



# 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.

## 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

  (217)  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 26, 2014

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

By Sal Cangelosi on August 15, 2013 at 11:45 am | [7 Comments](#)

## 'Smart' home devices used as weapons in website attack

 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 

THE EXPERTS

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

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

# The Washington Post

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

By Andrea Peterson October 26, 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 Wise, USATODAY Published 6:44 p.m. ET Oct. 3, 2016 | Updated 8:02 p.m. ET Oct. 3, 2016



## 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



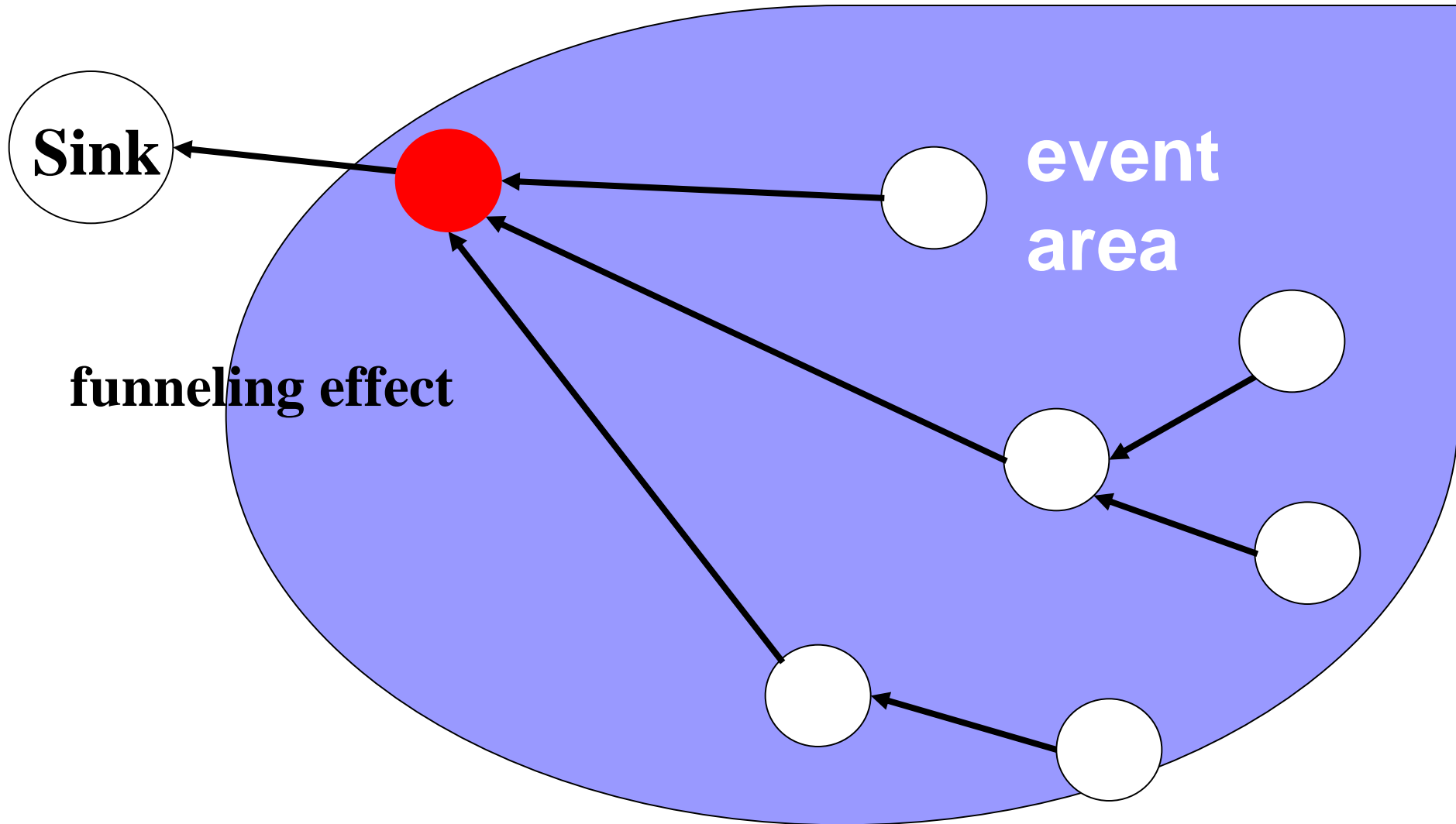
# Motivation

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



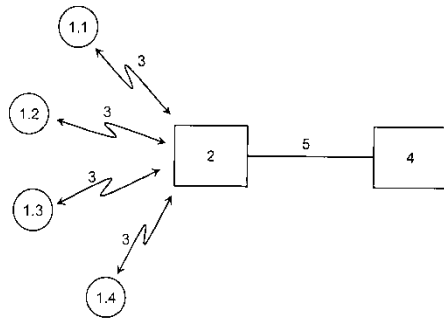
# Patents Search



(19) United States  
 (12) Patent Application Publication  
 Westhoff  
 (10) Pub. No.: US 2007/0067631 A1  
 (43) Pub. Date: Mar. 22, 2007

(54) METHOD FOR AUTHENTICATION  
 (72) Inventor: Dirk Westhoff, Heidelberg (DE)  
 Correspondence Address:  
 YOUNG & THOMPSON  
 745 SOUTH 2ND STREET  
 2ND FLOOR  
 ARLINGTON, VA 22202 (US)  
 (73) Assignee: NEC Corporation, Tokyo (JP)  
 (21) Appl. No.: 11819329  
