Energy Exhaustion Attacks in Wireless Networks

Vladimir Shakhov

Automobile/Ship Electronics Convergence Center, University of Ulsan, Korea
Institute of Computational Mathematics and Mathematical Geophysics, Novosibirsk, Russia

Outlines

- Introduction
- State of Arts
- DoS vs DoB
- Model and Metrics
- PE
- Conclusion

Introduction

- The emerging Internet of Things has tremendous potential, but also tremendous dangers.
- The world community was seriously concerned about the societal costs of the IoT outweigh its benefits. A few investigations have repeatedly shown that many IoT device manufacturers and service providers are failing to implement common security measures in their products.
- Cyber security experts report that only 10% of enterprises feel confident that they can secure those devices against intrusions, whereas IoT threats will disable home security systems, flood fields, paralysis of traffic, and disrupt hospitals.

The Economist | World politics | Business & finance | Economics | Science & technology | Culture

Cyber-security

The internet of things (to be hacked)

Hooking up gadgets to the web promises huge benefits. But security must not be an afterthought

Jul 12th 2014 | From the print edition | Timekeeper | Like 217 | Tweet 594

How the Internet of Things Could Kill You

By Fahmida Y. Rashid JULY 18, 2014 7:30 AM - Source: Tom's Guide US | 5 COMMENTS

Hacking the Fridge: Internet of Things Has Security Vulnerabilities

JESS SCANLON | MORE ARTICLES
JUNE 28, 2014

Philips Hue LED smart lights hacked, home blacked out by security researcher

By Sal Cangeloso on August 15, 2013 at 11:45 am | 7 Comments

BBC WORLD NEWS

'Smart' home devices used as weapons in website attack

CNN tech | business | culture | gadgets | future | startups

The Cybercrime Economy

Internet of fails: What's wrong with connected devices

FBI Warns Public on Dangers of the Internet of Things

TREND MICRO

The Washington Post

Can anyone keep us safe from a weaponized 'Internet of Things?'

By Andrea Peterson October 25, 2016

BUSINESS INSIDER | BI INTELLIGENCE

A major red flag about security could threaten the entire IoT

Andrew Meola
Mar. 3, 2016, 12:12 PM 6,184

The New York Times

POLITICS

A New Era of Internet Attacks Powered by Everyday Devices

By DAVID E. SANGER and NICOLE PERLROTH OCT. 22, 2016

Internet of Things comes back to bite us as hackers spread botnet code

Elizabeth Weise, USATODAY Published 6:44 p.m. ET Oct. 3, 2016 | Updated 8:02 p.m. ET Oct. 3, 2016

BBC WORLD NEWS

How easy is it to hack a home network?

By Mark Ward
Technology correspondent, BBC News

25 February 2016 | Technology

THE WALL STREET JOURNAL.

Home | World | U.S. | Politics | Economy | Business | Tech | Markets | Opinion | Arts | Life | Real Estate

