A biztonságos elektronikus kereskedelem alapjai
(BMEVIHIM219)

Házi feladat

Elektronikus aukció

Készítette: Knapp Ádám, DG2228

2010. 11. 21.

I. Tartalomjegyzék

1. Bevezetés

Az elektronikus aukció napjainkban már teljesen elterjedt, hétköznapi fogalom. Bárki, aki rendelkezik internet hozzáféréssel könnyedén részt vehet az ilyen árveréseken. Számos weboldal kínálja az ingyenes aukció-szervező szolgáltatását, így az átlagos felhasználó számára is egyszerűen érhető el a kereskedelem e formája.

Ebben a riportban törekedtem arra, hogy egy átfogó képet adjak az elektronikus aukció témaköréről. Ennek megfelelően az második fejezet az elektronikus akció fogalmát és a hozzá kapcsolódó szereplőket mutatja be. Ezután a teljesség kedvéért összefoglalom az aukciók típusait. Végül néhány szót ejtek a világ legnagyobb árverésekkel foglalkozó weboldaláról az eBay-ről.

A további fejezetekben két különböző, az elektronikus aukció témaköréből származó, számomra érdekesnek talált cikkekről írok. Próbáltam úgy összeválogatni őket, hogy érintsék a különféle, aktuális kutatási területeket. Ismertetésük során azonban nem részletezem a pontos eljárásokat és eredményeket. A célom nem az volt, hogy a cikkek minden részletét leírjam, hanem hogy kiemeljem a felvetett problémákat, a megoldásukhoz szükséges ötleteket és a konklúziókat.

A harmadik fejezet az elektronikus aukciós csalók felderítésének módszeréről szól. (Az eljárás leginkább az eBay környezetében érvényes.) Az ötlet arra épül, hogy a csalók legális felhasználóknak szeretnének látszani. Ahhoz, hogy ez valóban sikerüljön nekik, a hitelességüket mérő pontszámot megfelelő szintre kell emelniük. Ezek a hírnévépítő eljárások az aukciós tranzakcióikban jól azonosíthatók. A szerzők e minták felismeréséhez javasolnak egy, a korábbiakhoz képest lényegesen hatékonyabb eljárást.

A negyedik fejezet egy konkrét protokollt mutat be, aminek a célja, a licitálók teljes anonimitásának biztosítása. Erre azért van szükség, mert előfordulhat az, hogy a licit kimenetelét illegális módon szeretnék befolyásolni bizonyos emberek. Ezért a protokollnak nem csak a megszemélyesítéses támadás ellen kell védeni, hanem a legális felhasználók kilétét is el kell rejtenie. A szerzők által javasolt protokoll kielégíti ezeket a követelményeket, és egy korábbi hasonló céllal született eljáráshoz (C-C protokoll) képest kisebb a számítási és üzenetküldési igénye.

2. Az elektronikus aukció

Az elektronikus aukció egy zárt elektronikus piactéren keresztül szervezett valós idejű versenyeztetés. A pályázók az elektronikus aukció koncentrált időtartamában versenyeznek egymással Internet kapcsolaton keresztül saját környezetből. A pályázók az aukciós rendszer beállításának függvényében

látják a legjobb ajánlatot, ugyanakkor nem látják a pályázók számát és nevét. Az aukció időtartamában a pályázóknak többszöri ajánlattételre van lehetőségük, így a klasszikus aukcióban ismert szabályok szerint folyamatos licitálás mellet kialakulhatnak éles versenyek.

Az elektronikus akciók előnyei, hogy akár több tíz pályázó párhuzamosan versenyeztethető, a versenytárgyalás valós időben történik, koncentrált időtartamban, költség hatékony és verseny semleges, emellett hiteles, tisztességes versenykörülményeket és esélyegyenlőséget biztosít, beszerző előítéletektől mentes, valamint felmerülnek pszichológiai előnyök is.

Az elektronikus aukciókban háromféle szereplőt különíthetünk el. Az első szereplő az ún. szervező vagy eladó, aki az aukciós kiírást elkészíti. Ebben pontosan meghatározza az aukció tárgyát, a hozzá kapcsolódó fizetési, szállítási es egyéb feltételeket, ezáltal kézben tartja az egész aukciót. Az eladó fogadja a vevőktől beérkező árajánlatokat.

A második szereplő az ún. résztvevő vagy vevő, aki az adott aukcióra meghívást nyert, és ott a szervező által definiált feltételeket elfogadta. A vevő licitál az aukció tárgyát képező termékre vagy szolgáltatásra.

Az utolsó szereplő az ún. szolgáltató, aki a semleges harmadik felet játszza. Feladata az aukciókban részt vevő nagyszámú eladó és vevő számára rögzíteni a legalapvetőbb szabályokat és lebonyolítani magát a cserét. Másféle megközelítésben a szolgáltató az aukciós rendszer üzemeltetője. Biztosítja, hogy ez a rendszer - a felekkel megkötött szerződésekben rögzített feltételekkel - elérhető legyen a szervezők és a résztvevők számára.

