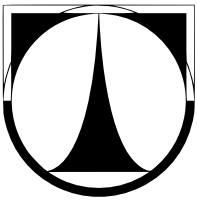
TECHNICKÁ UNIVERZITA V LIBERCI

Fakulta mechatroniky a mezioborových inženýrských studií



SAMOSTATNĚ PRACUJÍCÍ BEZPEČNOSTNÍ MODEL PRO DYNAMICKÁ DISTRIBUOVANÁ PROSTŘEDÍ

2008 ROMAN ŠPÁNEK

Samostatně pracující bezpečnostní model pro dynamická distribuovaná prostředí

Autoreferát dizertační práce

Ing. Roman Špánek

Studijní program: 2612V Elektrotechnika a informatika
Studijní obor: 2612V045 Technická kybernetika
Pracoviště: Ústav mechatroniky a teoretické informatiky
Fakulta mechatroniky a mezioborových inženýrských studií
Technická univerzita v Liberci

Studentská 2, Liberec, 461 17

Školitel: Ing. Július Štuller, CSc.

Dizertační práce je k nahlédnutí na děkanátu FM, TU v Liberci
Studentská 2, budova A, tel.: +420 485 353 110

Autoreferát dizertační práce
Samostatně pracující bezpečnostní model
pro dynamická distribuovaná prostředí

Obsah

1 Úvod

Moderní telekomunikační prostředky bezpochyby ovlivnily a stále ovlivňují velkou část lidské populace. Nové metody a technologie pro komunikaci mezi lidmi zkrátily vzdálenosti mezi přáteli či obchodními partnery, výměna informací je snažší než kdy byla. Úspěch těchto technologií lze nalézt v odvěké potřebě lidí komunikovat. Bez komunikace by lidstvo jen velmi obtížně, pokud vůbec dosáhlo současného pokroku.

Prvopočátky technologického pokroku v telekomunikačních technologiích lze spojit s prvními mikropočítači. Od mikropočítačů to byl již jen krůček k prvním počítačovým sítím. Z kraje to byly jen velmi jednoduché a technologicky omezené počítačové sítě, nicméně byly to právě ony, které položily základ pro pozdější celosvětovou síť dnešních dnů – internet.

S internetem přišla doba, kdy vzdálenosti mezi lidmi byly redukovány na vzdálenosti mezi nejbližšími k internetu připojenými počítači. Nicméně i tato vzdálenost se ukázala býti příliš velká. Nová technologie, která by umožnila téměř kdykoli a kdekoli komunikaci mezi lidmi, na sebe nenechala dlouho čekat. Mobilní telefony přinesly lidem požadovanou míru svobody v komunikaci.
Mobilní telekomunikace přinesla celou řadu výhod a také několik problémů. Mezi jeden z velmi palčivých patří zajištění bezpečnosti v prostředí, kde je část přenosu realizována pomocí bezdrátových technologií a počet uživatelů je obrovský.

Myslíme, že by se zabezpečovací mechanismy neměly věnovat pouze kryptografii, tedy způsobu zabezpečení přenosu a uložení dat, ale také řešení otázky, zda-li je možné informace zpřístupnit a také komu. Tuto myšlenku podpořila rešerše, která byla vypracována během prvního roku doktorského studia. Z rešerše jasně vyplynulo, že hlavně v distribuovaných systémech, kde není žádná centralizovaná správa zajišťující mimo jiné i zabezpečení komunikace, se dá otázka zabezpečení hrubě rozdělit na:

- **zabezpečení přenosu dat** - silná kryptografie zabezpečuje vlastní přenos mezi uživateli, tak aby nedošlo k získání dat třetí osobou, aby data byla doručena kompletní, nepodvržená a atd.
- **systémy pro správu a budování důvěry** - důvěra se používá k zodpovězení otázky, zda-li mohou být požadovaná data zpřístupněna žadateli.

Řešit správu a budování důvěry v systémech, kde není žádná nebo jen velmi omezená centralizovaná správa, kde se počet uživatelů může

velmi dramaticky měnit a kde jednotlivé dvojice komunikujících uživatelů nemusí mít žádné a priori informace využitelné pro vytvoření důvěry, může být velmi zajímavým a komplikovaným problémem. Nejen tato komplikovanost, ale i zřetelná orientace na reálné problémy každodenního života, byly a stále jsou hlavní motivací a výzvou určující směr mé vědecké práce, která je zaveršena předkládanou disertační prací.

2 Současný stav problematiky

Pojem důvěry je používán v různých oblastech lidského bádání a proto se v této kapitole zaměřím na vymezení problému budování důvěry mezi uživateli v decentralizovaných systémech.

Jednou z oblastí, kde je důvěra využívána pro účely zlepšení bezpečnosti jsou **mobilní databáze**. Mobilní databáze se jako vědecký obor objevily v souvislosti s příchodem mobilní telekomunikace a také internetu. Autoři v [1] představují nový směr vývoje takzvaného "okraje internetu" (the edge of the internet). Zatímco současným převládajícím terminálem připojeným k internetu jsou domácí počítače, v následujících letech se počítá s nárůstem množství mobilních zařízení, které budou mít dostatečné výpočetní a komunikační kapacity, aby postupně nahrazovaly osobní počítače. Dalším fenoménem, který se v této souvislosti objevil, jsou tzv. *agentové systémy*, kde autonomní programy budou schopné vykonávat netriviální operace pro uživatele.
Obecně lze mobilní databáze specifikovat jako architekturu, kde mají uživatelé možnost kdekoli a kdykoliv přistupovat k datům pomocí mobilních zařízení [2],[3],[4]. Mezi hlavní problémy, které je nutné v mobilních databázích řešit, patří:

- omezené přenosové pásmo bezdrátových komunikačních kanálů,
- jejich značná chybovost,
- limitovaná kapacita baterií napájecích mobilní zařízení,
- omezené zobrazovací schopnosti,
- výpočetní a paměťové možnosti a
- samozřejmě také otázka zabezpečení.

Mobilní databáze jsou velmi rychle se rozvíjejícím vědním oborem a tak vedle obecně známé architektury celulárních sítí jsou dnes velmi živým oborem také takzvané **ad-hoc sítě** [5],[6],[7]. Hlavním rozdílem oproti celulárním sítím je absence jakékoli pevné infrastruktury. Data jsou jednoduše přeposílána od zařízení k zařízení, dokud nedojde k doručení dat či překročení maximálního možného počtu přeposlání.

Dalším rozšířením, a vlastně speciálním druhem ad-hoc sítí, jsou **senzorové sítě** [8]. Na rozdíl od ad-hoc sítí jsou senzorové sítě tvořeny miniaturními senzory schopnými bezdrátové komunikace se svým nejbližším okolím a také měřením určité veličiny.

Velmi perspektivní architekturou, kde se také velmi často využívá důvěry pro zlepšení zabezpečení, jsou **Peer-To-Peer (P2P) sítě** [9],[10]. Hlavním specifikem takovéto architektury je absence centrálního řízení, jak jej známe z klasické architektury klient-server. Není proto žádným překvapením, že hlavním přínosem P2P sítí je odstranění hlavních problémů klient-server architektury:

- *rozšiřitelnost*
- *centrální řízení*
- *nevyužité zdroje.*

Jako příklad P2P sítí, které jsou nebo byly dostupné, patří především sítě pro sdílení souborů na internetu jako Napster, Kazaa, Kazaa Lite a Gnutella.

Není nezajímavé, že P2P architekturu považují někteří odborníci za budoucí architekturu internetu.

Velmi zajímavým pojmem jsou **výpočetní gridy**. Termín byl poprvé zaveden v 90 letech minulého století pro distribuovanou výpočetní infrastrukturu realizující komplikované vědecké a inženýrské úkoly. V [11] autoři definují pojem **virtuální organizace** (VO), který se objevuje v mnoha dalších oborech (mobilní databáze, internet, P2P), jako:

dočasné nebo dlouhodobé uskupení geograficky rozprostřených jednotlivců, skupin, organizačních jednotek či celých organizací, které sdílí zdroje, služby a informace pro dosažení společného cíle za konkrétně definovaných mechanismů a pravidel kdy, co a jak sdílet.

Výpočetní gridy mají definovanou architekturu tvořenou několika vrstvami, tak aby bylo dosaženo požadované funkcionality [12].
Výpočetní gridy lze v určitém úhlu pohledu považovat za příklad distribuované heterogenní architektury, jejíž modifikace lze nalézt v mnoha jiných architekturách (viz. mobilní databáze, internet, P2P).

Vzhledem k zaměření disertační práce se budeme v další části věnovat způsobům zabezpečení pro gridy, jakými jsou např.:

- *VOMS* [13],
- *PERMIS* [14] projekt,
- *AKENTI* [15],
- *PRIMA* [16].

Společným jmenovatelem těchto zabezpečovacích mechanismů je využití určitého typu certifikátu. Certifikáty jsou následně použity pro ověření uživatele žádajícího přístup ke zdrojům či službám. Je-li certifikát podepsán důvěryhodnou certifikační autoritou (CA), pak i obsah certifikátu je považován za důvěryhodný.
Certifikáty ve své podstatě velmi přesně modelují systém VO, tedy systém skupin či jednotlivců kooperujících na společném úkolu. Celá řada dnes běžně používaných zabezpečovacích mechanismů používá certifikáty pro ověření totožnosti či odvození míry důvěryhodnosti uživatelů.