 (22) Filed: Sep. 13, 2006  
 (30) Foreign Application Priority Data  
 Sep. 20, 2005 (JP) 2005-044349-2

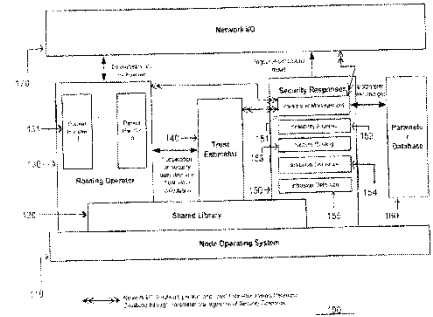
Publication Classification  
 (51) Int. Cl. H04L 9/00 (2006.01)  
 (52) U.S. Cl. 713/158  
 (57) ABSTRACT  
 A method for authentication between at least two nodes within a network, preferably a wireless sensor network, is disclosed. The sending node comprises a first long code value by using a hash function h. A transmission of possibly few additional data over the network is designed in such a way that from the sending node to the receiving node only factors of the hash value are transferred as truncated hash value. Wherein h is a 1X but arbitrary natural number between 1 and 1-1. The transmitted hash value is compared to a computed hash value at the receiving node.



(19) United States  
 (12) Patent Application Publication  
 ZHIVING et al.  
 (20) Pub. No.: US 2008/0084294 A1  
 (43) Pub. Date: Apr. 10, 2008

(54) WIRELESS SENSOR NETWORK AND ADAPTIVE METHOD FOR MONITORING THE SECURITY THEREOF  
 (75) Inventor: Yao ZHIVING, Daejeon (KR); Yunsang BOK, Daejeon (KR); Sung Jung KIM, Daejeon (KR); CheolSik PYO, Daejeon (KR); Jaegwan CHOI, Daejeon (KR)  
 Correspondence Address:  
 ILC PARK & ASSOCIATES, PLLC  
 8801 LEBANON PIKE, SUITE 5000  
 VIENNA, VA 22182  
 (73) Assignee: ILC ELECTRONICS AND TELECOMMUNICATIONS, KOREA (KR)  
 (21) Appl. No.: 11876084  
 (22) Filed: Oct. 5, 2006

