Mobile Node Dynamism using Particle Swarm Optimization to fight against Vulnerability Exploitations

Subburaj.V,
Ph. D Research Scholar, Manonmaniam Sundaranar University, Tirunelveli &
Assistant Professor
Department of MCA,
Thiagarajar School of Management,
Madurai, Tamilnadu, India

K.Chitra
Assistant Professor
Department of Computer Science
Government Arts College, Melur
Sivagangai Dist,
Tamilnadu, India

ABSTRACT
Gateway in Mobile Adhoc networks used to connect intermediate and neighboring nodes of MANET. In this way of classifying nodes based on its arrangement, each and every node depends upon other nodes for packet transmission and acknowledgement. The vulnerabilities arise in the form of attack further leads to web exploits and other notable attacks (worm hole and its exploits) arise from a node in a network. In this paper, we have proposed a strategy for node dynamism for implementing PSO based accessing mechanism to get rid of attack exploitation for every node in the network. In Node dynamism each and every node were configured with PSO based fitness function, which will reflect on its gateway to avoid various attack like worm hole attack and web exploits etc. To avoid this type of attack, an external node (source of attack inspiration to mislead the transformation) when involved in the Mobile attack has to be configured with node dynamism. This node dynamism also reflect on inside attack (a node knows the best route for an attack) fight against it. The need for node dynamism also ensures node efficient performance measures using rule based detection of individual node.

Keywords
Node Dynamism, PSO, IDS, Intelligent Node

1. INTRODUCTION
We do have number of measures to eradicate IDS in networking [5]. With the dawn of latest technology (mobile, PDA, Smart Phone) there is growth of security measures [7] arises in parallel with the latest mobile phones trends (Smart Phones). The main source of attack comes from the attacker who knows the well about the network and tries to get into a network or to collapse it with various logical flaws [6]. The attacker initiates the attack from a node and tends to spread it to all other nodes. The first issue is more dangerous compared with the second. In order to ensure a node for its efficient performance, a node has to be subjected to PSO to check its efficiency. Elbert and Hard [2] defines the PSO with the intelligence of swarm. This approach provides efficient optimization algorithm to scrutinize the node, by providing node based efficiency using PSO optimization. The implication of the PSO also provides good alarm rates in terms of efficient optimization towards security.

The impact of black hole attack makes the node inaccessible. In the aspect of Relay transmission it requires the MAC protocol, further node posed towards Denial of Services Attack if it falls within the zone of attack. Gateway in the mobile adhoc network places a vital role for plotting the possibility of attack. The attack comes from any node (node may be within the scope or out of scope) of the network. The data transmission passes through the gateway. Gateway will identify the node boundary and the delay (latency link) and using its gateway discover phase it will identify the attacking node.

The attacking node tries to implement Denial of Service by negotiating broadcast message, by adjunct the node to stop further communication. This type of attack referred as message bombing by reducing the efficiency of node. The node when attacked with this kind will further be out of the communication range and it will be restricted from broad casting messages. This attack will further outperform the nodes efficiency and it will be difficult to counteract when attack simulates on each and every nodes via its transmission range.

The propose work towards node dynamism will work in different towards various attack, in specific towards black hole attack and worm hole attack by providing rule base extraction for a node plotted as attacking node. This work will further share its efficiency to its neighboring nodes and eradicating the attack happens in the gateway of Mobile adhoc network.

2. PSO TOWARDS NODE DYNAMISM
Genetic algorithm [15] plays a vital role in Intrusion detection system for fixing the node dynamism. PSO comes from the Genetic algorithm family. Basically PSO used for intelligent simulation of birds foraging behavior. In this work, we have proposed to incorporate PSO towards mobile nodes for individual reference to communicate with other nodes and to choose next best node out of its best foraging behavior. As this iteration proceeds it leads to best node to be efficient against attack. The mathematical representation of PSO described as follows: Assuming each Search space D as dimension (Dimension refer to the node boundary in MANET) and each and every swarm has N Particles (Particles refer to be the node of MANET).

Each and every node particle in the Mobile Adhoc Network were as each i^{th} particle (assumed to be mobile node) represented in terms of the search Space D were represented as $X_i=(x_{i1},x_{i2},\ldots x_{iD})$ [3]. In order to identify the best node in terms of its efficiency, it is been represented as Xg [3]. In [3] Xg is marked as best swarm particle index.
In order to classify the neighboring nodes based on its distance (mobile distance) which can be represented as $V_i=(v_{i1},v_{i2},\ldots v_{iD})$. In order to calculate the current distance in terms of its pervious distance, represented as $P_i=(p_{i1},p_{i2},\ldots p_{iD})$.

