International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 14
November 2017

# Optimization of Malware Propagation in Wireless Sensor Networks

**Srilakshmi Rayapaneni[1] & Dr.B.A.S.Roopa Devi[2]**

[1]M.Tech Student, Dept of CSE, QIS College of Engineering and Technology, Ongole, AP, India.

[2] HOD, Dept of CSE, QIS College of Engineering and Technology, Ongole, AP, India.

## Abstract I.

Malware is vindictive programming in network systems and spreading broadly all through in network area and make a basic danger in network security. Till date we don't know about malware behavior in network systems. In this paper, we will discover how malware spreads in networks and fabricate a two layer epidemic model for malware propagation and we utilize the SI model, which is the least complex for epidemic investigation. In proposed model our examination says that conveyance of a given malware takes after exponential dissemination and power law distribution with a short exponential tail and power law distribution at its early, late and last stages and tests likewise done by taking two true malware data collections and results confirm our hypothetical values.

**Keywords** — Malware, Propagation, Two Layer Epidemic Modeling, Power law Distribution.

## INTRODUCTION

Malware is the general term covering all the different types of alerts to your system security, for example, infections, spyware, worms, Trojans, root packs and so on, assemble sensitive information, get access to private computer systems, or show unfortunate post. Malware is sense by its antagonistic target, respond inverse to the requests of the system client, and does not cover software programming that causes inadvertent damage because of a few shortages. The word malware is as often as possible utilized, and request to both genuine (vindictive) malware and unintended harmful software programming. The epidemic theory plays a main part in malware spreading planning. The present models for malware spread separate in two types: the study of epidemiology and the control theoretic plan. This task portrays the spreading of malware in words of systems (e.g., autonomous systems (AS), Internet

Service Provider spaces, conceptual systems of smart mobiles who distribute similar vulnerabilities) at tremendous amounts. In this kind of setup, we have an enough size of data at a tremendous scale to cover the necessities of the SI model. Dissimilar to from the conventional epidemic designs, we split our outline into two sections. As a matter of first importance, for a given time since the breakout of a malware, we discover what number of systems has been compromised in view of the SI model. Second, for a compromised network, we discover how many numbers of hosts have been compromised since the time that the system was compromised. With this two layer configuration set up, we can find the aggregate number of compromised hosts and their allotment as systems. Through our fastidious investigation, we find that the dispensation of a given malware takes after an exponential agreement at its essential stage, and executes a power law distribution with a little exponential tail at its last stage, and at last meets to a power law distribution.

## II. BACKGROUND WORK

The epidemiology models have one basic condition that is a vast vulnerable population in light of the fact that their rule depends on various conditions. We can discover more details about epidemiology model by D.J.Daley and J.Gani. Zhou et al by utilizing Susceptible-infected (SI) show at beginning period he anticipate development of web worms .A Susceptible-infected recovered model (SIR) utilized by Geo and Liu to depict mobile infection propagation. The Distribution of malware in huge scale systems has an adequate volume of information to meet the prerequisites of the SI model. Aside from epidemic model, we partitioned our model in to two layers. To start with, for a given time we figure what numbers of systems have been traded off in light of SI model. Second, for undermine network we calculate what number of host have been undermine from the time that system have been undermine. From this investigation we find that the circulation of given malware takes after power law distribution at ahead of schedule organize, and acknowledge control law dispersion with short exponential tail at its late stage. The two layer epidemic model better in huge scale systems contrasted and single layer epidemic model.

## III. EXISTING SYSTEM

The present models for malware isolated in to two types. the study of epidemic model and control theoretic model. The control framework theory based models attempt to identify the spread of malware. The studies of epidemic model are more focus on number of undetermined hosts and their distributions said by S.H.Sellke, N.B.Shroff and S.Bagchi. The epidemic hypothesis assumes a major part in malware propagation.

**Disadvantages:**

a) One critical condition for the epidemic models is a large vulnerable population because their principle is based on differential equations.

b) As pointed by Willinger et al. the findings, which we extract from a set of observed data, usually reflect parts of the studied objects. It is more reliable to extract theoretical results from appropriate models with confirmation from sufficient real world data set experiments.

