Modeling and Simulation concept for evaluating the Performance of Computers in a Network under Cyber Attack

Anil Kumar Mishra, Tarini Charan Panda, Sujata Dash

Abstract— This paper gives an current survey on application of modeling and simulation .We have focused on what we observed as some of the the major mathematical challenges in Cybersecurity.This review paper presents mathematical or statistical modeling for cybersecurity. Different types of modeling concepts are discussed.When systems connected through the internet are attacked how the system survives what is the rate of survival will be calculated.Cyber security models and possible elements of the models are also discussed.We have organized our ideas into modeling large scale networks, performance evaluation and reliability study.

Index Terms— Virus, Worm, Epedemics, Networks, Modeling, Reliability, Hazard function.

1 INTRODUCTION

The rapid growth of attacks and securirt measures degrades not only information system infrastructure and assurance, but also the performance of computers,networks and wireless devices[1,3,13].Due to the sharing of the resources on the web or network, it becomes easy for attackers to attack.Each year more complex malwares such as viruses,worms,botnets and Trojans are launched via internet.These malwares are used for attacking on :

Availability: To reduce communications/computation capacity or to prevent the availability of information and communication systems.

Confidentiality: To Compromise the confidential information.

Privacy: To obtain detailed information about individuals and organizations.

Integrity:To create uncertainnity about information.

Ko-tenko in2005 and stytz et. Al 2010 have discussed about cyber attackers and its prevention.Modelling and Simulation tools are also available (OM-NeT++, cayiric and Marincic) for simulating cyber attacks.However, mathematical modeling plays a major role in Cyber Security .

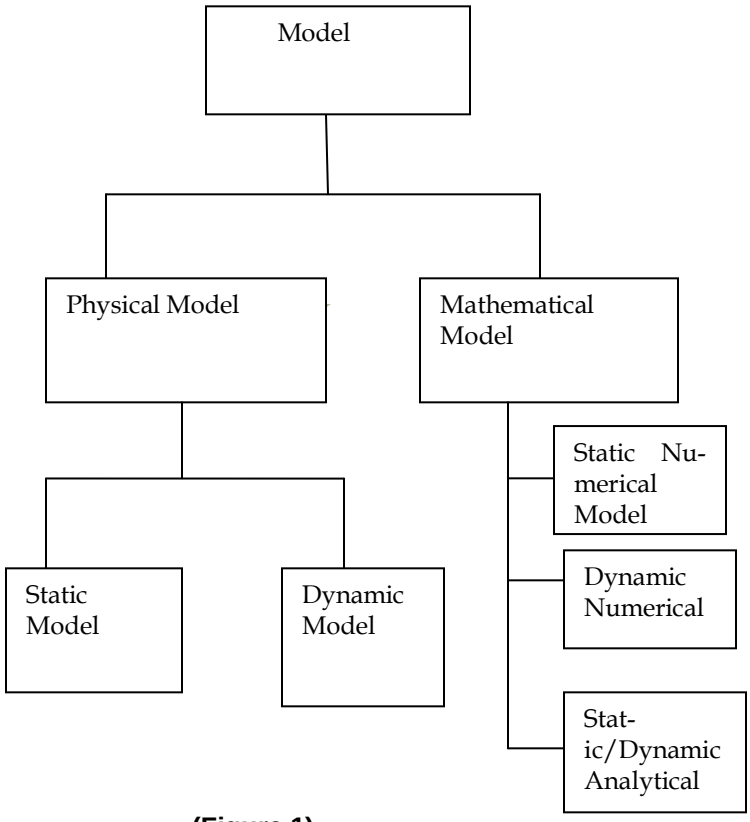
Cyber attack may create a situation which is very difficult to face for the decision makers due to lack of information available to predict attack.The insinuation and consequences of this phenomenon are serious.Therefore, practical solutions and procedures against it should be developed, tested and trained, which requires efficiency in modeling and simulation techniques[5,10,12].

In this paper we aim to discuss the basics to relate cyberattacks and how to prevent the systems by evaluating their performance of the systems connected through network.

