1 a) Similarity value ~~is~~ between two samples is calculated according to the formula

$$\frac{1}{|A|} \sum_{\forall a \in A} \frac{\min(f_1(a), f_2(a))}{\max(f_1(a), f_2(a))}$$

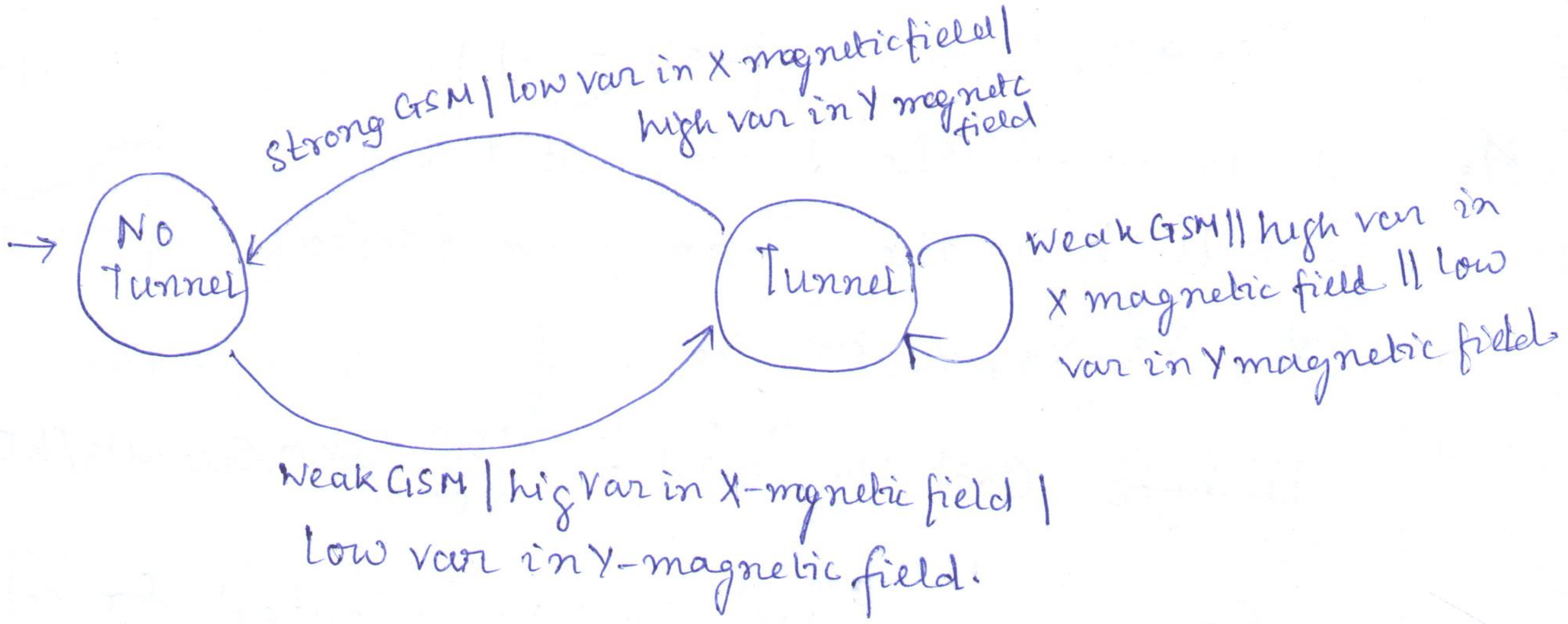
Similarity between S_1 and S_2 $= \frac{1}{8}\left(\frac{3}{2} + \frac{1}{2} + 2\right)$

$= 0.687$

Similarly the distances between each pair of samples can be calculated –

	S_1	S_2	S_3	S_4
S_1	–	0.68	0.83	0.858
S_2	0.68	–	0.562	0.587
S_3	0.83	0.562	–	1.0
S_4	0.885	0.587	1.0	–

b)



2 a) $d(P_e) \leq T_d$

$d(P_d) > T_d$

$e_n(P_n) = e_n(P_e)$

$d(P_n) \leq T_d$

b) The most cost efficient path is $1 \to 2 \to 5 \to 6 \to 8$ (cost = 12)
and the time delay associated with this path is ~~12~~ 12
which is less than the deadline and hence is a feasible solution.