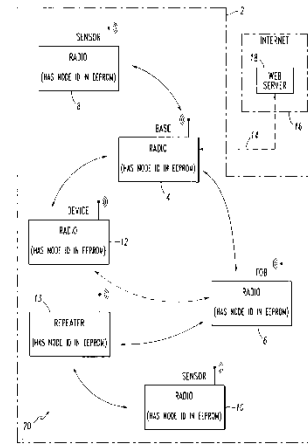
Publication Classification  
 (51) Int. Cl. G08B 00/00 (2006.01)  
 (52) U.S. Cl. 340/670,222  
 (57) ABSTRACT  
 The present invention relates to a sensor network having nodes and a base station performing monitoring of neighboring sensor nodes, and to an adaptive method for monitoring that manages chain of neighboring sensor nodes for monitoring security in the sensor network. The sensor network includes a base station and a plurality of sensor nodes for reporting sensed information packets to the base station, wherein radiofrequency signals relayed by other sensor nodes. A single sensor node may have a time constraint to be able to communicate with the base station at a neighboring sensor node by determining a personal reference and receiving personal reference from one sensor node. Based on the radiofrequency signal, the single node transmits a node for transmitting packets to the base station.



(19) United States  
 (12) Patent Application Publication  
 Pereira et al.  
 (10) Pub. No.: US 2006/0159260 A1  
 (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  
 (75) Inventor: Luis R. Pereira, Milwaukee, WI, US; Kamalavasan Srinivasan, Madison, WI, US  
 Correspondence Address:  
 MARTIN J. MORAN, ESQ.  
 Eaton Electrical, Inc.  
 Technology & Quality Center  
 170 Indiana Drive, HDX, Park West  
 Pittsburgh, PA 15275-1432 (US)  
 (73) Assignee: EATON CORPORATION  
 (21) Appl. No.: 11/035,898  
 (22) Filed: Jan. 14, 2006

Publication Classification  
 (51) Int. Cl. H04L 9/00 (2006.01)  
 (52) U.S. Cl. 380/44  
 (57) ABSTRACT  
 A method enables and decodes messages between nodes of a wireless communication network. A first node, such as a job, is mixed with a secure node, such as a base station, of the wireless communication network. A time duration of the mixing is determined in the job. The time duration of the mixing is also determined in the base station. An encryption key is generated based upon the time duration of the job. The encryption key is also generated based upon the time duration in the base station. Subsequently, communication messages over the wireless communication network are encrypted and decrypted between the job and the base station, employing the encryption key.



authentication,  
 trust estimator, secure key,  
 encoding and decoding messages