2.1. Az aukció típusai

Az aukcióknak két fő típusa van, a beszerzési, illetve az eladási aukció. Az beszerzési, más néven fordított vagy hátra aukció esetén a szervező célja az aukció feltételeiben ismertetett termék, vagy szolgáltatás beszerzése. A résztvevők csökkenő árakkal licitálnak. A beszerzési aukció kiírásakor a vevő egy maximális árat (nyitó ár) határoz meg és a szállítók egyre alacsonyabb árat kínálva versenyeznek a termék vagy szolgáltatás szállításának lehetőségéért. Az aukciót szervező vállalatnak lehetősége nyílik az áron kívül a szállítási és a fizetési határidő versenyeztetésére is.

A beszerzési aukció legnagyobb előnye a beszerzési munkafolyamatok lényeges lerövidülése mellett, hogy a termékek, szolgáltatások a piacon elérhető legkedvezőbb áron szerezhetők be, illetve új beszerzési kapcsolatok alakíthatóak ki.

A beszerzési aukció fontosabb típusai: az összevont vagy bundle aukció, a kimazsolázó vagy cherry picking aukció, a paraméteres aukció és a felsorakoztatott vagy ranking aukció. Ezek részleteire nem térek ki, mivel ezeket leginkább a vállalatok használják.

Az eladási vagy előre aukció esetén a szervező célja az aukció feltételeiben ismertetett termék, vagy szolgáltatás értékesítése. A résztvevők növekvő árakkal licitálnak. Az eladási aukció kiírásakor a szervező egy minimális árat határoz meg és a résztvevők egyre magasabb árat kínálva versenyeznek a termék megvételéért. Az eladási aukció legnagyobb előnye, hogy a termékek a lehető legmagasabb

áron, gyorsan, hatékonyan értékesíthetőek, azonban az eladási aukció nem alkalmas a klasszikus értelemben vett értékesítésre.
Az eladónak nincsen pontos információja arról, hogy a leendő vevők közül ki mennyit hajlandó fizetni a felkínált tárgyért. Ezt a maximális összeget a közgazdaságtanban az egyén rezervációs árának nevezik. Az eladó gyakran nem tudja azt sem, hogy ki jöhet szóba vevőként.
A következőkben az eladási aukció típusait mutatom be részletesen.

2.1.1. Angol típusú aukció

Az angol típusú vagy más néven legmagasabb ár (highest-price sale) aukción vételárként a legmagasabb kínálati árat fogadják el, a licitálás nyílt, azaz minden licitáló szabadon tehet ajánlatot, akár többször is és mindenki hallja az összes licitet. A licitálás akkor ér véget, ha már egyik licitáló sem emeli az árat. A köznapi értelemben ezt a típust szokás árverésnek nevezni, a legismertebb és legelterjedtebb aukciós forma. A terméket a legtöbbet kínáló veheti meg, és éppen az általa bemondott összeget kell kifizetnie vételárként. Az angol típusú árverésnek különböző változatai vannak: az aukció levezetője mindig egy meghatározott összeggel emeli a licitet; az aukció levezetője bármikor saját belátása szerint emelheti a licitet; a játékosok kedvük szerint emelik a licitet; szabad kilépéses licit. Az utóbbinak az a lényege, hogy az ár folyamatosan nő, és a játékosok kötelesek nyilvánosan bejelenteni, ha kiszállnak a licitálásból, vagyis ha az aktuális árat már nem hajlandók megadni (ezután a licitálás folytatására nincsen lehetőségük).

2.1.2. Versenytárgyalás

A versenytárgyalás aukció a vételárnak a legmagasabb kínálati árat tekinti. Ezt a fajta aukciót alkalmazzák műkincsek, ingatlanok eladásakor, valamint az Egyesült Államok kormánya is ily módon ítéli oda az ásványkincsek feletti rendelkezési jogot.
Minden résztvevő egyetlen árajánlatot tesz, a többiek licitjét nem ismerve. Az vásárolhatja meg a terméket, aki a legmagasabb licitet teszi, és kifizeti az ennek megfelelő összeget. Ebben a rendszerben a licitálók nem tudják, hogy hány ellenfelük van, s a többiek rezervációs áráról és licitjéről is csak feltételezéssel élhetnek. Ha úgy gondolják, hogy sok licitáló van, akkor az árajánlatok közel lesznek a rezervációs árakhoz.

2.1.3. Holland típusú vagy virágvásár aukció

A holland típusú vagy csökkenő áras (descending price) aukció ereszkedő, ami azt jelenti, hogy az eladó megállapít egy árat, majd ezt folyamatosan csökkenti, egészen addig, amíg egy vevő azt nem jelzi, hogy az aktuális árért hajlandó megvásárolni a terméket. A legtöbbet kínáló veheti meg az aukció tárgyát, és éppen az általa bemondott összeget kell kifizetnie vételárként. A holland aukció kimenetele azonos a versenytárgyalásával. Ha a legmagasabb rezervációs árral rendelkező résztvevő nem a rezervációs árnál állítja meg a licitvezetőt, akkor növeli annak az esélyét, hogy valaki előtte közbeszól,

és elviszi a terméket. Ám ha mégis nyer, akkor a vételi ár alacsonyabb lesz. Ez a fajta aukció igen közkedvelt: legtöbbször így adják el a vágott virágot Hollandiában (innen kapta ez a típus a nevét), a halat Izraelben vagy a dohányt Ontarióban. (Ez utóbbinak még az is a sajátossága, hogy a dohány eladójának jogában áll az árverést követően a vevők ajánlatait visszautasítani, ha a végső árat túl alacsonynak tartja.)

