Genetic Optimization of Access Control Schemes in Virtual Local Area Networks

Igor Saenko and Igor Kotenko

St. Petersburg Institute for Informatics and Automation (SPIIRAS)

Previous Works

[Hidemoto Nakada, etc., 2009]: propose to employ Genetic Algorithm (GA) method to solve the virtual machine packing problem in cloud systems, but the goal is to enable efficient resource provisioning.

[Ning Hu, etc., 2006]: is a good example of applying GA in information security problems, but not for VLAN and in conjunction with the RBAC.

[Cheng-Feng Tai, etc., 2010]: propose to assist the best known clustering algorithms for constructing a virtual subnet, but the goal is to improve group communication efficiency.

Task Statement

We have:

- local network with **VLAN** opportunities;
- **required** access scheme of users to information resources;
- resources may have the shared access flags without passwords

We need:

- distribute users and resources on network nodes;
- set flags on resources;
- divide network onto subnets

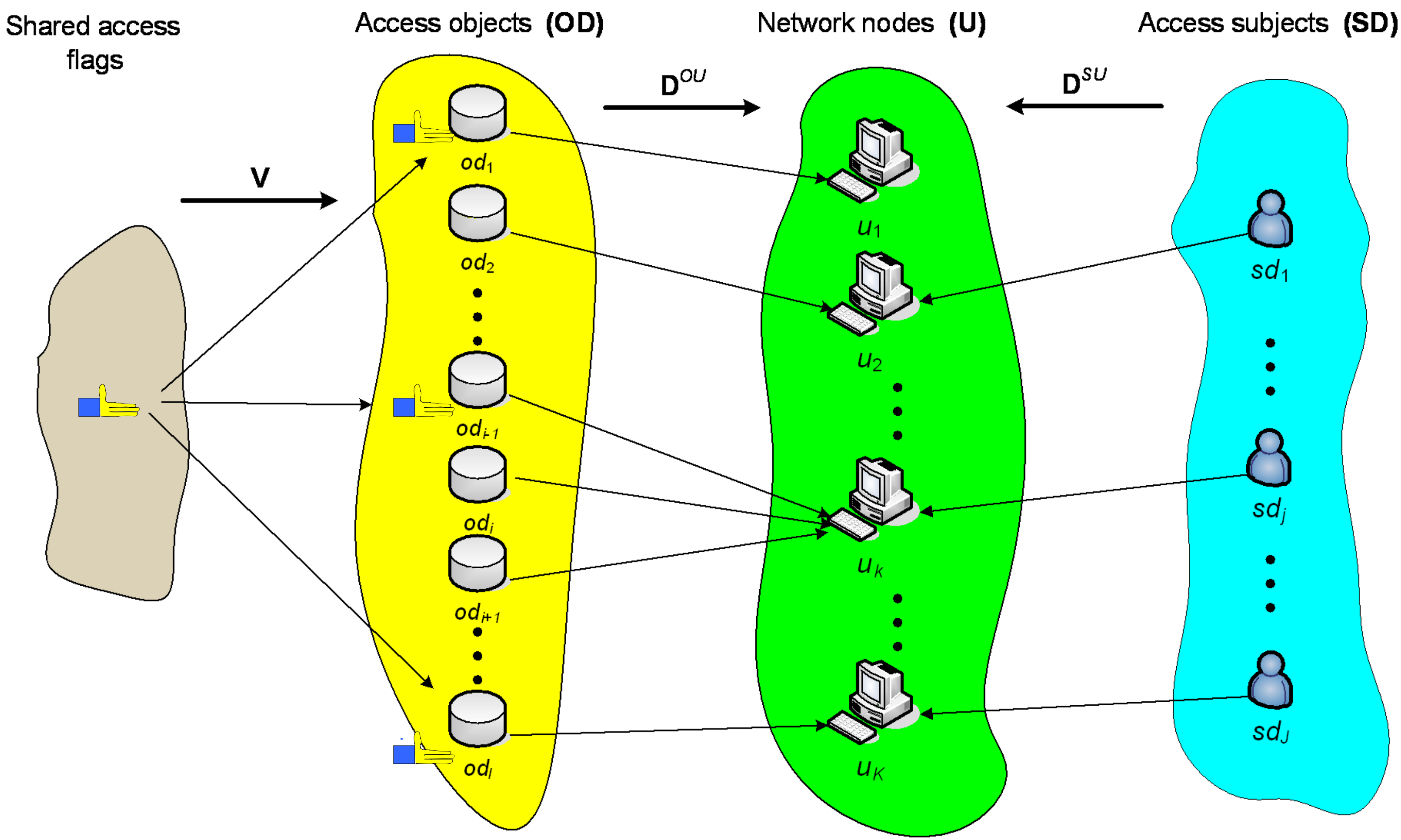
in order to

- ensure **confidentiality** and **availability** of information

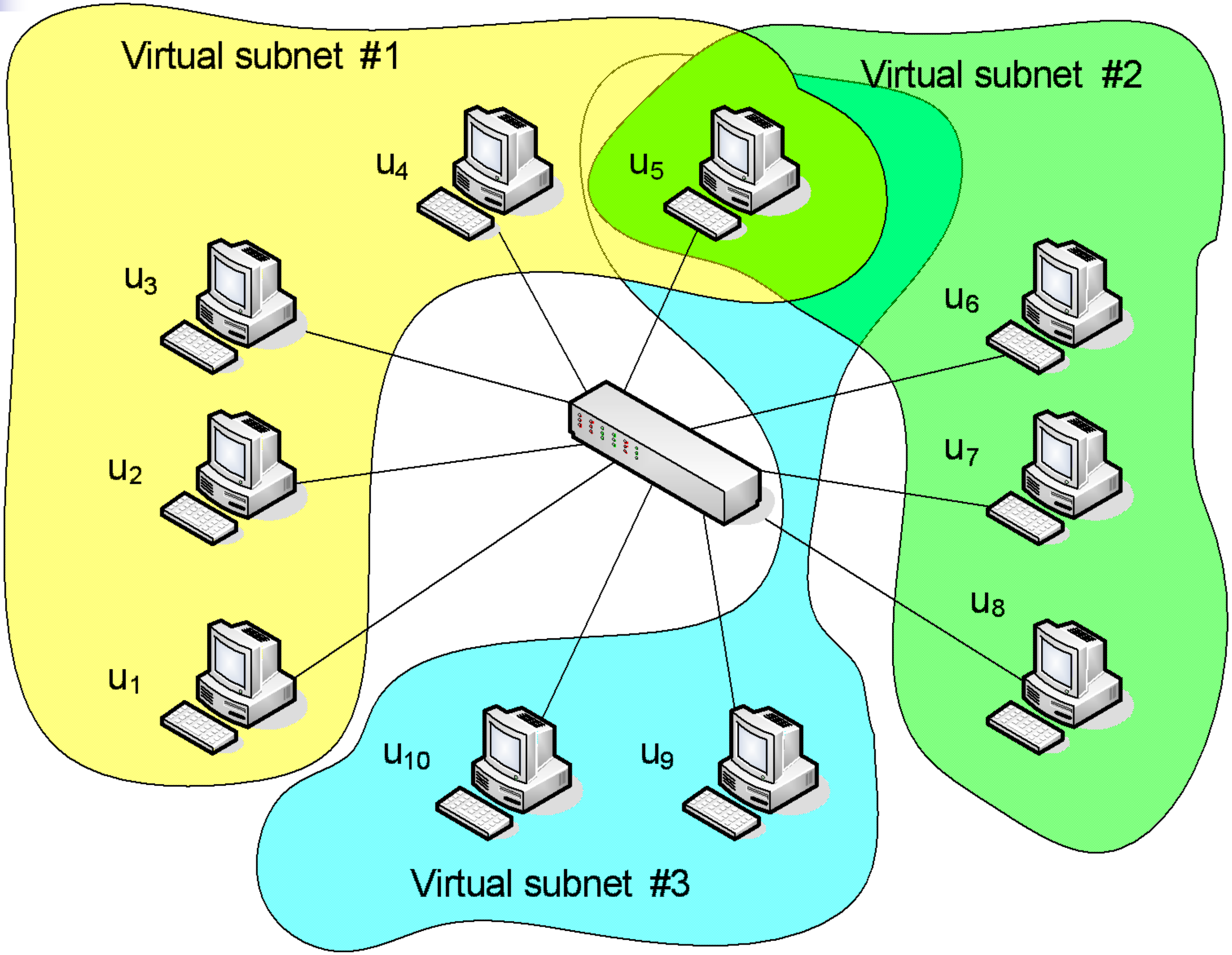
Outline (1)

- **Access Control Mechanisms in VLAN**
- Formal Task Statement
- Method of Solving (Genetic Algorithm)
- Evaluation
- Conclusion and Future Work

Distribution Information Resources and Users on Network Nodes



Virtual Subnets



Access Rules in VLAN

No.	Predicates for Subject S access Object O
1	(V(O) = 0) & (R(S, U) = 1) & (H(O, U) = 1)
