A Quantitative Approach Towards Detection of an Optimal Attack Path in Wireless Network using Modified PSO Technique

Nirnay Ghosh Saurav Nanda S.K. Ghosh

School of Information Technology
Indian Institute of Technology, Kharagpur, India
Email: {nghosh, sauravn}@sit.iitkgp.ernet.in ; skg@iitkgp.ac.in

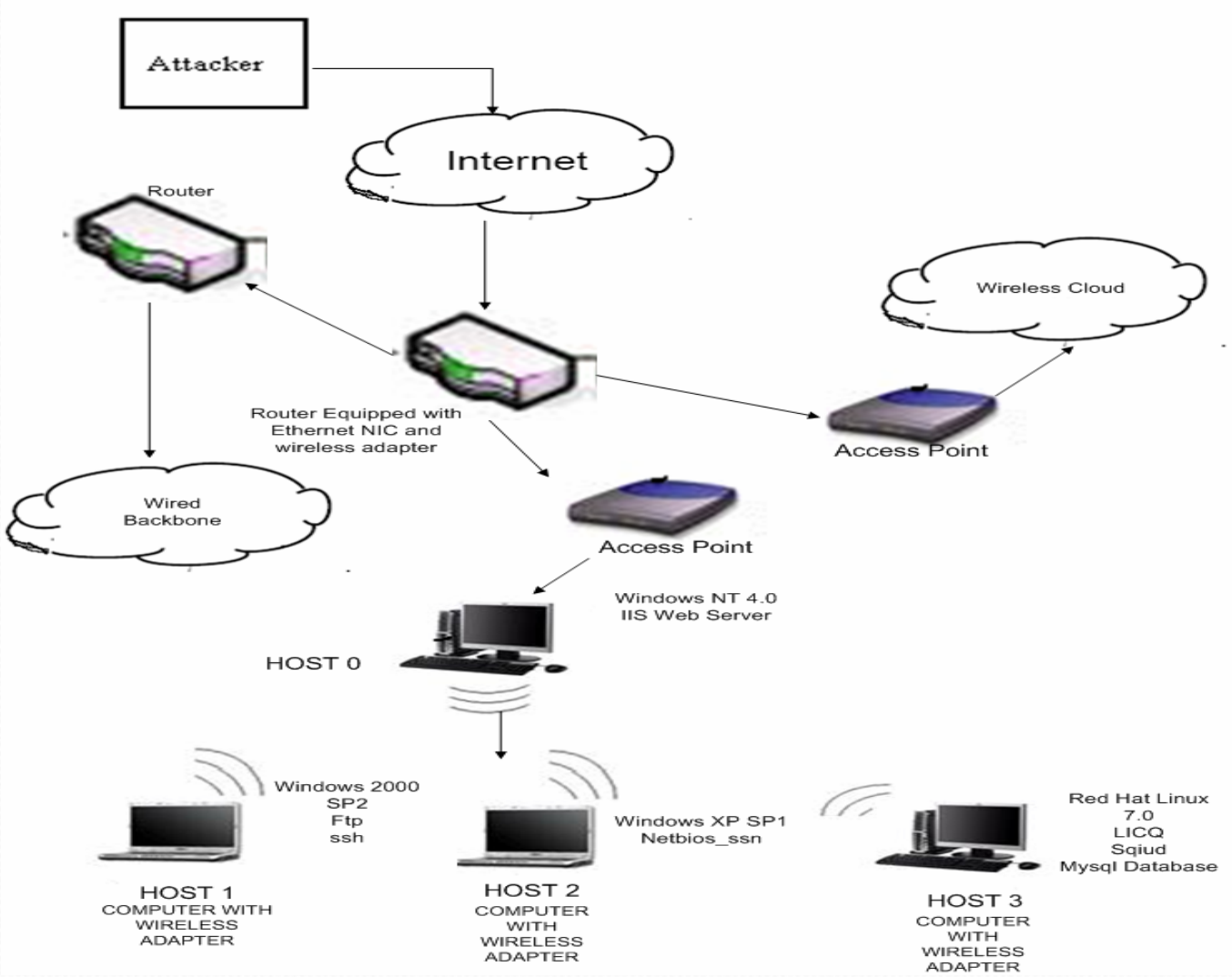
Contents

- Introduction
- Motivation
- Problem Definition
- Classical PSO Technique
- Proposed Approach : Risk Quantification & Customized PSO
  - Algorithms
  - Example and Case Study
  - Experimentation & Results
- Conclusion
- References

Introduction

- Immense proliferation of wireless networks.
- Becoming increasingly vulnerable to attacks.
- Network Security assumes great importance.