2.1.4. Vickrey-féle aukció

A Vickrey-féle aukció vagy másodlicites versenytárgyalás eladási árnak a második legmagasabb rezervációs árat tekinti. Minden licitáló egy árajánlatot tesz, miközben a többiekét nem ismeri. A terméket a legmagasabb licitet bemondó résztvevő veheti meg, de csak a második legmagasabb licitbemondásnak megfelelő összeget kell kifizetnie vételárként. Ha valaki a saját rezervációs áránál alacsonyabb árajánlatot tesz, növeli az esélyét annak, hogy nem ő nyeri meg az aukciót. Ezért érdemes emelnie a licitet, hiszen ezzel emelkedik a nyerési esélye, a vételár pedig úgysem függ a nyertes licitjétől.

Látszólag ez lehetne az szervezők számára az optimális megoldás, hiszen minden résztvevő a saját rezervációs árának megfelelő ajánlatot teszi. Azonban az eladó - az aukció szabályából adódóan - csak a második legmagasabb rezervációs áron tudja értékesíteni a tárgyat. Az angol aukción kialakuló vételár legalább ekkora, sőt sok esetben a licit minimális emelésének nagyságával meg is haladja az itt kapott értéket. Ezért a szervező - mivel általában ő határozhatja meg terméke értékesítésének körülményeit - előnyben fogja részesíteni az angol aukciót ezzel a típussal szemben.

2.1.5. Kereslet aggregálás

A kereslet aggregálás (demand aggregation) olyan árverés, amikor a vevők egy ad hoc csoportban gyűlnek össze bizonyos javak megvásárlására. Minél több vevő gyűlik össze, annál alacsonyabb lehet a darabonkénti ár.

2.2. Az eBay

Az angol aukcióra tipikus példa a világ egyik legnagyobb online aukcióval foglalkozó weboldala, az eBay. Az oldal biztonságát több tényező biztosítja. Az eBay titoktartási nyilatkozatában (privacy policy) egy leírás található a felhasználói adatok kezeléséről, amit az eTrust cég szabályrendszere alapján működtet az oldal. Ez a szabályrendszer magában foglalja a felhasználói adatok biztonságos megőrzésének és kezelésének módját. Ha az eTrust hitelesít egy weboldalt, akkor az oldal felhasználói biztosak lehetnek abban, hogy adataik nem kerülnek illetéktelen kezekbe. Ez azt jelenti, hogy biztosítva van a megfelelő fizikai védelem és titkosítás, valamint jelszavas rendszerrel is védik a szerverekhez való hozzáférést.

Az eBay az SSL protokollt használja a szerver és a kliens közötti titkosított kommunikációra. Ahhoz, hogy ez a megfelelő biztonságot nyújtsa, szükség van tanúsítványokra. Az eBay számára a VerySign

cég bocsát ki a tanúsítványokat, ami tartalmaz egy privát és publikus kulcspárt. Az SSL handshake során ezekkel a kulcsokkal hitelesíti egymást a szerver és a kliens.

3. Csalók detektálása elektronikus aukciókban

A fejezetet a [3] alapján készítettem el.

Az elektronikus aukció egyszerű megoldást nyújt termékek eladására és vásárlására. A világ legnagyobb aukciós weboldala az eBay, ami óriási mennyiségű felhasználóval rendelkezik. (2005-re 147,1 millióan regisztráltak.) A rendszer több millió dollár összértékű tranzakciókat bonyolít le naponta. Ennek következtében megjelentek a csalók is, ami az eBay legkomolyabb problémájának bizonyult. A rosszul viselkedő felhasználók átlagos 200 dollárt csaltak ki az áldozataiktól. Ezt úgy teszik meg, hogy egy nem létező terméket hirdetnek árverésre. A vétlen felhasználó normálisan licitál az adott tárgyra, majd miután megnyerte az aukciót, elküldi a vételárat, azonban a terméket nem kapja meg.

A probléma megoldására, azaz a csaló felhasználók felderítésére számos heurisztikus módszert találtak már ki és ajánlanak szerte a weben különböző fórumokon, de az első tudományos alapokon nyugvó módszer kidolgozása a szerzők nevéhez fűződik. Céljuk a csalók szisztematikus felderítése és detektálása és a módszer formalizmusba öntése.

A problémát a következőképp definiálták a cikk írói. A cél a potenciális csalók felderítése, mielőtt a csalást elkövetnék. Ehhez olyan információk szükségesek néhány, az elektronikus aukción résztvevő felhasználóról, mint a profiljuk és a tranzakciós előzményük. Ezek elérhetőek az eBay weboldaláról. Ezen kívül korábban már lebukott csalók adatait is felhasználják, amiket újságcikkekből, az eBay felhasználói fórumáról, valamint különböző vevők és eladók nagyszámú negatív visszajelzése alapján csalónak minősített felhasználókról megszereztek.

