

The Research of Worm Propagation in the Next Generation Network

Ting Liu

Xi'an Jiaotong University

P. R. China

Outline

- **Worm Research**
- **IPv6 VS Worm**
- **Dual-stack Worm**
- **Conclusion & Future Work**
- **Q & A**



Worm Research

History of worm

<i>Name</i>	<i>Damage</i>	<i>Description</i>
<i>Morris</i>	Infect 6,000 hosts	The first worm. 1988
<i>Code Red</i>	2.6 billion dollars	2001/1/31. MS IIS
<i>Slammer</i>	1.25 billion dollars	2003/1/24. MS SQL Server 2000
<i>Blaster</i>	2 billion dollars	2003/8/12. MS DCOM RPC

Worm

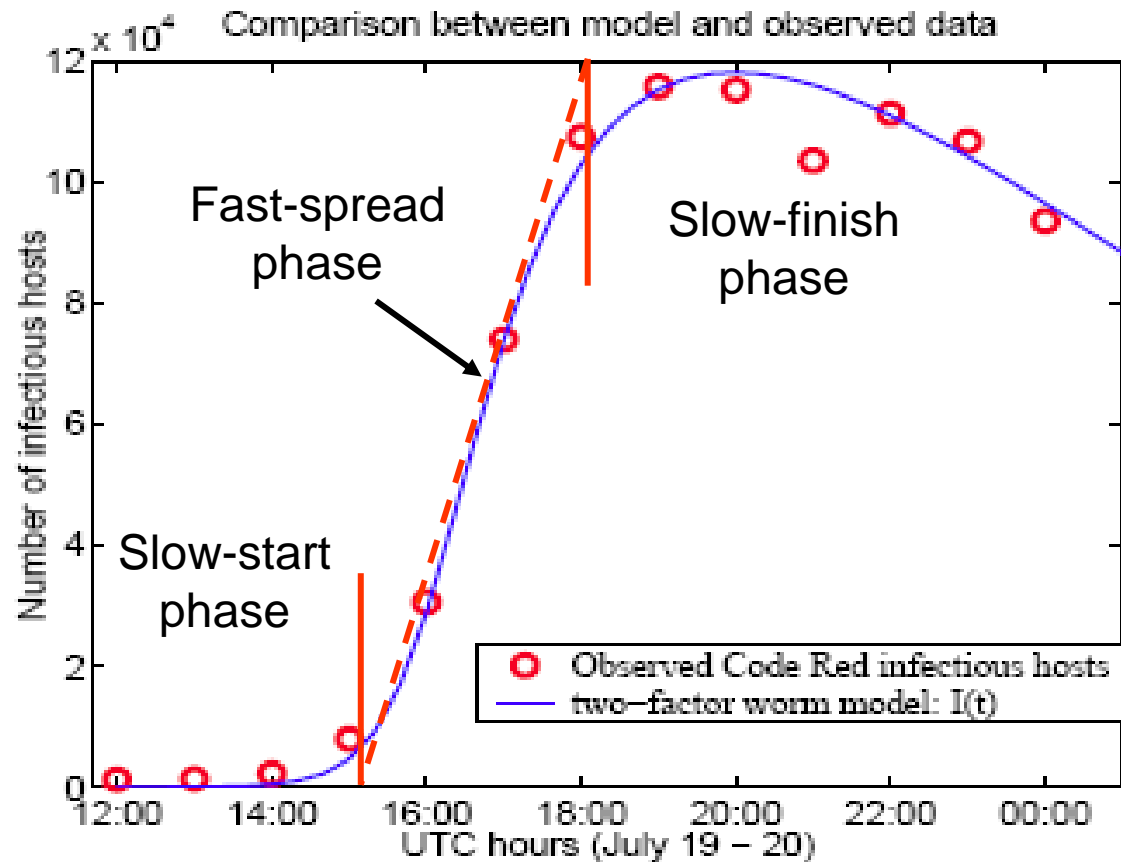
卡斯基最新的月度分析

2006. 12. 01. 卡斯基实验室

排名	排名改变	名称	百分比
1.	☐ New	Email-Worm.Win32.Warezov.gj	18.27
2.	☐ +3	Email-Worm.Win32.Warezov.ev	14.88
3.	☐ Return	Email-Worm.Win32.Nyxem.e	9.89
4.	☐ Return	Email-Worm.Win32.NetSky.t	7.54
5.	☐ -1	Email-Worm.Win32.Scano.gen	6.57