V předchozím textu byly zmíněny systémy, kde se využívá důvěry pro správu přístupu k datům, službám či prostředkům. Nicméně jsme se nevěnovali konkrétním způsobům jak správu a vytváření důvěry konkrétně řešit. K tomuto účelu složí tzv. **systémy řízení důvěry** (Trust Management Systems). Systémy řízení důvěry lze podle způsobu řízení rozdělit do tří základních skupin:

- systémy pracující s *doporučeními* a *systémy s definovanou bezpečnostní politikou*;
- *reputační systémy*,
- systémy využívající *sociálních sítí*.

Systémy s definovanou bezpečnostní politikou byly navrženy v kontextu *otevřených* prostředí a prostředí s *distribuovanými službami* [17],[18],[19],[20],[21]. Jejich hlavním úkolem je spravovat řízení přístupu. K tomuto účelu slouží systém definovaných pravidel (definovaných v daném jazyce) a prostředků umožňujících odvozování a usuzování nad pravidly pro odvození míry důvěry.
Vlastník zdrojů definuje požadavky na případné zájemce o tyto zdroje a systém pak samostatně na základě předložených dokumentů žadatele umožní či zamítne přístup.

Reputační systémy poskytují uživatelům možnost odvozovat míru důvěry na základě vlastních zkušeností poskytovatele s žadatelem či na základě doporučení ostatních uživatelů majících s žadatelem konkrétní zkušenost. Tento přístup byl poprvé uveden v systémech elektronického obchodování např. eBay, déle pak v distribuovaných systémech, jako jsou

P2P sítě (např. XREP [22]), mobilních ad-hoc sítích a také pro internet (např. NICE [23], DCRC/CORC [24], EigenTrust [25]).

Poslední kategorií jsou systémy pro řízení důvěry využívající **sociálních sítí**. V tomto případě se na celý systém, ve kterém je řízena důvěra, nahlíží jako na sociální síť a pro odvozování důvěry jsou využívány metody sociální sítí. Tyto systémy jsou vhodné především tam, kde je značné množství a velká heterogenita uživatelů. Jako příklady takovýchto systémů lze uvést Regret [26], NodeRanking [27].
Důležitý je přechod od *důvěry* k *reputaci*. Obecně uznávaný přechodem je definice, kdy lze důvěru T odvodit z reputace R

$$T = \phi(R, t) \tag{2.1}$$

kde t je čas ([28]).

3 Cíle disertační práce

Cílem disertační práce je návrh, ověření a implementace nového bezpečnostního modelu pro obecně distribuované systémy, kde pro řízení přístupu k datům či službám je využívána míra důvěry mezi komunikujícími entitami. Cílové prostředí je považováno za silně dynamické, změny (přidání, úprava či smazání) ve vztazích mezi entitami mohou být velmi rychlé. Systém správy a budování důvěry mezi entitami musí navíc korespondovat s lidským chápáním důvěry, protože takové řešení bude jistě lépe přijatelné uživateli.

Jako motivační příklad lze uvést následující scénář: *Předpokládejme dva komunikující uživatele, uživatele A a uživatele B. Dále předpokládejme, že uživatel B požaduje po uživateli A privátní data. Uživatel A má dvě možnosti, buď požadavek odmítnout, protože nechce zpřístupnit svá citlivá data libovolnému uživateli nebo data poskytnout. Z bezpečnostního hlediska je lepší požadavek zamítnou, to však povede k zamítnutí velké části požadavků. Má-li ovšem uživatel A možnost zjistit jak důvěryhodný je uživatel B, pak může daleko snáze přístup povolit.*

Na základě představeného scénáře je tedy možné upřesnit cíle práce

- navrhnout stabilní systém pravidel pro správu a řízení důvěry mezi entitami systému,
- navrhnout model pro správu a řízení důvěry, který bude odpovídat lidskému chápání důvěry,
- navrhnout bezpečnostní model, který bude na základě budované důvěry řídit přístup k datům či službám.

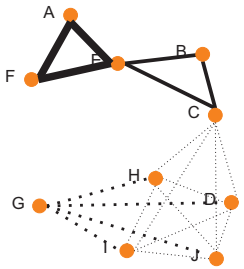
4 Způsob řešení

Práce je rozdělena na část teoretickou a experimentální. Obě části mají následující strukturu:

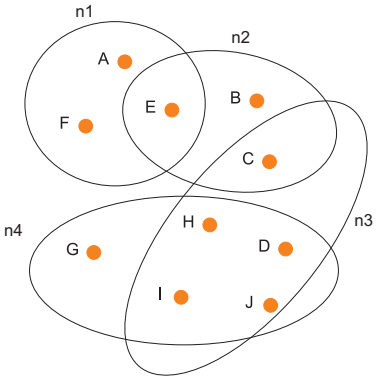
1. návrh modelu pro správu a budování důvěry mezi entitami,
2. algoritmy pro transformaci obecného grafového vstupu do navrženého modelu,
3. algoritmus pro správu dynamiky,
4. bezpečnostní subsystém.

4.1 Model pro správu a budování důvěry

Současné modely pro správu důvěry mezi entitami nejčastěji používají grafového modelu, kde jsou entity modelovány jako vrcholy ohodnoceného orientovaného grafu a vztahy mezi entitami odpovídají hranám. Míra důvěry odpovídá ohodnocení hrany mezi konkrétními vrcholy (viz. Obr. 4.1).



Obr. 4.1: Grafový model pro reprezentaci vztahů mezi entitami. (orientace je vynechána pro lepší přehlednost)



Obr. 4.2: Hypergrafový model zobrazující stejnou situaci jako v Obr. 4.1

Navrhovaný model vychází ze základní myšlenky, že důvěra v rámci lidské společnosti nemusí být vždy založena pouze na konkrétních vztazích mezi dvěma osobami, jak to věrně prezentuje grafový model, ale že důvěra může být společná pro určitou skupinu osob. Jako příklad uveďme organizace lékařů, skupiny přátel hrajících golf, atd. V tomto případě je možné říci, že členové takovéto skupiny mají k sobě navzájem

stejnou důvěru. Např. lékař umožní přístup jinému lékaři k datům týkajících se onemocnění, ale nepřipustí, aby stejné informace byly dostupné prodavači v trafice.

Vzhledem k takto šířeji chápané důvěře bylo nutné navrhnout vhodný matematický model, který by dostatečně efektivně modeloval skupiny uživatelů, kde jeden uživatel může být členem více skupin. Náš model využívá k tomuto účelu teorie hypergrafů.

Hypergraf $H = (U, N)$ je definován jako množina vrcholů U a množina hyperhran N mezi vrcholy.
Každá **hyperhrana** $n_j \in N$ je podmnožinou množiny vrcholů U.
Vrcholy obsažené v hyperhraně n_j značíme $pins[n_j]$.
Množina hyperhran napojených na vrchol u_j je označována jako $hyperedges(u_j)$.

Náš model popisující skupiny uživatelů vyjádříme hypergrafem $H = (U, N, W_U, W_N)$, kde:

1. *vrcholy* reprezentují *uživatele*
2. *hyperhrany* reprezentují *skupiny uživatelů*
3. *ohodnocení hyperhrany* W_{n_i} reprezentuje *důvěru sdílenou skupinou uživatelů* n_i
4. *ohodnocení vrcholu* W_{u_j} reprezentuje *atributy uživatele* u_j
5. $hyperedges(u_j)$ reprezentuje *množinu skupin* uživatele u_j

Obr. 4.2 ukazuje příklad hypergrafu, který modeluje čtyři skupiny deseti uživatelů.

4.2 Algoritmy pro transformaci vstupu do navrženého modelu

Předchozí odstavec uvedl hypergrafový model, který je základním stavebním prvkem našeho bezpečnostního modelu. Vzhledem ke skutečnosti, že většina vztahů mezi uživateli je popsána grafovým modelem, bylo nutné navrhnout algoritmy pro transformaci obecného grafového vstupu popisujícího vztahy mezi uživateli do hypergrafového modelu.

4.2.1 G2H Algoritmus

Pro transformaci obecného grafového vstupu do hypergrafového modelu byly v rámci disertační práce navrženy dvě varianty G2H (Graph to Hypergraph) algoritmu:

1. *G2H založený na silně souvislých komponentách [29]*,
2. *G2H založená na triadách[30].*

G2H algoritmus založený na silně souvislých komponentách se snaží identifikovat skupiny uživatelů v grafovém vstupu na základě silně souvislých komponent (**Silně souvislou komponentou** grafu G je podgraf, ve kterém pro každé dva vrcholy x a y existuje cesta z x do y).