THE EXPERTS

Here's Why the Internet of Things Could Be a Security Nightmare

By ROBERT PLANT
Feb 23, 2016 11:00 am ET

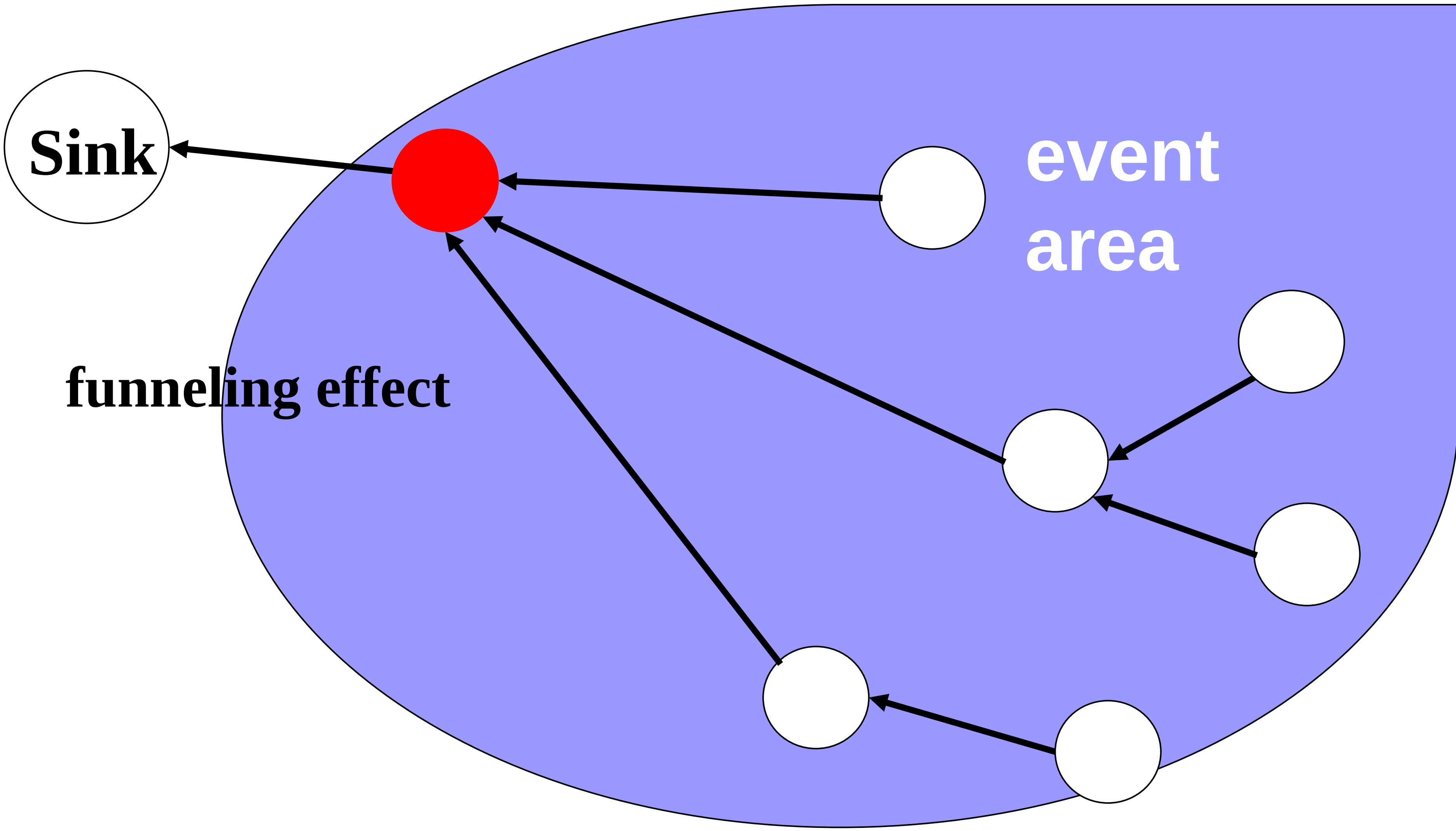
Motivation

To unlock the IoT potential it needs to improve the security of IoT applications.

WSNs problems

- A cost of sensor components is a **critical** consideration in the design of practical sensor networks.
- A cost of sensor network increases with sensor battery power.
- By this reason a battery power is usually a scare component in wireless devices.

Example



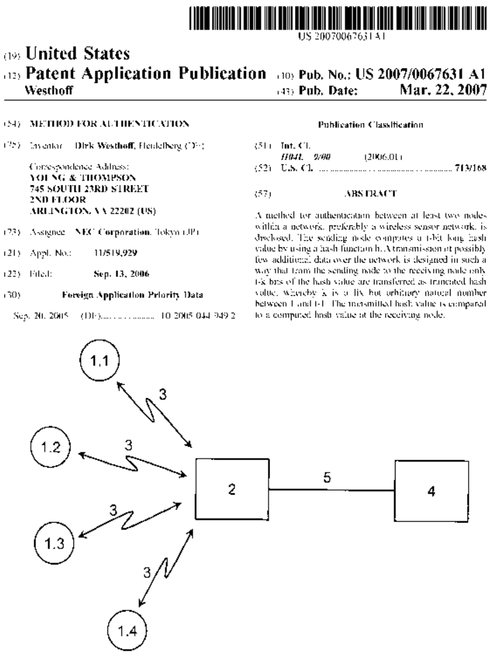
Attacks Taxonomy

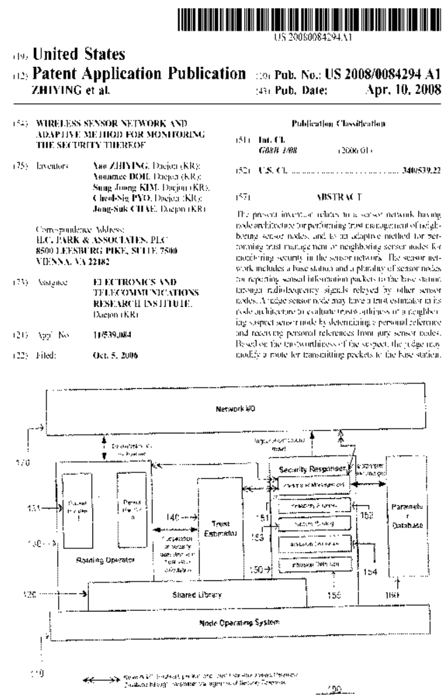
Protocol layer	Attacks	Defenses
Physical	Jamming	Detect and sleep Route around jammed regions
	Node tampering or destruction	Hide or camouflage nodes Tamper-proof packaging
Link/MAC (medium access control)	Interrogation	Authentication and antireplay protection
	Denial of sleep	Authentication and antireplay protection Detect and sleep Broadcast attack protection
Network	Spoofing, replaying, or altering routing-control traffic or clustering messages	Authentication and antireplay protection Secure cluster formation
	Hello floods	Pairwise authentication Geographic routing
	Homing	Header encryption Dummy packets
Transport	SYN (synchronize) flood	SYN cookies
	Desynchronization attack	Packet authentication
Application	Overwhelming sensors	Sensor tuning Data aggregation
	Path-based DoS	Authentication and antireplay protection
	Deluge (reprogramming) attack	Authentication and antireplay protection Authentication streams