# Additionally

## *Link Layer Threats*

- Eavesdropping
- Collisions in specific packets
- Packet-tracing

## *Network Layer Threats*

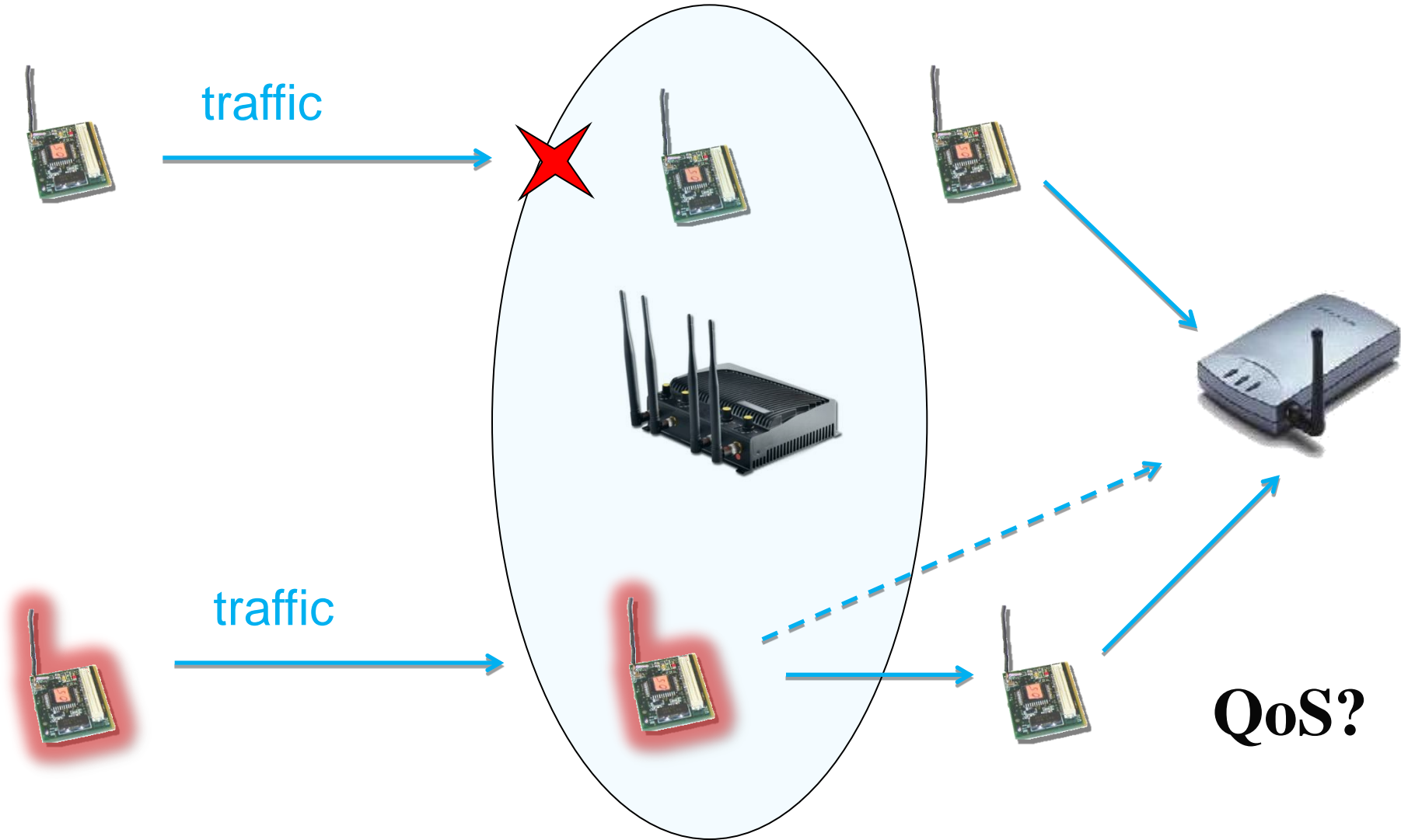
- Sybil
- Selective forwarding
- Sinkhole
- Blackhole
- Wormholes
- Acknowledgment spoofing

