scenarios**
   HIP messages and their traveling through the infrastructure.
   Hi^3 parameters and latency of HIP messages.

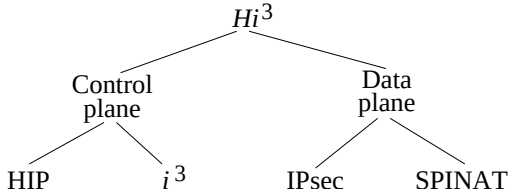
3. **Scalability analysis**
   Hi^3 deployment, workload, Hi^3 size, resilience to attacks.

Hi^3 architecture

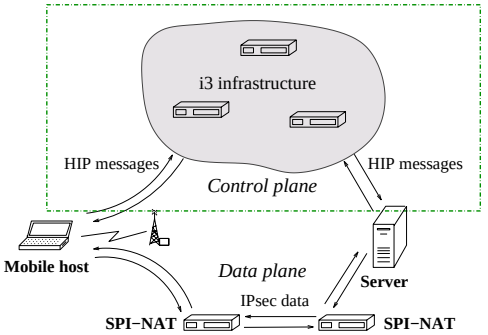


- Host identity layer between transport and network layers
- IP address is a topological label
- i^3 trigger (id, R)
- Separating control and data
- Protecting data traffic

HIP messages (control plane):
- base exchange
- mobility exchange
- ...



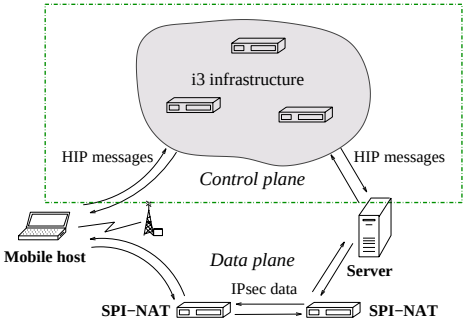
Hi^3 Analysis: 1. Aim and Subject



Scalability properties ?

- HIP messages:
  - base exchange
  - mobility exchange
- i^3 messages:
  - trigger insertion
  - trigger refreshment
  - HIP processing delegation
- Attacks to Hi^3:
  - burst of HIP messages
  - burst of i^3 messages

Hi^3 Analysis: 2. Assumptions

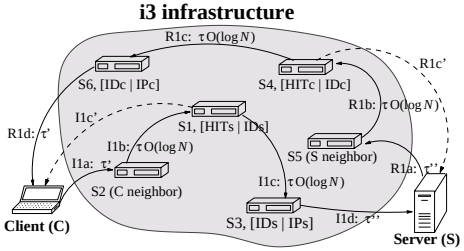


- A few parameters
  - manageable
  - outside i^3
  - required characteristics
- Uniformity of parties involved:
  - i^3 servers
  - mobile hosts
  - Internet servers
- Inexhaustible communication:
  - worst case
  - averaging

Basic trends for scalability ?

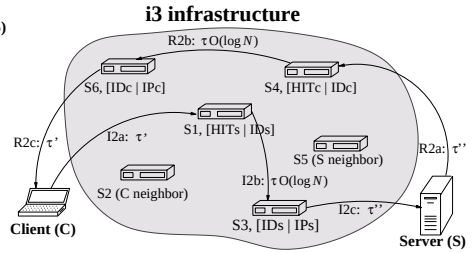
Average estimates for a “globally worst case”

Hi^3 scenarios: 1. Pure association setup (1/3)