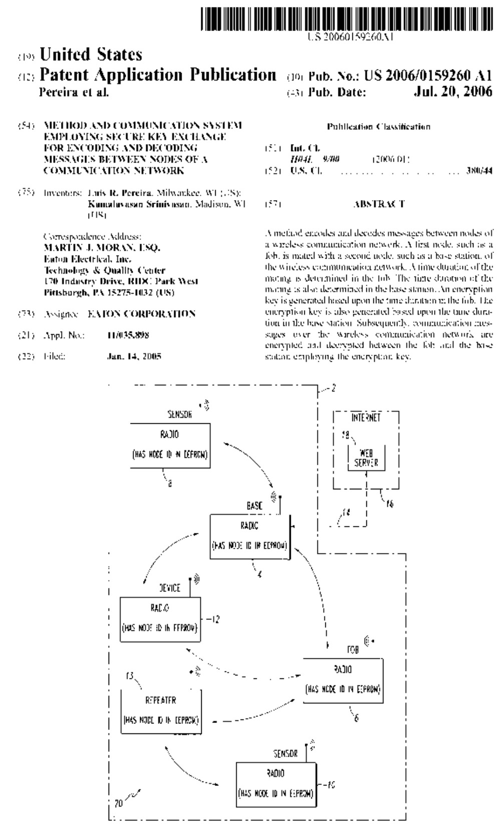
Raymond, D.R., Midkiff : S.F. Denial-of-Service in Wireless Sensor Networks: Attacks and Defences, IEEE Pervasive Computing, 2008, pp.74 – 81.

Patents Search

NEC | ETRI www.etri.re.kr | EATON


(19) United States
(12) Patent Application Publication (10) Pub. No.: US 2007/0067631 A1
Westhoff (43) Pub. Date: Mar. 22, 2007
(54) METHOD FOR AUTHENTICATION
(73) Assignee: NEC Corporation, Tokyo (JP)
(21) Appl. No.: 11/519,929
(22) Filed: Sep. 13, 2006


(19) United States
(12) Patent Application Publication (10) Pub. No.: US 2008/0084294 A1
ZHIYING et al. (43) Pub. Date: Apr. 10, 2008
(54) WIRELESS SENSOR NETWORK AND ADAPTIVE METHOD FOR MONITORING THE SECURITY THEREOF
(73) Assignee: ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE, Daejon (KR)
(21) Appl. No.: 11/539,084
(22) Filed: Oct. 5, 2006


(19) United States
(12) Patent Application Publication (10) Pub. No.: US 2006/0159260 A1
Pereira et al. (43) Pub. Date: Jul. 20, 2006
(54) METHOD AND COMMUNICATION SYSTEM EMPLOYING SECURE KEY EXCHANGE FOR ENCODING AND DECODING MESSAGES BETWEEN NODES OF A COMMUNICATION NETWORK
(73) Assignee: EATON CORPORATION
(21) Appl. No.: 11/035,898
(22) Filed: Jan. 14, 2005