6.	☐ +8	Net-Worm.Win32.Mytob.c	5.68
7.	☐ -6	Email-Worm.Win32.NetSky.g	5.25
8.	☐ Return	Email-Worm.Win32.Zafi.b	4.40
9.	☐ +3	Email-Worm.Win32.NetSky.aa	2.77
10.	☐ Return	Net-Worm.Win32.Mytob.t	2.01
11.	☐ Return	Email-Worm.Win32.LovGate.w	1.48
12.	☐ +1	Email-Worm.Win32.NetSky.b	1.41
13.	☐ New	Email-Worm.Win32.Warezov.fh	1.29
14.	☐ +1	Trojan-Spy.HTML.Bankfraud.od	1.08
15.	☐ Return	Net-Worm.Win32.Mytob.u	1.04
16.	☐ New	Email-Worm.Win32.Warezov.gl	0.97
17.	☐ -6	Email-Worm.Win32.Warezov.do	0.87
18.	☐ -10	Email-Worm.Win32.Mydoom.l	0.77
19.	☐ -16	Email-Worm.Win32.Bagle.gen	0.76
20.	☐ Return	Net-Worm.Win32.Mytob.w	0.73
其他恶意程序			12.34

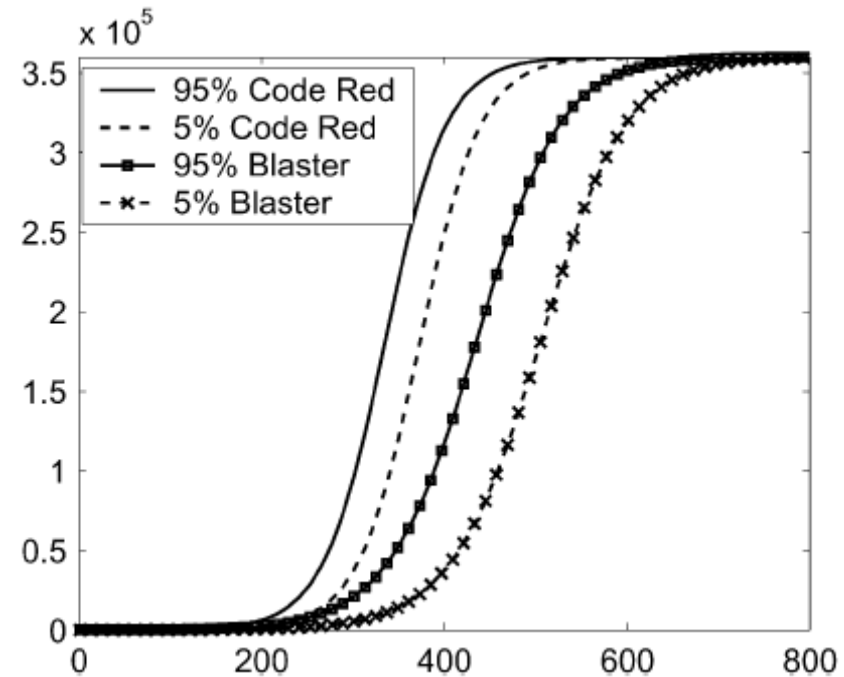
Worm propagation

- Slow-start
- Fast-spread
- Slow-finish



Scanning Strategy

- Random scan
Code Red, Slammer
- Sequential scan
Blaster
- New strategy
Email, P2P, IM (Instant message) ...