Budeme-li se zabývat sémantikou takové struktury, pak interpretace obecného grafu, ve kterém vrcholy reprezentují uživatele a hrany reprezentují vztahy mezi uživateli, může být následující: *Uživatelé, kteří o sobě mohou navzájem zjistit informace buď přímo nebo pomocí ostatních členů, jsou členy jedné silně souvislé komponenty a jsou tedy vhodní kandidáti pro vytvoření skupiny.*

Hlavní předností této verze G2H je její malá časová složitost, která je dána složitostí algoritmu navrženého Tarjanem [31],[32],[33] včetně jeho modifikací. Složitost tohoto algorithmu pro hledání silně souvislých komponent v grafu je

$$O(N), \tag{4.1}$$

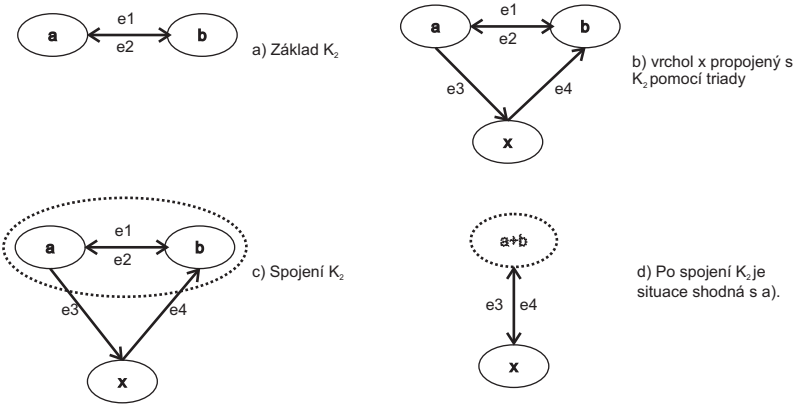
kde N je počet vrcholů grafu.

G2H algoritmus založený na triadách využívá pro identifikaci skupin navzájem propojených uživatelů jiný mechanismus tzv. triady [30]. G2H založený na triadách je popsán pseudo kódem v algoritmu 1.

Základní myšlenka toho algoritmu je graficky zobrazena v Obr. 4.3. Během první fáze jsou vytvořeny takzvané *základy* budoucích skupin (procedura SearchSeed v algoritmu 1). Jako *základ* je použit kompletní graf K2. Pro každý základ je prohledáno jeho okolí pro vrcholy, které jsou se základem propojeny pomocí jedné ze dvou akceptovaných triad (procedura AppendSeed v algoritmu 1). Na obr. 4.3 je hledání triady zobrazeno za b). Pokud je takový vrchol x nalezen je přidán k základu a celá operace se opakuje dokud nejsou prohledány všechny vrcholy grafu.

Algorithm 1 G2H algoritmus

procedure SEARCHSEED($G = (V, E)$)
  for all $a \in V$ **do**
    if $(\exists b \in V)(a \to b \in E \wedge b \to a \in E)$ **then**
      přidej a, b do $h_i \in H$
      $AppendSeed(G, h_i, max(|a \to b|, |b \to a|))$
      $i = i + 1$
    end if
  end for
end procedure
procedure APPENDSEED(G, h, max)
  while $(\exists x \in V : x \notin h, a \in h, b \in h)(a \to x \in E \wedge x \to b \in E) \vee (b \to x \in E \wedge x \to a \in E)$ **do**
    if $(|a \to x \to b| \geq max) \vee (|b \to x \to a| \geq max)$ **then**
      přidej x do h
    end if
  end while
end procedure



Obr. 4.3: G2H Algoritmus založený na triadách

Hypergraf $H = (U, N, W_U, W_{1N}, W_{2N})$ je ze vstupu
$G = (V, E, W_V, W_E)$ vytvořen tak, že

- vrcholy U v H odpovídají vrcholům V v G,
- ohodnocení vrcholů W_N v H odpovídá ohodnocení vrcholů W_V v G,
- $pins(n_i)$ v H odpovídají skupinám vrcholů $\{h_i\}$,
- ohodnocení hyperhran W_{1N} v H odpovídá maximálnímu rozdílu v ohodnocení hran v základu $K2$ h_i,
- ohodnocení hyperhrany W_{2N} v H odpovídá rozdílu mezi ohodnocením hran v základu $K2$ h_i.

Časová složitost toho algoritmu je

$$O(\sum_{v \in V} |Adj(v)|) \tag{4.2}$$

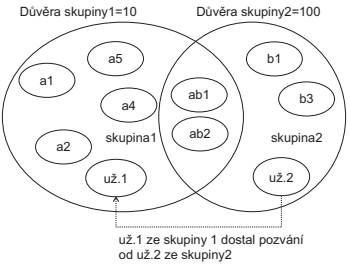
Složitost je dána procedurou *SearchSeed*, která hledá základy K2 ve vstupním grafu ($\sum_{v \in V} |Adj(v)|$ kroků).

4.3 Algoritmus pro správu dynamiky

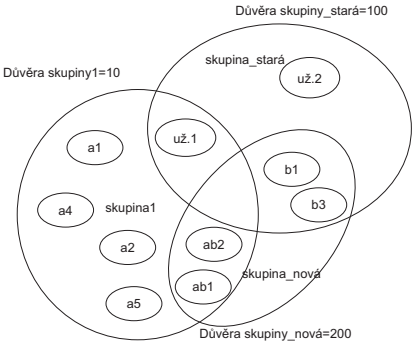
Jedním z požadavků na bezpečnostní model je schopnost pracovat i v dynamických prostředích, kde dochází ke změnám ve vztazích a také v míře důvěry mezi uživateli. Tuto schopnost realizuje SD (Structure Dynamics) algoritmus, který reaguje na dynamické změny v systému skupin. Hlavním úkolem SD algoritmu je zachovat důvěru skupin i v dynamických prostředích. Dynamika je v našem případě popsána jako pozvání nového uživatele do skupiny jedním ze stávajících členů. Tato situace může v reálných podmínkách nastávat velmi často a je zřejmé, že pozvání nedůvěryhodného uživatele do velmi důvěryhodné skupiny může představovat bezpečnostní riziko pro ostatní členy.

Příklad chování SD algoritmu je graficky popsán v Obr. 4.4 a 4.5. Na Obr.4.4 je zobrazena situace, kdy *už1* obdržel pozvání od *už2*. V tuto chvíli by se měl *už1* dostat také do *skupiny2*. Nicméně poznamenejme, že *skupina1* má značně nižší důvěru v porovnání se *skupinou2*. Z tohoto důvodu je na základě takovéhoto pozvání *skupina2* rozdělena na *skupina_nová* a *skupina_stará*. Zatímco ve *skupině_nové* jsou pouze uživatelé *skupiny2* mimo *už1* a *už2*, ve *skupině_staré* jsou *už1*, *už2* a všichni uživatelé, kteří nebyli členy obou skupin před rozdělením.
Důvodem rozdělení skupin je skutečnost, že v našem případě existovali dva uživatelé (*ab1*, *ab2*), kteří byli členy obou skupin a tedy věděli o rozdílných úrovních důvěry. Tito uživatelé nejsou ochotni akceptovat nově

příchozího a také uživatele, který jej pozval. Na druhou stranu, ostatní uživatelé nemají důvod k tomuto rozdělení a proto zůstávají členy obou skupin (*skupina_nová* i *skupina_stará*). Díky tomuto rozdělení si uživatelé zachovávají historii chování svého okolí v hypergrafovém modelu, bez nutnosti evidovat konkrétní vztahy.

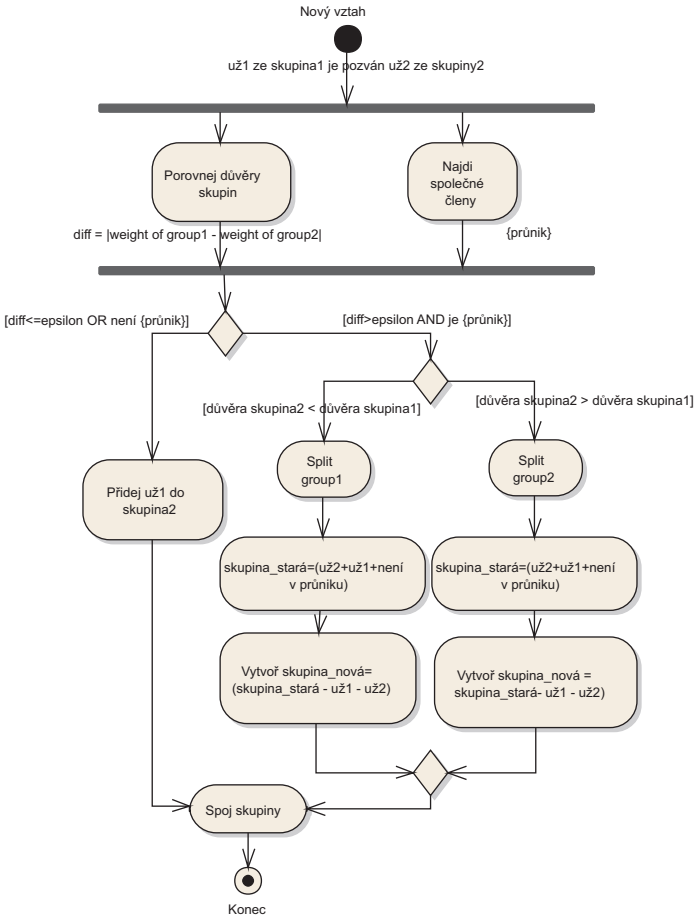


Obr. 4.4: Výchozí situace dvou skupin



Obr. 4.5: Situace pro rozdělení skupin

Obrázek 4.7 zobrazuje jednotlivé kroky SD algoritmu. Na začátku je pozvání mezi uživateli. Následuje identifikace společných členů skupin a také porovnání důvěry sdílené ve skupinách. Pokud nejsou žádní uživatelé členy obou skupin nebo rozdíl důvěry je menší než ϵ, pak je možné pozvání akceptovat, neboť skupiny mají podobné sdílené důvěry nebo neexistují uživatelé, kteří by případný větší rozdíl byli schopeni identifikovat. Na druhou stranu pokud tyto podmínky nejsou splněny, je skupina s vyšším ohodnocením rozdělena. Nakonec je také spuštěna procedura, která se pokusí identifikovat skupiny, které je možné sloučit, protože mají hodně společných členů a mají podobné sdílené důvěry. Spojování je řízeno parametrem λ.