Backbone Network



Motivation

- Networks are becoming vulnerable to attacks.
- Attack Graph: a tool that provides all possible attack scenarios that jeopardize the network.
- Attack Path: a series of *exploits* where each exploit in the chain lays the groundwork for subsequent exploits.
- Complete attack graphs have the following problems:-
  - Scalability
  - Exponential time complexity
  - Contains redundant nodes and edges
  - Difficulty in understanding
- *Minimal* attack graph: consists of *minimal* attack paths.

Contd..

- Finding out an optimal attack path from a given set of *minimal* attack paths.
- Optimality of an attack path is given by the *effort* required on path of the attacker to reach the *goal* following that path.
- Not much work related to wireless network security using attack path has been reported till date.

Problem Definition

- To determine near optimal attack path in WLAN based on the Risk Values associated with the hosts of the WLAN using Soft-Computing Technique, Particle Swarm Optimization (PSO).
- Problem decomposed as
  - Simulation of a Wireless scenario
  - Assignment of risk values to the Wireless Hosts
  - Attack Path Identification using PSO

Particle Swarm Optimization (PSO)

- PSO model consists of a swarm of particles[18], which are initiated with a population of random candidate solutions.

$$\overrightarrow{v_i}(t) = w * \overrightarrow{v_i}(t-1) + c_1 * \phi_1 * (\overrightarrow{pi} - \overrightarrow{x_i}(t-1)) + c_2 * \phi_2 * (\overrightarrow{p_g} - \overrightarrow{x_i}(t-1))$$

$$\overrightarrow{x_i}(t) = \overrightarrow{x_i}(t-1) + \overrightarrow{v_i}(t)$$

Where, w [23]is an inertia weight which is employed to control the impact of the previous velocity on the current velocity.

The *c1 & c2 are the social/cognitive coefficients and Ø1 & Ø2 [23] are the two uniform* random numbers in the range [0,1].

Detection Of Optimal Attack Path In A Wireless Network Using Modified PSO Techniques

Severity Measurement

- Classical formula of risk by *Y. Chen, B. Boehm, L. Sheppard* [13]:

  $$Risk = P_{success} \times SizeOfLoss$$

- $P_{success}$ *is the probability that such an attack will be successful*
- ***SizeOfLoss*** characterizes how much the loss will be if such an attack happens.

Relevance	Attributes	Sub – attributes
$P_{success}$	Access (Acc)	Access Vector(AV)
		Authentication(Auth)
		Attack Complexity(AC)
	Vulnerability (Vul)	Availability(Avail)
		Popularity
		Remediation Level(RL)
		Report Confidence(RC)
SizeOfLoss	Vulnerability	Damage Potential(DP)
	Target Asset	Asset Value Impact Association(AVIA)
	Affected Value	Value Importance(VI)

Ref: [14][13][15][16][17]

$P_{success}$ & *SizeOfLoss* Relevant Attribute Ratings

CVE – ID	AV	Auth	AC
CVE-2002-0364	Network Access(0.646)	Not Required(0.704)	Low(0.71)
CVE-2008-1396	Network Access(0.646)	Not Required(0.704)	Low(0.71)
CVE-1999-1455	Network Access(0.646)	Not Required(0.704)	Low(0.71)
CVE-1999-0180	Network Access(0.646)	Not Required(0.704)	Low (0.71)
CVE-2003-0661	Network Access(0.646)	Not Required(0.704)	Low (0.71)
CVE-2001-0439	Network Access(0.646)	Not Required(0.704)	Low(0.71)
CVE-2001-1030	Network Access(0.646)	Not Required(0.704)	Low(0.71)
CVE-2006-3368	Network Access(0.646)	Not Required(0.704)	Low(0.71)