IPv6 VS Worm

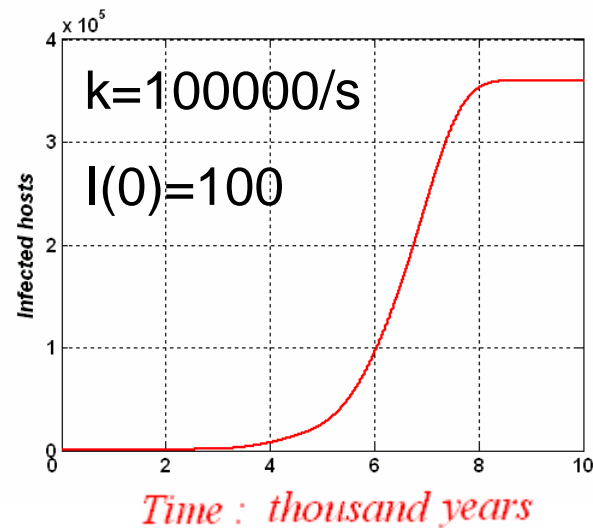
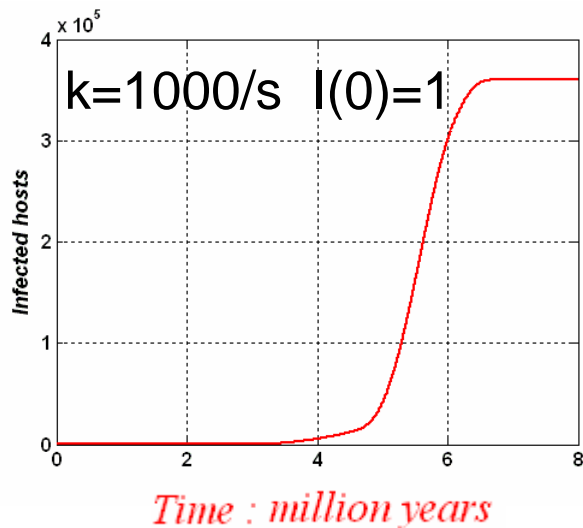
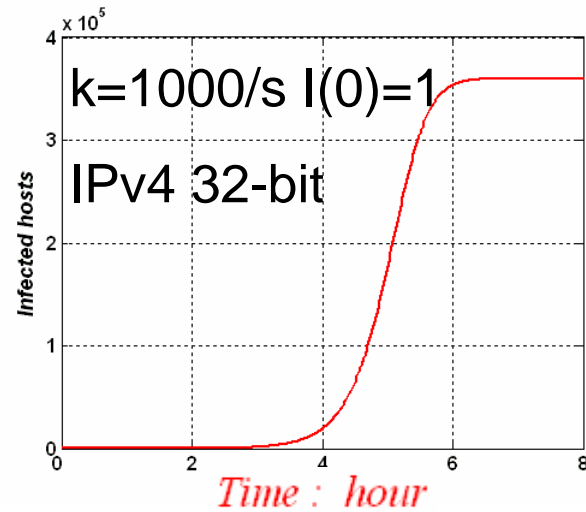
IPv6 VS Worm

- Most fast-propagate worms adopt Internet scanning strategy
- IPv6 has a huge address space – 128-bit address space

It is difficult for worms to propagate in IPv6 network

Worm propagate in IPv6

- IPv4 network
32-bit address space
- IPv6 network
128-bit address space
64-bit in present simulation





Dual-stack worm

Dual-stack network

- Deployment of IPv6 is not going to happen overnight.
- isolated “islands” -- gradual global saturation.
- Dual-stack: IPv4 and IPv6
- Dual-stack network

IPv6 applications	IPv4 applications
Sockets API	
UDP/TCP v4	UDP/TCP v6
IPv4	IPv6
L2	
L1	