A szerzők megfigyelték, hogy a csaló felhasználók tipikus viselkedésmintát követnek az aukciós weboldalon eltöltött élettartamuk alatt. Arra a megállapításra jutottak, hogy mielőtt a csalás (csaló tranzakció) megtörténne, a csalók mindent megtesznek annak érdekében, hogy látszólag egy legitim felhasználó látszatát keltsék és ehhez megfelelő hírnevet szerezzenek maguknak. A hírnév egy nagyon fontos mérőszáma a hihetőségnek az elektronikus aukciós weboldalakon. Az eBay-en a felhasználó hírnevét egy ún. feedback score reprezentálja, ami a többi résztvevő által adott pozitív (+1) és negatív (-1) értékek összegzéséből képződik. Minél magasabb ez a szám, annál nagyobb a felhasználó hírneve és megbízhatósága, ebből következően növekszik a sikeres csalás esélye is.

Ezek alapján megállapítható, hogy a csaló felhasználók által végrehajtott, ún. „jó-hírnév építő procedúra” jelentősen eltér a valódi felhasználóktól. A szerzők úgy gondolják, hogy azonosítani tudják e hírnév építő eljárásokat a profilokból és a tranzakciós előzményekből származtatott tulajdonságok alapján.

A csaló célja, hogy minél nagyobb – egyszeri – haszonra tegyen szert, amilyen gyorsan csak lehet. Ennek érdekében tipikusan közepes vagy nagy értékű tárgyat kínál eladásra, majd a győztes licitáló által kifizette összeg átvételét követően, nem kézbesíti számára a terméket.

Az ismert és nyilvánosságra került csalásokat megvizsgálva arra a megállapításra jutottak a szerzők, hogy a következő alapvető lépéseket használva építik fel a támadók a hírnevüket:

1. Számos kis értékű üzletet kötnek (alacsony áron adnak és vesznek), hogy minél olcsóbban, minél több pozitív értékelést kapjanak a többi felhasználótól.
2. Eladnak és vesznek különböző nagy értékű termékeket (tipikusan elektronikai cikkeket) ún. kollaboránsoktól. A kollaboráns felhasználók nem mutatnak semmilyen csalókra emlékeztető tulajdonságot, látszólag legitim felhasználóként viselkednek. Ezzel a csalóknak az a céljuk, hogy „megszerezzenek" néhány igen erős pozitív értékelést anélkül, hogy ez valódi, jelentős költséget generálna számukra.
3. A fenti 2 lépést kombinálják, hogy látszólag egy legitim felhasználó illúzióját keltsék.
4. A hírnévépítési procedúrát nagyon rövid idő alatt hajtják végre, mivel minél tovább maradnak az aukciós oldalon, annál magasabb lesz a lebukás veszélye.

A fentebb említett adatokból (profil és tranzakciós előzmények) a következő tulajdonságokat, értékeket lehet egyszerűen meghatározni, amelyek segítenek a megfigyelt minták felismerésében és így a csalók és a legális felhasználók megkülönböztetésében:

1. Médián, összeg, átlag vagy standard eltérés az eladott/megvett termékek árai alapján, egy meghatározott időtartam alatt.
2. Eladott/megvett termékek száma egy meghatározott időtartam alatt.
3. Az eladott vagy megvett termékek aránya az összes tranzakciókhoz képest egy meghatározott időtartam alatt.

A szerzők az összes lehetséges tulajdonságok, értékek közül a következő 17-et választották ki, melyek szerintük a lehető legjobban jellemzik a megfigyelt mintákat:

- Az eladott termékek árának mediánja az első 15, első 30, utolsó 15, utolsó 30 napban.
- A megvett termékek árának mediánja az első 15, első 30, utolsó 15, utolsó 30 napban.
- Az eladott termékek árának standard eltérése az első 15, első 30, utolsó 15, utolsó 30 napban.
- A megvett termékek árának standard eltérése az első 15, első 30, utolsó 15, utolsó 30 napban.
- A megvett termékek számának aránya az összes tranzakcióhoz képest.

A cikk további részében bemutatják a szerzők, hogy hogyan is használják fel a korábbiakban részletezett ötleteiket. Először leírják, hogyan vonják ki és tárolják a felhasználók adatait. Ezután az adatokkal betanítanak egy döntési fákon alapuló rendszert, mely így képes felismerni a csalók hírnévépítő stratégiáját a megfigyelt minták alapján.

A következő fejezetben megvizsgálják a rendszer hatékonyságát. A kísérleteket 3 beállítással is elvégzik, melyek a kivont jellemzők számában különböznek. A kapott eredmények alapján kiszámították az eljárás pontosságát, valamint a tévesztés arányát a különböző beállítások mellett.