$P_{success}$ Relevant Base metrics for CVE-IDs

CVE – ID	Avail	Popularity	RL	RC
CVE-2002-0364	Proof-of-concept(0.9)	High(1.0)	Official-fix(0.87)	Confirmed(1.0)
CVE-2008-1396	Functional(0.85)	High(1.0)	Workaround(0.95)	Confirmed(1.0)
CVE-1999-1455	Unproven(0.85)	High(1.0)	Unavailable (1.0)	Unconfirmed(1.0)
CVE-1999-0180	Not defined(1.0)	High(1.0)	Not defined(1.0)	Not defined(1.0)
CVE-2003-0661	Functional(0.95)	Medium(0.7)	Workaround(0.95)	Uncorroborated(0.95)
CVE-2001-0439	Not defined(1.0)	High(1.0)	Workaround(0.95)	Confirmed(1.0)
CVE-2001-1030	Functional(0.95)	High(1.0)	Official-fix(0.87)	Uncorroborated(0.95)
CVE-2006-3368	Functional(0.95)	Medium(0.7)	Unavailable(1.0)	Confirmed(1.0)

$P_{success}$ Relevant Temporal Metrics for CVE-IDs

CVE – ID	DP	AVIA	VI
CVE-2002-0364	Low(0.1)	Medium(0.62)	Medium(0.6)
CVE-2008-1396	Low(0.1)	Complete(0.96)	Medium(0.6)
CVE-1999-1455	Low(0.1)	Medium(0.62)	Medium(0.6)
CVE-1999-0180	High(0.5)	Medium(0.62)	Medium(0.6)
CVE-2003-0661	Medium-high(0.4)	Medium (0.62)	Medium(0.6)
CVE-2001-0439	Medium-high(0.4)	Complete(0.96)	Medium(0.6)
CVE-2001-1030	Low(0.1)	Medium(0.62)	Medium(0.6)
CVE-2006-1030	Medium-high(0.4)	Low(0.275)	Medium(0.6)

SizeOfLoss Attribute Ratings

Ref : [14][15][16][17]

Computation of CVE-ID Risk

- $P_{success}$ attribute is the sum of the Acc and Vul and is given as:

$$P_{success} = Acc + Vul$$

- Acc and Vul depends on different sub-attributes viz. Access Vector(AV), Authentication(Auth), Attack Complexity (AC) and Availability(Avail), Popularity, Remediation Level(RL), and Report Confidence(RC) respectively.

$$Acc = AV \times Auth \times AC$$

$$Vul = Avail \times Popularity \times RL \times RC$$

$$P_{success} = (AV \times Auth \times AC) + (Avail \times Popularity \times RL \times RC)$$

Attack Index (AI) & Size of Loss Index (SI)

- The contribution of *Acc and Vul towards the calculation of* $P_{success}$ *will vary as per the* security requirements of the organization.

$$AI = W1 \times Acc + W2 \times Vul$$

$$AI = 0.6 \times Acc + 0.4 \times Vul$$

- Sub-attributes that constitute *SizeOfLoss are Damage Potential(DP), Asset Value Impact Association(AVIA), Value Importance(VI).*

$$SizeOfLoss = DP + AVIA + VI$$

- Considering *equal contributions of DP, AVIA, VI towards the calculation* of *SizeOfLoss*

$$SI = 0.33 \times (DP + AVIA + VI)$$

Severity Measure

- Finally, the classic risk calculation formula is:

$$\boldsymbol{Risk = AI \times SI}$$

- If a particular host has *n number of vulnerabilities each with corresponding CVE-ID, then* using the above formulae the risk associated with each such CVE-IDs may be computed as:

$$Severitymeasure(host_i) = \sum_{j=1}^{j=n} Risk(CVE - ID_j)$$

Algorithm: Severity Calculation

Input: Set of Vulnerabilities in terms of CVE-IDs
Output: severity measures and the Connectivity among the nodes
foreach *Host i* **do**
  Find vulnerabilities associted with *i*
  foreach *Vulnerability j in host i* **do**
    Calculate *Risk*(*j*)
    severity measure(*i*)=$\sum$(Risk$_j$)
  end
end
Call **Connectivity**
Print *OptimalAttackPath*