Scan strategy in IPv6 subnet

- Multicast ping

FF02::1 is the link-local scope all-nodes multicast address

Time	Source	Destination	Info
2.680078	fe80::20d:87ff:fe61:a530	ff02::1	Echo request
2.680224	fe80::20d:87ff:fe61:aa08	fe80::20d:87ff:fe61:a530	Echo reply
2.680239	fe80::212:3fff:fe24:9244	fe80::20d:87ff:fe61:a530	Echo reply
2.680245	fe80::212:3fff:fe24:8f38	fe80::20d:87ff:fe61:a530	Echo reply
2.680252	fe80::20d:87ff:fe61:a536	fe80::20d:87ff:fe61:a530	Echo reply
2.680258	fe80::211:43ff:fec2:9806	fe80::20d:87ff:fe61:a530	Echo reply
2.680265	fe80::290:27ff:fee5:e4f6	fe80::20d:87ff:fe61:a530	Echo reply
2.680274	fe80::200:e2ff:fe52:e0c6	fe80::20d:87ff:fe61:a530	Echo reply
2.680289	fe80::200:e2ff:fe56:331c	fe80::20d:87ff:fe61:a530	Echo reply
2.680295	fe80::200:e2ff:fe52:c338	fe80::20d:87ff:fe61:a530	Echo reply
2.680302	fe80::200:e2ff:fe9a:8ecd	fe80::20d:87ff:fe61:a530	Echo reply
2.680311	fe80::201:6cff:fe35:7a7c	fe80::20d:87ff:fe61:a530	Echo reply
2.680320	fe80::20d:87ff:fe2f:aaad	fe80::20d:87ff:fe61:a530	Echo reply
2.680331	fe80::211:43ff:fec3:950	fe80::20d:87ff:fe61:a530	Echo reply
2.680345	fe80::200:e2ff:fe9a:4b64	fe80::20d:87ff:fe61:a530	Echo reply
2.680351	fe80::201:6cff:fe38:86c4	fe80::20d:87ff:fe61:a530	Echo reply
2.680358	fe80::200:e2ff:fe89:61ff	fe80::20d:87ff:fe61:a530	Echo reply
2.680369	fe80::20f:1fff:fefa:bb33	fe80::20d:87ff:fe61:a530	Echo reply
2.680482	fe80::20d:66ff:fe2e:8ca	fe80::20d:87ff:fe61:a530	Echo reply