To measure the particle distance for every neighboring nodes in the network, represented by the formulae

$$Vid = w^* Vid + Ci * r1(pid-id)+c2+a/r2(pgd-xid) \quad (1)$$

$$Vid = \begin{cases} V\max, & if\ Vid \geq V\max \\ -V\max, & if\ Vid \geq -V\max \end{cases} \quad (2)$$

$$xid = xid + Vid \quad (3)$$

These mathematical representations were used to measure the particle distance in based on its random movement [3]. In our proposed method we have simulated the formulae for measuring node performance and hence it leads to node dynamism.

Here the inertia weight were calculated based on the constant c1 and c2 which are positive values and Vmax and –Vmax were used to set the limit to the node boundary.

Fig 1 represents the values for Vmax and –Vmax to be set as the node boundary. If there are 'n' nodes in the network, then the simulation results were applicable to all its nodes. This node boundary provides the max and min for each and every node based on the node boundary. The simulation result works based on the number of nodes with the boundary set as one of the parameter.

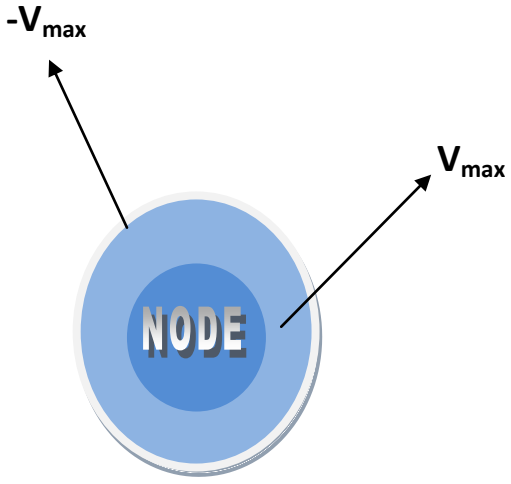

Fig 1: Node boundary

3. PROPOSED WORK

3.1 Fitness Function for Node Dynamism

In this work the fitness function used to evaluate the node dynamism to fight against attack.
The fitness function were given by as of [4]

$$Fitness(p) = a/A - b/B \quad (4)$$

Here 'a' denotes number of attacks and in this work 'a' in (4) denotes the attack like black hole [9], worm hole and web exploits. A-b ensures total attacks (A) and identified by single node (b). B is the total number of connection irrespective of attacks. In order to change the fitness value depends upon the attack, we have classified it according to the attack like black hole [9], work hole, web exploits.

In order to solve all these attacks the paper proposed new fitness function for all the three attack mentioned above.

Fitness function for Black hole attack

$$Fitness(n) = a/A \quad (5)$$

Here in this formulae 'a' is the attack classified as black hole, worm hole or web exploits. The purpose of being classification of attack is to ensure the node is well secured from all the there, since impact of one attack paves the way for other attack.
This fitness value was applied in the route segments of Gateway. This process is the gateway verification phase, to find the node on that route from source node to destination node. The gateway verification phase were described by

$$\prod(i,j) \leftarrow \eta(i) + \eta(j)/2 \quad (6)$$

$$\sigma(i,j) \leftarrow h(i) \times \prod(i,j) \quad (7)$$

By comparing these two equations we will identify the type of attack and this will be checked further with hello packet attack of [1], [14]. The result of gateway verification is to ensure the type of attack; it will ensure the attack in inside guaranteed and outside guaranteed region.

In [1],[14] the result of gateway attack is to check pseudo attack generated from the set of routes with effected route ratio and its classification percentage. In this work the gateway verification along with the fitness ratio generated in respect with the packet transmission beneath the node of the network, fight against attack with node dynamism.

The result of gateway verification and fitness function address each and every node, once works perfectly that node is said to safe from various attack mentioned in this work.

The save zone node (node dynamited) reflects its efficiency to its neighboring nodes lying on the route. The node works on the fitness function to trap the attack (Black Hole, Work Hole and web exploits).

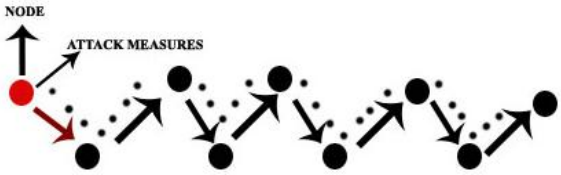

Fig 2: Node Dynamism

Fig 2 shows the attack measures based on the node color. Here in Fig 2 red color indicates vulnerable node and its data transmission, which affects the entire path. This diagram shows the simulated view of node vulnerability. The dotted line shows the transmission path by which the entire nodes were affected with the transmission of data initiated from the vulnerable node. The node dynamism was implemented with way point access by which the node replacement was done based on the vulnerable issues arises from the attacked node.