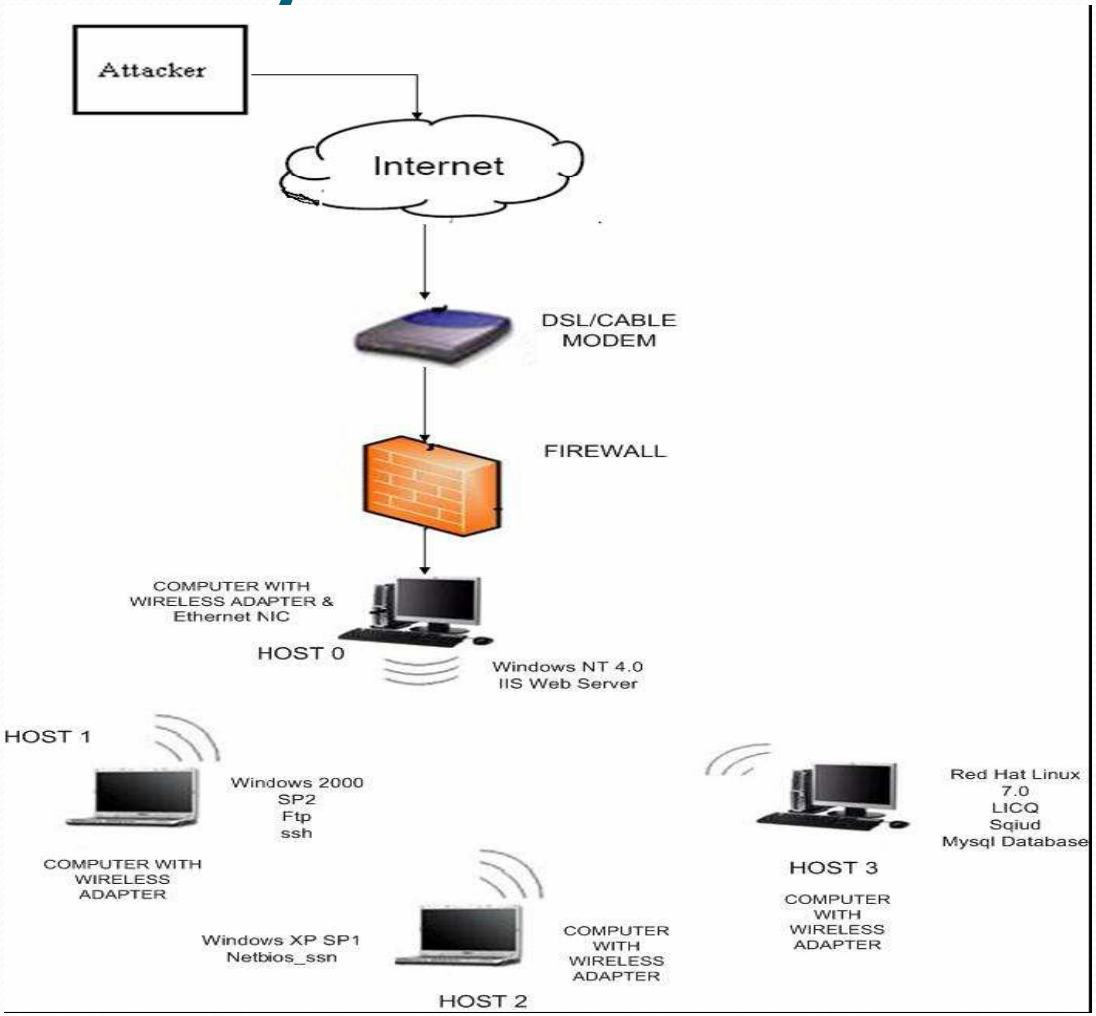
Algorithm: Connectivity

Input: Network Region,Threshold Range
Output: Connectivity relationship among wireless nodes
while *true* **do**
  if $CheckTimer(T_{max}) = 1$ **then**
    foreach *Host i* **do**
      Initialize the position
      Calculate the $Range(Host_i)$
    end
    foreach *Host i* **do**
      if $Range(Host_i) < Threshold$ **then**
        Print *ConnectivityRelationship*
      end
    end
    Read *Source*
    Read *Destination*
    Call **PSOfitness**(*Source*, *Destination*)
  end
end

