lec 18

Social Secret sharing SSS

Social SS: in this scheme, share are allocated based on a player's repatation value & the way he interacts with other players. During the social tuning phase, weights of players are adjusted such that players who cooperate will end up with more shares than those who defect.

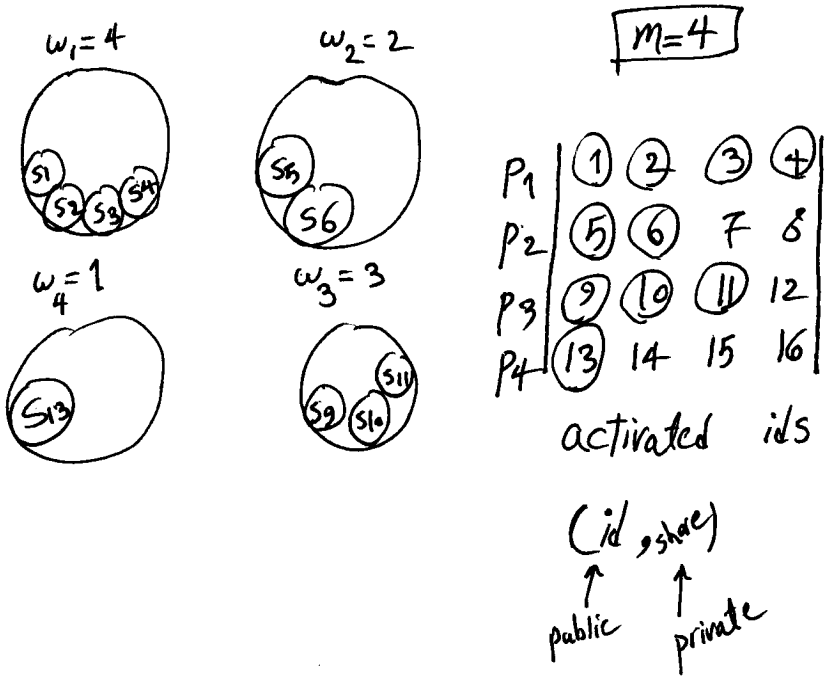
Motivation: in many application, componet of a secure system may have differat levels of importance (# of shares a player has) and reputation (i.e., cooperation by other players for secret recovey or share renewal). As such, we would like to balance these two faetors

Construction: each player initially receives a constant # of shares. As time passes, players are assigned weights based on their behavior. Consequenty, players receive # of shares corresponding to their repatation values.

Def #1: Cooperation $P_i(C)$: P_i is available at the time of share renewal or recovery & sends correct shares to ther players. Defection $P_i(D)$: P_i is not available at the required time or may respond with delay. Corruption $P_i(X)$: P_i has been compromised by a passive adversary.

Def 2#: the social SS scheme is a three-tuple denoted as $S^*(Sha, Tun, Rec)$ consisting of secret sharing, social tuning, secret recovery. Tun: the weight of players are adjusted based on their trust/reputation values.

Conditions the total weight of uncorrupted players $\in \Delta$ must be equal or greater than the threshold. on the other hand, the total weight of colluders $\in \nabla$ must be less than the threshold. Finally, the weight of each player is bounded to a parameter much less than t, i.e., $w_i \leq m \ll t$.



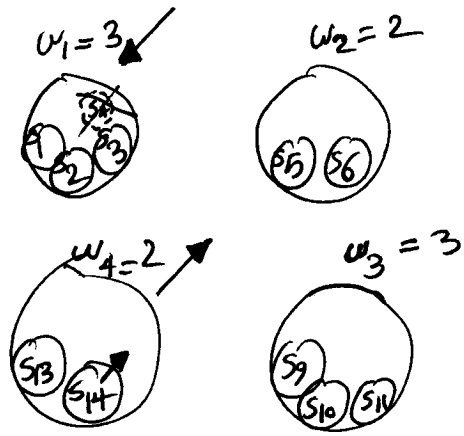
$m = 4$

P_1	1	2	3	4
P_2	5	6	7	8
P_3	9	10	11	12
P_4	13	14	15	16

activated ids

(id, share)

↑ public ↑ private



(*) to decrease weigh of P_1 we need to use proactive SS (disenrollment) protocol to deactivate s_4 for P_1

(*) to increase weight for P_4, we need to use enrollment protocol to generat s_{14} for P_4

T_i^p : reputation value of p_i ⟶ public info (see page 6~7 for trust functions)

w_i^p : weight of p_i at period "p" ⟶ public info

① **Sharing phase** the dealer initiates a ss scheme by $f(x) \in \mathbb{Z}_q[x]$ of degree "t-1" where $f(0) =$ secret α. He sends shares of p_i for $1 \le i \le n$ according to his weight w_i^p.