Amennyiben a fentebb leírt, mind a 17 jellemzőt használják a döntési eljárás során, akkor 11% a fals pozitív döntések aránya a 83%-os helyes pozitívokhoz képest. Az eredmények alapján megállapítható, hogy az ajánlott eljárásuk lényegesen jobb az egyéb heurisztikus megközelítésekhez hasonlítva.
A gyakorlati alkalmazáshoz elkészítettek a szerzők egy JAVA nyelven írt grafikus felületű alkalmazást, mely a bementként kapott felhasználókról megállapítja, hogy csalók vagy legális felhasználók.
Végül összefoglalják az elért eredményeket és a jövőbeli terveiket. Ezek között szerepel az eljárás pontosítása, ami más jellemzők bevonását jelenti a döntési procedúrába. Ezen kívül bővíteni is szeretnék a rendszerüket, hogy csaló és kollaboráns felhasználók hálózatát is felfedjék. Ehhez azt a megfigyelést használják fel, hogy a rosszul viselkedők csak néhány „hop"-ra helyezkednek el egymástól.

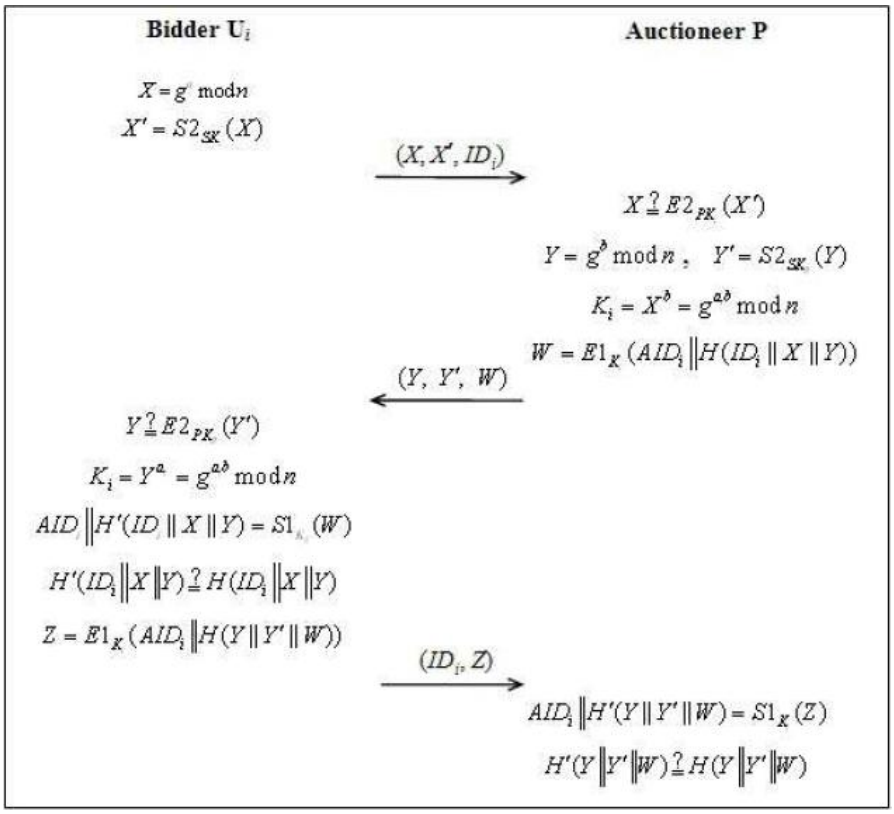
4. A GDH feltevésre épülő anonim aukciós protokoll

A fejezetet a [4] alapján készítettem el.
A cikkben bemutatott protokoll a 2006-ban megjelent C-C protokollra épül, ám annak hibáit próbálja kijavítani. A C-C protokoll célja az elektronikus akcióban részt vevő licitálók anonimitásának biztosítása volt. Ez ahhoz szükséges, hogy rosszakaratú emberek ne befolyásolhassák az árverés kimenetelét azáltal, hogy megfenyegetik a tisztességes felhasználókat. A licitálók kilétének titokban tartása mellett azonban fontos az is, hogy egy támadó ne személyesíthesse meg őket. A szerzők által javasolt protokoll biztonsága a Gap Diffie-Hellman feltevéssel egyenlő.
A cikkben a növekvő áras (angol) és a csökkenő áras (holland), valamint a zárt licites (egykörös) aukciótípusokra készítették el az eljárásokat. 2003-ban Chang és Chang javasoltak egy egyszerű anonim aukciós protokollt. Ebben a licitáló kilétét egy kapcsolatkulcs létrehozásával védték, azonban a kulcsmegegyezés és az azonosítás nem volt igazán hatékony. Ezt kiküszöbölendő, 2006-ban egy továbbfejlesztett protokollt publikáltak, ami C-C protokoll néven terjedt el. Itt az azonosítást és a kulcsmegegyezést egy fázisba vonták össze. Azonban a licitáló kilétét nem védte semmi a kezdeti fázisban. Így az előbb említett probléma továbbra is fennállt. A szerzők ezért egy olyan eljárást dolgozta ki, mely már a kommunikáció kezdetétől anonimitást biztosít.
A C-C protokollban létezik egy tanúsítvány kibocsátó (CA), egy aukciós szervező (P) és *m* db licitáló (U_i, $1 \leq i \leq m$). A publikus rendszerben a Diffie-Hellman protokoll szerint 2 paraméter van: *n* nagy prímszám és *g eleme* Z^*_n. P titkos-publikus kulcspárja (SK_P, PK_P), míg U_i-é (SK_i, PK_i). U_i egyedi azonosítója ID_i. $E2_{PK}(m)$ az aszimterikus kódolás algoritmusa, $D2_{SK}(m)$ az aszimmetrikus dekódolás algoritmusa (pl. RSA), $E1_K(m)$ a szimmetrikus kódolás, $D1_K(m)$ a szimmetrikus dekódolás algoritmusa *K* kapcsolatkulccsal (pl. AES), $H(.)$ egy ütközés-ellenálló hash függvény, *T* az időbélyeg, *m* a nyílt üzenet, *m eleme* Z_n.
A kezdeti fázisban P azonosítja U_i-t, majd létrehozzák a kapcsolatkulcsot és egy ideiglenes azonosítót

