CYBER SECURITY

7. forduló

Continental The Future in Motion

A kategória támogatója: Continental Automotive Hungary Kft.

Ismertető a feladathoz

A blokklánc (angolul blockchain) egy olyan decentralizált adatbázis, ahol különböző, akár ellenérdekelt felek tudnak hitelesen, megbízhatóan tranzakciókat végrehajtani hamisítást kizáró módon. Működés során egy egyre bővülő, megváltoztathatatlan log készül minden egyes tranzakció után, amik egy-egy adatblokkot alkotnak. A blokkláncok alkalmazása többek között a kriptovaluták terén létfontosságú.

Mivel nincs központi ellenőrző rendszer, kiemelt szerepet kap a rendszerben a hitelesítés.

Felhasznált idő: 00:00/40:00 **Elért pontszám:** 0/10

Indítás utáni csatolmányok

1. feladat 0/10 pont

Blokkláncok terén egy speciális kiszűrendő hiba az úgynevezett bizánci hiba.

A bizánci hiba egy olyan típusú meghibásodás, ahol a hálózat egy eleme különböző információt továbbít a többiek felé. Az elnevezés a bizánci tábornokok problémájáról keletkezett:

Tegyük fel, hogy „n” darab bizánci sereg körbekerít egy ellenséges erődítményt. A tábornokok tanácskoznak maguk között, hogy rohamozzanak-e aznap este, vagy másnapra halasszák a rohamot. Sajnos árulók vannak a berkeikben, akiknek céljuk a többiek összezavarása. A tábornokok személyesen nem találkozhatnak, csak futárok által üzenhetnek egymásnak. Korábbi megbeszélés alapján a többség döntése alapján fognak cselekedni, hiszen akár támadnak, akár (ideiglenesen) visszavonulnak, az a céljuk, hogy egységesek maradjanak, ha a hűséges seregek egyik fele támad, és a maradék visszavonul, akkor a csata elveszik.

Ha példaképpen 11 tábornok közül 1 áruló van, és a hűséges tábornokok egyenlően 5-5 arányban akarnak támadni és visszavonulni, akkor az áruló össze tudja őket zavarni, hogy felüknek támadásról, felüknek visszavonulásról szóló akaratról ír. Ekkor pont elkerülendő eset áll fent, hiszen a hű tábornokok közül öten támadni fognak, hiszen a hozzájuk elérkezett szavazatok 6-5 arányban efelé dőltek, a maradék meg pont fordított okból visszavonulnak.

Ha viszont a tábornokok azt is körbekérdezik egymástól, hogy a társaiktól mit hallottak, ki tudják következtetni, hogy ki az, aki következetlenül szavazott a döntéséről, és ezáltal áruló.

Ezt az eljárást akár többször is el tudják ismételni, hogy több árulót is kiszűrjenek; első fordulóban mindenkitől csak a saját szavazatát kérik el, minden további fordulóban pedig az összes előző fordulóban kapott információt.

11 bizánci tábornok esetén mennyi az a maximális árulószám, ami esetén a hű parancsnokok még azonos cselekvés mellett tudnak dönteni?

Válasz

A helyes válasz:

3

Magyarázat

Először is tekintsük meg a 3 tábornok, 1 áruló esetét, legyen a három tábornokunk ekkor A, B és C.

Tegyük fel A-hoz a következő üzenetek jutnak el:

- B: „Azt mondom támadjunk”
- C: „Azt mondja B, hogy ne támadjunk”

Bár A számára nyilvánvaló, hogy két társa közül van áruló, sem azt nem tudja eldönteni, ki az, sem azt, hogy a másik hogyan akar dönteni.

Ezt általánosítva megmutatható, hogy minden új áruló 2 hűséges tábornok összezavarására képes, avagy megfordítva: a hűséges tábornokoknak akkor van esélyük, ha kevesebb, mint egy-harmaduk áruló, ez 11 tábornok esetén legfeljebb 3.

2. feladat 0/0 pont

Korábbi példát követve tegyük fel, hogy a 11 tábornokunk értesül arról, hogy pontosan 2 áruló van maguk között. Ebből az információból kiindulva, elkérik egymástól levélben nem csak azt, hogy mi a döntésük, de azt is, hogy a többi tábornoktól ki mit hallott.