2 MATHEMATICAL MODELING CONCEPT

Modeling is a mathematical tool to develop a prototype of a proposed system before it is developed or implemented[1].For many scenarios it is not feasible(Technically feasible and economical feasible) to develop prototype of a systemto study the characterstics of a system. A prototype is not only replacement to a large system but also the simplification o the system.[9,10]

2.1 Classification of different models



(Figure 1)

Physical Model: These models are based on some methodology of Electrical, Hydraulic, and Mechanical Systems.

Mathematical Model: Models which can be represented in the form of mathematical equations, example- economics students apply linear algebra for input/output models.

Physical static Model: These models don't change their behavior as time changes.

Physical dynamic model:These models change their behavior as time changes.

Mathematical Static Model:These mathematical models give a mathematical equation when the system is in equilibrium stage.

Mathematical Dynamic Model: In these mathematical models allow change of attributes as the function of time.

Mathematical Static Analytical Model:These are small static mathematical models which can be solved by conventional mathematics.

Mathematical/Dynamic Analytical Model:These are small dynamic mathematical models which can be solved by simulation.

2.2 MATHEMATICAL MODELING PRINCIPLE FOR CYBER DEDFENCE SYSTEM

Cyber attacks are major problem of today's world.To overcome this problem it is necessary to understand the behavior of malicious objects.For this mathematical modeling play an important role. It can help to fix possible parameters of malacious objects,those are important to tell how the malicious objects can propagate through internet[3,5,6,14].The reason for cyberdefence is due to various malicious objects like Trojan,worm,virus, spam etc.The attacks on internet and internet attached systems have grown more sophisticated while the amount of skill and the knowledge required to mount an attack has declined[5,6].The attacks have become more automated and can cause greater amount of damage.

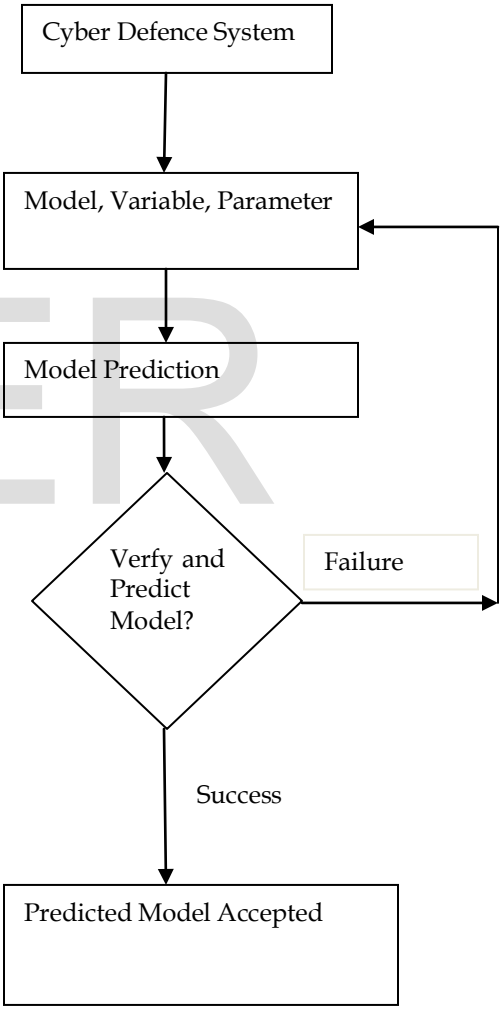
Types of attacks	Internet Social Engineering attack
	Sniffer
	Packet Spoofing
	Hijacking Sessions
	Automated probes/sacns
	GUI introduer tool
	DOS attack
	Executable code attack
	Attack on DNS infrastructure
	Trojan horse distribution
	Email propagation of malicious code
	DDOS attack

Table 1

Table 1 gives information about different types of attack we came across.For providing security for this type of attacks we must be aware of behavior of malicious objects and it can be understood by using modeling.

3 WAYS TO STUDY A CYBER DEFENCE SYSTEM

The figure 1 given below gives a pictorial idea to study cyber defence system by using the mathematical modeling techniques[2,8].The mathematical and statistical techniques can be used for evaluating the performance of systems under attack or for the prediction of attack.From the network traffic comes to our system we must know about the existience of malicious objects or data which force our system to behave abnormally.The length of data, source of data, how it affect our system and how we can measure the reliability under the such type of attacks are topics for prediction using mathematical or stastical techniques.