authentication,

trust estimator, secure key,

encoding and decoding messages

Additionally

Link Layer Threats

- Eavesdropping
- Collisions in specific packets
- Packet-tracing

Network Layer Threats

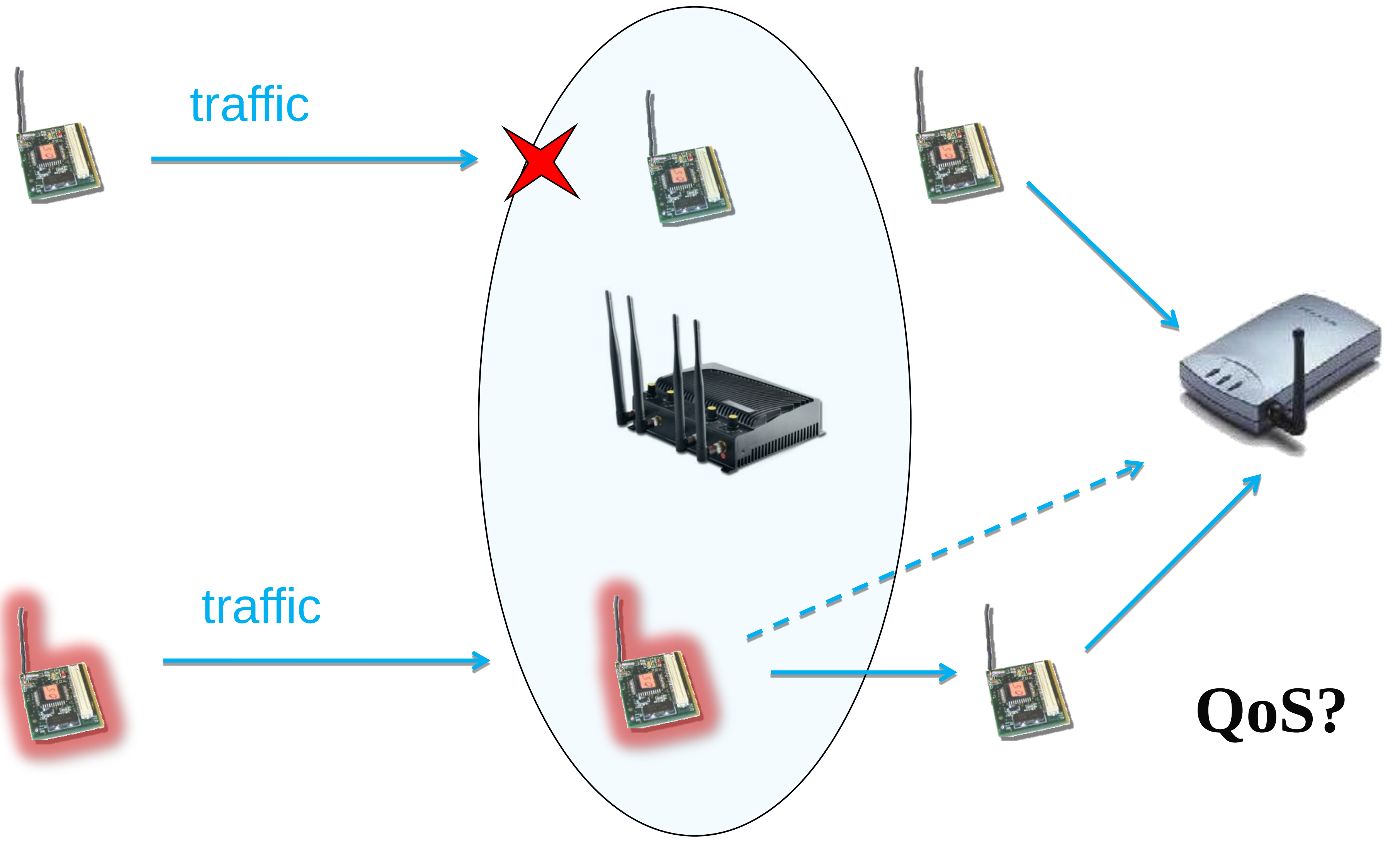
- Sybil
- Selective forwarding
- Sinkhole
- Blackhole
- Wormholes
- Acknowledgment spoofing

Application Layer Threats

- Byzantine Attacks

DoS (Energy Exhaustion, Vampire attack etc. **)**

Jamming



Symptoms of DoS

- unusually slow
- unavailability
- inability to access
- dramatic increase in the transmitted packets
- connectivity degradation