## *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

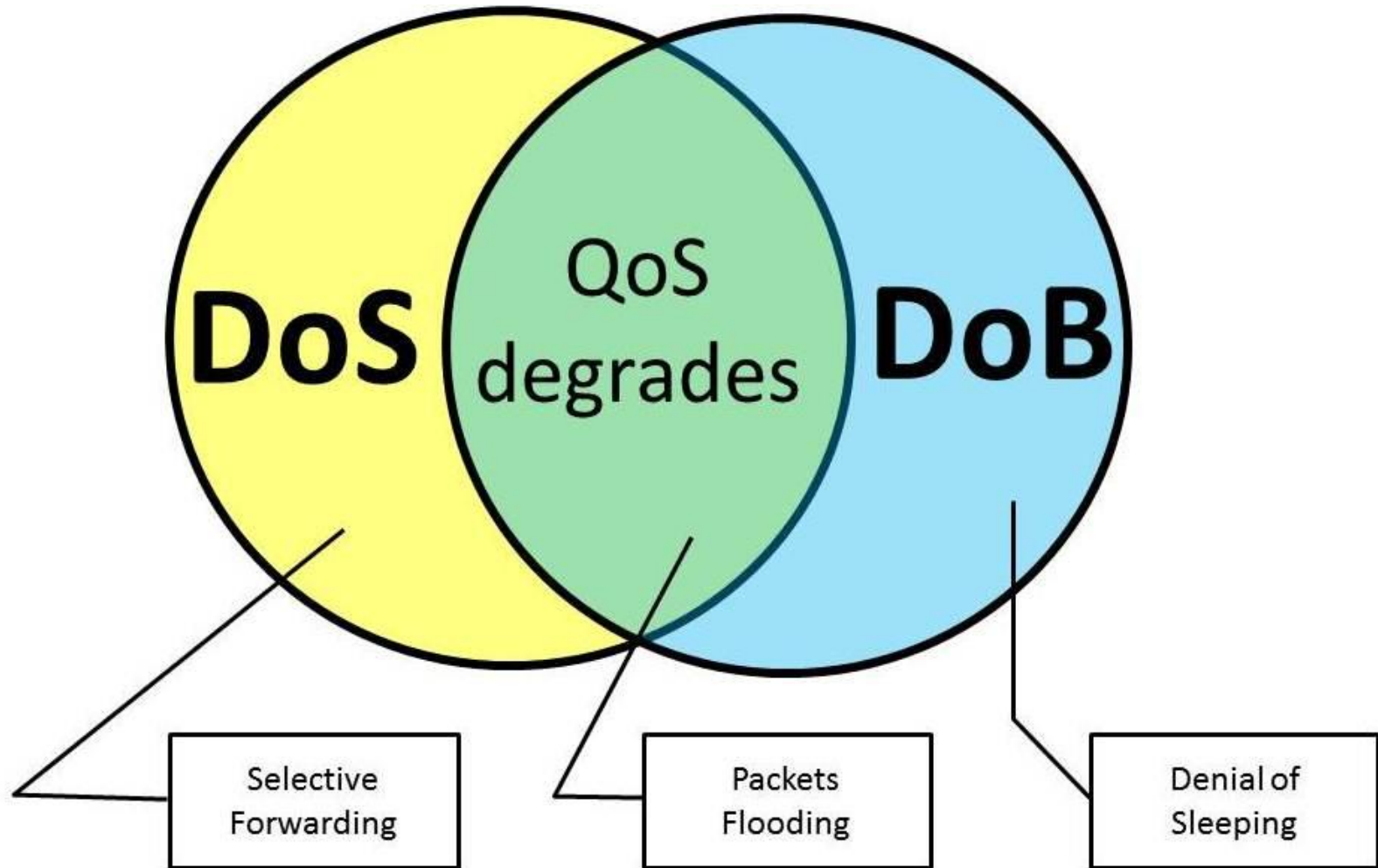
Up to some time moment

- 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

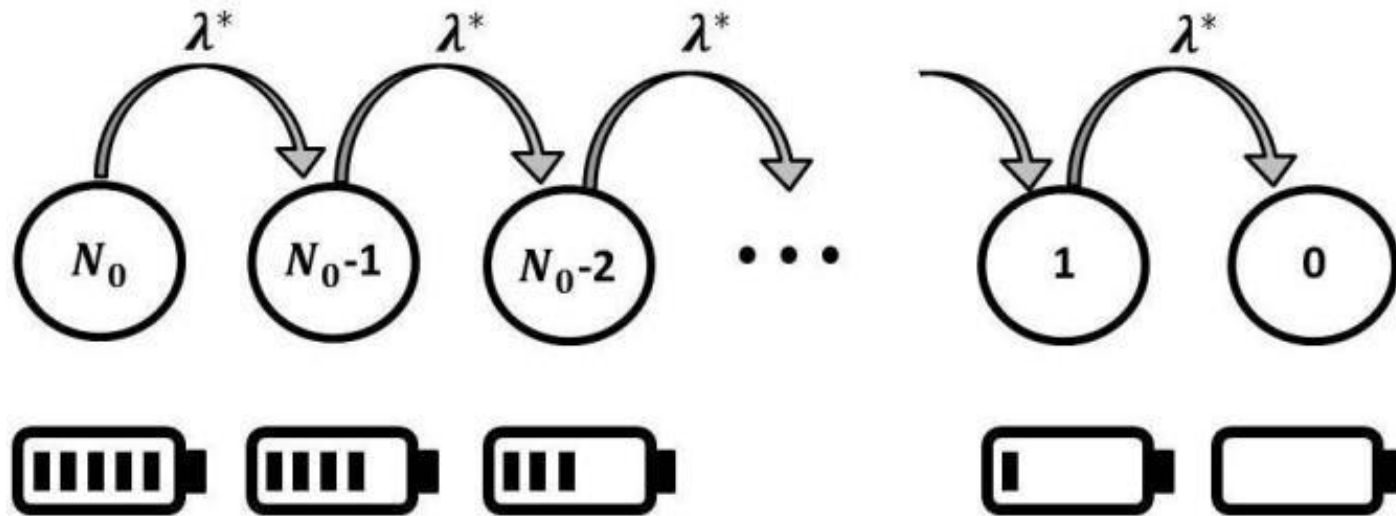
Etc.