## IV.PROPOSED METHODOLOGY

In this paper, we have investigated the issue of malware distribution in huge scale networks. There are numerous headings that could be additionally investigated. We show some essential ones as takes after.

a) Epidemic model for the proposed two layer technique. In this paper, we utilize the SI model, which is the least complex for epidemic investigation. More reasonable models, e.g. SIS or, then again SIR, could be served the same issue. b) Multi layer modeling. We employ the liquid model in both of the two layers in our analysis as the two layers are sufficiently vast furthermore; meet the conditions for the modeling techniques. With a specific end goal to enhance the accuracy of malware propagation, we may expand our work to n (n > 2) layers. In another situation, we may hope to model malware propagation for middle scale systems, e.g. An ISP connects with numerous sub networks. c) The progress from exponential distribution to power law distribution. It is vital to explore when and how a malware distribution moves from an exponential distribution to the power law. In different words, in what capacity would we be able to clearly characterize the transmission point between the beginning stages what’s more, the late stage.

## III. LITERATURE SURVEY

### Distributed Detection of Node Replication Attacks in Sensor Networks

**Authors:** Bryan Parno† Adrian Perrig‡

The minimal effort, off-the-shelf equipment parts in unshielded sensor-arrange nodes abandon them helpless to compromise. With little exertion, a challenger may catch nodes, examine and repeat them, and surreptitiously embed these imitations at strategic areas inside the network system. Such attacks may have serious outcomes; they may enable the challenger to damage system information or even detach node parts of the system. To address these key constraints, we propose two new methodologies in light of developing properties, i.e., properties that emerge just through the collection activity of various nodes. Randomized Multicast distributes node area data to randomly chosen witnesses, misusing the birthday paradox to recognize replicated hopes, while Line-Selected Multicast utilizes the topology of the system to identify replication.

**BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks**

**Authors:** Rongxing Lu,, Xiaohui Liang

Injecting false information attack is a notable genuine threat to remote sensor systems, for which an adversary reports false data to sink causing error choice at upper level and energy misuse in on the way nodes. In this paper, we propose a novel transmission capacity effective cooperative authentication (BECAN) technique for separating infused false information. In this paper, we have proposed a novel bandwidth efficient cooperative verification (BECAN) technique for filtering the injected false information. By theoretical examination furthermore, simulation assessment, the BECAN technique has been shown to accomplish not just high en-routing separating probability additionally high dependability with multi-reports. Because of the straightforwardness and effectiveness, the BECAN technique could be connected to other quick and appropriate authentication situations, e.g., the efficient verification in remote mesh networks. In our future work, we will explore how to protect/moderate the posse injected false information attack from mobile compromised sensor devices.

**Lifetime and Energy Hole Evolution Analysis in Data-Gathering Wireless Sensor Networks**

**Authors:** Yaoxue Zhang, Kuan Zhang, Xuemin

Network System lifetime is an essential performance metric to evaluate information gathering remote sensor systems (WSNs) where battery-controlled sensor nodes periodically sense the earth furthermore, forward composed samples to a sink node. In this paper, we propose a logical model to evaluate the whole network system lifetime from system initialization until the point when it is totally disabled, and decide the limit of energy gap in an information gathering WSN. In this paper, we have built up a scientific model to estimate the traffic load, energy utilization and lifetime of sensor nodes in an information gathering WSN. With the scientific show, we have computed the network topology lifetime under guaranteed rate of dead nodes, and broke down the developing time also, area of energy gap, and in addition its development procedure.

## IV. IMPLEMENTATION

### Network Setup Module

Our first module is setting up the remote sensor network model. We consider a large-scale, standardized sensor network consisting of resource-constrained sensor nodes. Corresponding to previous distributed malware detection approaches; we assume that two layer epidemic model feature is accessible in the wireless sensor network. In this work, we consider a network topology infrastructure with one network router and a huge number of remote sensor nodes randomly circulated in the system. We utilize the source node as the beginning of the system organizer. In light of the area of the network router, the network topology region is for all intents and purposes isolated into neighboring rings, where the width of each ring is the same as the transmission scope of sensor nodes. The system is a thickly deployed WSN, i.e., i) for every node, there exist sensor nodes situated in each neighboring ring, and for each ring, in each ring, and there are sufficient sensor nodes to develop a directing path along the ring.