US-CERT

United States Computer Emergency Readiness Team

DoB effect

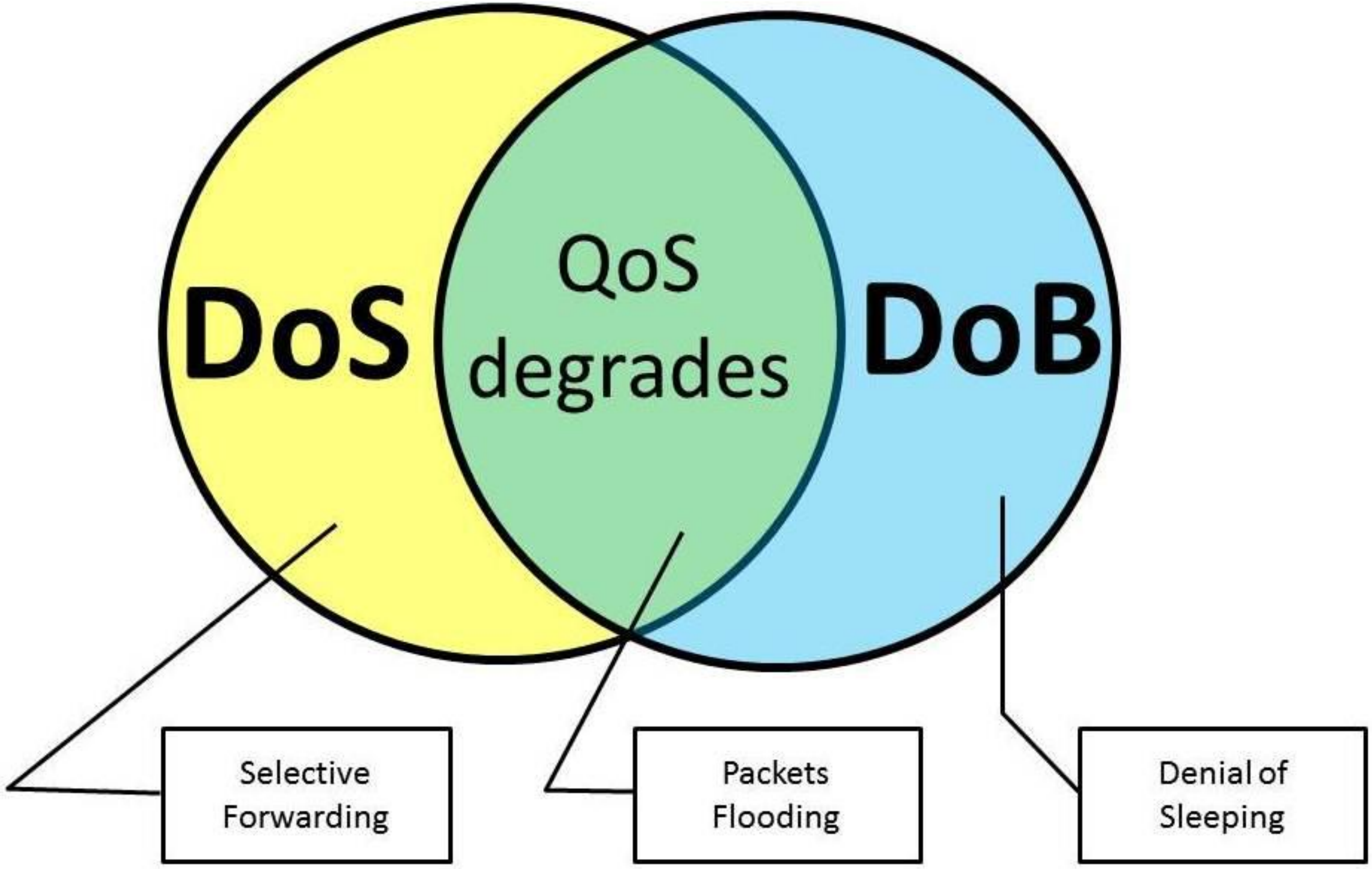
Up to some time moment

- reduced latency
- SNR can be improved
- reduced number of packets
- higher connectivity

US-CERT

???

DoB Positioning



DoS EE

- wormhole attack
- clone attack (nodes replication attack).
- nodes inactivation
- encryption based DoS
- malware

Etc.

DoS EE

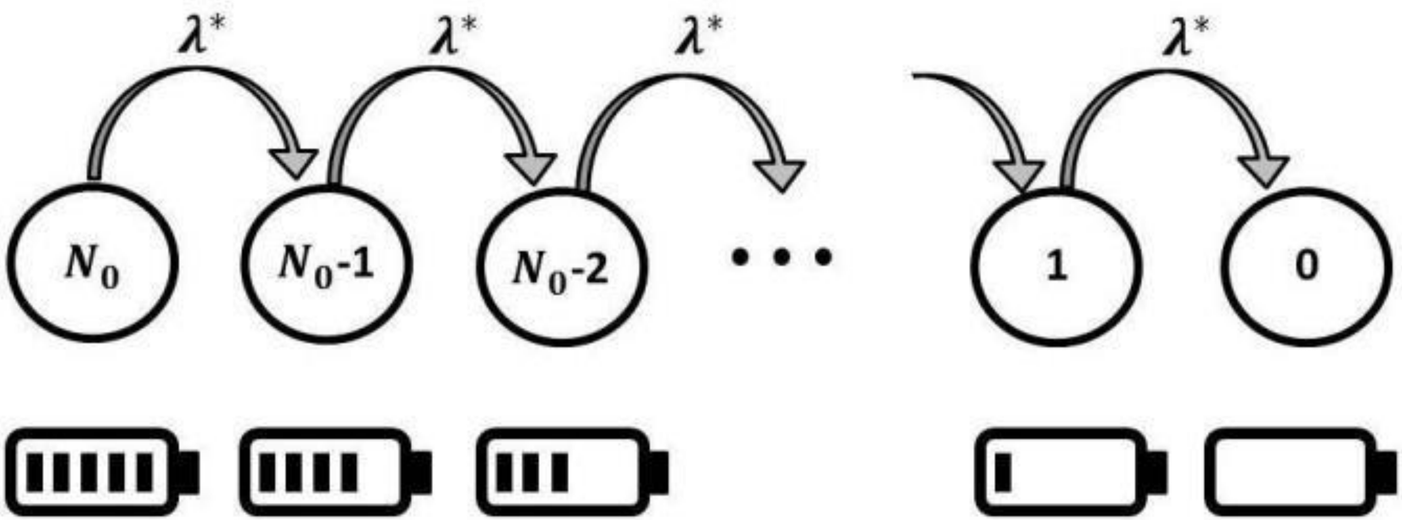
- malware
- relaxed jamming
- Denial-of-Sleep attack (MAC vulnerabilities)
- Encryption based DoS
- Malware

Etc.