Obr. 4.6: UML Aktivity Diagram (popisující procedury SD Algoritmu).

4.4 Bezpečnostní subsystém

Návrh bezpečnostního subsystému byl veden následujícími body:

1. **Nepoužívat dlouhodobé přístupové klíče**. Dlouhodobé bezpečnostní klíče se ukazují být slabým místem mnoha současných bezpečnostních mechanismů, protože je nutné takovéto klíče uchovávat na relativně velmi bezpečném místě. V dlouhodobém měřítku je velmi pravděpodobné, že klíč bude prozrazen nebo jinak znehodnocen.

2. **Neaplikovat změny příliš rychle**. V dynamických systémech je nutné zachovávat určité zpoždění mezi akcí a reakcí systému. Pokud by systém reagoval příliš rychle, uživatelé by neměli čas změny sledovat a po čase by došlo ke ztrátě důvěry v takovýto systém.
3. **Redukovat reputace třetích stran**. Reputace třetích stran jsou často používány v mnoha systémech pro řízení důvěry, nicméně tyto reputace jsou zdrojem mnoha problémů a velmi často jsou bezpečnostním rizikem.

4.4.1 Návrh bezpečnostního subsystému

Shadow Groups: každý nově pozvaný uživatel je nejprve členem tzv. *Shadow Group* (stínová skupina) do té doby než obdrží potřebný počet podpisů od plnoprávných členů skupiny. Členové stínové skupiny mají omezené pravomoci (např. nemohou pozvat nového člena do skupiny).

Group	GroupFrom	Base|user	$Sign_{u1}$ ... $Sign_{un}$	Trust	λ	ε	α	TTL

Obr. 4.7: Struktura tKey.

tKey: každý uživatel udržuje jeden *tKey* pro každou skupinu v níž je členem.

tKey obsahuje:

- Pole *Group* obsahující identifikaci skupiny.
- Pole *GroupFrom* obsahující identifikaci skupiny, ze které byl uživatel pozván.
- Pole *Base|user* obsahující *otisk(y)* pozvaného uživatele [1] společně s otiskem uživatele, který vydal pozvání do této skupiny.
- Pole $Sign_{u1} \dots Sign_{un}$ obsahující podpisy obdržené od ostatních členů skupiny. Připojením svého podpisu stávající člen akceptuje nového člena.
- Pole *Trust* obsahující míru důvěry pro tuto skupinu.
- Parametry λ a ϵ řídící *rozdělování* a *slučování* skupin v SD Algoritmu.
- Parametr α reprezentující počet podpisů v poli $Sign_{u1} \dots Sign_{un}$ nutných pro plnoprávné členy skupiny.
- *TTL* čas do vypršení platnosti *tKey*.

[1] Otisky budou popsány dále v textu.

tKey - správa a ověřování: v této části se budeme věnovat jednotlivým operacím nutným pro realizaci bezpečnostního subsystému.

- **Vytvoření tKey**: předpokládejme pozvání u_i ze skupiny n_i do skupiny n_j uživatelem u_j. Nový *tKey* u_i pro skupinu n_j je vytvořen podle následujícího schématu:

  1. u_j pošle u_i pole *base* svého tKey společně s novým TTL
  2. u_i připojí svůj otisk k *base* čímž vytvoří nové pole $Base|user$ budoucího tKey
  3. u_i se stane členem stínové skupiny dokud platí, že počet podpisů v poli $Sign_{u1} \dots Sign_{un}$ je menší než hodnota parametru α.

- **Ověřování tKey**: bezpečnostní subsystém umožňuje uživatelům nalézt společné skupiny (připomeňme, že společné skupiny jsou hlavním vodítkem pro odvození důvěry) dle následujícího schématu:

  1. Uživatelé si vymění své *tKeys*.
  2. Uživatelé prověří pole *group* každého obdrženého *tKey*: *Pokud je nalezen stejný*, pak dojde k ověření *tKey*:
     (a) kontrola členství ve stínové skupině,
     (b) kontrola pole *base* vyjadřující kým byl uživatel pozván,
     (c) kontrola pole TTL.

  Následně uživatelé mají informace:

  – zda-li existují společné skupiny, v kladném případě pak také
    1. *zda* jsou *plnoprávnými* členy nebo *stínovými* členy
    2. *kým* byl *tKey* dosud podepsán
    3. *kým* byli uživatelé pozváni
    4. *do kdy* je tKey *platný*.

- **tKey a SD algoritmus**: důležitým aspektem představeného bezpečnostního subsystému je skutečnost, že jednotlivé operace SD algoritmu lze pomocí tKey realizovat.

  – **Přidání nového člena** je snadné a vyžaduje pouze vydání nového tKey.
  – **Rozdělení skupin** závisí na schopnosti zjisti společné členy více skupin. Připomeňme, že členové si vyměňují všechny tKey, které mají. Pak lze tedy snadno zjistit členy skupiny,

zda-li je nově přijatý člen členem i jiných (méně důvěryhodných) skupin. Pole *Base*|*user* navíc obsahuje informaci o tom, kým byl člen pozván.

– **Slučování skupin** je možné realizovat pomocí stejného schématu jako rozdělování skupin.

5 Experimentální ověření

V rámci disertační práce byly navrženy:

1. hypergrafový model pro správu a budování důvěry mezi entitami,
2. algoritmy pro transformaci obecného grafového vstupu do navrženého modelu,
3. algoritmus pro správu dynamiky,
4. bezpečnostní subsystém.

Pod pojmem SecGrid budeme dále rozumět výše uvedené části a také jejich experimentální implementaci (naprogramovanou v ANSI C).

5.1 Experimenty pro G2H Algoritmus

G2H algoritmus transformuje obecný grafový vstup do navrženého hypergrafového modelu. Cílem experimentů bylo ověřit, že takováto transformace dovoluje zachytit v hypergrafu sociální vztahy reprezentované vstupní strukturou (obecného)grafu.

Celý experiment byl rozdělen na dvě základní části:

1. *ručně vytvořené* vstupní grafy,
2. *grafy popisující reálná společenství.*

Ručně vytvořené vstupní grafy: hlavním cílem těchto experimentů bylo ověřit použitelnost obou verzí G2H algoritmů pro transformaci speciálně navržených vstupních grafů.

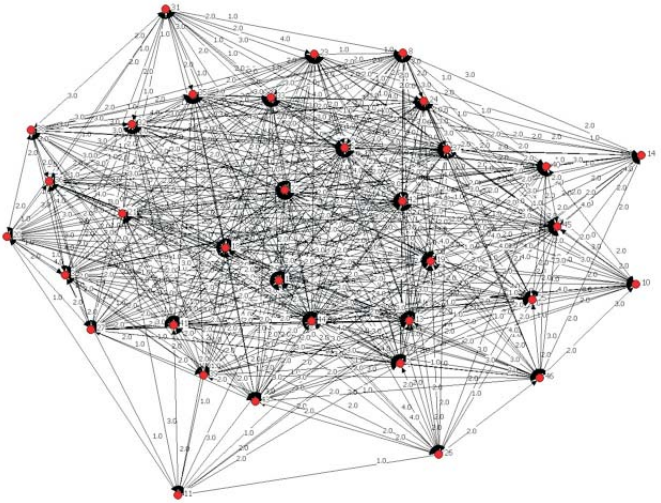
Během experimentů bylo zjištěno, že verze G2H algoritmu založeného na silně souvislých komponentách je nevhodná pro grafy s jednou cestou procházející většinou vrcholů (v tomto případě jsou všechny vrcholy součástí jedné skupiny v hypergrafovém modelu, což není vhodné).

G2H využívající triad se na druhou stranu nevykazoval tento nedostatek.