Algorithm: PSOfitness

Input: Source node and Destination node
Output: An optimized attack path
if *source* = *destination* **then**
  return
end
Mark *Source* →Visited
foreach *Host j* **do**
  if *connection exits between source and Host j && Host j is not visited* **then**
    Set flag → 1
    arr[*i* + +]← *host*j
  end
end
foreach *Host i* **do**
  Calculate max(*risk*(*arr*[*i*]))
  next←arr[i]
end
if *risk*[*next*] > pbest **then**
  gbest=*risk*[*next*]
end
else
  gbest = *pbest*
end
Mark *next* →Visited
Call **ComputeAttackVector**(*gbest*, *pbest*)
Call **PSOfitness**(*next*, *destination*)

Case Study


Attacker
Internet
DSL/CABLE MODEM
FIREWALL
COMPUTER WITH WIRELESS ADAPTER & Ethernet NIC
HOST 0
Windows NT 4.0 IIS Web Server
HOST 1
Windows 2000 SP2 Ftp ssh
COMPUTER WITH WIRELESS ADAPTER
Red Hat Linux 7.0 LICQ Sqiud Mysql Database
HOST 3
COMPUTER WITH WIRELESS ADAPTER
Windows XP SP1 Netbios_ssn
COMPUTER WITH WIRELESS ADAPTER
HOST 2

System Characteristics

Host	Services	Ports	Vulnerabilities	CVE – IDs	OperatingSystem
H0	IIS Web Service	80	IIS buffer overflow	CVE-2002-0364	Windows NT 4.0
H1	ftp	21	ftp rhost overwrite	CVE-2008-1396	
	ssh	22	ssh buffer overflow	CVE-1999-1455	Windows 2000 SP1
	rsh	514	rsh login	CVE-1999-0180	
H2	Netbios-ssn	139	Netbios-ssn nullsession	CVE-2003-0661	Windows XP SP2
	rsh	514	rsh login	CVE-1999-0180	
H3	LICQ	5190	LICQ-remote-to-user	CVE-2001-0439	
	Squid Proxy	80	squid-port-scan	CVE-2001-1030	Red Hat Linux 7.0
	Mysql DB	3306	local-setuid-bof	CVE-2006-3368	

Host – ID	CVE – ID
H0	CVE-2002-0364
H1	CVE-2008-1396
	CVE-1999-1455
	CVE-1999-0180
H2	CVE-2001-0439
	CVE-1999-0180
H3	CVE-2001-0439
	CVE-2001-0103
	CVE-2006-3368

Ref : [19][20]

Calculations

$$AI = 0.6 \times (0.646 \times 0.704 \times 0.71) + 0.4 \times (0.9 \times 1.0 \times 0.87 \times 1.0)$$
$$= (0.6 \times 0.322) + (0.4 \times 0.783) = 0.193 + 0.313 = 0.506$$

$$SI = 0.33 \times (0.1 + 0.62 + 0.6) = 0.33 \times 1.32 = 0.436$$

$$Risk = 0.506 \times 0.436 = 0.220$$

$$Severity(Host0) = 0.220$$

Contd…

CVE – ID	Risk
CVE-2008-1396	0.304
CVE-1999-1455	0.232
CVE-1999-0180	0.337
CVE-2003-0661	0.232
CVE-2001-0439	0.307
CVE-2001-1030	0.221
CVE-2006-3368	0.193