Scan strategy in IPv6 subnet

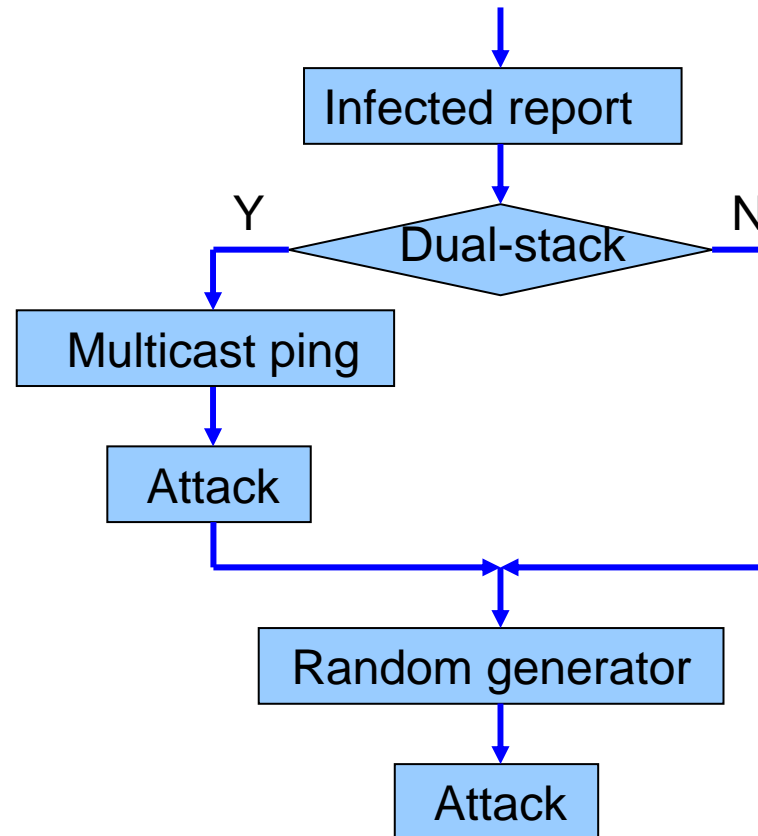
- Router-spoof

Send Router Advertisement to FF02::1

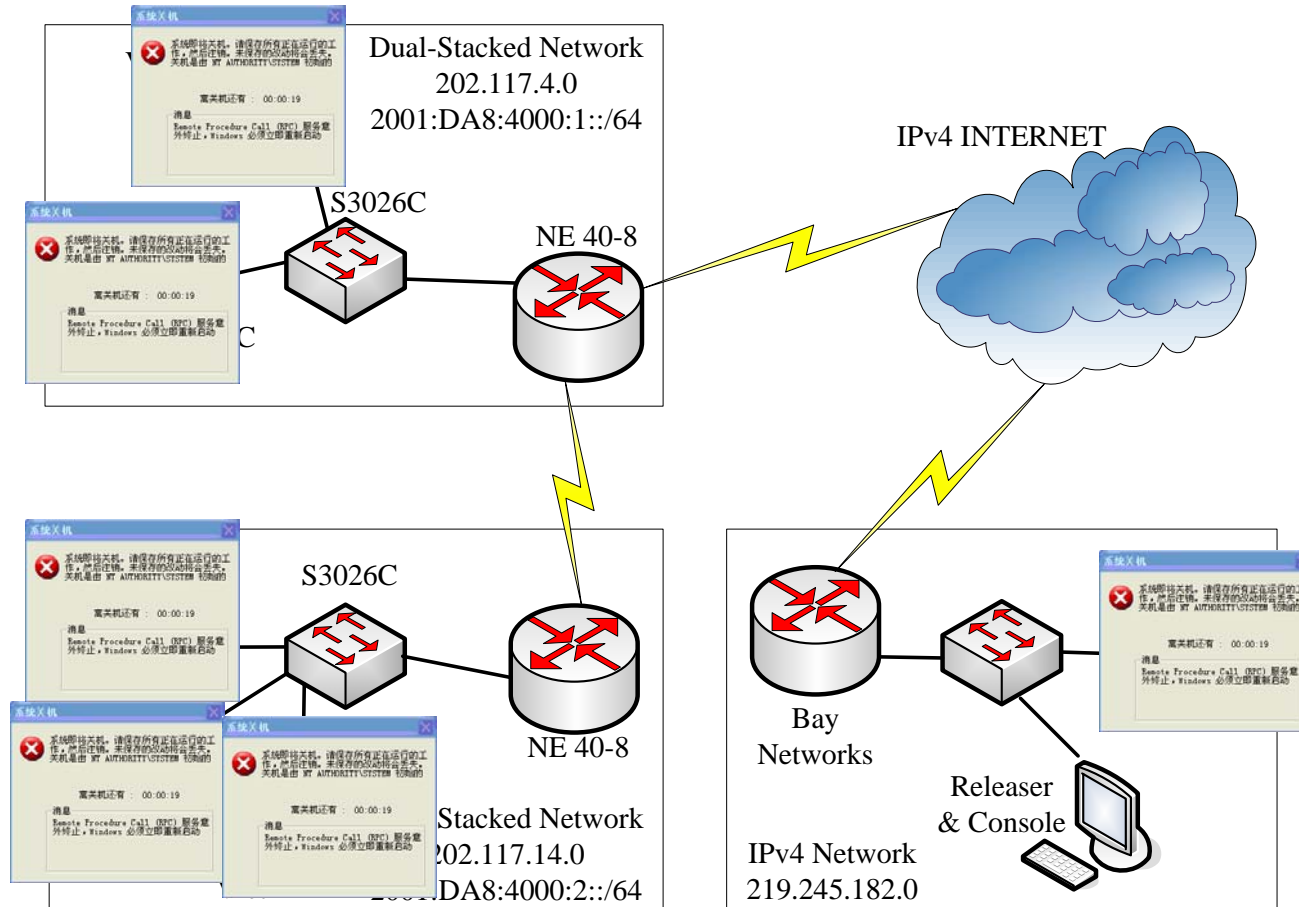
Time	Source	Destination	Protocol	Info
2.977256	fe80::20d:87ff:fe61:a530	ff02::1	ICMPv6	Router advertisement
2.978604	fe80::2e0:4cff:fe68:e5fa	ff02::1:ffae:30de	ICMPv6	Multicast listener report
2.978665	::	ff02::1:ffae:30de	ICMPv6	Neighbor solicitation
2.978751	::	ff02::1:ff68:e5fa	ICMPv6	Neighbor solicitation
2.999670	fe80::211:43ff:fec3:815	ff02::1:ffab:ef51	ICMPv6	Multicast listener report
2.999675	::	ff02::1:ffab:ef51	ICMPv6	Neighbor solicitation
2.999678	::	ff02::1:ffc3:815	ICMPv6	Neighbor solicitation
3.002202	fe80::2ac:a3ff:fe73:fd75	ff02::1:ffb0:671c	ICMPv6	Multicast listener report
3.002206	::	ff02::1:ffb0:671c	ICMPv6	Neighbor solicitation
3.002219	::	ff02::1:ff73:fd75	ICMPv6	Neighbor solicitation
3.004454	fe80::200:e2ff:fe53:bf4b	ff02::1:ff08:3cec	ICMPv6	Multicast listener report
3.004477	::	ff02::1:ff08:3cec	ICMPv6	Neighbor solicitation
3.004481	::	ff02::1:ff53:bf4b	ICMPv6	Neighbor solicitation
3.006801	fe80::210:5cff:fee9:c7b0	ff02::1:ffc2:b981	ICMPv6	Multicast listener report