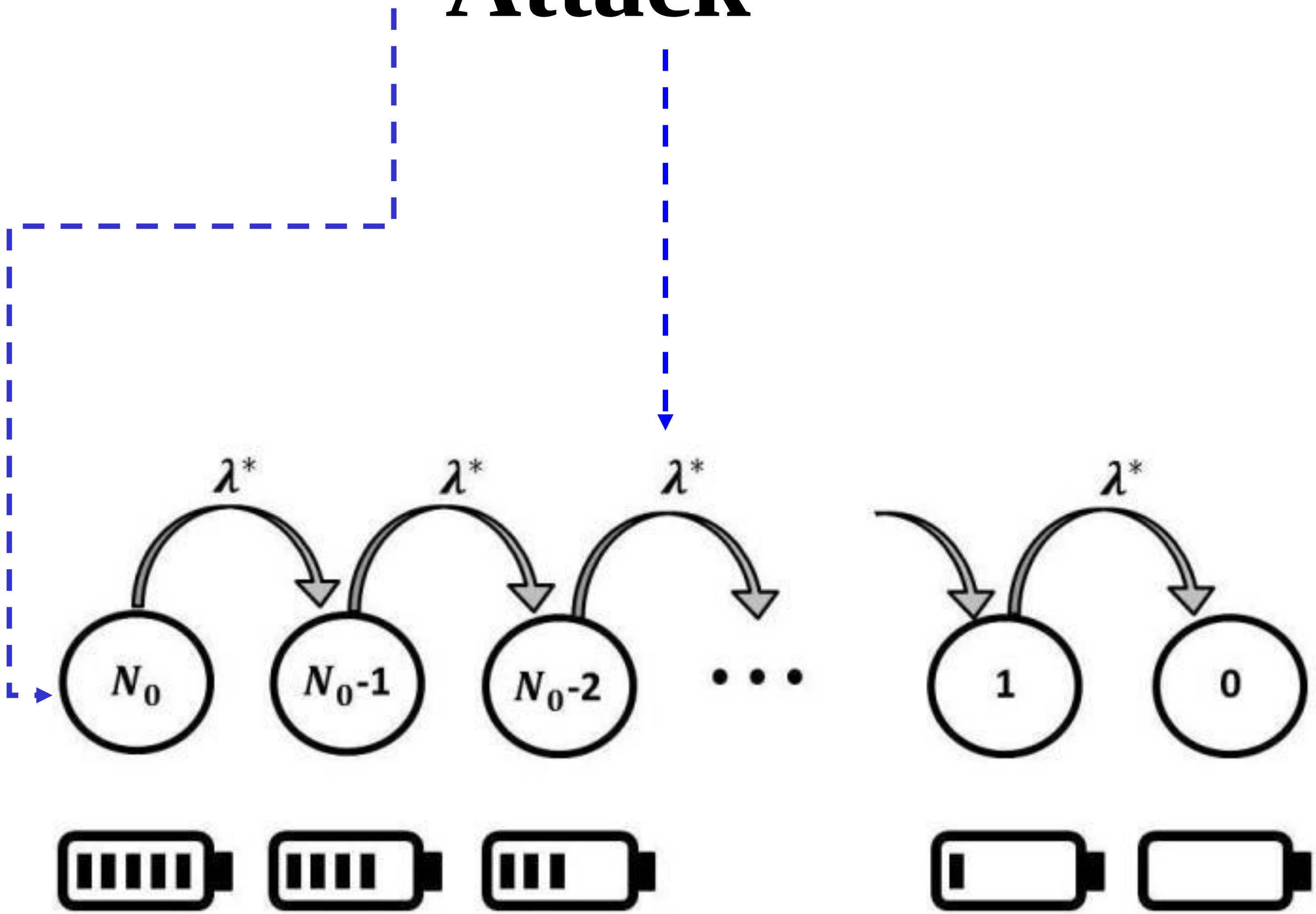
System Model

CTMC

$$\{X(t), t \geq 0\}, \quad X(0) = \frac{N_0}{e_0}$$



Attack



Equations

$$\frac{dP_k(t)}{dt} = -\lambda P_k(t) + \lambda P_{k+1}(t),\ \ 0 < k < N_0,$$

$$\frac{dP_{N_0}(t)}{dt} = -\lambda P_{N_0}(t),$$

$$\frac{dP_0(t)}{dt} = \lambda P_0(t),$$

$$P_k(t) = \frac{(\lambda t)^{N_0-k}}{(N_0-k)!} e^{-\lambda t}, \qquad 0 < k \le N_0.$$

$$P_0(t) = 1 - e^{-\lambda t} \sum_{k=1}^{N_0} \frac{(\lambda t)^{N_0-k}}{(N_0-k)!} = 1 - e^{-\lambda t} \sum_{k=0}^{N_0-1} \frac{(\lambda t)^k}{k!}.$$