Risk Values of the Vulnerabilities

Host – ID	severitymeasure
H1	0.873
H2	0.644
H3	0.721

severity measures of each Host

Calculation of *gbest* & Attack Vector Scenario 1

$$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Connectivity matrix

Host – ID	gbest	AttackVector
H2	0.644	0.219972
H3	0.721	0.162986

Attack Vectors of the visited hosts

Optimal attack path with this connectivity matrix is :

$H_0 \rightarrow H_2 \rightarrow H_3$

Scenario 2

$$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

Connectivity matrix

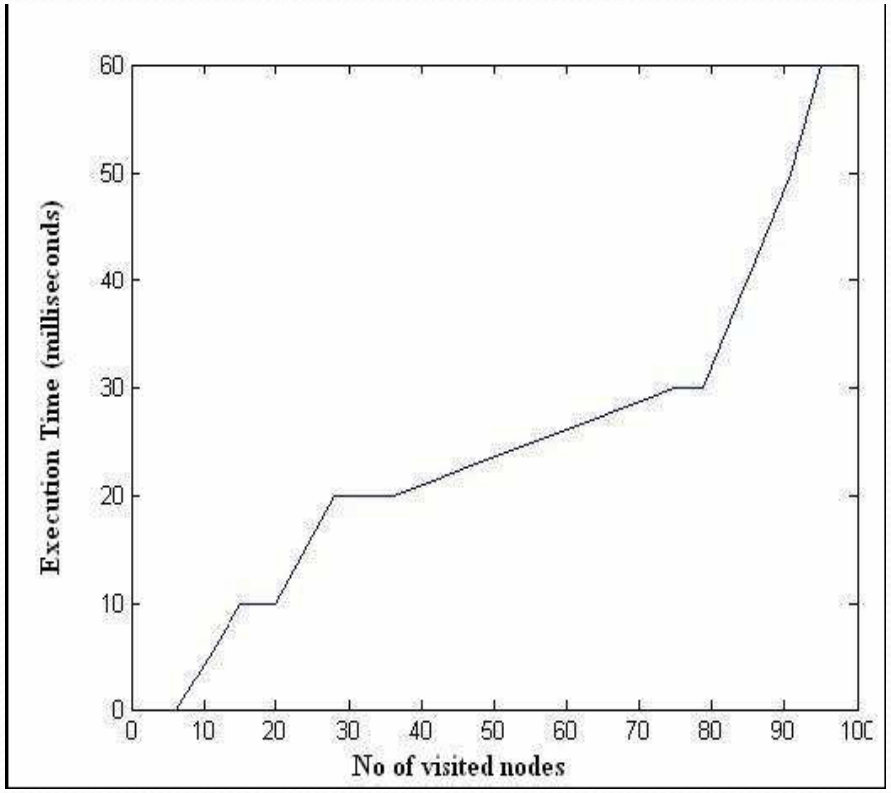
Host – ID	*gbest*	AttackVector
H2	0.644	0.149176
H1	0.873	0.024638
H3	0.873	0.021534