Dual-stack worm

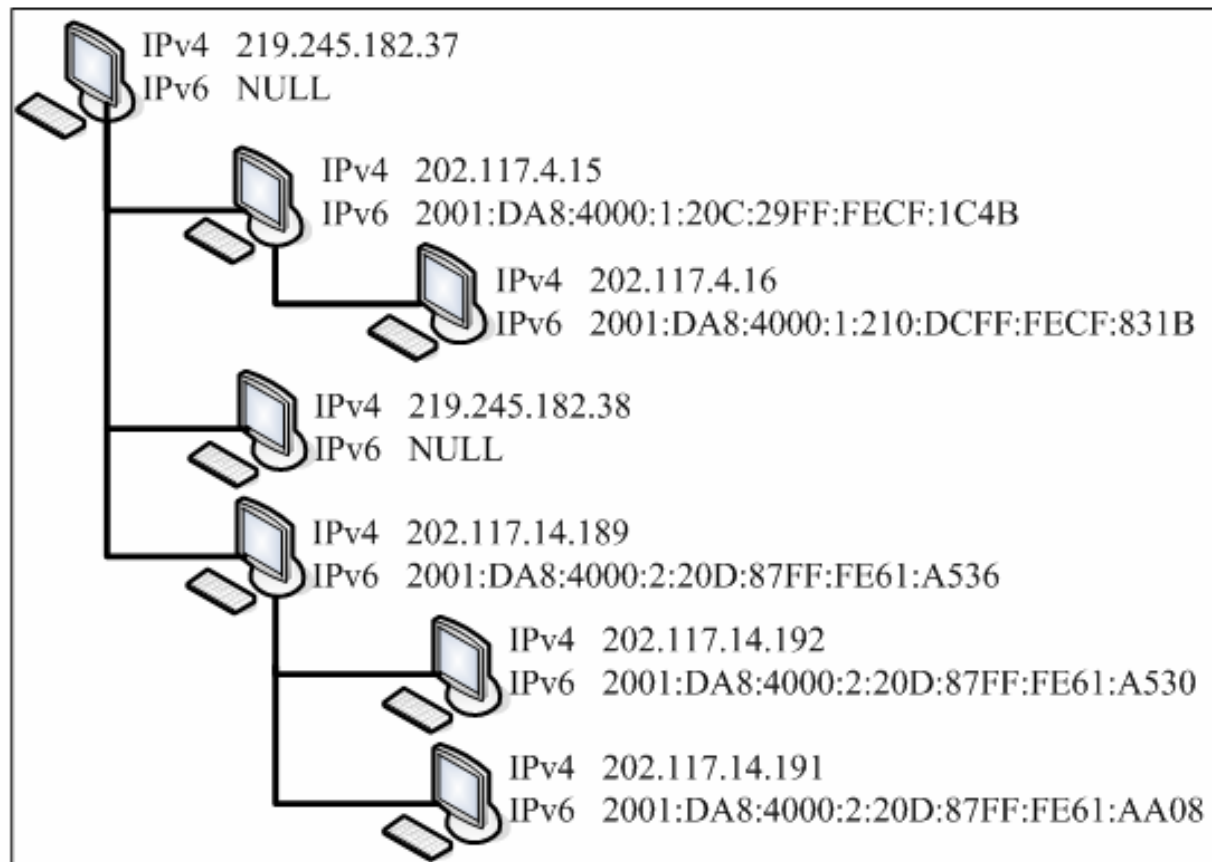
- Infected report
- Dual-stack detect
- Multicast ping & attack
- Random IPv4 address attack