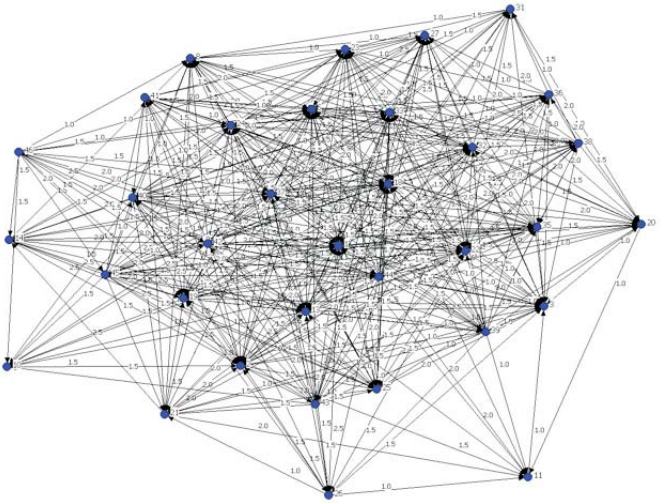
Grafy popisující reálná společenství: ve druhé skupině experimentů byly jako vstupní grafy použity:

1. EIES sociální síť [34],
2. záznamy hovorů mobilního operátora ve Slovenské republice.

Na Obr. 5.1 (na další straně) je zobrazena vstupní struktura EIES grafu. Z obrázku je patrné, že vstupem graf obsahující velmi mnoho hran. Obr. 5.2 (na další straně) ukazuje, jak se projeví hlavní nevýhoda silně

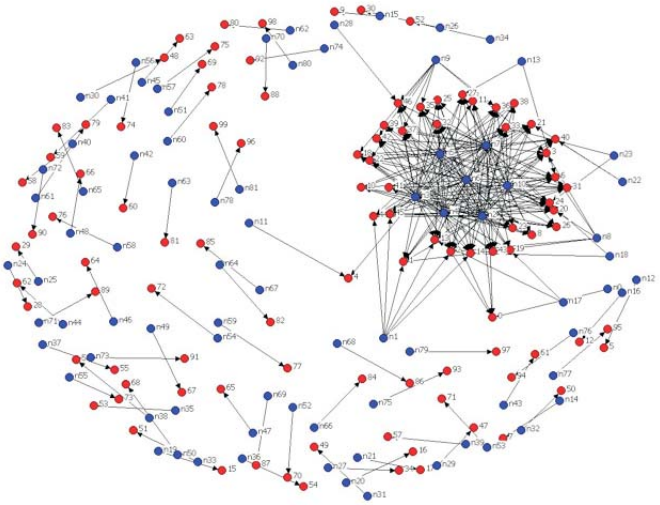


Obr. 5.1: Vstupní graf pro EIES.



Obr. 5.2: Výstup G2H Algoritmu založeného na silně souvislých komponentách.

souvislých komponent, kdy jsou uživatelé členy jedné skupiny (vyjma izolovaných).



Obr. 5.3: Výstup G2H Algoritmu založeného na triadách (členové stejné skupiny jsou napojeny na stejné modré ovály).

Tab. 5.1: Distribuce uživatelů do skupin

Velikost skupiny	**Počet skupin**
2	104
3	6
5	1
6	1

V následujícím Obr. 5.3 je vidět výsledek získaným G2H založeným na triadách.

Druhý experiment byl proveden pro záznamy telefonních hovorů v mobilní síti ve Slovenské republice. Vzhledem k rozsahu vstupního grafu (7898 vrcholů a 8609 hran) byl pro experimenty použit pouze G2H založený na triadách. Výsledek je v Tab. 5.1 (izolované vrcholy nejsou v tabulce zahrnuty).

5.2 Experimenty pro SD Algoritmus

Hlavním účelem experimentů bylo ověřit, že SD algoritmu nevytvoří:

1. **jedné skupiny obsahující všechny uživatele systému**,
2. **velmi mnoho malých skupin**.

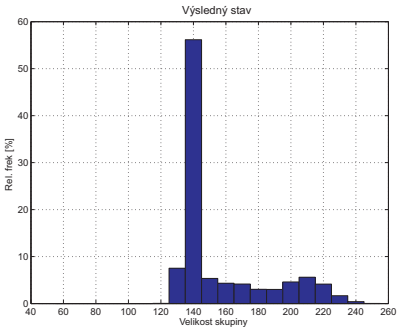
Experimenty byly řízeny parametry λ and ϵ SD algoritmu

- λ *ovlivňuje* **spojování skupin** – větší znamená λ více spojování,
- ϵ *kontroluje* **rozdělování skupin** – nižší ϵ znamená větší pravděpodobnost rozdělování skupin.

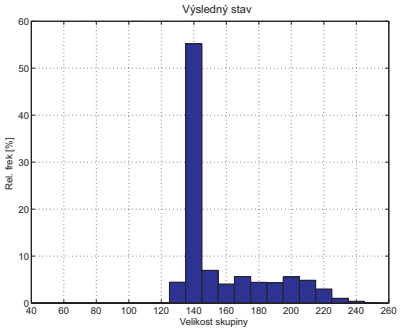
Experimenty byly provedeny pro dva typy experimentálních dat

1. záznamy hovorů z mobilní sítě ve Slovenské republice,
2. vstupní data pro tři různá statistická rozdělení.

Experimenty pro vstupní data popisující hovory v mobilní síti ve Slovenské republice: pro účely experimentů bylo vybráno 161 404 telefonních hovorů mezi 121 672 uživateli. Každý hovor vyjadřoval pozvání telefonujícího uživatele telefonujícímu do jedné ze svých skupin. Jako počáteční konfigurace byl zvolen systém s 908 skupinami ozna-



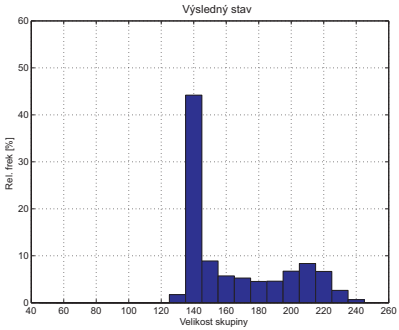
Obr. 5.4: Výsledný histogram pro parametry $\lambda = 1$, $\epsilon = 1$, $\Omega = 908$



Obr. 5.5: Výsledný histogram pro parametry λ =1, $\epsilon = 3$, $\Omega = 908$

čovaný dále jako Ω. Výsledky jsou prezentovány jako histogramy pro relativní frekvenci výskytu skupin jako závislosti na jejich velikostech.

Vyhodnocení experimentu: SD algoritmus v žádném případě nevytvořil limitní případ jedné velké skupiny nebo mnoha malých skupin a to i pro různé kombinace parametrů. Na druhou stranu je nutné říci, že parametry algoritmu mají vliv především na počátek vývoje systému skupin, zatímco v konečné podobě mají vliv menší.



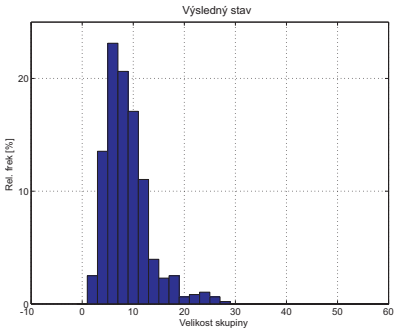
Obr. 5.6: Výsledný histogram pro parametry $\lambda = 3$, $\epsilon = 1$, $\Omega = 908$

Experimenty pro data generovaná podle statických rozdělení: cíle experimentu bylo ověřit závislost chování SD algoritmu na vstupních datech.

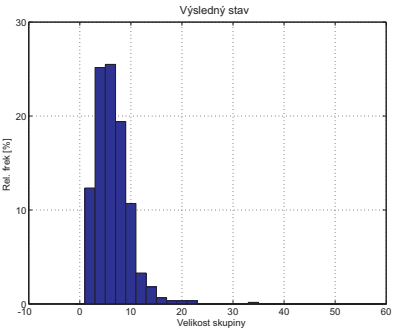
Vstupní data byla generována pro tři různá statistická rozdělení náhodných dat:

1. rovnoměrné rozdělení,
2. normální rozdělení,
3. exponenciální rozdělení.

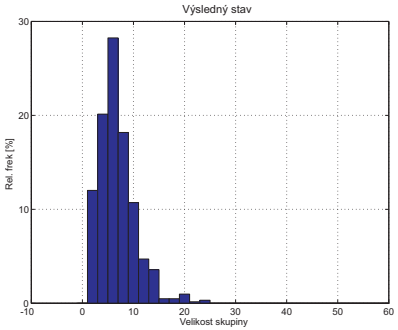
Parametry SD algoritmu byly zvoleny $\lambda = 2$, $\epsilon = 1$.



Obr. 5.7: Výsledný histogram pro rovnoměrné rozdělení ($\lambda = 2$, $\epsilon = 1$, $\Omega = 20$).



Obr. 5.8: Výsledný histogram pro normální rozdělení ($\lambda = 2$, $\epsilon = 1$, $\Omega = 100$).



Obr. 5.9: Výsledný histogram pro exponenciální rozdělení ($\lambda = 2$, $\epsilon = 1$, $\Omega = 10$).

Experimenty ukázaly, že různé vstupy mají vliv na distribuci uživatelů do skupin. Na druhou stranu je nutné poznamenat, že výsledné distribuce se liší pouze málo a lze tedy konstatovat, že i v tomto případě se SD algoritmus vykazoval stabilní chování.

5.3 Experimenty pro bezpečnostní subsystém

Porovnání grafového a hypergrafového modelu. SecGrid využívá hypergrafů pro reprezentování skupin uživatelů. Cílem následujícího experimentu je ukázat, že hypergrafový model je vhodnější pro budování důvěry ve velkých systémech, kde uživatelé mají pouze omezené možnosti udržovat konkrétní vztahy se svým okolím.