Továbbá új feltevésként vegyük úgy, hogy az ostromlott város tökéletes kémekkel rendelkezik, akik a különböző táborokba belopakodnak, és fültanúi lesznek minden támadási / visszavonulási szándéknak, illetve a tábornokok egymásnak küldött üzeneteinek a tartalmának. A megszerzett információt továbbítják a városba, ahol az alábbi formában összesítik az adatokat a kémfőnök számára, amiket a csatolt 'Bizanci_tabornokok.txt' fájl tartalmaz:

- D[i][i][i] = i. -ik tábornok saját döntése, amit ha hűséges, akkor csak ezt továbbít (i=0...10)
- D[i][i][j] = i.-ik tábornok milyen üzenetet kapott, j.-ik tábornok szándékáról (i!=j, i, j=0...10)
- D[i][j][k] =i.-ik tábornok j-iktől mit hallott k-ik döntéséről (i,j,k=0...10, páronként különbözőek)

Hogyan fognak dönteni a (nem áruló) tábornokok, ha feltételezzük, hogy tökéletesen dolgozzák fel a rendelkezésükre álló információkat?

Válasz

- (●) Minden hű tábornok támadni fog
  Ez a válasz helyes, de nem jelölted meg.
- ( ) Minden hű tábornok vissza fog vonulni
- ( ) Nem fognak egységesen dönteni a hű tábornokok

Magyarázat

Kedves Versenyzők!

A feladatot 0 pontosra állítottuk:

- ***a 0/1 értelmezése nem lett definálva, bár többnyire kitalálható volt, de semmiképp nem szerencsés az egyértelműsítés hiánya***
- ***a megadott adattömbben szereplő adatokban is hiba van, amely nem teszi egyértelművé a feladat megoldását***

Elnézést kérünk a kellemetlenségért, és köszünjük szépen megértéseteket!

Nincs elsőre triviális megoldása a feladatnak, annak ellenére, hogy kevesebb, mint tábornokok harmada áruló, tudniillik ebben az esetben csak akkor van garantált megoldás, ha árulók száma +1 (azaz jelen esetben 3) környi információcsere zajlik, itt pedig csak két kör volt.

A hű tábornokok nem tudnak mást csinálni, mint „lefuttatni" az egy áruló esetére készült algoritmust, és reménykedni, hogy az árulók nem hatékonyan hazudtak.

j-ik tábornok számára D[i][j][k] adatok (i,k =0..10) állnak rendelkezésre. 0 áruló esetén simán lehetne venni D[j][j][k] (k=0..10) móduszát (azaz ha többségében vannak támadásra szavazatok, akkor azt, fordított esetben visszavonulás)

Ehelyett, hogy direktben a bemondott szavazatokat értékelnék (pl. k.-ik tábornok nekik mit mondott), összevetik azzal, amit a többi tábornoktól kaptak k szándékát illetően. Ha a többség másként hallott k felől, akkor az saját magának felvésett k-hoz tartozó értéket felülírják.

Szemléletesen ez oszloponkénti kiértékelést takar, az oszlop leggyakrabbik eleme kerül a további kiértékelésre váró tömbbe.

Miután minden oszlopon végigmentünk, a minden tábornok végigmegy a frissített tömbén a 0 árulónál bemutatott módon, és ha a többség esetleg mást akar, akkor a saját korábbi döntését is ez alapján bírálja felül.

Jelen esetben minden tábornok számára az 1-es azaz támadási parancs lenne többségbe, így a hű tábornokok mind ezt fogják követni.

Implementált példa algoritmus így nézhet ki pythonban:

```
n = len(D[0][0])

def ColumnMajority (j, k):
    s = 0
    for i in range(n):
        s += D[i][j][k]
    if s > n/2:
        D[j][j][k] = 1
    else:
        D[j][j][k] = 0

def RowMajority(i, j):
    s = sum(D[i][j])
    if s > n/2:
        D[i][j][i] = 1
    else:
        D[i][j][i] = 0


for i in range (n):
    for k in range(n):
        ColumnMajority(i, k)
    RowMajority(i, i)

for i in range(n):
    print (i, " ", D[i][i][i])
```