(Figure 1: Mathematical Modeling Process)

4 THE RELIABILITY, FAILURE DENSITY OF A SYSTEM DUE TO MALACIOUS OBJECTS BY USING THE RELIABILITY, FAILURE DENSITY AND HAZARD FUNCTION

In the current scenarios the internet system are prone to threat from various malicious objects which is discussed in table number 1.The host computer can be infected from the internet and it affects the total immune system of computer e.g. primary memory, secondary memory , the current messaging etc.
The attacks are totally stochastic and it is very difficult to predict the next time of attack[2,4].But we can study the reliability of a system under such situations.We have applied Continuos random variables for doing the study.

Let the random variable X be the life time or the time of failure of the system due to malicious objects or due to virus attack.The probability that the system will survive until some time 't' is called reliability R(t) of the system.

$R(t) = P(X>t) = 1-F(t)$ ——————(1)

Where F is the distribution function of the system life time, X.

The Component is assumed to be working properly at time t=0 [i.e. R(0)=1] and no system will work for ever without failure.Consider a fixed number of identical Systems. The number of systems under test is N_0.After time t, $N_f(t)$ systems or computers have failed in anetwork and $N_s(t)$ computers have survived.

$N_f(t) + N_s(t) = N_0$ —————— (2)

The Probability of survival of a system

$P(\text{survival}) = N_s(t)/ N_0$ —————— (3)

When, $N_0 \rightarrow \infty$, The P(survival) approaches to R(t).

Where R(t) is the reliability of the total system(Number systems exsists in a particular network).When $N_s(t)$ gets smaller and R(t) decreases.

$R(t) = N_s(t)/ N_0$

$= (N_0 - N_f(t))/ N_0$

$= 1 - N_f(t)/N_0$ —————— (4)

As the total number of computer numbers is constant in a network so the failed number of components N_f increases with time. Taking derivatives of both sides

$R'(t) = (-1/N_0)N'_f(t)$ —————— (5)

$N'_f(t)$ is the rate at which the computers of the network will fail due to virus attack. As $N_0 \rightarrow \infty$, the very right hand side maybe interpreted as negative of the failure density function, $f_x(t)$

$R'(t) = -f_x(t)$ —————— (6)

$f(t)\,\Delta t$ is the unconditional probability that a component will fail at the interval (t, t+Δt).The component of a system function upto time 't' and the failure will be different from $f(t)\Delta t$.This

causes instantaneous failure.The instantaneous failure rate h(t) at time 't' due to the virus attack is defined as

$h(t) = f(t)/R(t)$ —————— (7)

Here ,$h(t)\Delta t$ represents the conditional probability that a computer will survive in a network to the time 't' fail in the interval (t,t+Δt).
h(t) , Alternatively known as the hazard rate or force mortality of a computer.
Now, for modeling a cyber defence system one should know the different components and parameters required.Now, our proposed model is described below in Figure 2.