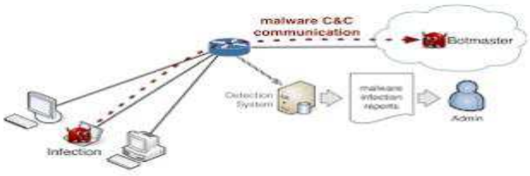

**Fig 1. System Architecture**

The topology model can be basically reached out into the instance of various network routers, where different routers utilize two layer epidemic model and power law distribution to correspondence with its sensor nodes. For every sensor, it needs to achieve the tasks of information collecting and malware recognition. In each information collecting cycle, sensors send the gathered information to the source node through multi-hop ways. To be equipped for directing authenticity verification, each sensor has a similar buffer storage ability to store the data.

### Filtering Malware Detection

As a general rule, various malware may in a similar place at the same network systems. Because of the way that distinctive malware concentrate on various vulnerabilities, the distributions of various malware may not be the same. It is testing and interesting, as far as wireless network systems to set up scientific models for numerous malware propagations. The two layers in the two layers are adequately large and meet the conditions for the demonstrating techniques. We may stretch out our work to layers in request to enhance the precision of malware proliferation.

**A Process of Malware Propagation**

In view of the proposed technique, our analysis demonstrates that the distribution of a given malware takes after exponential distribution, power law circulation with a short exponential tail, and power law allocation at its initial, late and final stages, individually.

**Initial Stage:**

A beginning time of the breakout of a malware implies just a little percentages of helpless hosts have been compromised, and the distribution takes after exponential conveyances.

**Final stage:**

The last stage of the broadcast of a malware means that all vulnerable hosts of a given network system have been compromised.

**Late stage:**

A late stage means the time distance between the initial stage and the final stage.

**Epidemic Model Analysis**

The epidemic models have demonstrated effective what's more; suitable for a framework that has a vast number of powerless hosts. In other words, they are appropriate at a full scale level. Zou et al. showed that they were appropriate for the investigations of Internet based malware spread at the beginning period. We note that there are many variables that effect the malware spread or botnet enrollment recruitment, for example, system topology, enrollment recurrence, and connection status of helpless hosts. Every one of these variables adds to the speed of malware distribution. Luckily, we can incorporate all these elements into one parameter as infection rate b in epidemic hypothesis. Along these lines, in our analysis, let N be the aggregate number of defenseless has of an expansive scale network (e.g., the Internet) for a given malware. There are two statuses for any of the N nodes, either infected nodes or powerless nodes. Let L(t) be the quantity of infected hosts at time t, at that point we where R(t), and Q(t) speak to the number of excepted hosts from the polluted population, and the quantity of excepted hosts from the vulnerable population at time t.

$$\frac{dI(t)}{dt} = \beta(t)\,[N - R(t) - I(t) - Q(t)]\,I(t) - \frac{dR(t)}{dt}$$

The variable β (t) is the contamination rate at time t. For our examination, technique is excessively point by point and a bit much as we hope to know the engendering and conveyance of a given malware. Accordingly, we utilize the given susceptible infected technique.

$$\frac{dI\ (t)}{dt} = \beta I\ (t)\ [N - I\ (t)]$$

## V. PERFORMANCE EVALUATION

In this area, we look at our hypothetical analysis through two well known high scale malware: Android malware and Conficker. Android malware is a current quick developing and prevailing cell phone based malware. Various from Android malware, the Conficker worm is an Internet based state-of-the-art botnet. Both the informational collections have been broadly utilized by the group. From the Android malware informational collection, we have a review of the malware advancement from August 2010 to October 2011. There are 1260 tests altogether from 49 distinctive Android malware in the informational index.

For a given Android malware program, it just concentrates on one or a number of particular vulnerabilities. In this way, all smart phones share these vulnerabilities frame a particular system for that Android malware. In different words, there are 49 networks should organizes in the information set, and it is sensible that the number of populations in each system is large.