3. The trip starts from P_1

from P_1 it ~~will~~ can go to P_2, P_3, P_4 and P_9

~~It~~ Weights associated with $P_2 = \frac{1}{7}$, $P_3 = \frac{1}{5}$, $P_4 = \frac{1}{9}$, $P_9 = \frac{1}{4}$

P_9 has the highest weight associated. So it will go to P_9 next. Essentially it will go to the closest place every time. So the path is

$$P_1 \xrightarrow{4} P_9 \xrightarrow{4} P_4 \xrightarrow{5} P_6 \xrightarrow{5} P_5 \xrightarrow{5} P_2 \xrightarrow{4} P_3 \xrightarrow{8} P_7 \xrightarrow{9} P_8$$

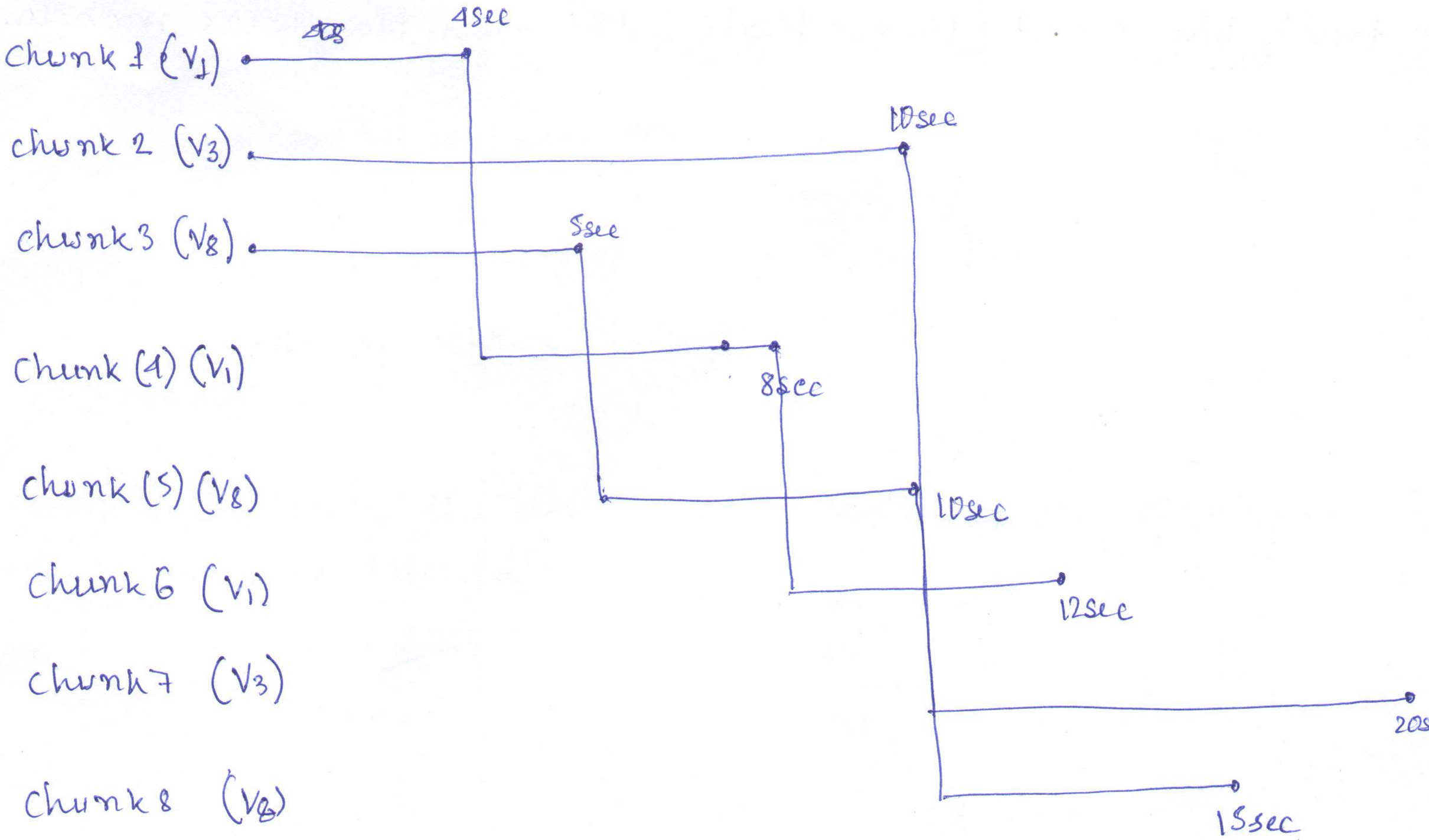
Total cost of the path = 44

4. u initiates the process at t=0
It will hear the I-am-alive messages from -

V_1, V_2, V_3, V_7 and V_8

~~Per byte~~ Cost threshold = $\frac{100}{800}$ = 0.5 units/kB

So V_1, V_3 and V_8 will be selected for collaboration
There are 8 chunks each of size 100 kB that needs to be downloaded.



The time taken to download the whole file = 20 sec

Total cost = $(300 \times 0.4) + (200 \times 0.3) + (300 \times 0.4)$

$= 120 + 60 + 120 = 300$ units.

5. A malicious channel can specify any origin for a page and associate an arbitrary script with a button. When the button is clicked the script is injected into the page and gains unrestricted access to the content from the page's origin. This is cross-site scripting vulnerability

An AR attacker can register a channel associated with a photo (may be of a license plate). When millions of users scan their background and the photo is prominent the channel is launched automatically. The information can then be transferred to the channels owner. The can

track the object (license plate) threrogh the users mobile.