I1 and R1 packets

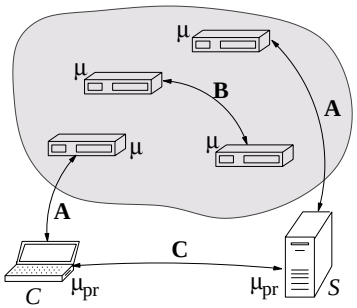
HIP base exchange in Hi^3



I2 and R2 packets

Hi^3 scenarios: Parameters

i3 infrastructure of size N



Number of i^3 servers: N

Transit time: in average, ms

A. host $\leftrightarrow$ i^3: $\tau' = \tau_C^{\mathrm{Hi3}}$, $\tau'' = \tau_S^{\mathrm{Hi3}}$

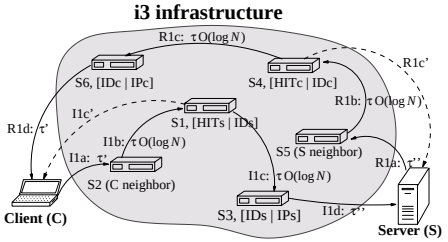
B. i^3 server $\leftrightarrow$ i^3 server
1. direct IP: τ
2. i^3 lookup: $\tau O(\log N)$

C. host $\leftrightarrow$ host: $\tau_{SC} = \tau_{CS}$

Processing time: in average, ms
1. one packet forward: μ
2. HIP cryptography: μ_{pr}

i^3 **lookup:** $(\tau+\mu)O(\log N) \sim \dfrac{\tau+\mu}{2}\log N$

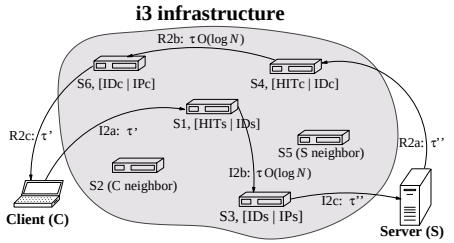
Hi^3 scenarios: 1. Pure association setup (2/3)



I1 and R1 packets

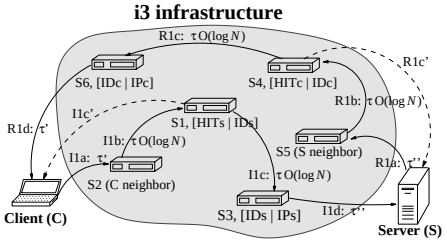
Latency L^{Hi3} ***?***

- Time inside i^3 and outside
- Four packets in HIP base exchange
- $L_{\mathrm{s}}^{\mathrm{Hi3}} = 4(\tau^{\mathrm{Hi3}} + \tau^{\mathrm{out}})$



I2 and R2 packets

Hi^3 scenarios: 1. Pure association setup (3/3)

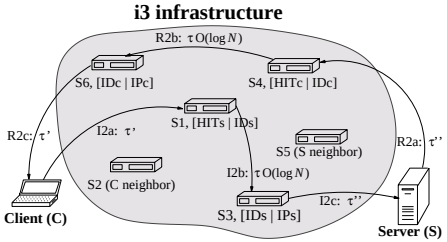


I1 and R1 packets

$$L_{\rm s}^{\rm Hi3} = 4\tau_C^{\rm Hi3} + 3(\tau+\mu)\log N + \\ + 4\tau_S^{\rm Hi3} + 2\mu_{\rm pr} \quad (1)$$

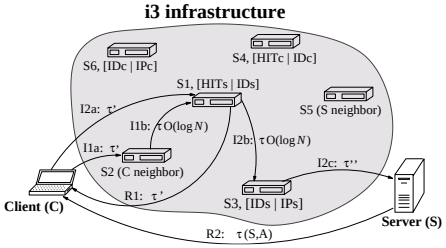
and

$$4\tau^{\rm Hi3} = 3(\tau+\mu)\log N \\ 4\tau^{\rm out} = 4\tau_C^{\rm Hi3} + 2\mu_{\rm pr} + 4\tau_S^{\rm Hi3} \quad (1a)$$



I2 and R2 packets

Hi^3 scenarios: 2. Optimized association setup



I1, R1, I2, and R2 packets

$$L_{\rm so}^{\rm Hi3} = 4(\tau^{\rm Hi3} + \tau^{\rm out}) \\ L_{\rm so}^{\rm Hi3} = 3\tau_C^{\rm Hi3} + (\tau+\mu)\log N + \\ + \tau_S^{\rm Hi3} + \tau_{SC} + 2\mu_{\rm pr} \quad (2)$$