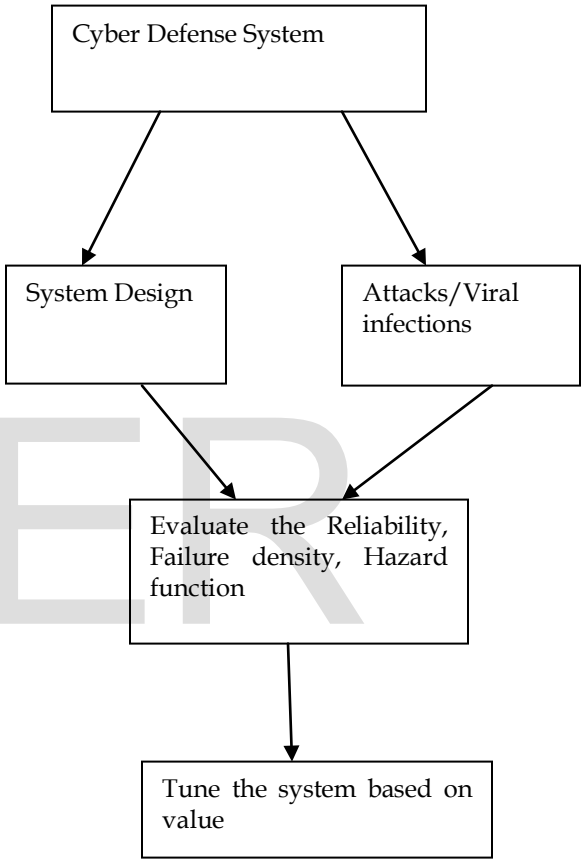


Figure 2

5 CONCLUSION AND FUTURE WORKS

It is very difficult to trace the attacker in cyberdence.All the features of malicious object's propagation have to be represented in the form of mathematical equations so it will be easy to predict the future behavior.And it is very difficult to calculate the actual reliability of the computers due to virus attack.In our future scope we are planning to apply the soft computing techniques in Computer Security. Most of the cyber defense Systems, when implemented create overheads like slow down in exsisting system performance, increase in packet length or take time for comparision etc.We have focused an area to do our research i.e IDS(intrusion detection system). We will model the IDS by using the soft computing

techniques.

.

- *Dr. Anil Kumar Mishra is currently working as an Associate Professor in Orissa Engineering College ,CSE Department,Bhubaneswar. E-mail: anilmishra.oec@gmail.com*
- *Dr. Sujata Dash is currently workingas a Reader in the Department of Computer Science and Applications in North Orissa University Baripada.E-mail: sujata_dash@yahoo.com.*

REFERENCES

[1] D.K. Saini "A Mathematical Model for the effect of malacious Object on Computer Network Immune Sytem" Applied Mathematical Modeling ,vol.35,pp.3777-3787 USA 2011.

[2] Kishor S. Trivedi, *Linear Probability & Statistics with reliability,Queing and Compter Science Application.* , Prentice Hall, New Delhi,India,2006.

[3] William Stallings, Cryptography and Network Security Principles and Practises, Prentice Hall, New Delhi, India, 2008.

[4] Ross, Sheldon M.,Introduction to Probability Models,Second Edition Academic Press,New York,1981.

[5] Neils Provos, Joe McClain, Ke Wang, "Search Worms",Proceedings of the 4th ACM workshop on Recurring Malcode WORM' 06, November 2006.

[6] Elbaum, Sebastian,Munson, John C, "Intrusion Detection : Through Dynamic Software Measurement", Proceedings of Workshops on Intrusion Detection and Network Monitoring, The USENIX Assiciation, April 9-12,1999.

[7] Moore, David, Paxon, Vern, Savage, Stefan, Shannon, Colleen, Stanoford, Stuart, Weaver,, Nicholas, "Inside Slammer Worm", IEEE Security and Privacy, July 2003.

[8] J.Kephart,S.White, "Directed graph epidemiology models of computer virus", Proceedings of the1991 Computer Society Symposium on Research in security and Privacy.

[9] Bimal Kumar Mishra, Dinesh Kumar Saini, "Mathematical Models on Computer Viruses", Int. J. Appl. Math. Comput. Vol.187,Issue 2,pp. 929-936.

[10] Bimal Kumar Mishra, Dinesh Kumar Saini, "SEIRS epidemic Model of Transmission of malicious object in computer network", Int. Journal of Applied Mathematics and Computing, vol. 188, Issue2,pp.1476-1482,2007.

[11] L. Nian et al., "Research on network security situation awareness technology based on artificial immunity system", Internation Forum on Information Technology and Applications,2009.

[12] John Markoff, "Computer experts unite to hunt worm", The New York Times, March 19, 2009.

[13] Adam J. Slagell, Kiran Lakkaraju and Katherine Luo, "Flaim: Amulti-level anonymization framework for computer and network logs, In LISA, pp. 63-77, 2006.

[14] V. Paxon and S. Floyd , "Why we don't know how to simulate the internet", In Proceedings of Winter Simulation Conference,pp.1037-1044,7-10 December 1997.