U_i számára:

1. U_i választ egy véletlen számot a_i-t, majd kiszámítja $X = g^a \ mod \ n$, $X' = S2_{sk}(X)$, értékeket és elküldi X-et, X'-et, ID_i-t P-nek.
2. P ellenőrzi, hogy $X =? \ E2PK(X')$. Ha nem egyenlő, P befejezi a protokollt. Ellenkező esetben P választ egy véletlen számot, b-t és kiszámítja $Y = g^b \ mod \ n$, $Y' = S2_{SKp}(Y)$, $K_i = X^b = g^{aib} \ mod \ n$, $W = E1_{Ki}(AID_i \mid H(ID_i \mid X \mid Y))$, ahol AID_i U_i ideiglenes azonosítója. Végül Y-t, Y'-t és W-t elküldi U_i-nek.
3. U_i ellenőrzi, hogy $Y =? \ E2_{PKp}(Y')$. Ha nem egyenlő, U_i befejezi a protokollt. Ellenkező esetben kiszámítja $K_i = Y^{ai} = g^{aib} \ mod \ n$ értékét, dekódolja W-t és ellenőrzi, hogy $H(ID_i \mid X \mid Y) =? \ H'(ID_i \mid X \mid Y)$. Ha nem egyenlő, U_i befejezi a protokollt. Ellenkező esetben kiszámítja $Z = E1_{Ki}(AID_i \mid H(Y \mid Y' \mid W))$ értékét és (ID_i, Z)-t elküldi P-nek.
4. P dekódolja Z-t és ellenőrzi a hash értékeket. Ha nem egyenlő, P befejezi a protokollt. Ezen a ponton U_i-nak és P-nek ugyanaz a kapcsolatkulcsa van, valamint U_i kapott egy ideiglenes azonosítót.

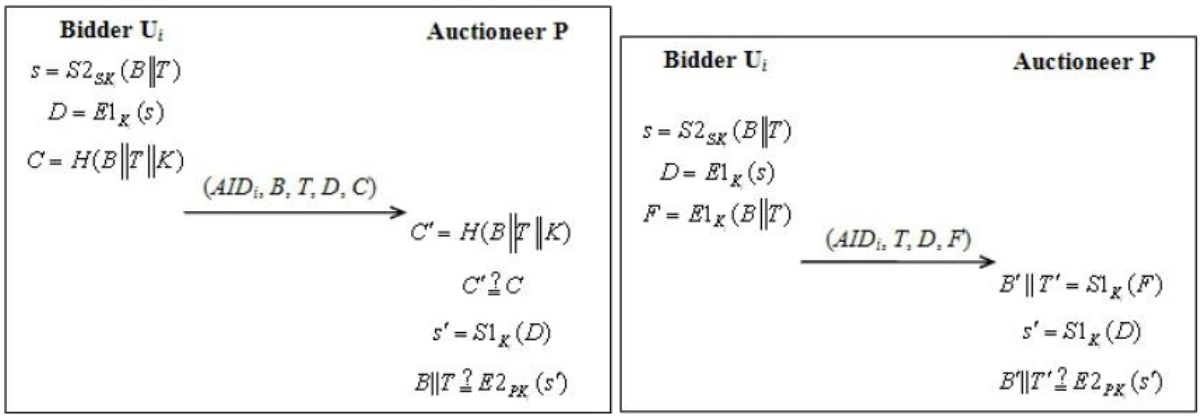
A protokoll első fázisának működése az 1. ábrán látható.



1. árba: A C-C protokoll kezdeti fázisa [4]

Rögtön feltűnhet a korábban említett probléma: U_i nyíltan elküldi az azonosítóját P-nek az első üzenetben, így nem fedi el U_i kilétét.

A 2. ábra a protokoll futását mutatja angol típusú és zárt-licites aukciókban.