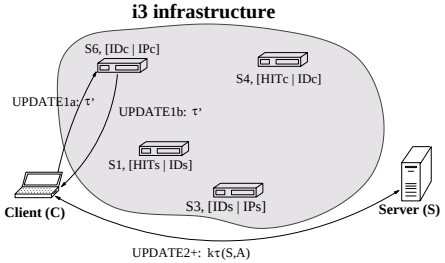
and

$$4\tau^{\rm Hi3} = (\tau+\mu)\log N \\ 4\tau^{\rm out} = 3\tau_C^{\rm Hi3} + 2\mu_{\rm pr} + \tau_S^{\rm Hi3} + \tau_{SC} \quad (2a)$$

The optimization benefit is more than $\frac{3}{2}(\tau+\mu)\log N + {\rm RTT}(S, {\rm Hi3})$

For $N \sim 500$ it is more than 1 second!

Hi^3 scenarios: 3. Location update



UPDATE1 and UPDATE2+ packets

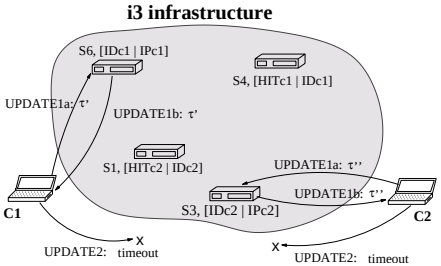
$$L_{\rm lu}^{\rm Hi3} = 2\tau_C^{\rm Hi3} + \mu + k\tau_{SC} \approx \\ \approx {\rm RTT}(C, {\rm Hi3}) + \frac{k}{2}{\rm RTT}(C,S) \quad (3)$$

and

$$2\tau^{\rm Hi3} = \mu \approx 0 \\ (2+k)\tau^{\rm out} = {\rm RTT}(C, {\rm Hi3}) + \\ + \frac{k}{2}{\rm RTT}(C,S) \quad (3a)$$

Infrastructure load is small

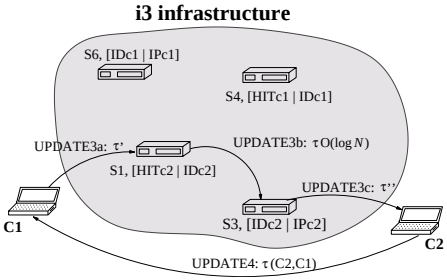
Hi^3 scenarios: 4. Simultaneous host movement



UPDATE1 and UPDATE2 packets

$$2\tau^{\rm Hi3} = \frac{\tau+\mu}{2}\log N \\ 2\tau^{\rm out} = \tau_{C1}^{\rm Hi3} + \tau_{C2}^{\rm Hi3} + \tau_{C2,C1} \quad (4a)$$

$$L_{\rm su}^{\rm Hi3} = 2(\tau^{\rm Hi3} + \tau^{\rm out}) \\ L_{\rm su}^{\rm Hi3} = \tau_{C1}^{\rm Hi3} + \frac{\tau+\mu}{2}\log N + \\ + \tau_{C2}^{\rm Hi3} + \tau_{C2,C1} \quad (4)$$