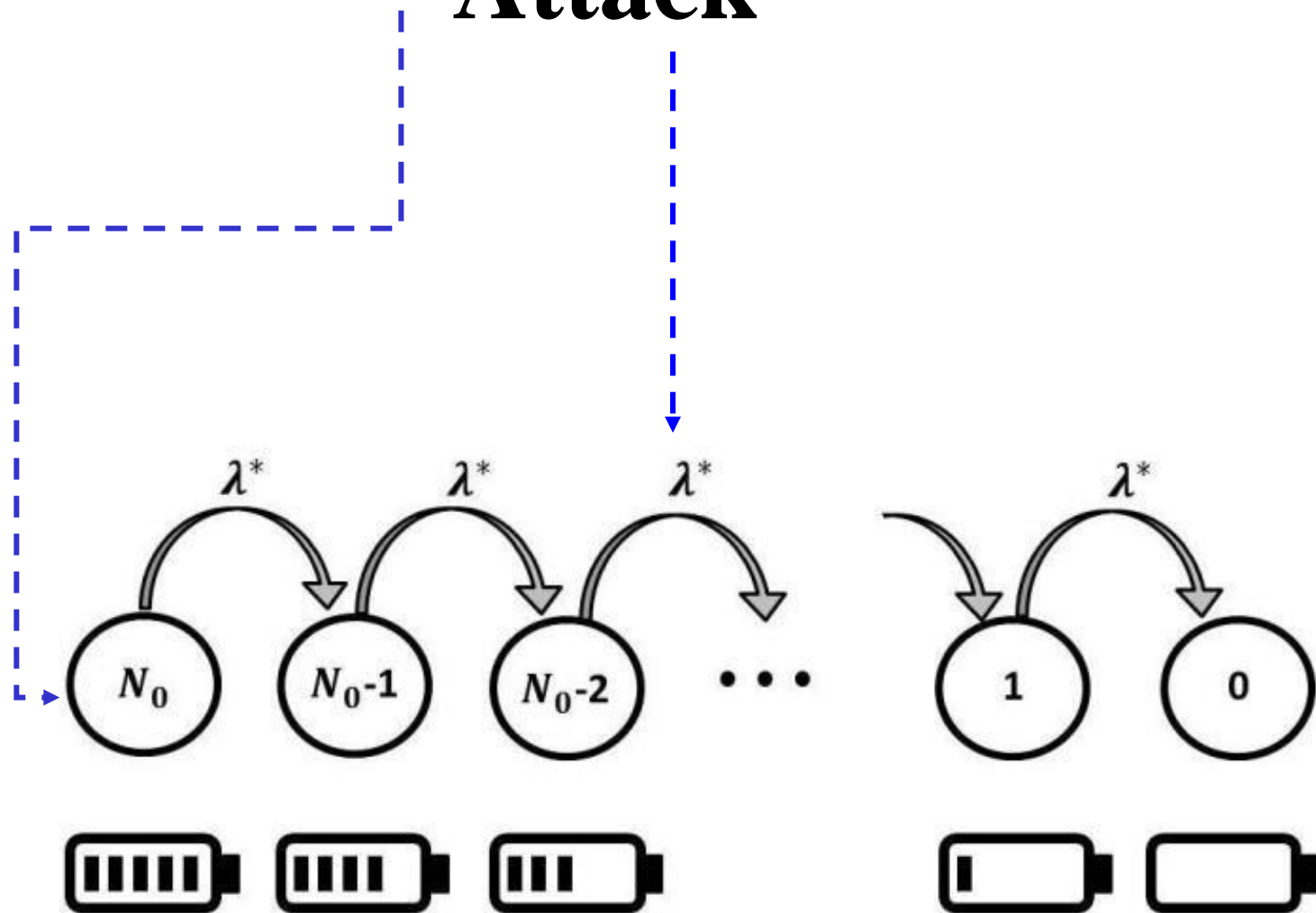
# System Model

CTMC

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



# Attack



# Equations

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

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

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

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

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