2	(V(O) = 1) & (R(S, U1) = 1) & (H(O, U2) = 1) & (VLAN(U1, U2) = 1)

V(O) – object O has flag;
R(S, U) – user S works on node U;
H(O, U) – object O is stored on node U;
VLAN(U1, U2) – node U1 and node U2 belong to the same subnet

Outline (2)

- Access Control Mechanisms in VLAN
- **Formal Task Statement**
- Method of Solving (Genetic Algorithm)
- Evaluation
- Conclusion and Future Work

Initial Data

Set of access objects	$\mathbf{OD} = \ od_i \ ,$
Set of access subjects	$\mathbf{SD} = \ sd_j$
Set of network nodes	$\mathbf{U} = \ u_k$
Required access control scheme	$\mathbf{R}^{\text{req}} = \left[r^{\text{req}}_{ij} \right],$ $r^{\text{req}}_{ij} \in \ 0;1$

Variables

Matrix of distribution of objects on network nodes	$\mathbf{D}^{OU} = \left[d^{OU}{}_{ik} \right]$
Matrix of distribution of subjects on network nodes	$\mathbf{D}^{SU} = \left[d^{SU}{}_{jk} \right]$
Vector of shared access flags	$\mathbf{V} = \ v_i$
Matrix of VLAN structure	$\mathbf{X} = \ x_{mn}\ ,$ $x_{mn} \in \ 0;1$

Object Function

Unconditional scheme $\mathbf{R}^{\text{un}}$: $r^{\text{un}}_{ij} = \sum_{k=1}^{K} d^{SU}_{ik} \cdot d^{OU}_{kj}$ (1)

"Conditional on V" scheme $\mathbf{R}^{\text{V}}$: $r^{V}_{ij} = r^{\text{un}}_{ij} + v_i \; 1 - r^{\text{un}}_{ij}$ (2)

Real scheme $\mathbf{R}^{\text{real}}$: $r^{\text{real}}_{ij} = \sum_{k=1}^{K} x_{ik} \cdot r^{V}_{kj}$ (3)

Indicator of confidentiality: $F^{\text{conf}} = \sum_{i=1}^{I} \sum_{j=1}^{J} \max \; 0, \; r^{\text{real}}_{ij} - r^{\text{req}}_{ij}$ (4)