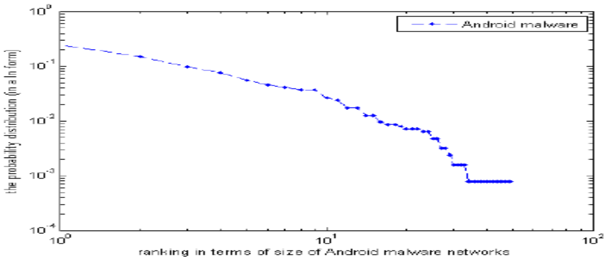

**Fig 2.The probability allocation of Android malware in terms of networks**

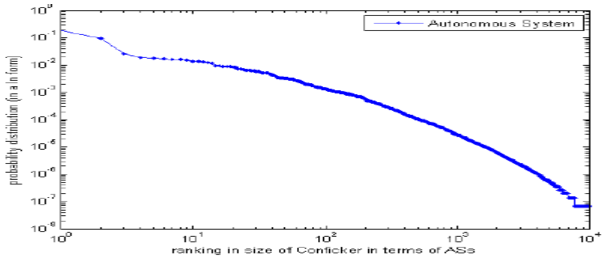

**Fig 3. Power law distribution of Conficker in terms of autonomous networks.**

We sort the malware subclasses as indicated by their size (number of tests in the informational index), and present them in a loglog design in Figure 2, the outline is around a straight line. As it were, we can say that the Android malware distribution in terms of network systems takes after the power law distribution.

## VI. CONCLUSTION

In this paper we totally known the issue of malware distribution at huge scale wireless sensor network systems and answer for this issue is given by cyber defender as the network security group. Contrasting and single layer epidemic model, this two layer epidemic model demonstrate enhances accuracy. In this two layer, upper layer focus on the networks of a huge scale and lower layer focus on the hosts of a given network. After playing out the confined examination in light of the proposed model we acquire three conclusions: The given malware in systems take after exponential distribution, power law distribution at its initial, late and last stage. After performing tests by taking two true large scale malware their outcomes accommodates hypothetical values.

## FEATURE WORK

In this idea mainly we need to think about when and how malware distribution moves from an exponential distribution to the power law distribution. In actuality at a similar network numerous malware may exist together yet the way that diverse malware concentrate on different vulnerabilities, and distribution of various malware may not be same. We can discover more information about the length of exponential tail of a power law distribution at late stage. Safeguards can focus more on systems. In this paper we concentrated just on one malware, In future we are interested to discover appropriation of numerous malware on huge scale systems.

## VII. REFERENCES

[1] B. Stonee-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, ―Your compromised network is my botnet: Analysis of a botnet takeover in Proc. ACM Conf. Computer. Communication Security, 2009, pp. 635–647.

[2] M. A. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, ―My compromised network is larger than yours (maybe, superior than yours): Why size calculation remain challenging,‖ in Proc. 1st Conf. 1st Workshops Hot Topics conception of Botnets, 2007, p. 5.

[3] D. Dagon, C. Zou, and W. Lee, ―Designing compromised network propagation using time zones,‖ in Proc. 13th

Network Distributed Systems. Security Symps. 2006.

[4] P. V. Mieghem, J. Omic, and R. Kooij, ―Virus spread in networks,‖ IEEE/ACM Trans. Networks, vol. 17, no. 1, pp. 1–14, Feb. 2009.

[5] Cabir. (2014). [Online]. Accessible: http://www.f-secure.com/en/Webs/Lab Global/2004-warning-summary

[6] Brador. (2014). [Online]. Available: http://www.fsecure.com/vdescs/brador.shtml

[7] S. Peng, S. Yu, and A. Yang, ―Smartphone malware and its spreading modeling: A survey,‖ IEEE Communication Surveys Tuts., vol. 16, no. 2, pp. 925–941, 2014.

[8] Z. Chen and C. Ji, ―An information-practical view of network aware malicious attacks,‖ IEEE Transaction Information. Forensics Security, vol. 4, no. 3, pp. 530–541, Sep. 2009.

[9] A. M. Jeffrey, X. Xia, and I. K. Craig, ―When to start HIV treatment: A control theoretic approach,‖ IEEE Trans. Biomed. Eng., vol. 50, no. 11, pp. 1213–1220, Nov. 2003.

[10] C. Gao and J. Liu, "Modeling and restraining mobile virus propagation," IEEE Trans. Mobile Computing, vol. 12, no. 3, pp. 529–541, Mar. 2013.

[11] D. J. Daley and J. Gani, Epidemic Modeling: An Introduction. Cambridge, U.K. Cambridge Univ. Press, 1999.

[12] W. Willinger, D. Alderson, and J. C. Doyle, "Mathematics and the internet: A source of enormous confusion and great potential," Notices Amer. Math. Soc., vol. 56, no. 5, pp. 586–599, 2009.

[13] Y. Zhou and X. Jiang, "Dissecting android malware: Characterization and evolution," in Proc. IEEE Symp. Security Privacy, 2012, pp. 95–109.