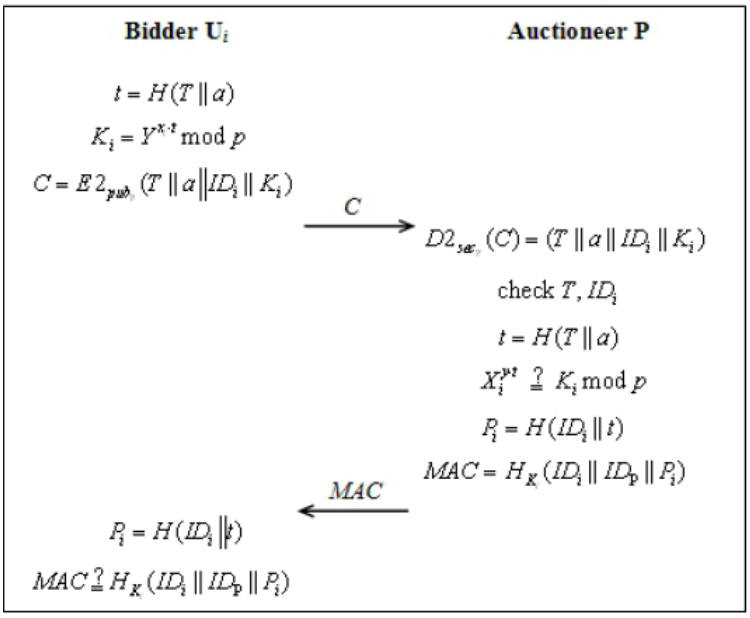
2. ábra: A C-C protokoll licitálási fázisa angol típusú (bal oldal) és zárt-licites (jobb oldal) aukciókban [4]

A szerzők által javasolt protokollban nem küldik el nyíltan a licitáló azonosítóját. Ezen kívül, a korábbiakkal ellentétben a licitáló generálja a kapcsolatkulcsot és az ideiglenes azonosítót, de a rendszerparamétereken is változtattak. Legyen p és q két nagy prímszám, $Z_p = \{0, 1, ..., p-1\}$ additív és multiplikatív csoport modulo p, Z_q egy additív csoport modulo q, g *eleme* Z^*_q egy g által generált ciklikus csoport, $H(.)$ a Z_q-nak megfelelő kimenetű, ütközés-ellenálló hash függvény, és $H_K(.)$ hasonló tulajdonságú, de K kulccsal kulcsolt hash függvény. Minden U_i választ egy X_i *eleme* Z_q titkos kulcsot és az ehhez tartozó publikus kulcs $X_i = g^x \bmod p$ lesz. P is választ egy y *eleme* Z_q titkos kulcsot és a hozzá tartozó publikus kulcsot $Y = g^y \bmod p$. Ezen kívül a P-nek még van további publikus-titkos kulcspárja pub_P és sec_P. A publikus X_i és Y kulcsokat a CA hitelesítette.

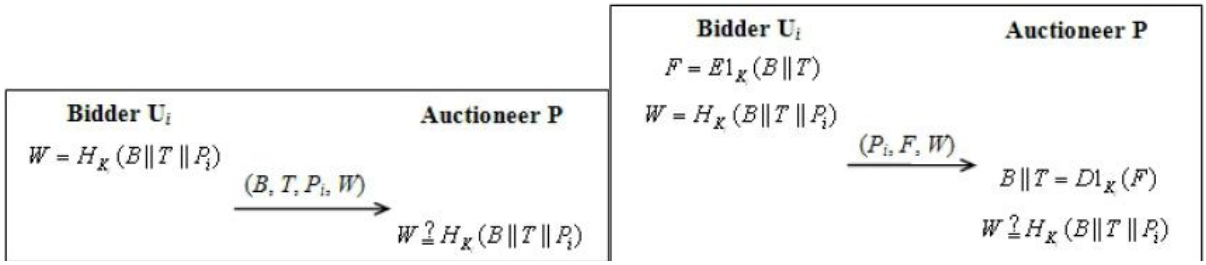
A kezdeti fázis működése:

1. U_i választ egy véletlen számot a *eleme* Z_q-t és létrehozza a T időbélyeget. Ezután kiszámítja $t = H(T \mid a)$, $K_i = Y^{xit} \bmod p$ és $C = E2_{pubP}(T \mid a \mid ID_i \mid K_i)$ értékeket. Végül elküldi C-t P-nek.
2. P dekódolja C-t és ellenőrzi, hogy az ID_i és T legális felhasználó és időbélyeg. Ha igen, akkor kiszámítja $t = H(T \mid a)$ értékét és ellenőrzi $X^{yt}_i = K_i \bmod p$ értéket is. Ha nem egyeznek, akkor P befejezi a protokollt. Ellenkező esetben kiszámítja $P_i = H(ID_i \mid t)$ és $MAC = H_{Ki}(ID_i \mid ID_P \mid P_i)$ értékeket, ahol P_i az U_i ideiglenes azonosítója. Végül elküldi a MAC-et U_i-nek és elmenti a (ID_i, P_i, K_i) hármast.
3. U_i kiszámítja $P_i = H(ID_i \mid t)$ értéket és ellenőrzi a MAC-et. Ha nem egyenlők, akkor U_i befejezi a protokollt. Ellenkező esetben megbizonyosodik (K_i, ID_i, P_i) helyességéről. Ezen a ponton U_i-nak és P-nek van egy közös K_i kapcsolatkulcsa, valamint U_i-nak egy ideiglenes azonosítója.

A protokoll kezdeti fázisának működését a 3. ábrán követhetjük nyomon, míg a 4. ábra az angol típusú és zárt-licites aukciókban való futását szemlélteti.