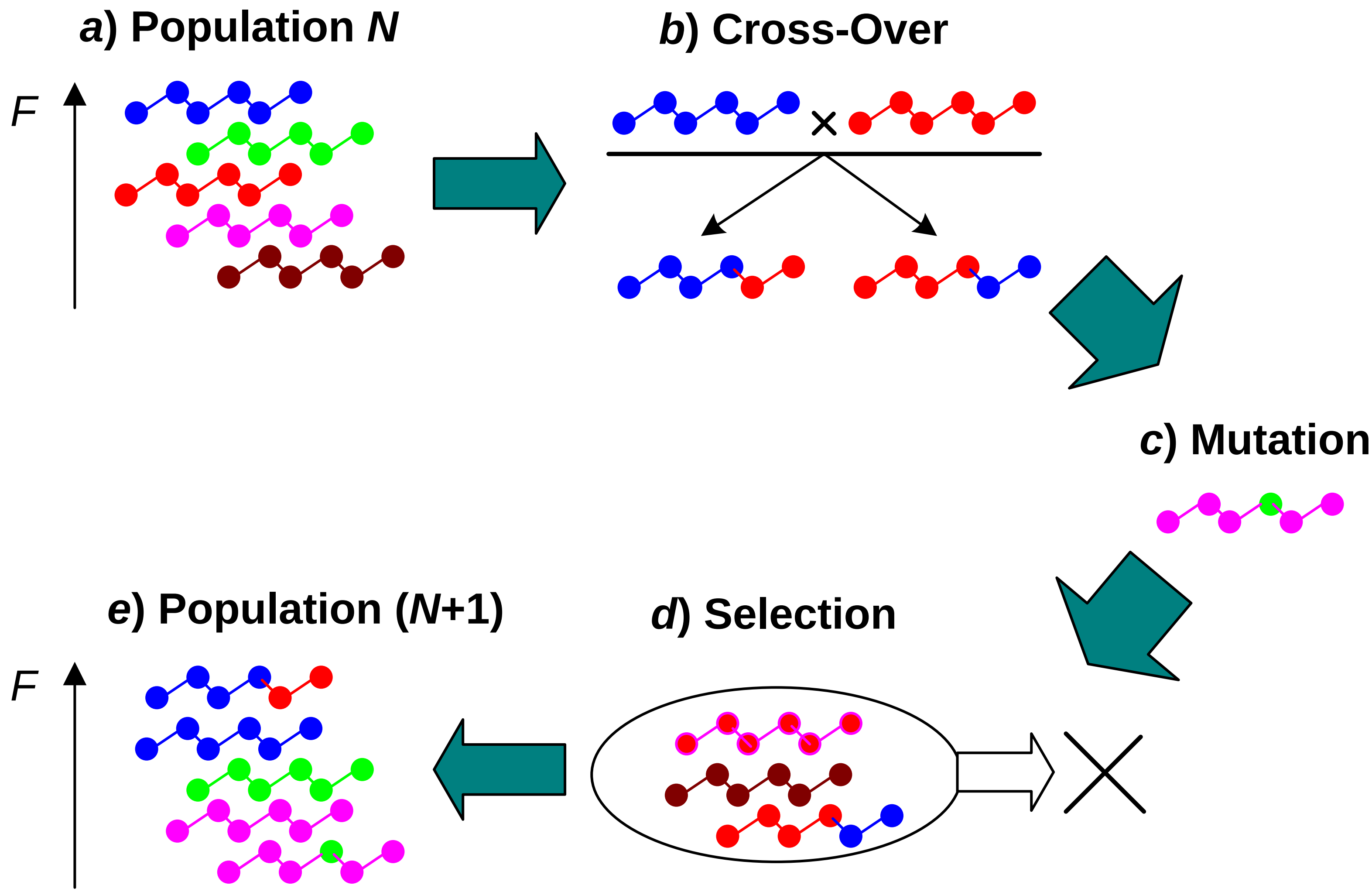
Indicator of availability: $F^{\text{conf}} = \sum_{i=1}^{I} \sum_{j=1}^{J} \max \; 0, \; r^{\text{req}}_{ij} - r^{\text{real}}_{ij}$ (5)

Object function: $F = \alpha F^{\text{conf}} + \beta F^{accs}$ (6)

Outline (3)

- Access Control Mechanisms in VLAN
- Formal Task Statement
- **Method of Solving (Genetic Algorithm)**
- Evaluation
- Conclusion and Future Work

What is Genetic Algorithm?



Chromosomes (Variable Coding)

1-st chromosome consists of file numbers $\{r_i\}$ which is stored on nodes $\{j\}$):

$$R_{chr} = r_1, r_2, \ldots, r_i, \ldots, r_I \ \ , r_i \in \ 1;2;\ldots;J \qquad (1)$$

For example: $R_{chr} = 4,1,3,5,2$

2-nd chromosome reflects shared access flags:

$$V_{chr} = v_1, v_2, \ldots, v_i, \ldots, v_I \ \ , v_i \in \ 0;1 \qquad (2)$$

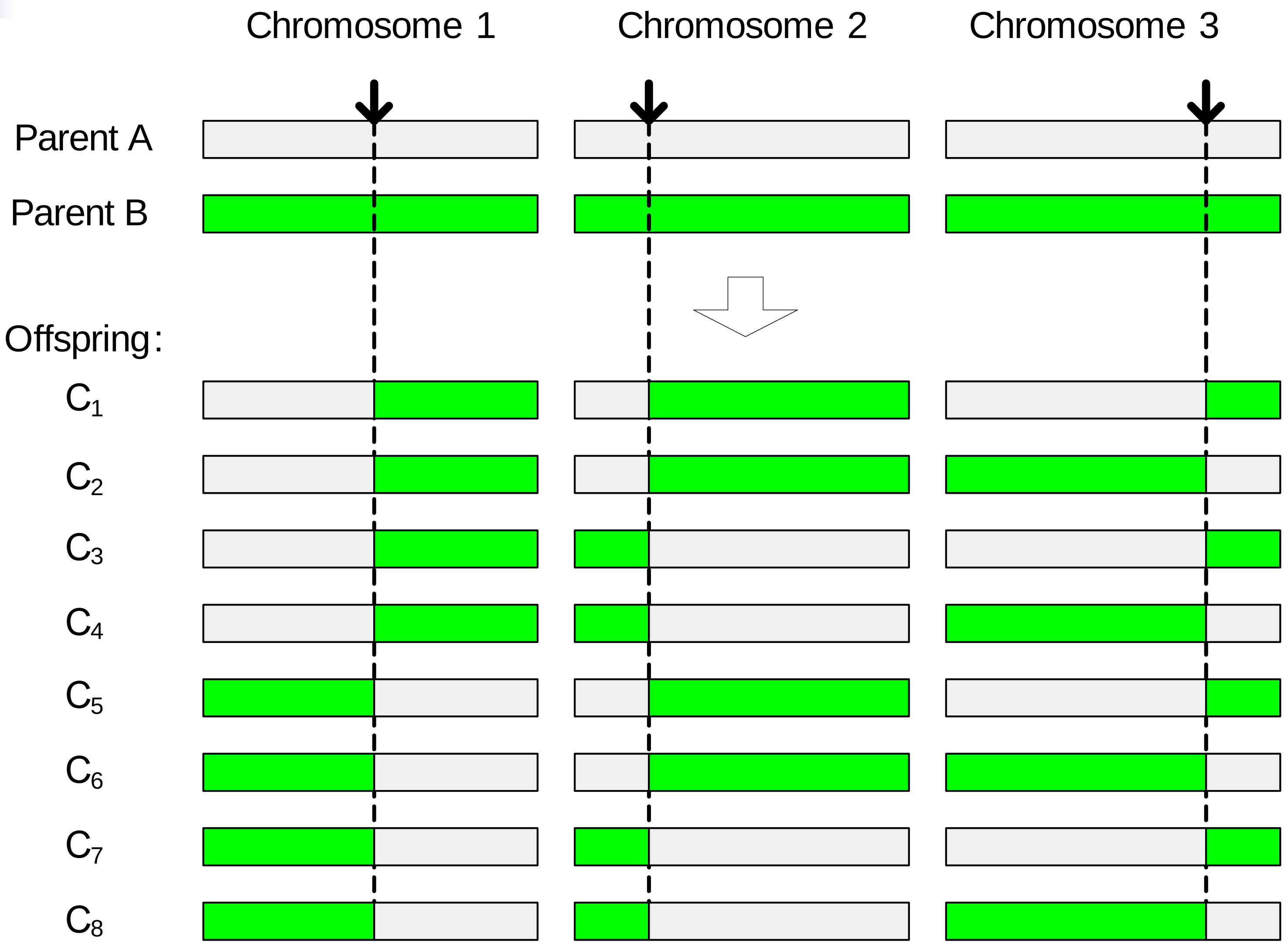
For example: $V_{chr} = 111010$

3-d chromosome consists of the elements of the matrix **X** under main diagonal: (3)

$$X_{chr} = x_{12}, \ldots, x_{1K}; x_{23}, \ldots, x_{2K}; \ldots; x_{K-1,K} \ \ , x_{ij} \in \ 0;1$$

For example: $X_{chr} = 0101|111|10|1$

Crossover


Chromosome 1
Chromosome 2
Chromosome 3
Parent A
Parent B
Offspring:
C1
C2
C3
C4
C5
C6
C7
C8

Outline (4)

- Access Control Mechanisms in VLAN
- Formal Task Statement
- Method of Solving (Genetic Algorithm)
- **Evaluation**
- Conclusion and Future Work

Required and Resulting Schemes

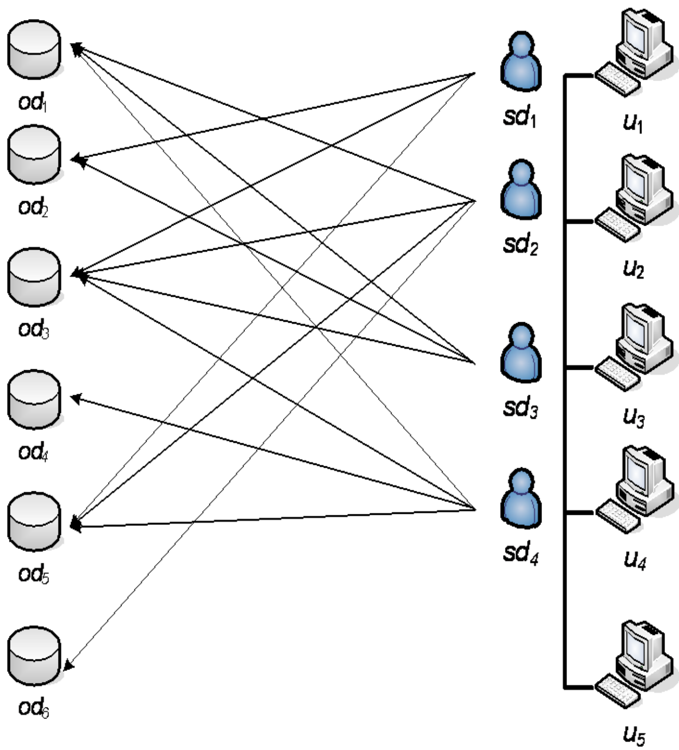
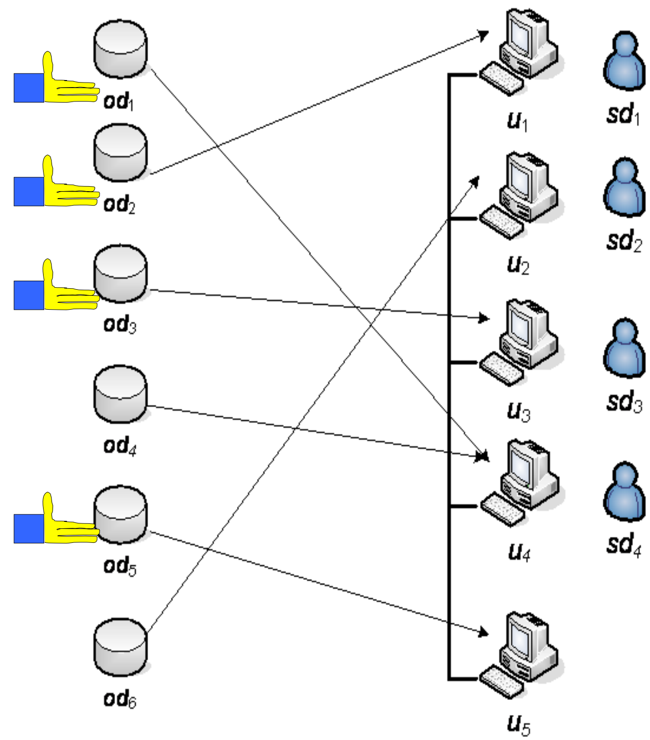