# MTTF

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

Network Lifetime

---

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

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

CDF of  $\tau$

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

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

# SSF

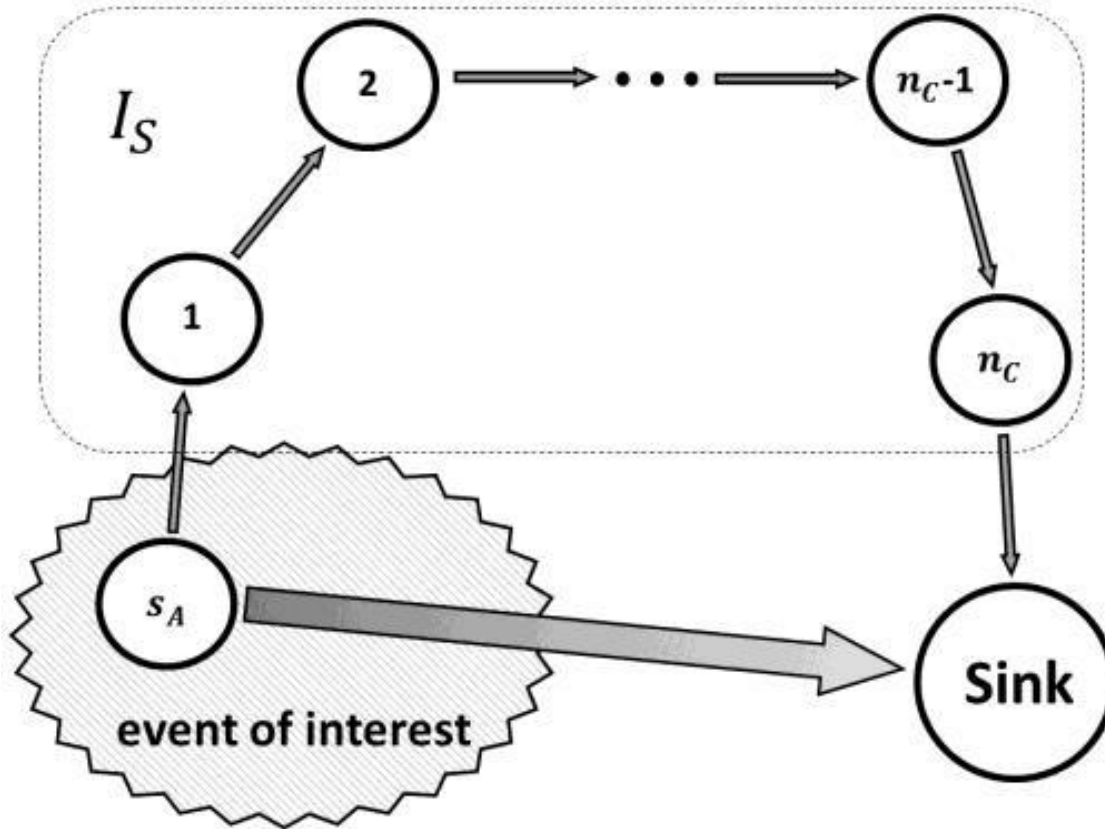
The probability that a network has not failed within time  $h$ :