3. ábra: A protokoll kezdeti fázisa [4]



4. ábra: A protokoll licitálási fázisa angol típusú (bal oldal) és zárt-licites (jobb oldal) aukciókban [4]

A szerzők összehasonlítják a protokolljukat a C-C protokollal, melynek eredményeként megállapítják, hogy mind a kommunikációs költség, mind a számítási igény jelentősen csökkent a C-C protokollhoz képest.

Végül elemzik a protokolljukat biztonsági szempontból is. Bebizonyítják, hogy a protokoll biztonsága egyenlő GDH problémával.

Legyen *G* egy multiplikatív csoport, *q* egy nagy prímszám, a csoport rendje és *g eleme G* a generátorelem. A CDH (Computational Diffie-Hellman) probléma a következő: válasszunk két nagy számot *G*-ből: *X*-et és *Y*-t. Ekkor algoritmikusan nehéz kiszámítani $Z = g^{xy}$ *eleme G*-t, ahol $x = log_g X$ és $y = log_g Y$. Ez a CDH feltételezés.

A DDH (Decision Diffie-Hellman) probléma ehhez hasonló. Ebben az esetben 3 számot választunk ki G-ből: *X*-et, *Y*-t és *Z*-t. A feladatunk annak az eldöntése, hogy $z =? xy \bmod q$, ahol $x = log_g X$, $y = log_g Y$ és $z = log_g Z$. A DDH feltételezés szerint ezt a problémát nehéz megoldani.

Abban az esetben, ha $z = xy \bmod q$, akkor az *(X, Y, Z)* hármast érvényes Diffie-Hellman hármasnak nevezzük.

A GDH probléma a korábbiakkal összefüggésben áll. Adott egy DDH problémamegoldó orákulum, ami egy determinisztikus algoritmus és kimenetele, hogy a kapott *(X, Y, Z)* hármas érvényes DH hármas-e. Ekkor egy *(X, Y)* párhoz szeretnénk kiszámítani a *Z*-t. Miközben ezt a CDH problémát

oldjuk meg, kérésekkel fordulhatunk az orákulumhoz. Ezt is egy nehéz feladatnak gondolunk, amit GDH feltételezésnek nevezünk.
A protokollban a GDH feltételezés szerint egy támadó csak elhanyagolható valószínűséggel tud meg információt a licitáló kilétéről, ezért a protokoll biztonsága egyenlő a GDH feltétezéssel. Ezen kívül a CDH feltételezés miatt egy támadó egy licitálót elhanyagolható valószínűséggel képes csak megszemélyesíteni.

Összefoglalás

Összegzésként elmondható, hogy az elektronikus aukció bár gyakorlatban nagyon elterjedt és jól működik, számos megoldásra váró feladat elé néz. Az elektronikus árverés terjedésével egyre kritikusabbak lesznek a nem legális felhasználókkal kapcsolatos problémák, akik a legkülönfélébb módokon próbálnak haszonhoz jutni a becsületes emberek kárára, hiszen ahol pénz van (márpedig itt nagyon sok pénz van), ott mindig előfordulnak csalók. Ahhoz, hogy a kutatók jó, gyakorlatban alkalmazható megoldásokat találjanak, széleskörű ismeretekre van szükségük.
A bevezetés után a második fejezetben áttekintettem mit érdemes tudni az elektronikus aukcióról általában. Ezután kiemeltem a világ legnagyobb aukciós weboldalának biztonsági eljárásait.
A harmadik fejezetben megismerkedhettünk az eBay-en elszaporodó csalók felderítésének módszeréről. A feldolgozott cikk legfontosabb észrevétele, hogy a csalók jól azonosítható hírnévépítési eljárásokat követnek, melyek a tranzakciós naplóból kiolvashatók. E minták alapján nagy valószínűséggel felismerhetők az illegális felhasználók.
A negyedik fejezetben egy elektronikus aukciós protokollt mutattam be, aminek legfontosabb feladata a licitálók anonimitásának biztosítása és a megszemélyesítéses támadás ellen való védekezés. A protokoll kulcsmegegyezési eljárása a GDH probléma nehézségére épül, ezért a kapcsolatkulcs és a licitálókkal kapcsolat információk megszerzésének valószínűsége elhanyagolhatóan kicsit.

II. Irodalomjegyzék

[1] Fehér Éva, dr. Szohár Ferenc, dr. Csiszér Gábor: Az elektronikus kereskedelem az Európai Unióban és Magyarországon,
Magyar Kereskedelmi és Iparkamara, 2009. június, ISBN: 987- 963-9008-95-3.

[2] Kocsis Éva – Szabó Katalin: Dinamikus árazás az elektronikus piactereken,
Közgazdasági Szemle, XLIX. évf. 858-874. oldal, 2002. október.

[3] Duen Horng Chau, Christos Faloutsos: Fraud Detection in Electronic Auction,
European Web Mining Forum at ECML/PKDD, 2005.
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.62.46&rep=rep1&type=pdf#page=93

[4] Fuw-Yi Yang, Cai-Ming Liao: An Anonymous Auction Protocol Based on GDH Assumption,
International Journal of Network Security, Vol.12, No.3, PP.171-177, May 2011.
http://ijns.femto.com.tw/contents/ijns-v12-n3/ijns-2011-v12-n3-p171-177.pdf