Fig.1. Required Scheme

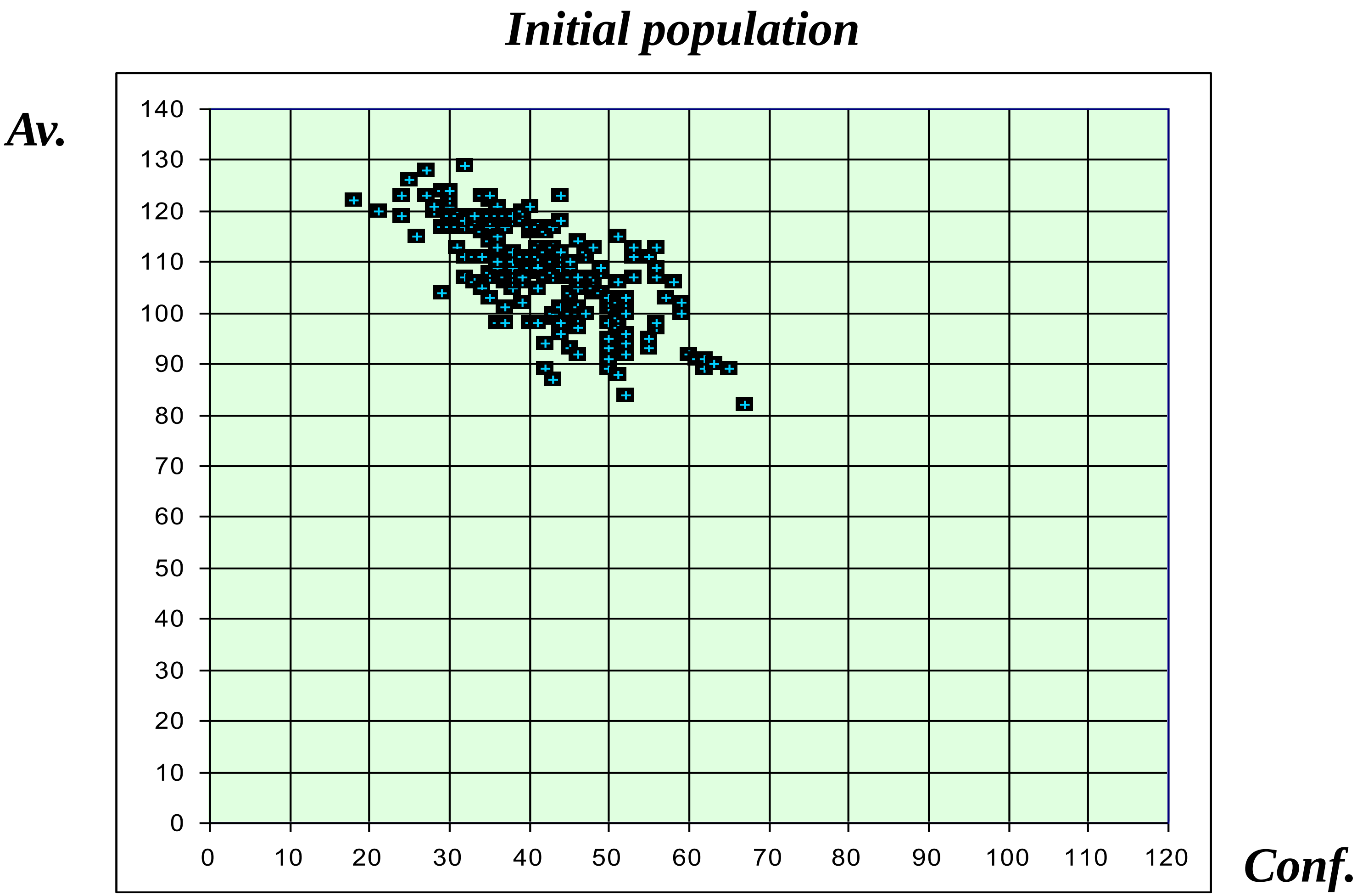


VLAN-matrix (**X**)