Attack Vectors of the visited hosts

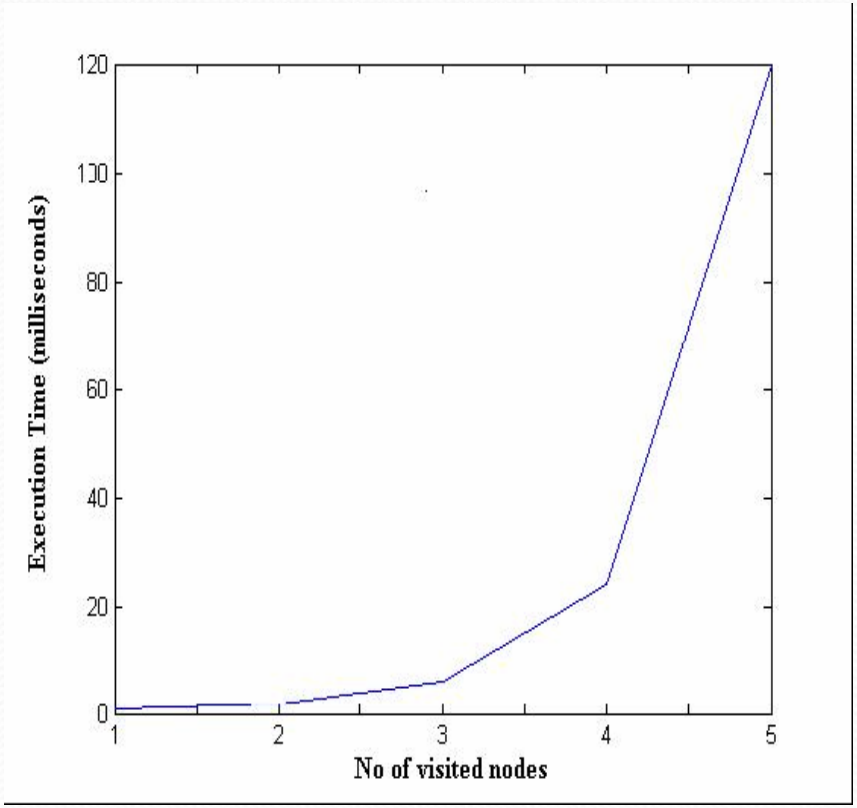
Optimal attack path with this connectivity matrix is :

$$H0 \rightarrow H2 \rightarrow H1 \rightarrow H3$$

Proposed Methodology *vs* Brute Force Technique (in terms of Execution Time)



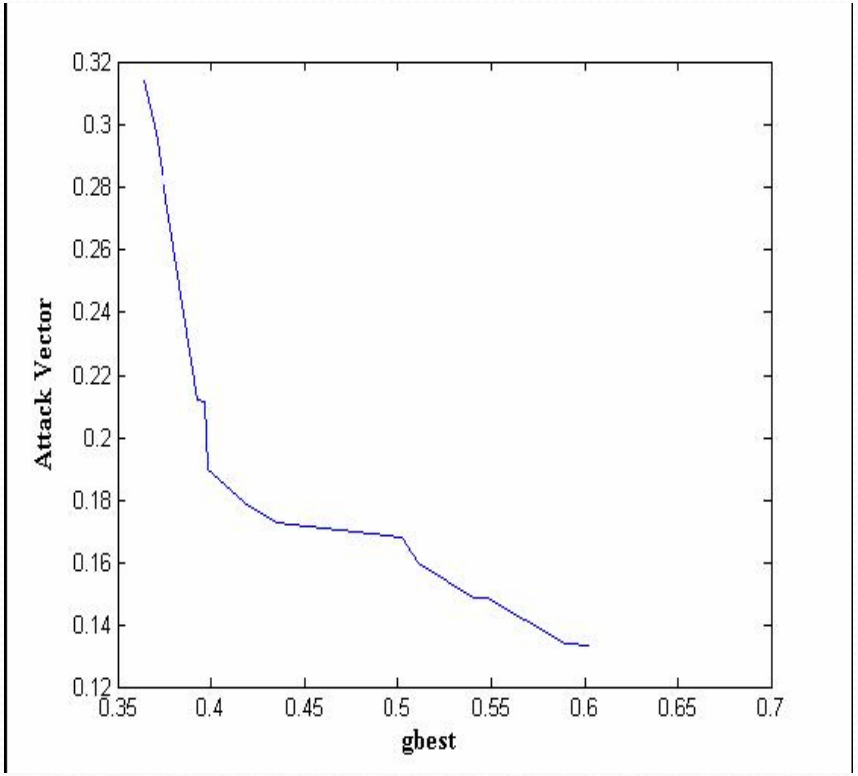
Proposed model



Brute force method

Result

- *Attack Vector values are inversely proportional* gbest.
- The gbest is the global maximum *severity measure and as it increases, the Effort* required to compromise the host *reduces*.



gbest vs Attack Vector (effort)

Conclusion

- An optimal attack path in a wireless network using modified PSO technique is detected.
- The wireless hosts in the test network are assigned some weightages in terms of risk parameters obtained from well known public sites.
- These weightages are computed by customized risk formulae.
- Finally, these *severity measures are input to PSO* based proposed algorithms to find out the optimal attack path in the wireless network.
- The output of the proposed model is compared with existing brute force technique to exhibit efficiency.

