

Domain based Security for Mobile Agents

Institut für
Computertechnik

ICT

Institute of
Computer Technology

Micheal Sonntag

Friedrich Kupzog

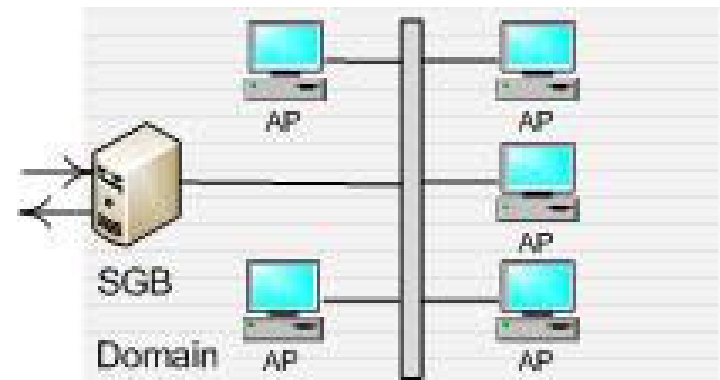
Najmus Saqib Malik

Presentation Layout

- Background
- Domain based security
 - Vulnerability Level (VL) and Reputation Value (RV)
 - Algorithm for mobile agent security
 - Process of changing VL
 - RV behaviour and restriction state
- Simulation
- Results
- Conclusion

Background

- Mobile Agent – MA
- Agent platform – AP
- Security Manager – SM
- Security Services
- Domain



Domain based security

- Vulnerability level – VL
 - Represents the value for domain
 - Higher value suggest bad
 - Lower value is good
- Reputation Value – RV
 - Degree of honesty for a platform
 - Larger RV => platform is safe to visit
- VL and RV are maintained by the security manager

Domain based security

Algorithm for mobile agent

- 1) start execution of task and collect the results
- 2) calculate the hash code itself without results
- 3) compare this hashcode with one calculate in previous AP
- 4) if not same discard new results and move to SM else continue
- 5) send the hash code to SGB
- 6) if VL is H send results to SM
- 7) if VL is M and $CP \% (n/m) = 0$, send results to SM
- 8) if VL is L then continue

- 9) fetch RV of next AP from SM
- 10) if RV is acceptable
 - 1) CP ++
 - 2) If RV of next AP is smaller then current AP then sends all the results to SM
- 11) else continue with step 9

Domain based security

Process for changing VL

- if 20% of mobile agents are modified, de-grade VL level
- if ($a \leq 5\% b$) then up-grade VL level
where a = No. of times the AP(s) are found malicious
 b = No. of times the AP(s) are found honest

Domain based security

RV behaviour and Restriction State

- RV is calculated every time when MA found malicious, as

$$RV = 1 - \frac{\sum_{i=1}^Y (i)}{\sum_{j=1}^X (j)}$$

where X = No. of MAs visit an AP

Y = No. of MAs that are modified by same AP

- if any platform modified certain percentage of visiting mobile agents then it is in *restriction state*
- no MA will visit AP until it comes out from restriction state