Experiment

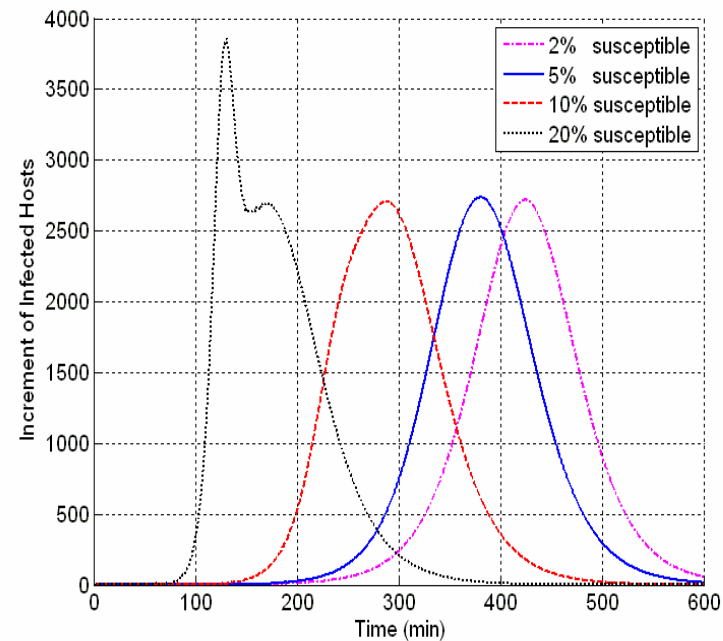
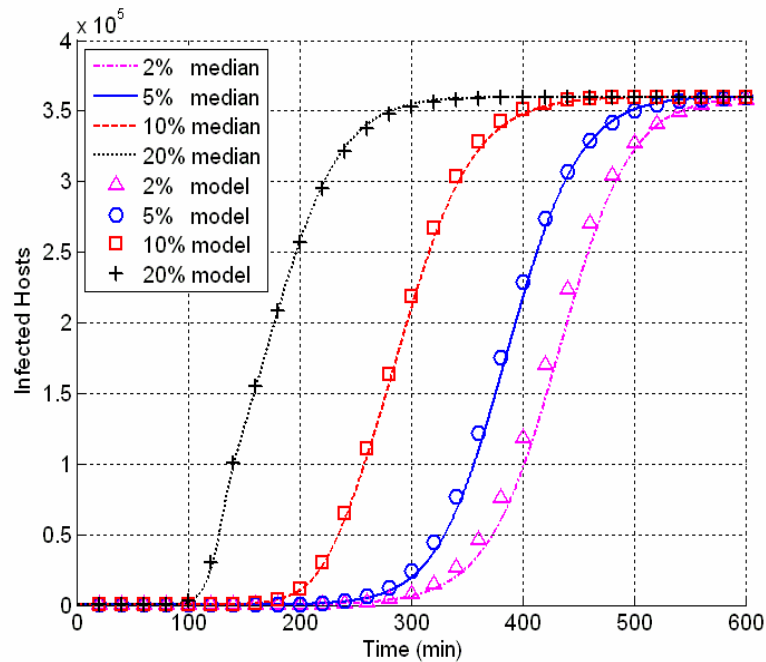