Jako měřítko pro porovnání je zvolen počet přímých vztahů, které je možné získat pro stejnou konfiguraci v grafovém a hypergrafovém modelu. V grafovém modelu je počet přímých vztahů dán velikostí množiny hran $|E|$). V hypergrafovém modelu je možné použít tzv. klikovou reprezentaci hyperhran, kdy je hyperhrana nahrazena kompletním grafem o velikosti $K_{|pins(n_i)|}$, kde n_i je reprezentovaná hyperhrana. Počet přímých vztahů je pak dán jako

$$|E| = n \cdot (n - 1) \tag{5.1}$$

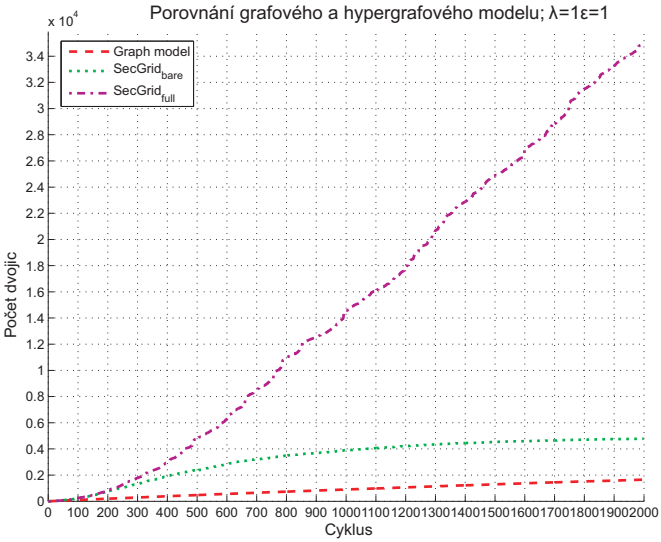
Experiment byl proveden pro tři kombinace parametrů SD algoritmu:

1. $\lambda = 1$, $\epsilon = 1$;
2. $\lambda = 1$, $\epsilon = 3$;
3. $\lambda = 3$, $\epsilon = 1$.

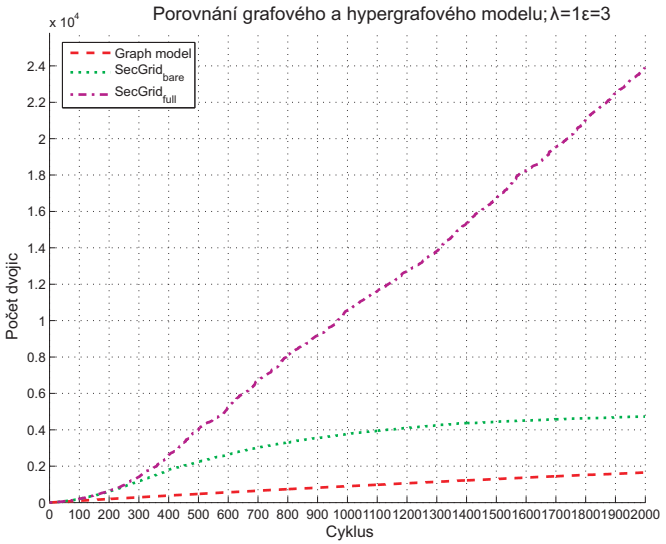
Vstup tvořilo 2000 dvojic *(už1,už2)*, které odpovídaly pozvání *už1* pro *už2* do jedné ze skupin *už1*, stejně jako tomu bylo v předchozím případě.

Výsledky jsou prezentovány jako graf, kde je na y ose počet přímých vztahů a na ose x počet zpracovaných pozvání. Pro porovnání je uveden mimo grafového a hypergrafového modelu i tzv. *bare hypergraph model*, který reprezentuje počet přímých vztahů mezi uživateli přičemž uživatel může přispívat pouze do jedné ze svých skupin.

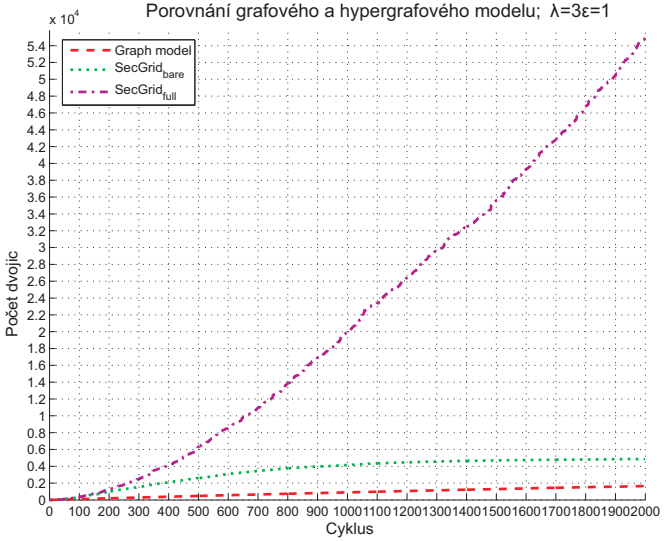
Následující obrázky (5.10, 5.11, 5.12) ukazují průběhy pro vstup generovaný pro rovnoměrné rozdělení. Z obrázků je patrné, že hypergrafový model poskytuje daleko více přímých vztahů v porovnání s grafovým modelem. I v případě *bare hypergraph modelu* je počet přímých vztahů větší než pro grafový model.



Obr. 5.10: Rovnoměrné rozdělení ($\lambda = 1$, $\epsilon = 1$).



Obr. 5.11: Rovnoměrné rozdělení ($\lambda = 1$, $\epsilon = 3$).



Obr. 5.12: Rovnoměrné rozdělení ($\lambda = 3$, $\epsilon = 1$).

5.4 Experimenty pro bezpečnostní subsystém

Experimenty pro bezpečnostní subsystém si kladly za cíl ověřit míru bezpečnosti, které je schopen SecGrid udržet. Pro potřebu experimentu byli uživatelé označeni jako *lstiví* (uživatelé, kteří nepůsobí újmu[1] ostatním členům) a *korektní* (uživatelé, kteří působí újmu ostatním členům). Hlavní **mírou bezpečnosti** je v hypergrafovém modelu počet *korektně* se chovajících uživatelů ve skupině (optimální hodnota je 100%).

Scénář použitý pro ověření bezpečnostního subsystému měl následující podobu:

1. v první fázi se n-krát provedou kroky SD algoritmu
2. v druhé fázi je k-krát provedou následující kroky
   (a) zvolí se náhodně jeden lstivý a jeden korektní uživatel
   (b) rozdělí se všechny jejich společné skupiny, tak že v nové skupině jsou uživatelé mimo lstivého a všech uživatelů, které pozval
   (c) nové skupině se zvýší míra důvěry

Parametry experimentu byly zvoleny

- $n = 300$,
- $k = 30$,
- 50 uživatelů

Kombinace parametrů SD algoritmu byly

1. $\lambda = 1$, $\epsilon = 1$,
2. $\lambda = 4$, $\epsilon = 1$,
3. $\lambda = 1$, $\epsilon = 4$.

Bylo provedeno celkem 8 různých experimentů pro výše uvedené parametry a pro různé procentuální poměry mezi lstivými a korektními uživateli (označované jako parametr Ψ)

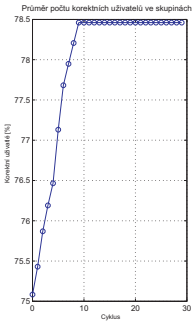
1. $\Psi = 95\%$,
2. $\Psi = 90\%$.
3. $\Psi = 80\%$,
4. $\Psi = 70\%$,
5. $\Psi = 50\%$,
6. $\Psi = 30\%$,
7. $\Psi = 20\%$,
8. $\Psi = 10\%$.

[1] Např. prozrazením důvěrných informací.

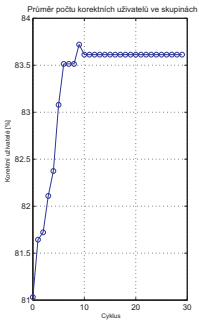
Kvůli rozsahu experimentů jsou prezentovány pouze výsledky pro $\Psi = 80\%$. Výsledky jsou prezentované jako grafy, kde

1. první tři grafy ukazují vývoj **průměru** Φ jako funkce ukončených cyklů. Poznamenejme, že dělení skupiny nemá vliv na původní skupinu, která se zůstává nezměněna, proto se celkový průměr korektních uživatelů ve skupinách mění pozvolna. Graf tedy ukazuje hlavně tendence ve vývoji průměru Φ.
2. Druhá trojice grafů ukazuje **vývoj každé skupiny** během experimentu.
   Na ose x jsou cykly a na ose y je procento korektních uživatelů ve skupinách (Φ).

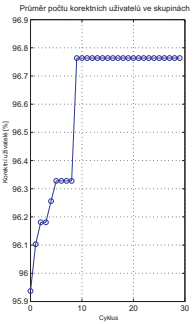
   - **Modré malé kružnice** ukazují skupiny, které se v daném okamžiku nedělí.
   - **Modrá úsečka** spojuje moment posledního dělení skupiny s momentem, kdy je skupina opět rozdělena.
   - **Nově vzniklé skupiny** jsou zobrazeny jako **červené hvězdičky**.
   - **Červená čerchovaná úsečka** propojuje starou a nově vzniklou skupinu. Pokud je počet korektních uživatelů větší v nové skupině, pak tato úsečka směřuje nahoru.