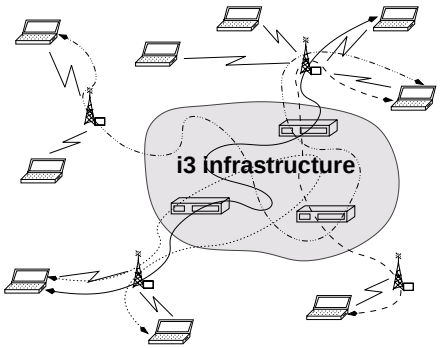


UPDATE3 and UPDATE4 packets

Hi^3 scenarios: Summary

Scenario	#pkts	Inside Hi^3	Outside Hi^3	Occurrence
Pure setup	4	$3(\tau+\mu)\log N$	$4\tau_C^{\mathrm{Hi3}}+2\mu_{\mathrm{pr}}+4\tau_S^{\mathrm{Hi3}}$	medium
Opt. setup	4	$(\tau+\mu)\log N$	$3\tau_C^{\mathrm{Hi3}}+2\mu_{\mathrm{pr}}+\tau_S^{\mathrm{Hi3}}+\tau_{SC}$	medium
Loc. update	$2+k$			frequent
phase 1	2	μ	$\mathrm{RTT}(C,\mathrm{Hi3})$	
phase 2	k	0	$\frac{k}{2}\mathrm{RTT}(C,S)$	
Sim. update	6			rare
phase 1	$2+2$	2μ	$\mathrm{RTT}(C1,\mathrm{Hi3})+\mathrm{RTT}(C2,\mathrm{Hi3})$	
timeout	—	—	—	
phase 2	2	$\frac{\tau+\mu}{2}\log N$	$\tau_{C1}^{\mathrm{Hi3}}+\tau_{C2}^{\mathrm{Hi3}}+\tau_{C2,C1}$	

Scalability: 1. Mobile peers 1/4



- M is #(mobile hosts)
- N is #(i^3 servers)
- λ is intensity of a mobile host to send a HIP message (λ_{s}, λ_{so}, λ_{u})
- P_{su} is probability that a location update becomes a simultaneous update.
- Workload W is #requests (average) to an i^3 server:

$$W = \frac{\lambda M}{N} \cdot \#(i^3 \text{ servers for a HIP message})$$

Scalability: 1. Mobile peers 2/4

Scenario	Hi^3 workload, W	Inside i^3, T^{Hi3}
Pure setup	$\frac{3\lambda_{\mathrm{s}} M\log N}{N}$	$3(\tau+\mu)\log N$
Opt. setup	$\frac{\lambda_{\mathrm{so}} M\log N}{N}$	$(\tau+\mu)\log N$
Update	$\frac{\lambda_{\mathrm{u}} M}{N}\left(1+\frac{1}{2}P_{\mathrm{su}}\log N\right)$	$\mu + P_{\mathrm{su}}\frac{\tau+\mu}{2}\log N$ $\approx P_{\mathrm{su}}\frac{\tau+\mu}{2}\log N$ or $\approx (\tau+\mu)\left(1+\frac{P_{\mathrm{su}}}{2}\log N\right)$

$$N \approx \frac{\lambda M\cdot T^{\mathrm{Hi3}}}{(\tau+\mu)W} = \frac{\lambda M\cdot T^{\mathrm{Hi3}}(N)}{(\tau+\mu)W(N)} \qquad (5)$$

Scalability: 1. Mobile peers 3/4

- HIP messages are mixed:

$$W_{\mathrm{tot}} = W_{\mathrm{s}} + W_{\mathrm{so}} + W_{\mathrm{u}}\ , \qquad T_{\mathrm{avg}}^{\mathrm{Hi3}} = \frac{\lambda_{\mathrm{s}} T_{\mathrm{s}}^{\mathrm{Hi3}} + \lambda_{\mathrm{so}} T_{\mathrm{so}}^{\mathrm{Hi3}} + \lambda_{\mathrm{u}} T_{\mathrm{u}}^{\mathrm{Hi3}}}{\lambda_{\mathrm{s}} + \lambda_{\mathrm{so}} + \lambda_{\mathrm{u}}}$$

- More precise:

$$W_{\mathrm{tot}} = \frac{\lambda_{\mathrm{tot}} M\log N}{N} + \frac{\lambda_{\mathrm{u}} M}{N}\ , \quad T_{\mathrm{avg}}^{\mathrm{Hi3}} = \frac{\lambda_{\mathrm{tot}}}{\lambda_{\mathrm{s}} + \lambda_{\mathrm{so}} + \lambda_{\mathrm{u}}}(\tau+\mu)\log N\ ,$$