0	1	0	1
	1	1	1
		1	0
			1

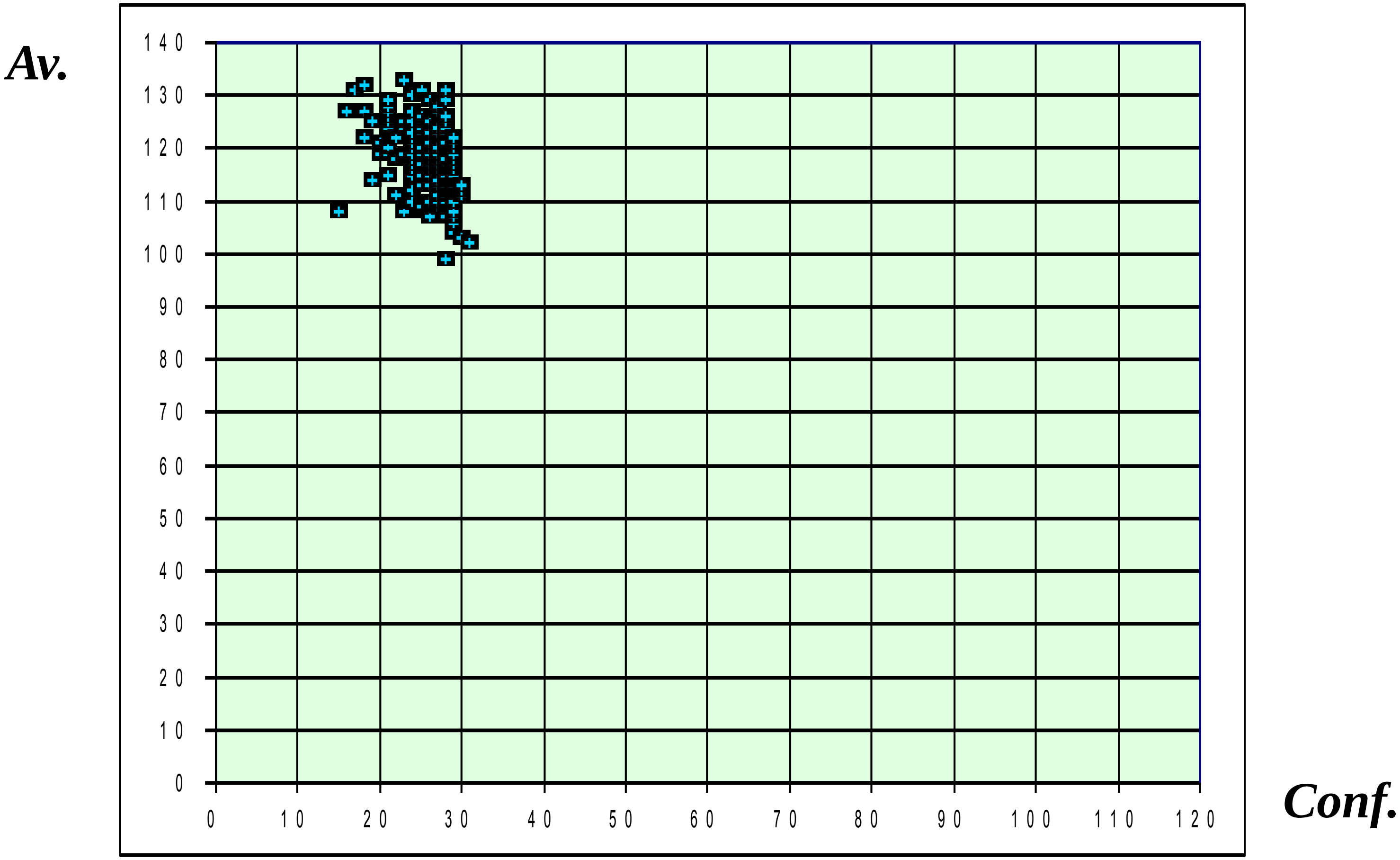
Fig.2. Resulting distribution and VLAN-dividing