Fig 3 is the result of implementation screen shot taken from ns2. The result were implemented in ns2 mobility pack by setting the way point from the node n0 to n2 with the intermediate nodes like n3, n1, n5, n4.

The path leads from n0 to n5 via the gateway connected all the nodes and the n0 is set to node dynamism. The node n0 and n3 were set for waypoint.

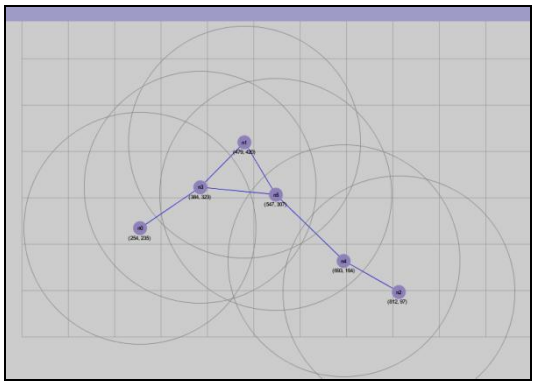

Fig 3: Node Gateway

4. SIMULATION RESULT

```
#Create 6 nodes
set n0 [$ns node]
$n0 set X_ 254
$n0 set Y_ 235
$n0 set Z_ 0.0
$ns initial_node_pos $n0 20
set n1 [$ns node]
$n1 set X_ 479
$n1 set Y_ 420
$n1 set Z_ 0.0
$ns initial_node_pos $n1 20
set n2 [$ns node]
$n2 set X_ 812
$n2 set Y_ 97
$n2 set Z_ 0.0
$ns initial_node_pos $n2 20
set n3 [$ns node]
$n3 set X_ 384
$n3 set Y_ 323
$n3 set Z_ 0.0
$ns initial_node_pos $n3 20
set n4 [$ns node]
$n4 set X_ 693
$n4 set Y_ 164
$n4 set Z_ 0.0
$ns initial_node_pos $n4 20
set n5 [$ns node]
$n5 set X_ 547
$n5 set Y_ 307
$n5 set Z_ 0.0
$ns initial_node_pos $n5 20
//Generate node Movement (waypoint)
$ns at 1 " $n0 setdest 812 97 10”
#Define a 'finish' procedure
proc finish {} {
global ns tracefile namfile
$ns flush-trace
close $tracefile
close $namfile
   exec nam out.nam &
   exit 0
}
for {set i 0} {$i < $val(nn) } { incr i } {
   $ns at $val(stop) "\$n$i reset"
}
$ns at $val(stop) "$ns nam-end-wireless $val(stop)"
$ns at $val(stop) "finish"
$ns at $val(stop) "puts \"done\" ; $ns halt"
$ns run
```

5. SIMULATION RESULT IN TRACE FILE

The result of the above code update the trace file which ensures the data transferred between two nodes and further act against the node for attack.

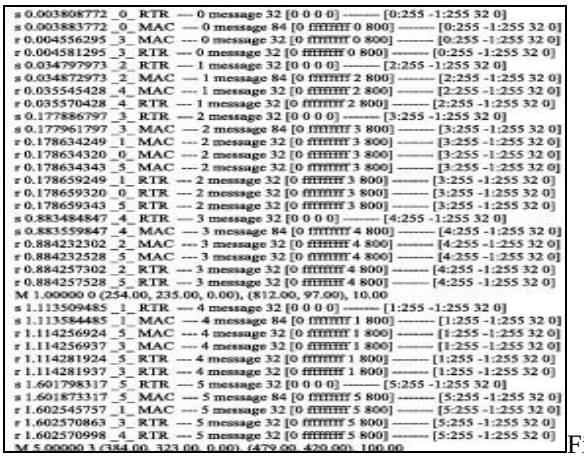

Fig 4: Node Trace file based on simulation

Figure 4 is the screen shot of the trace file generated as the result of simulation.

6. ALGORITHM AND ITS WORKING STRATEGY

The fitness function of PSO generated for each and every node combined with the Gateway verification phase ensures attack and eradicates the attack in its process.
The functional flow of algorithm was represented with the following steps.