Obr. 5.13: $\lambda = 1$, $\epsilon = 1$, $\Psi = 80\%$



Obr. 5.14: $\lambda = 4$, $\epsilon = 1$, $\Psi = 80\%$

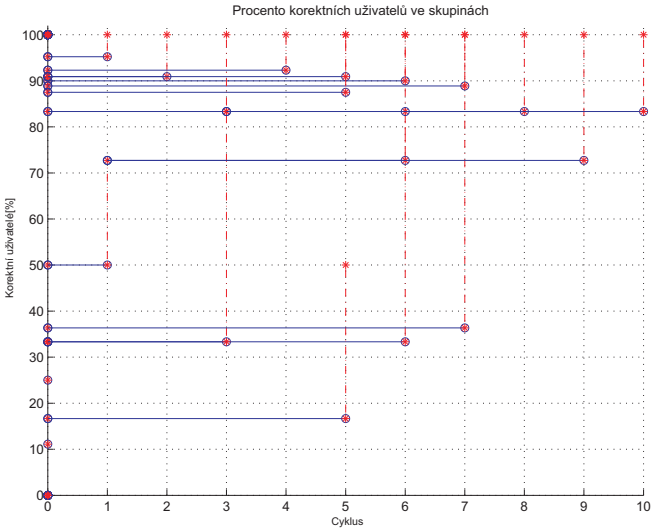


Obr. 5.15: $\lambda = 1$, $\epsilon = 4$, $\Psi = 80\%$

První sada obrázků 5.13, 5.14, 5.15 ukazuje tendence ve vývoji procentuálního poměru mezi lstivými a korektními uživateli pro tři různé kombinace parametrů SD algoritmu. Na obrázku je vidět, že různé kombinace parametrů dávají různé zisky v průměru Φ. Zatímco kombinace $\lambda = 1$, $\epsilon = 1$ poskytuje nejnižší výchozí úroveň průměru Φ (okolo 75

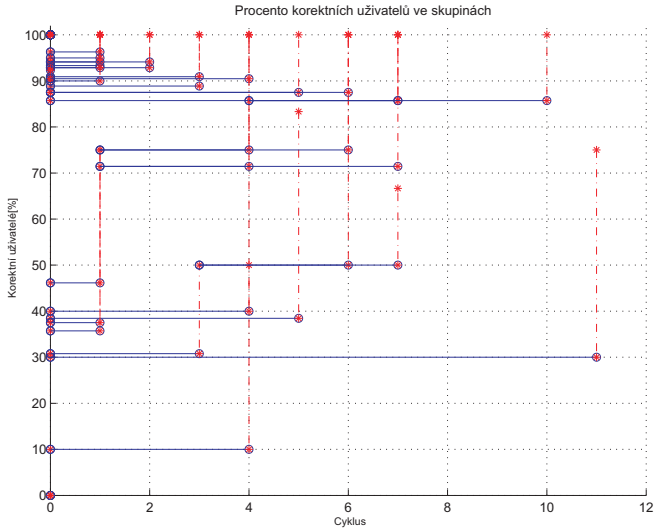
%) v porovnání např. s kombinací $\lambda = 1$, $\epsilon = 4$ s průměrem Φ okolo 96 %. Na druhou stranu je zisk v prvním případě největší (okolo 3,5 %). Důležitým momentem je skutečnost, že všechny kombinace parametrů λ a ϵ vedou ke zlepšování průměru Φ, což odpovídá zlepšování míry bezpečnosti navrženého modelu.

Následující tři grafy (Obr. 5.16, 5.17, 5.18) zobrazují vývoj míry bezpečnosti pro jednotlivé skupiny v systému. V prvním případě, pro parametry $\lambda = 1$, $\epsilon = 1$, je vidět, že počet skupin, které mají počáteční poměr (osa y) mezi lstivými a korektními uživateli menší než 50 %, je přibližně polovina. Tento poměr dobře odpovídá i počáteční nižší hodnotě průměru Φ v obrázku 5.13. V průběhu experimentu (osa x) je dobře vidět, jak se zlepšuje míra důvěry pro nově vytvořené skupiny, protože všechny červené čerchované úsečky směřují vzhůru. Na konci experimentu lze konstatovat, že vyjma jedné skupiny, všechny dosáhly ideálního průměru 100% dobrých uživatelů ve skupině.

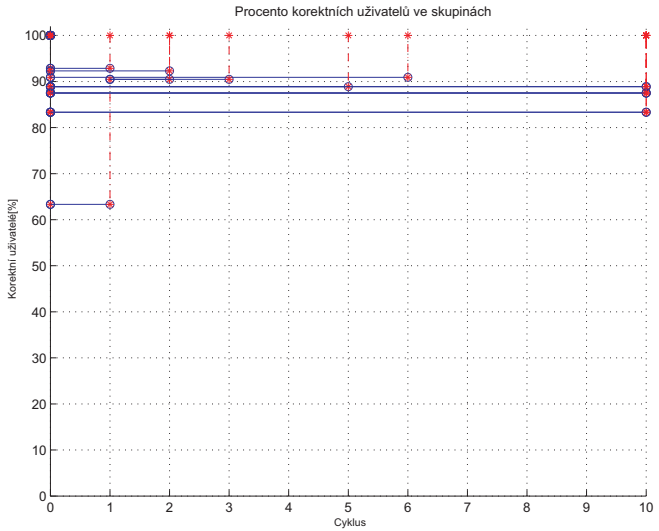


Obr. 5.16: Vývoj skupin pro parametry $\lambda = 1$, $\epsilon = 1$, $\Psi = 80\%$

Následující dva obrázky ukazují vývoj ve skupinách pro další dvě kombinace parametrů. Z obrázků je patrné, že počáteční stav je ovlivněn parametry SD algoritmu λ a ϵ. Dále je vidět, že všechny nově vytvořené skupiny mají lepší poměr dobrých uživatelů.



Obr. 5.17: Vývoj skupin pro parametry $\lambda = 4$, $\epsilon = 1$, $\Psi = 80\%$



Obr. 5.18: Vývoj skupin pro parametry $\lambda = 1$, $\epsilon = 4$, $\Psi = 80\%$

5.5 Experimentální implementace SecGrid modelu

Poslední částí disertační práce je experimentální aplikace implementující model SecGrid, která si kladla za úkol ověřit použitelnost modelu v reálném prostředí pomocí reálných a dostupných prostředků. Za hlavní míru pro ověření použitelnosti, byla zvolena schopnost uložit a následně si také vyměňovat tKeys. Důvodem je skutečnost, že schopnost ukládat a vyměňovat tKeys je základním atributem pro odvozování důvěry mezi uživateli.

Za cílová zařízení byly zvoleny mobilní telefony, protože jsou obecně rozšířeným výpočetním prostředkem, které mají dostatečné výpočetní a paměťové prostředky. Další výhodou mobilních telefonů je skutečnost, že je uživatelé mají při sobě po většinu dne.
Aplikace MyKeys byla napsána v jazyce Java (konkrétně verzi pro mobilní zařízení J2ME). Jako médium pro výměnu tKeys bylo zvolen Bluetooth, především pro svojí rozšířenost. Pro uložení a získávání tKeys z paměti mobilního telefonu bylo použito Record Management System (RMS).

Cílem experimentů pro MyKeys bylo otestovat schopnost aplikace přenášet tKeys

- ve volném prostoru,
- uvnitř budov (budovy Technické university v Liberci).

Obecně lze konstatovat, že maximální vzdálenost, na kterou je možné navázat spojení pomocí Bluetooth, je v otevřeném prostředí okolo 30 metrů.
V budovách Technické university v Liberci, kde je většina zdí cihlových o tloušťce až 50 cm, byla maximální vzdálenost pro připojení velmi proměnlivá. Průměrná hodnota byla okolo 10 metrů.

6 Přínosy disertační práce

V disertační práci byl navržen **nový bezpečnostní model SecGrid**, který používá nově navržený **hypergrafový model** pro vytváření a správu důvěry mezi uživateli v obecně distribuovaných prostředích s velkým počtem uživatelů.
Hypergrafový model se liší od dnes většinou využívaného grafového modelu, především v chápání důvěry ne jako konkrétní hodnoty pro dvojici uživatelů (jako tomu je u grafového modelu), ale jako sdílenou hodnotu pro určitou skupinu uživatelů. Důvěra mezi konkrétními uživateli je pak odvozena na základě společných skupin.

Práce zejména obsahuje následující komponenty.

- Vzhledem ke skutečnosti, že v současné době je většina reálných sociálních vztahů mezi lidmi popsána přímo jako grafové struktury (nebo se dají převést na grafové struktury), bylo nutné v rámci řešení disertační práce navrhnout **algoritmus**, který provádí korektní transformaci obecného grafového vstupu do modelu hypergrafů (korektní transformací je zde myšlena skutečnost, že výsledná hypergrafová struktura odpovídá sémantice vztahů vstupní grafové struktury). Byly navrženy dvě základní modifikace algoritmu:
  - algoritmus založený na silně souvislých komponentách,
  - algoritmus založený na triadách.
- Další součástí bezpečnostního modelu je **algoritmus** (SD algoritmus), který se stará a řešení dynamických změn ve vztazích mezi uživateli. V reálných situacích je nutné považovat otázku dynamiky za velmi důležitou, neboť reálné skupiny uživatelů se budou jistě v čase vyvíjet. Tento algoritmus byl navržen tak, aby na základě hypergrafového modelu udržoval vysokou míru důvěry uživatelů i v případě silně dynamických systémů, kde je počet a rychlost změn ve vztazích mezi uživateli velká.
- Poslední komponenta, která byla navržena v rámci disertační práce, je **bezpečnostní subsystém**, který se stará realizaci operací SD algoritmu v totálně distribuovaném prostředí. Pro potřeby bezpečnostního subsystému byla navržena nová struktura tKey, která obsahuje informace nutné pro odvozování důvěry mezi uživateli.
- Součástí disertační práce je popis **experimentální aplikace** pro mobilní telefony pro výměnu a ukládání tKeys v reálném prostředí.