MTTF

$$\text{MTTF} = \frac{N_0}{\lambda}$$

Network Lifetime

$$\tau = \min\{T_1, T_2, \dots, T_m\}.$$

$$\mathbb{P}(\tau > t) = \mathbb{P}\left(T_j > t \ \ \forall j \in \overline{1,m}\right) = \prod_{j=1}^{m}\left(1 - F_{T_j}(t)\right).$$

CDF of τ

$$F_\tau(t) = 1 - \mathbb{P}(\tau > t).$$

$$F_\tau(t) = 1 - \left(1 - F_T(t)\right)^m = 1 - e^{-\lambda m t}\left(\sum_{k=0}^{N_0-1}\frac{(\lambda t)^k}{k!}\right)^m.$$

SSF

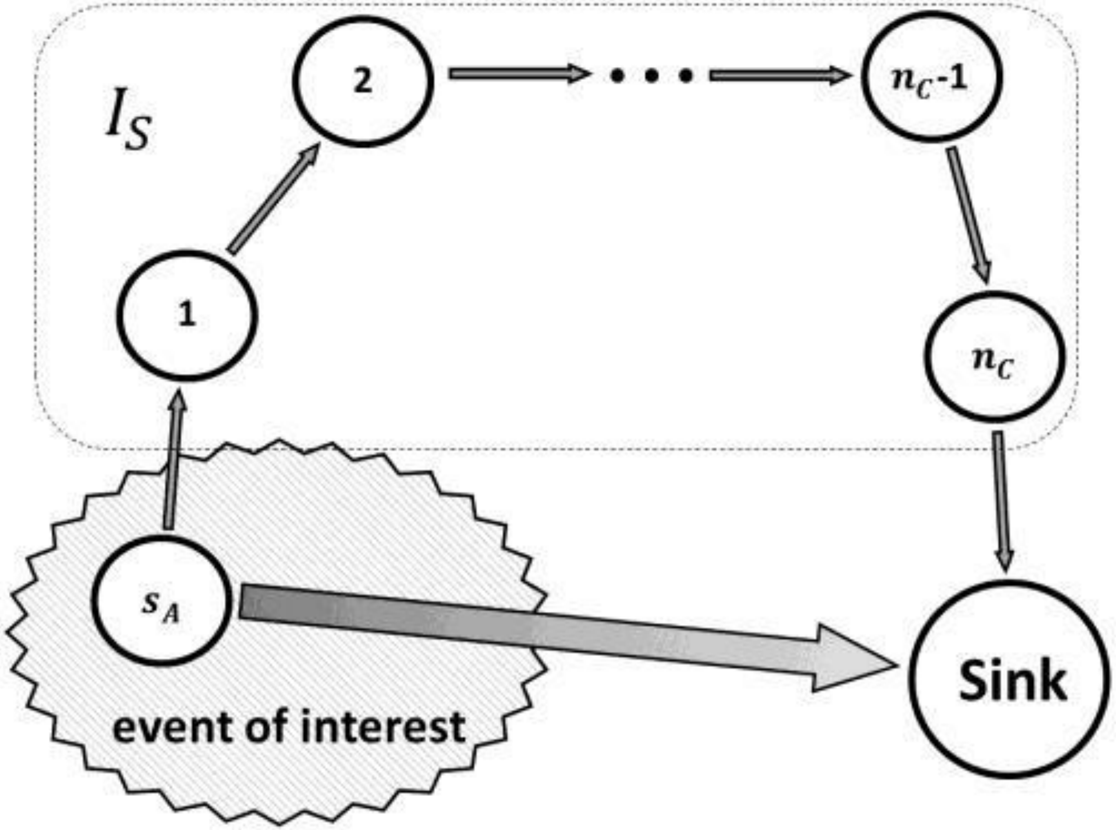
The probability that a network has not failed within time h:

$$\mathcal{H}(h, \lambda, y) : \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \times \mathbb{N} \rightarrow \mathbb{R}_{[0,1]}$$

$$\mathcal{H}(h, \lambda, y) = e^{-\lambda\, m\, h} \left(\sum_{k=0}^{y-1} \frac{(\lambda\, h)^k}{k!} \right)^m .$$