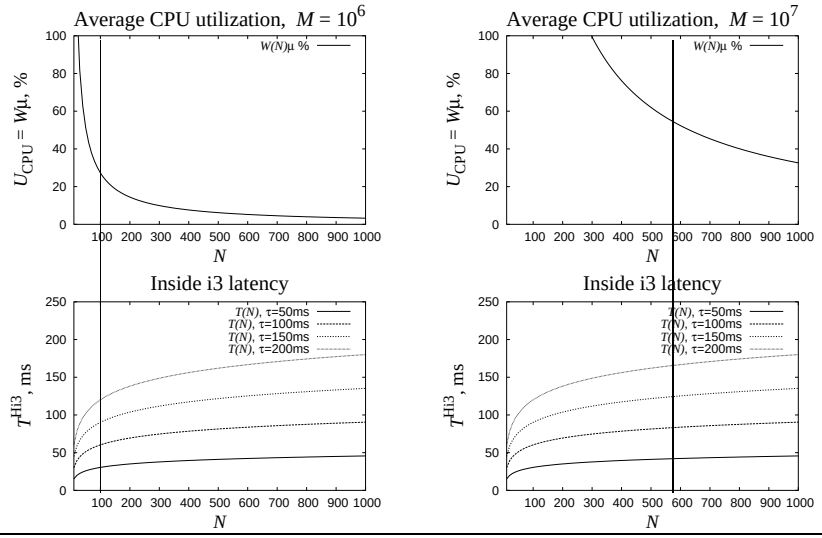
  where $\lambda_{\mathrm{tot}} = 3\lambda_{\mathrm{s}} + \lambda_{\mathrm{so}} + \frac{P_{\mathrm{su}}}{2}\lambda_{\mathrm{u}}$

- Scalability estimation:

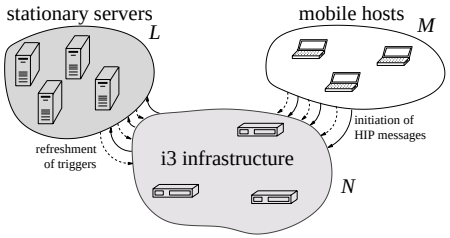
$$N = \frac{\lambda M\cdot T_{\mathrm{avg}}^{\mathrm{Hi3}}}{(\tau+\mu)W_{\mathrm{tot}}} \qquad (6)$$

Scalability: 1. Mobile peers 4/4

$\lambda_s = \lambda_{so} = 30\text{min}^{-1}$, $\lambda_u = 1\text{min}^{-1}$, $P_{su} = 10^{-2}$, $\mu = 1\text{ms}$



Scalability: 2. Stationary and mobile hosts



- M is #(mobile hosts)
- N is #(i^3 servers)
- L is #(stationary Internet servers)
- λ is intensity of a mobile host to send a HIP message (λ_s, λ_{so}, λ_u, P_{su})
- λ_r is intensity of a server to refresh its public trigger in i^3.

$$W_{tot} = \frac{\lambda_{tot} M \log N}{N} + \frac{\lambda_u M + 2\lambda_r L}{N}$$

Scalability: Summary

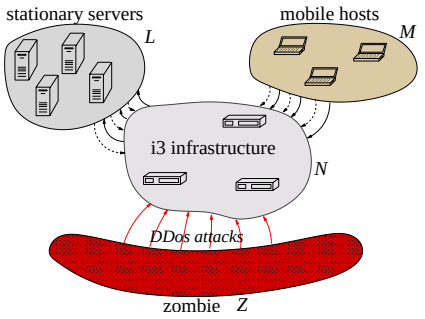
Increasing N leads to:

- Workload decreases as $W = C_1(\lambda, \#) \cdot \frac{\log N}{N} + C_2(\lambda, \#) \cdot \frac{1}{N}$
- Inside latency increases as $T^{\text{Hi3}} = C_3(\lambda, \tau + \mu) \cdot \log N$