Domain based security

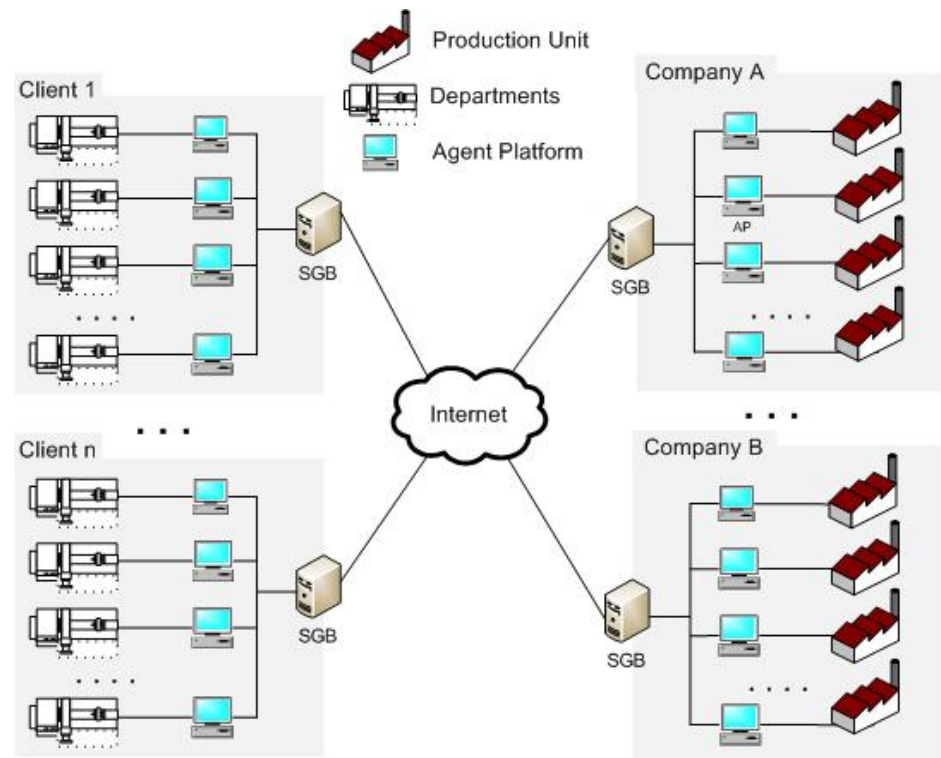
when AP is in Restriction State then

- SM send dummy MA to AP
- if dummy MA is modified on return
 - Recalculate RV value
 - if $RV < 0.4$ then terminate the AP
- else if No. of dummy MA is equal to Y
 - increment X
 - recalculate RV

when $RV > 0.6$, AP's Restriction State is over

Scenario from Production Area

A MA from a company visit its different client's site to collect orders.



- OMNetpp is used for simulation
- Initially
 - Domain's VL = 1 (low) and each AP has RV = 1 (high)
 - The RV and VL assigned to MA is shown below

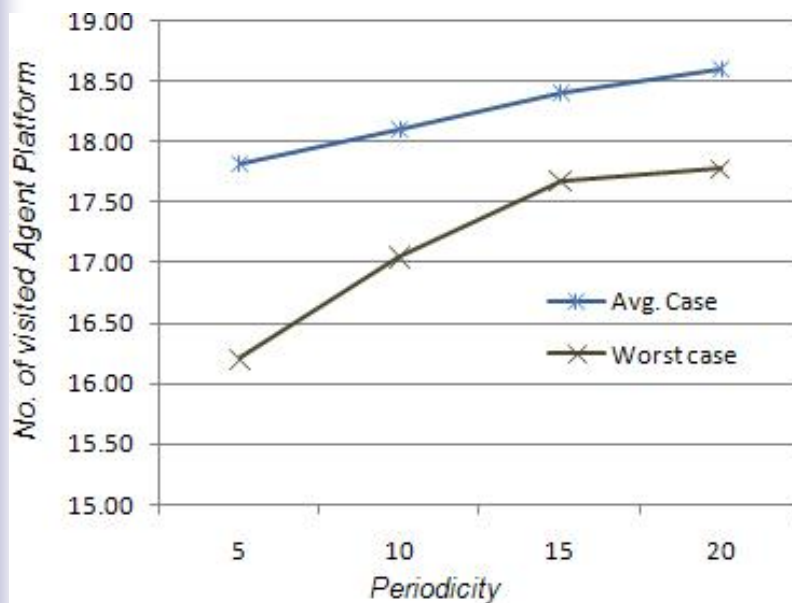
MA	RV	VL
50%	1.00	1.00
30%	0.95	2.00
20%	0.90	

- Two cases:
 - Average case : half of the AP modify the mobile agent with different periodicity
 - Worst case : more the half of the AP modify MA with different periodicity
- Periodicity