Population Changing

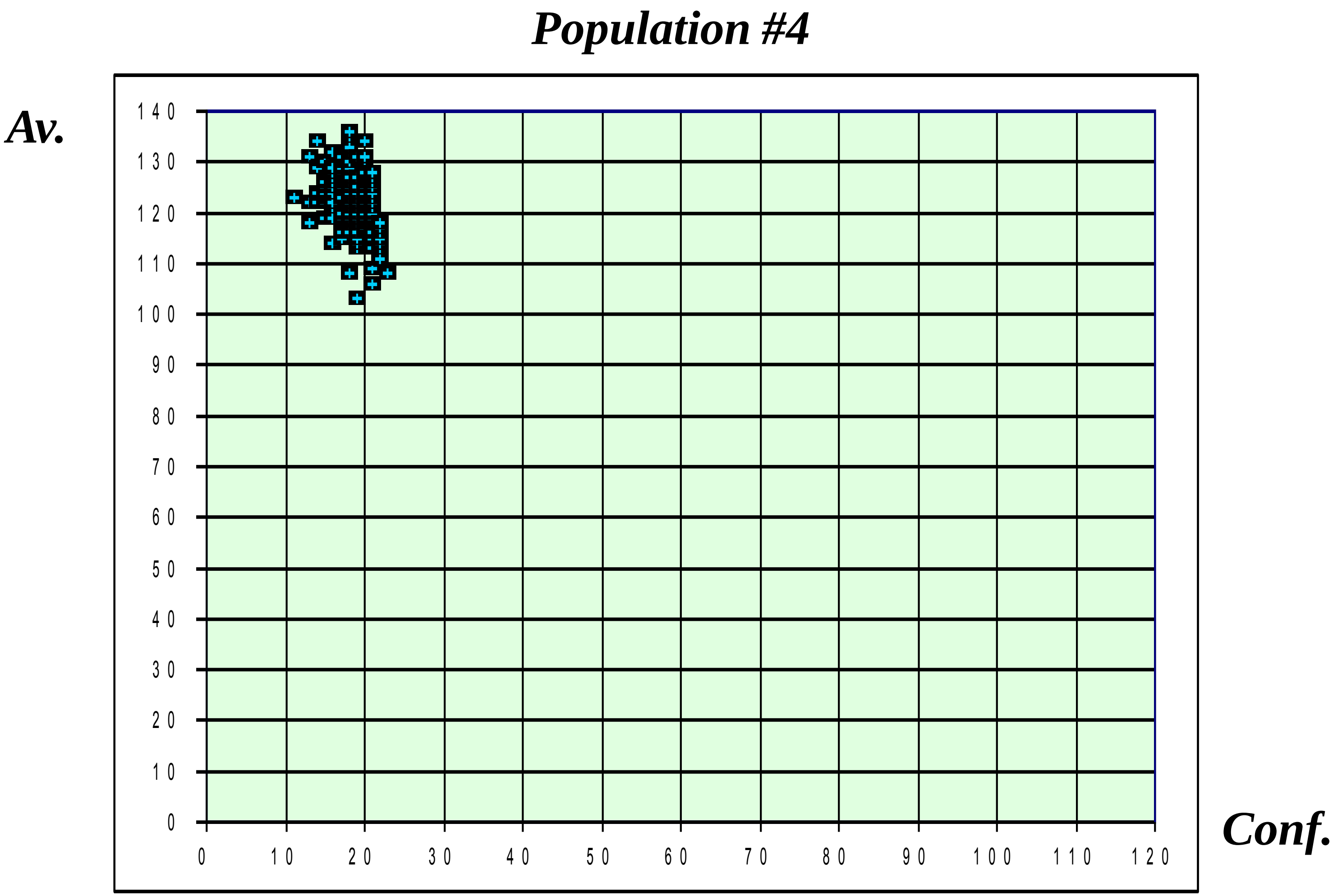


Population Changing

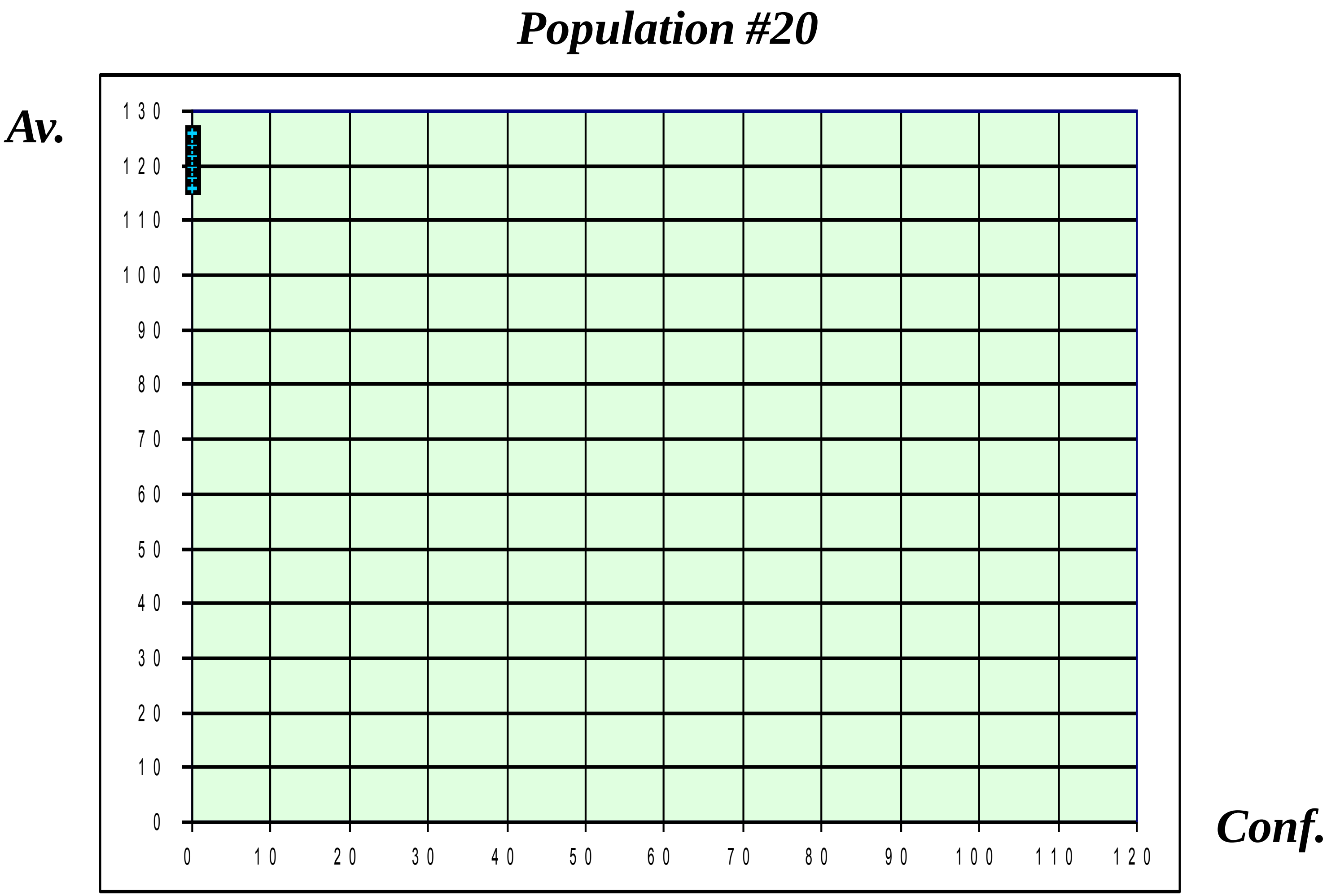
Population #2



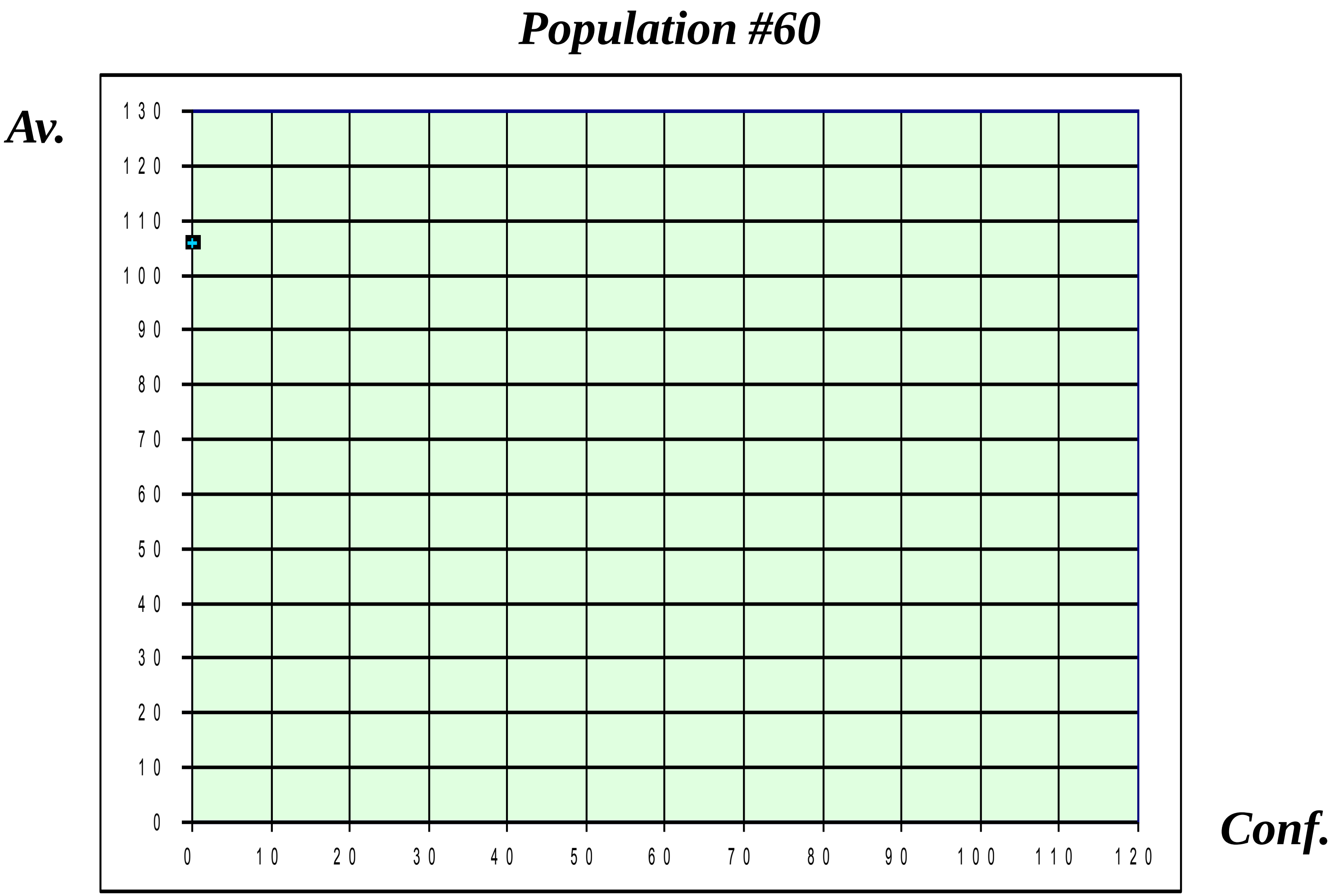
Population Changing



Population Changing



Population Changing



Security Evaluation

I	P_0	p_{pw}	N_1	N_2	P_1	P_2	k_{UAA}
6	10^{-4}	10^{-4}	6	0	0,00070	10^{-4}	**7,00**
6	10^{-5}	10^{-4}	6	0	0,00061	10^{-5}	**60,98**
6	10^{-4}	10^{-5}	6	0	0,00016	10^{-4}	**1,60**
12	10^{-4}	10^{-4}	12	5	0,00130	0,00060	**2,17**
12	10^{-4}	10^{-4}	12	5	0,00121	0,00051	**2,37**
12	10^{-4}	10^{-5}	12	5	0,00022	0,00015	**1,47**
20	10^{-4}	10^{-4}	20	18	0,00210	0,00190	**1,11**
20	10^{-4}	10^{-4}	20	18	0,00201	0,00180	**1,11**
20	10^{-4}	10^{-5}	20	18	0,00030	0,00028	**1,07**

where P_0 – the probability of unauthorized access the information caused by the reasons other than the compromise of shared passwords;

p_{pw} – the probability of password compromising;

N_1, N_2 – the number of objects which require access password protection in the traditional case and in the case of using the proposed method, respectively;

P_1, P_2 – the probability of unauthorized access in the traditional case and in the case of using the proposed method, respectively;

$k_{UAA} = P_1 / P_2$ – degree of security increase.

Outline (5)

- Access Control Mechanisms in VLAN
- Formal Task Statement
- Method of Solving (Genetic Algorithm)
- Evaluation
- **Conclusion and Future Work**

Conclusion and Future Work

- Poly-chromosomal GA is a flexible and powerful method for tasks with various access control criteria
- We plan to implement GA for solving Role-Mining Problem.

Thank you!