Infrastructure size N is proportional:

- $N \approx C_4(\lambda, \#, \frac{1}{\tau + \mu}) \cdot \frac{T^{\text{Hi3}}}{W}$

Application scenarios: 3. Zombie attacks 1/3



Workload:
average #requests to an i^3 server

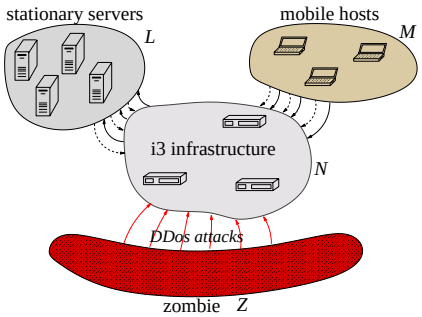
Attack types:

- Trigger insertion: $W_{zi} = \frac{\lambda_{zi} Z \log N}{N}$
- Initiation of association setup
  1. send I1
  2. receive R1
  3. immediately reply with I2 and wrong puzzle solution

Pure base exchange: $W_{zs} = \frac{5\lambda_{zs} Z \log N}{2N}$

Optimized base exchange: $W_{zso} = \frac{\lambda_{zs} Z \log N}{N}$

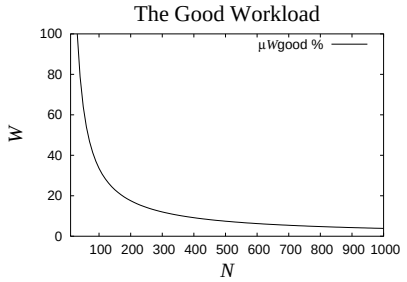
Application scenarios: 3. Zombie attacks 2/3

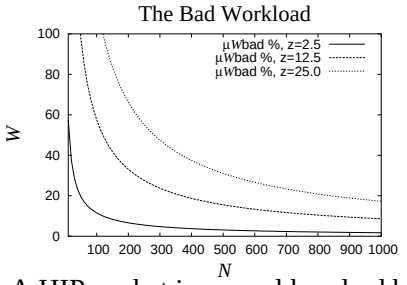


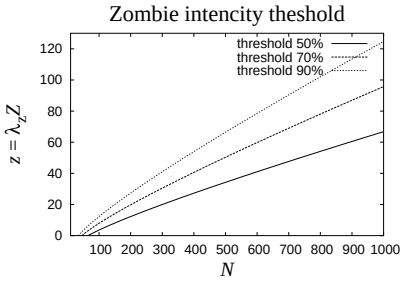
- $W_{\text{good}} = W_{\text{s}*} + W_{\text{u}} + W_{\text{r}}$
  $W_{\text{bad}} = W_{\text{z}*} = \dfrac{\lambda_{\text{z}} Z \log N}{N}$
- $W_{\text{tot}} = W_{\text{good}} + W_{\text{bad}}$
- Criteria: $W_{\text{tot}}\mu \leq W_{\text{threshold}}\mu$
  e.g. $W_{\text{threshold}}\mu = 50\%, 70\%, 90\%$
- Threshold: $z = \lambda_{\text{z}} Z = ?$

$$z = (W_{\text{threshold}} - W_{\text{good}})\frac{N}{\log N}$$

Application scenarios: 3. Zombie attacks 3/3







A HIP packet is several hundred bytes, or ≈ 0.5 Kbytes $= 4$ Kbits.

$\max \lambda_{\text{z}} \approx 0.25$ for 1Mbs throughput

Z	$z = \lambda_{\text{z}} \cdot Z$	N
10	2.5	< 50
50	12.5	< 100
100	25.0	< 200

Conclusion

1. Simple assumptions leads to ***basic trends only***
2. Hi^3 has ***acceptable inside latency*** and ***satisfactory scalability property***
3. Infrastructure of ***a few nodes*** ($\sim 10^2$) is suffi cient for ***a large set*** of HIP hosts ($\sim 10^6..10^7$)