Phase I: Detecting the source node
Phase II: Apply Gateway verification phase for pseudo route attack and its types [1] both inside and outside region (node boundary)
Phase III: Apply PSO fitness function to identify the type of attack and its measures to get rid of the attack.

7 .FUTURE WORKS

The future works will focus on other types of attack by building individual PSO fitness value for each and every attack by exploiting it. It further address the node level processing to increase the efficiency of node, which will further increases the bandwidth of the Adhoc network. This study will also address on Waypoint access by which a node once identified as vulnerable will be replaced by existing neighbor node for its further transactions. The need for waypoint access mechanism further increases the efficiency of node data transmission.

8. ACKNOWLEDGEMENT

1. Seethalakshmi.S Assistant Professor, Dept of MCA, Thiagarajar School of Management, Madurai
2. Sarathkumar.J, Student of MCA, Thiagarajar School of Management, Madurai
3. Prem Kumar M, Student of MCA, Thiagarajar School of Management, Madurai

9. REFERENCE

[1] Gautam Das, M.Fazio, Vulnerabilities of Internet Access Mechanism from Mobile Adhoc Networks, IEEE Proceeding 2006.

[2] Kennedy J, Eberhart RC, "Particle Swarm Optimization," In: Proceeding of the IEEE Int. Conf. Neural Networks: 1942-1948, 1995.

[3] Zhao Chang, Wang Wei-ping, "An Improved PSO – Based Rule Extraction Algorithm for Intrusion Detection, Proceeding of IEEE Computer Society.

[4]. Chen Guolong, Chen Qingliang and Guo Wenzhong, " A PSO-Based Approach to Rule Learning in Network Intrusion Detection," Fuzzy informationand Engineering (ICFIE), ASC 40, pp. 666-673, 2007.

[5]. S. Buchegger and J.L. Boudec. Performance analysis of the confidant protocol, cooperation of nodes – fairness in dynamic adhoc networks. In Proc of MobiHOC, june 2002

[6] S. Buchegger and J. L. Boudec. The effect of rumor spreading in reputation systems for mobile ad hoc networks. In *Proc. Of WiOpt'03*, March 2003.

[7]. S. Buchegger and J.-Y. L. Boudec. Coping with false accusations in misbehavior reputation systems for mobile ad hoc networks. Technical Report IC/2003/31, EPFL, 2003.

[8]. S. Marti, T. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of MOBICOM 2000*, pages 255–265, 2000.

[9]. *Junqi Zhang, Kun Liu , Ying Tan, and Xingui He,* "RANDOM BLACK HOLE PARTICLE SWARM OPTIMIZATION AND ITS APPLICATION" IEEE Int. Conference Neural Networks & Signal Processing, Zhenjiang, China, June 8~10, 2008.

[10]. J. J. Liang, A. K. Qin, P. N. Suganthan and S. Baskar, "Comprehensive learning particle swarm optimizer for global optimization of multimodal functions," *IEEE Trans. on Evolutionary Computation*, vol. 10, 2006, pp. 281-296.

[11]. L. N. de Castro, "Learning and Optimization Using the Clonal Selection Principle" *IEEE Transactions on Evolutionary Computation*, Vol.6, 2002, pp. 239-251.

[12]. R. Stoleru, H. Wu, H. Chenji , Secure Neighbor Discovery in Mobile Ad Hoc Networks, 2011 Eighth IEEE International Conference on Mobile Ad-Hoc and Sensor Systems

[13]. http://www.codecogs.com/latex/eqneditor.php used in this paper for creating online equations with LATEX.

[14] Dasgupta D, Gonzalez FA, "An Intelligent Decision Support System for Intrusion Detection and Response," MMM-ACNS, Lecture Notes in Computer Science, 2052:1–14, 2001.

[15] Chittur A., Model Generation for an Intrusion Detection System Using Genetic Algorithms

AUTHORS PROFILE

Subburaj.V, working as Assistant Professor in Department of Computer Application, Thiagarajar school of management, Madurai and Research scholar of Manonmaniam Sundaranar University, Tirunelveli. He received his M.E degree from Anna University, Trichy 2010, MCA degree from Madurai Kamarajar University in 2004 and M.Phil from Madurai Kamaraj University 2006. He has nearly 6 years experience in academia and 3 years in industry.

Dr.K.Chitra, working as Assistant Professor in Department of Computer science, Government Arts College, Melur. Her Area of Specializations is Mobile Computing, Advanced Java Technology, Object Oriented Analysis, Design and Programming. She has significant publication in ACM. Her research area includes Mobile Database Management, Object Technology, Search Engine Optimization, and Web & Text Mining.