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

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

*System Survivability Function*

# Problem of Distributed Detection



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

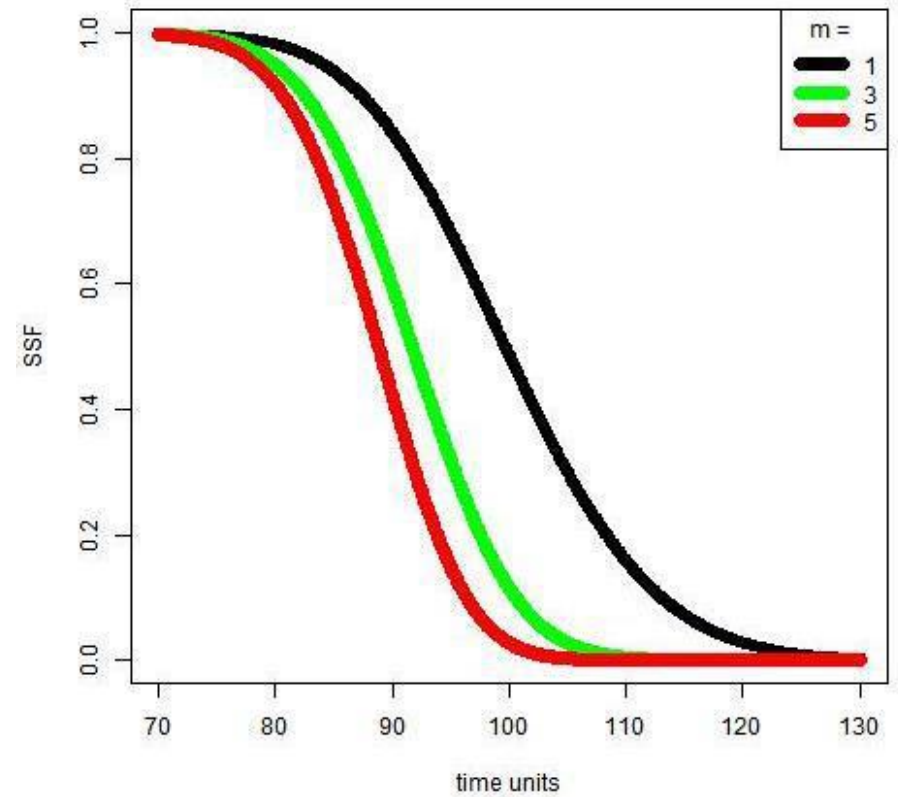
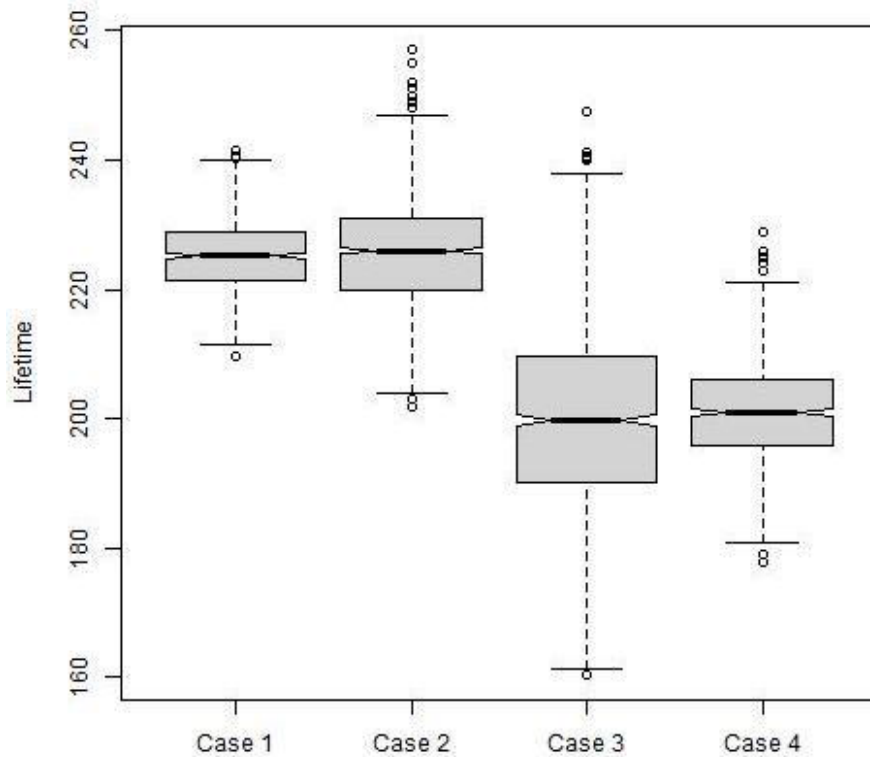
$$\forall j \in I_S \quad e(j) = e(s_A) = a \cdot d^Y$$

$$E_N = (n_c + 1) \cdot a \cdot d^Y$$

$$E_A = a \cdot d_S^Y$$

$$E_A < E_N$$

# 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