$s_{ij} = f(v_{ij})$ for $1 \le j \le w_i$, where $v_{ij} = i * m - m + j$

m: max of weight for all players

Examples

$i = 3$ p_3 $w_3 = 2$

$m = 4$

$v_{31} = 3 \times 4 - 4 + 1 = 9$

$v_{32} = 3 \times 4 - 4 + 2 = 10$ ids

$i = 1 \longrightarrow p_1$ $w_1 = 3$

$m = 4$

$v_{11} = 1 \times 4 - 4 + 1 = 1$

$v_{12} = 1 \times 4 - 4 + 2 = 2$

$v_{13} = 1 \times 4 - 4 + 3 = 3$ ids

② **Social Tuning phase**

II.1 Inactivate non-cooperative players' shares

II.2 activate cooperative players' shares

II.3 use enrollment protocol & proactive SS (disenrollment) protocol to generate shares for activated ids & remove shares corresponding to inactivated ids

II.1 # one approach is to inactivate a # of shares/ids for each player p_i proportional to the amount that the player's trust value T_i^P is decreased.

ω_i^P & T_i^P :

$p_i(D)$: defection $\Longrightarrow$ $\omega_i^P = \left\lfloor \omega_i^{P-1} * \left(1 - \frac{\tau}{2}\right) \right\rfloor$ (e.g., 0.75)

such that $\tau = T_i^{P-1} - T_i^P \geq 0 \longrightarrow$ positive

↳ coefficient of the weight reduction for non-coop players

$-1 \leq T_i^P \leq +1$ → map to $0 \sim +1$

δ^P : total # of shares/ids that must be activated

$$\delta^P = \sum_{i : p_i(D)} \left(\omega_i^{P-1} - \omega_i^P\right)$$

$i : p_i(D)$: defective players

II.2 given the # of ids/shares to be activated, we now define which players should receive extra shares & how many newcomers can join the scheme.

For each p_i consider the following ratio $f = \frac{T_i^P}{\omega_i^P}$

* this ratio f in increased by trust value and it is decreased by weight of p_i

As a result, it's reasonable to activate ids in players for whom this ratio is highest (e.g. highest trust value & lowest weight) but this not enough since we need to consider newcomers (their trust value is zero). As such:

(a) * first priority is given to cooperative players for whom this ratio "$\frac{t}{w}$" is both highest & positive.

(b) * second priority is given to newcomers.

(c) * Third priority is given to other cooperative players with negative trust value.

II.3 using enrollment & disenrollment protocols.

Secret Recovery similar to weighted secret sharing scheme:

Authorized players $\in \Delta$ are able to recover the secret if $\sum_{P_i \in \Delta} w_i \geq t$ through Lagrange interpolation.

Trust Function

Social: trust is the willingness of a person to become vulnerable to the actions of another person irrespective of the ability to control those actions.

Computer: trust is defined as a personal expectation that a player has with respect to the future behavior of another party, i.e., a personal quantity.

Reputation is the perception that players have with respect to another player's intention, i.e., a social quantity.

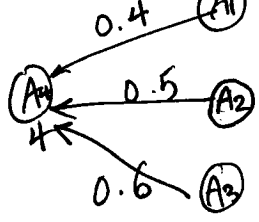
Applications area: Rational crypto, security, humanoid Robotics Game theory, p2p networks, Multi-agent systems e-commerce, psychology & sociology.

---

trust value * T_{ij}^{p} denotes the trust value assigned by P_j to P_i in period "p"

reputation * $T_i^p = \frac{1}{n-1} \sum_{j \neq i} T_{ij}^p$ where $-1 \leq T_i^p \leq +1$ &