Result analysis



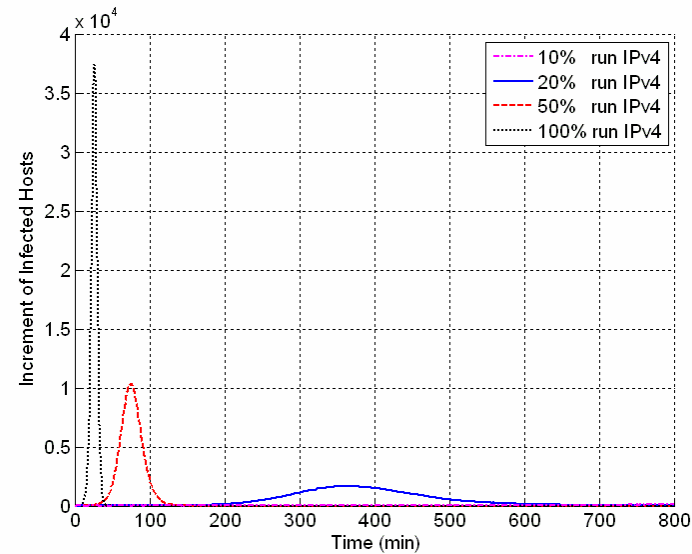
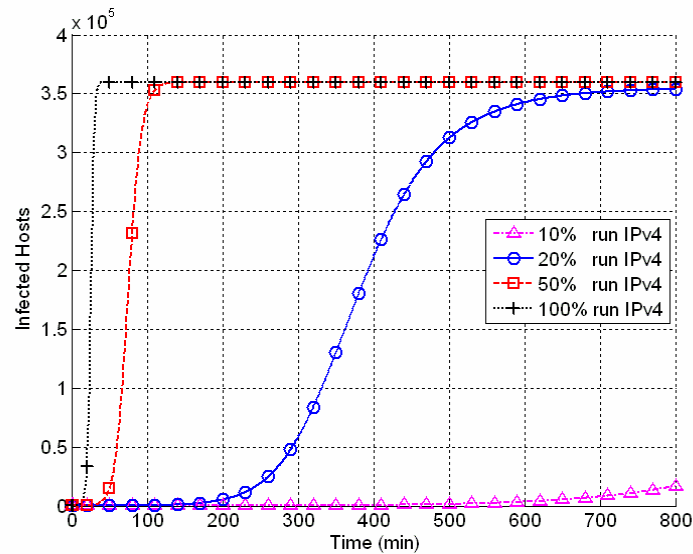
Simulation

More dual-stack hosts, faster worm-propagate



Simulation

Less IPv4 Internet, slower worm-propagate



Conclusion

- Dual-stack worm could spread in the IPv6 Internet
- Dual-stack network could accelerate worm-propagation
- The worm research in next generation Internet is significant.

Future work

- Model
- Scan strategy in IPv6 Internet
- Detection
- Defense strategy
- Anti-worm system



Q & A

Thank You

Ting Liu
Xi'an Jiaotong University
P. R. China
tliu@sei.xjtu.edu.cn

References

- J. Yang. Fast worm propagation in IPv6 networks.
<http://www.cs.virginia.edu/~jy8y/FinalProjectReport.pdf>
- C. C. Zou et al. The monitoring and early detection of Internet worms. IEEE/ACM Transactions on networking, VOL. 13, NO. 5. October 2005.
- D. G. Waddington, F. Chang. Realizing the Transition to IPv6. IEEE Magazine of Communications, June 2002.
- <http://www.viruslist.com/>
- <http://www.symantec.com/>