References

[1] Web : http://www.cs.umd.edu/~waa/wireless.pdf

[2] Phillips. C., and Swiler, L.P., "A graph based system for network vulnerability analysis", Proceedings of the 1998 workshop on the New Security Paradigms (NSPW'98), pages 71-79, Charlottesville, VA, 1998.

[3] Swiller, L., Phillips, C., Ellis, D., and Chakerian, S.,"Computer-Attack Graph Generation Tool". *In Proceedings of DARPA Information Survivability Conference & Exposition II*, June 2001.

[4] P. Ammann, D. Wijesekera, and S. Kaushik. Scalable graph based vulnerability analysis, In Proceedings of 9th ACM Conference on Computer and Communication Security (CCS'02), November 2002.

[5] Ritchy, R., and Ammann, P., "Using model checking to analyse network vulnerabilities". In *Proceedings of the IEEE Symposium on Security and Privacy*, May 2001.

[6] Oleg Sheyner, Jeannette Wing, "Tools for Generating and Analyzing the Attack Graphs", FMCO 2003, LNCS, pp 344 -371, 2004.

[7] Ammann, P., Pamula, J., Ritchey, R. and Street, J., "A host-based Approach to the Network Attack Chaining Analysis". In *Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC 2005),* 2005.

[8] P. Ammann, D. Wijesekera, S. Kaushik, "Scalable, graph-based network vulnerability analysis", In Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS), Washington, DC, USA, November 18-22,2002, pp. 217-224.

References

[9] M.L. Artz, "NetSPA: a network security planning architecture", Master's Thesis, Massachusetts Institute of Technology, May 2002.

[10] R. W. Ritchey and P.Ammann, "Using model checking to analyze network vulnerabilities", In Proceedings of the 2000 IEEE Symposium on Security and Privacy (Oakland 2000), pages 156-165, Oakland, CA, May 2000.

[11] L. Swiler, C. Phillips, D. Ellis, S. Chakerian, "Computer-attack graph generation tool", In Proceedings of the DARPA Information Survivability Conference & Exposition (DISCEX), Anaheim, California, June 12, 2001, pp. 307-321.

[12] C. Bettstetter and C. Wagner, "The Spatial Node Distribution of the Random Waypoint Mobility Model", In Proceedings of GermanWorkshop on Mobile Ad-Hoc Networks (WMAN), Ulm, Germany, GI Lecture Notes in Informatics, no. P-11, pp. 41-58, Mar 25- 26, 2002.

[13] Y. Chen, B. Boehm, L. Sheppard," Value Driven Security Threat Modeling Based on Attack Path Analysis", In Proceedings of 40th Annual Hawaii International Conference on System Sciences, HICSS, Jan. 2007, pp. 280a - 280a.

[14] National Vulnerability Database. Automating vulnerability management, security measurement, and compliance checking. http://nvd.nist.gov/ (Accessed on 31st October,2008)

[15] M.Schi®man, "Common Vulnerability Scoring System (CVSS)", http://www.¯rst.org/cvss/ (Accessed on 31st October,2008)

[16] SANS Top 20 Most Critical Vulnerabilities, SAN http://www.sans.org/top20/. (Accessed on 31st October,2008)

References

[17] Symantec Threat Severity Assessment, http://www.symantec.com/avcenter/threat.severity.html. (Accessed on 31st October,2008)

[18] Inthachot M., Supratid S., "A Multi-Subpopulation Particle Swarm Optimization: A Hybrid Intelligent Computing for Function Optimization", Third International Conference on Natural Computation (ICNC 2007)

[19] Oleg Mikhail Sheynar, "Scenario Graphs and Attack Graphs", Ph.D Thesis, School of Computer Science Computer Science Department Carnegie Mellon University Pittsburgh, PA

[20] T. Zhang, M. Hu, D. Li, L. Sun ,"Generate attack graph for network security analysis", Journal of Information & Computational Science (JICS), 2(3), 2005, pp. 605-615.

THANK YOU!!