$T_i^{\emptyset} = \emptyset \rightarrow$ initial trust/rep value

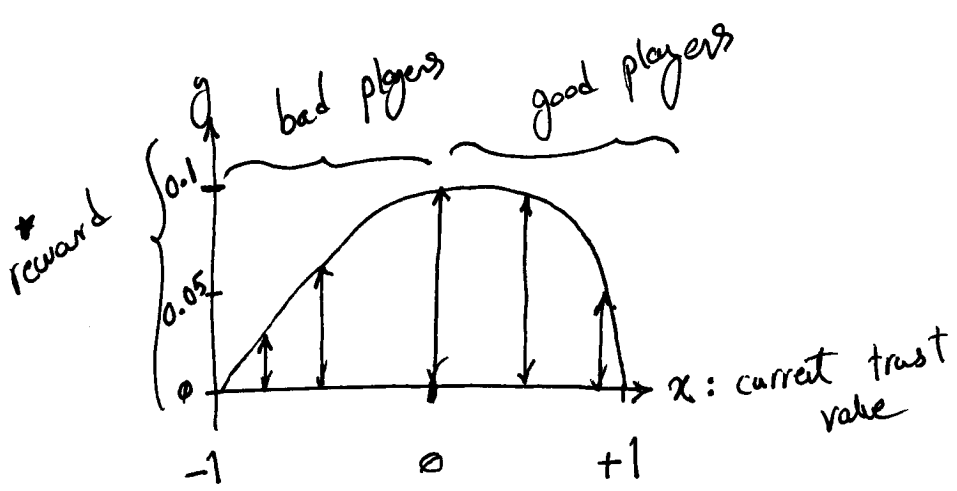


$\longrightarrow T_4^p = \frac{1}{3}(0.4 + 0.5 + 0.6) = 0.5$

Repatation

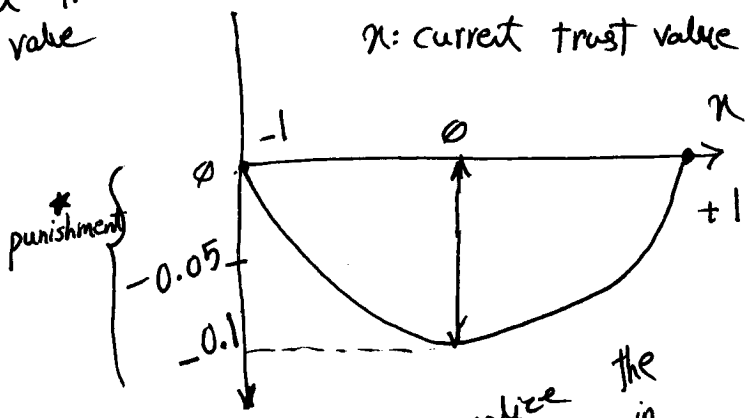
Example

(a) Function



reward function in the case of cooperation

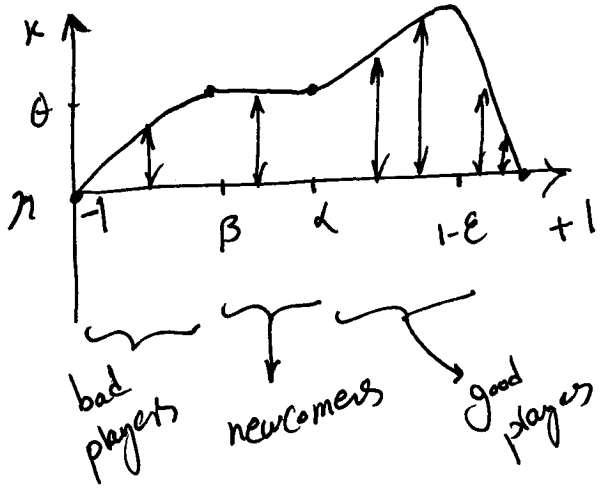
$$T_i^p = T_i^{p-1} + \underbrace{\mu(x)}_{\text{reward function}}$$

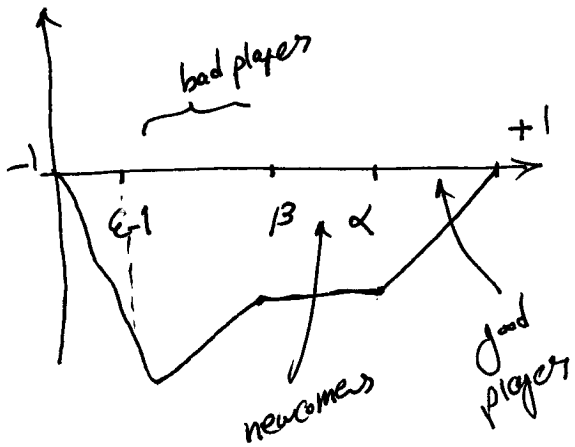


to penalize the players in the case of defection

$$T_i^p = T_i^{p-1} + \mu'(x)$$

(b) Function Example





systematic trust Modeling

1. Model Specification
2. Transformation to mathimatical model
3. Model evaluation
4. Modification & improvement.