System Survivability Function

Problem of Distributed Detection



$$E_N = \sum_{j=1}^{n_c} e(j) + e(s_A)$$

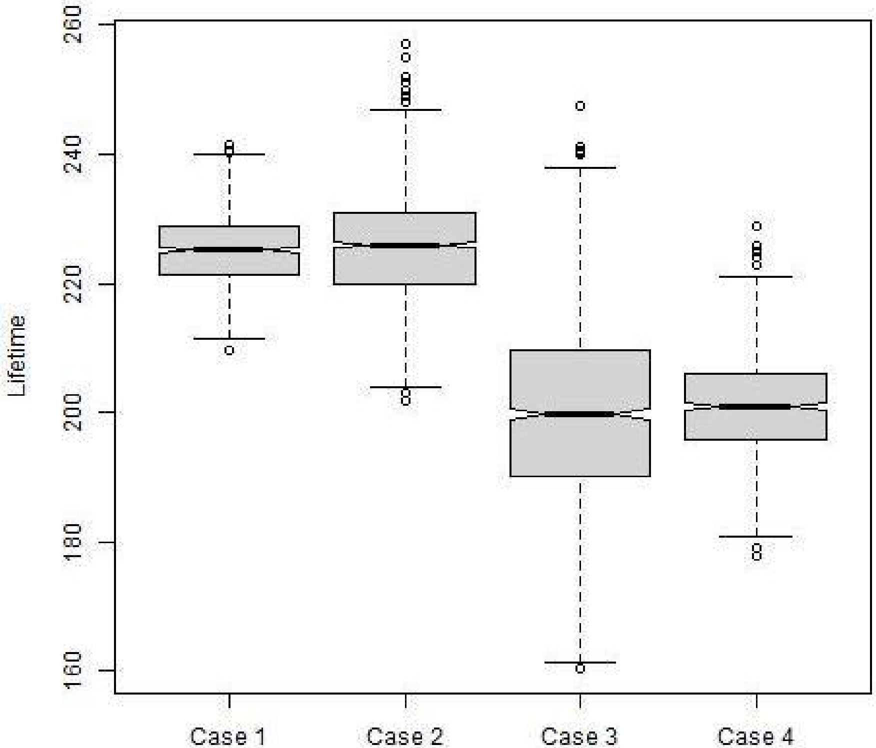
$$\forall j \in I_S \;\; e(j) = e(s_A) = a \cdot d^{\gamma}$$

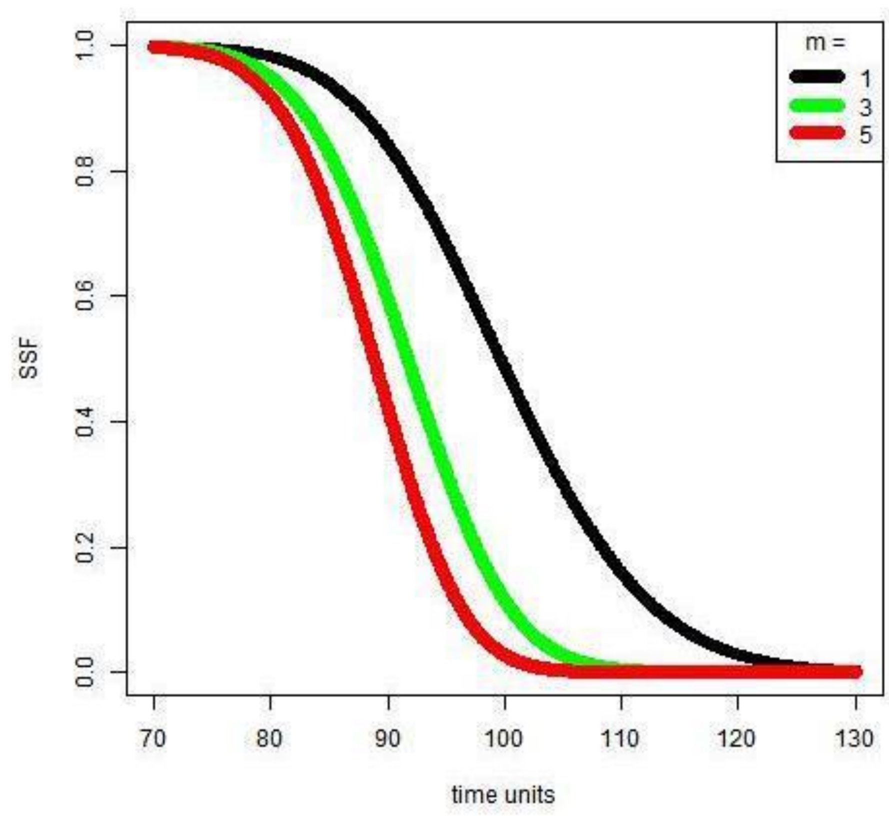
$$E_N = (n_c + 1) \cdot a \cdot d^{\gamma}$$

$$E_A = a \cdot d_S^{\gamma}$$

$$E_A < E_N$$

Performance Analysis





Conclusion

Novel Type of Attack : DoB

Novel Taxonomy

The attack can be caused by deliberate action or a random combination of circumstances.

To estimate the attack effect, CTMC based model are offered

Thank you for the attention!

Q&A