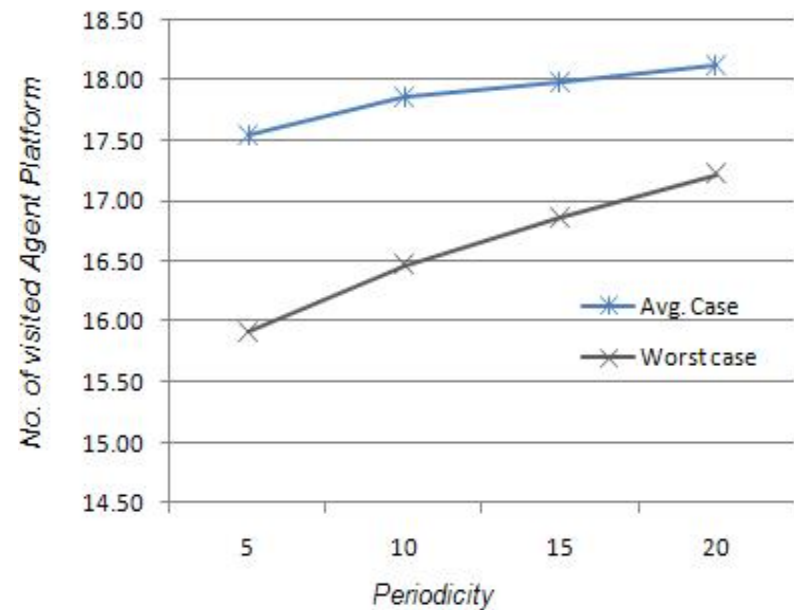
The size of a set of agents in which one agent is changed by AP

Two cases:

- Average case
- Worst case



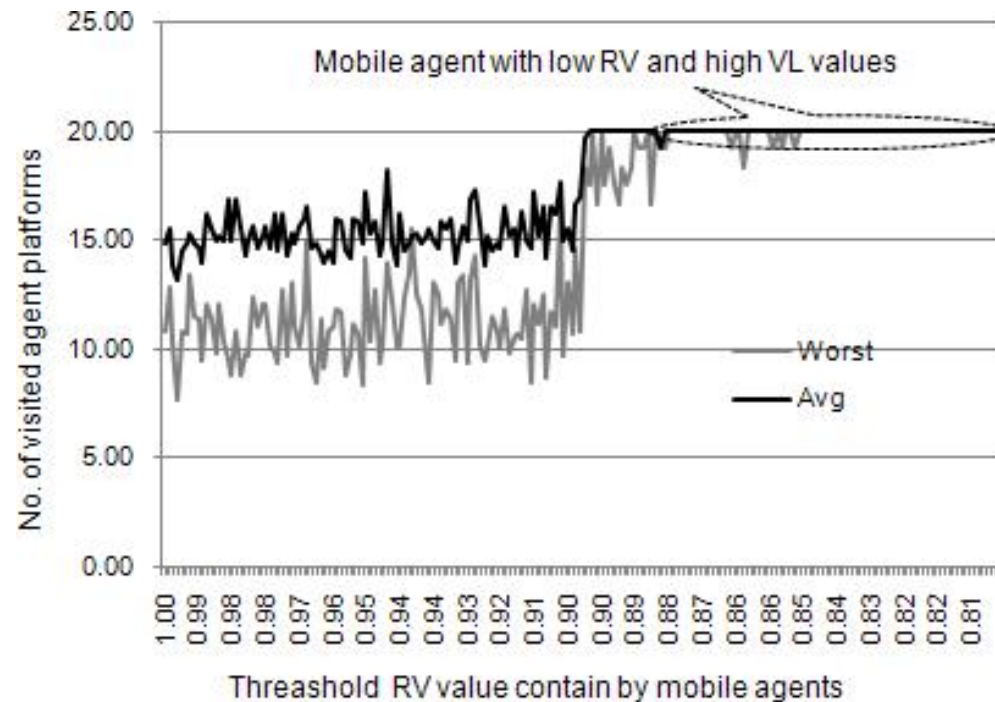
100 MAs



200 MAs

■ Periodicity

the size of a set of agents in which one agent is changed by AP



Conclusion

- MA can decide whether to visit a domain or not
- This cumulative decision save the turnaround time for mobile agent
- A global agreement upon the rules for RV and VL is required in a form of standard