Hlavním přínosem práce je **nové pojetí důvěry mezi uživateli** a **nový hypergrafový model**, který zobecňuje skutečné vztahy mezi lidmi ve společnosti. Teto model použít všude tam, kde je počet uživatelů a dynamika jejich vztahů velká. Díky novému pojetí důvěry je také možné odvozovat míru důvěry i mezi uživateli, kteří mezi sebou nemají žádný přímý vztah a to bez použití tzv. reputací třetích osob, jak je to v klasickém grafovém modelu.

7 Pokračování práce v daném tématu a oboru

V následujícím období se chci věnovat aktivitám, které navazují na mé výsledky disertační práci, konkrétně chci implementovat SecGrid v reálném prostředí pro sdílení a přístup k datům. Takovéto prostředí je v současné době připravováno se spolupráci s dalšími kolegy na Ústavu informatiky Akademie věd České republiky. V rámci toho prostředí bude třeba modifikovat některé části SecGrid tak, aby lépe odpovídaly požadavkům prostředí webových zdrojů.

Zejména bych se chtěl věnovat,

- rozšíření navržených G2H algoritmů a jejich použití v oblasti Social Network Analysis (SNA). Vzhledem k výsledkům prezentovaných v disertační práci, je schopnost algoritmů nacházet skupiny uživatelů ve vstupních datech velmi zajímavým směrem dalšího výzkumu.
- rozšíření současné implementace *MyKey*, tak aby plně podporovala navržené algoritmy SecGrid. Bude nutné vzít v potaz omezené výpočetní a paměťové prostředky mobilních zařízení obecně a případně modifikovat navržené části SecGrid.

Předmětem mého dalším vědeckého bádání zcela jistě zůstane oblast zabezpečení distribuovaných systémů, jako jsou např. mobilní databáze, peer-to-peer sítě a oblast budoucího internetu, které nastolují požadavky na nová řešení. Otázky spojené s bezpečností v distribuovaných prostředích, které se stále více prosazují jako nové architektury v systémech pro sdílení zdrojů a služeb, vyžadují maximální pozornost.

Literatura

[1] J. Waldo. Virtual organizations, pervasive computing, and an infrastructure for networking at the edge. *Information Systems Frontiers 4, Kluwer Academic Publishers*, 1:9–18, 2002.

[2] S. DasBit and S. Mitra. Challenges of computing in mobile cellular environment a survey. *Computer Communications*, 26:2090–2105(16), 2003.

[3] Y. Lu, B. Bhargava, W. Wang, Y. Zhong, and Wu X. Secure wireless network with movable base stations. *IEICE Trans. Community*, vol. E86-B, 2003.

[4] Y. Zong, B. Bhargava, and M. Mahoui. Trustworthiness based authorization on www. *IEEE Workshop on Security in Distributed Data Warehousing*, 2001.

[5] P. K. Behera and P. K.Meher. Prospects of group-based communication in mobile ad hoc networks. *Springer-Verlag Berlin Heidelberg*, 2002.

[6] A. Flaxman, A. Frieze, and E. Upfal. Efficient communication in an ad-hoc network. *Elsevier*, 2004.

[7] S. Basagni. Remarks on ad hoc networking. *Springer-Verlag, Berlin Heidelberg*, 2002.

[8] K. Akkaya and M. Younis. A survey on routing protocols for wireless sensor networks. *Elsevier Ad Hoc Network Journal*, 3/3:325–349, 2005.

[9] Ralf Steinmetz and Klaus Wehrle. *Peer-to-Peer Systems and Applications*. Springer, October 25, 2005.

[10] V. Muthusamy. An introduction to peer-to-peer networks. *Presentation for MIE456 - Information Systems Infrastructure II*, October 30, 2003.

[11] I. Foster, C. Kesselman, and S. Tuecke. The anatomy of the grid: Enabling scalable virtual organizations. *International J. Supercomputer Applications*, 15(3), 2001.

[12] I. Foster, C. Kesselman, J. Nick, and S. Tuecke. The physiology of the grid: An open grid services architecture for distributed systems integration. *http://www.globus.org/research/papers/ogsa.pdf, citeseer.ist.psu.edu/foster02physiology.html*, 2002.

[13] R. Alfieri, R. Cecchini, V. Ciaschini, L. dell'Agnello, A. Frohner, A. Gianoli, K. L″orentey, and F. Spataro. Voms: An authorization system for virtual organizations. *In the 1st European Across Grids Conference, Santiago de Compostela*, Feb. 2003.

[14] D. Chadwick and O.Otenko. The permis x.509 role based privilege management infrastructure. *In 7th ACM Symposium on Access Control Models and Technologies*, 2002.

[15] M. R. Thompson, A. Essiari, and S. Mudumbai. Tcertificate-based authorization policy in a pki environment. *ACM Trans. Inf. Syst. Secur.*, 6(4):566–588, 2003.

[16] M. Lorch, D. Adams, D. Kafura, M. Koneni, A. Rathi, and S. Shah. The prima system for privilege management, authorization and enforcement in grid environments. *In Proceedings of the 4th Int. Workshop on Grid Computing - Grid 2003, Phoenix, AZ, USA*, 2003.

[17] P. Bonatti and P. Samarati. Regulating service access and information release on the web. *In CCS 00: Proceedings of the 7th ACM conference on computer and communications security, ACM Press*, page 134–143, 2000.

[18] N. Li and J. Mitchell. A role-based trust-management framework. *In DARPA Information Survivability Conference and Exposition (DISCEX), Washington, D.C.*, Apr. 2003.

[19] R. Gavriloaie, W. Nejdl, D. Olmedilla, K. E. Seamons, and M. Winslett. No registration needed: How to use declarative policies and negotiation to access sensitive resources on the semantic web. *In 1st European Semantic Web Symposium (ESWS 2004), Heraklion, Crete, Greece, Springer*, 3053 of Lecture Notes in Computer Science:342–356, may 2004.

[20] M. Y. Becker and P. Sewell. Cassandra: distributed access control policies with tunable expressiveness. *In 5th IEEE International Workshop on Policies for Distributed Systems and Networks, Yorktown Heights*, June 2004.

[21] P. A. Bonatti and D. Olmedilla. Driving and monitoring provisional trust negotiation with metapolicies. *In 6th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2005), Stockholm, Sweden, IEEE Computer Society*, pages 14–23, jun 2005.

[22] E. Damiani, S. D. C. di Vimercati, S. Paraboschi, P. Samarati, and F. Violante. A reputation-based approach for choosing reliable resources in peer-to-peer networks. *In Proceedings of ACM Conference on Computer and Communications Security*, page 202–216, 2002.

[23] S. Lee, R. Sherwood, and et al. Cooperative peer groups in nice. *IEEE Infocom, San Francisco, USA*, 2003.

[24] M. Gupta, P. Judge, and et al. A reputation system for peer-to-peer networks. *Thirteenth ACM International Workshop on Network and Operating Systems Support for Digital Audio and Video, Monterey, California.*, 2003.

[25] S. Kamvar, M. Schlosser, and et al. The eigentrust algorithm for reputation management in p2p networks. *WWW, Budapest, Hungary*, 2003.

[26] J. Sabater and C. Sierra. Regret: A reputation model for gregarious societies. *4th Workshop on Deception, Fraud and Trust in Agetn Societies, Montreal, Canada.*, 2001.

[27] J. Pujol, R. Sanguesa, and et al. Extracting reputation in multi agent systems by means of social network topology. *First International Joint Conference on Autonomous Agents and Multi-Agent Systems, Bologna, Italy.*, 2002.

[28] Milan Petkovic and Willem Jonker. *Security, Privacy and Trust in Modern Data Management (Data-Centric Systems and Applications).* Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007.

[29] A. George and J.W.H. Liu. *Computer Solution of Large Sparse Positive Definite Systems.* Prentice Hall, 1981.

[30] Vladimir Batagelj and Andrej Mrvar. Pajek analysis and visualization of large networks. *Proceedings Graph Drawing*, 41:477–478, 2002.

[31] R. Tarjan. Depth first search and linear graph algorithms. *SIAM Jurnal of Computing*, 1(2):146–160, June 1972.

[32] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein. *Introduction to Algorithms.* McGraw-Hill Book Company, Boston, MA, 2001.

[33] Esko Nuutila and Eljas Soisalon-Soininen. On finding the strongly connected components in a directed graph. *Information Processing Letters*, 49(1), 1994.

[34] S.C. Freeman and L.C. Freeman. The networkers network: A study of the impact of a new communications medium on sociometric structure. *Social Science Research Reports, Irvine, CA: University of California.*, 46, 1979.

Seznam publikovaných prací

[35] R. Špánek. Security in mobile environment. *Doktorandský den '04 - (Hakl, F.), MATFYZPRESS*, pages 149–155, 2004.

[36] R. Špánek. Sharing information in a large network of users. *Doktorandský den '05 - (Hakl, F.), MATFYZPRESS*, pages 134–140, 2005.

[37] R. Špánek. Data pozičně závislá a jejich dopad v mobilních databázích. *ITAT'2005, Information Technologies - Applications and Theory - (Vojtáš, P.)*, pages 273–278, 2005.

[38] R. Špánek. Web search engines and linear algebra. *ICS AS CR - (Technical Report, V-975)*, 2006.

[39] R. Špánek. Rollingball: Energy and qos aware protocol for wireless sensor networks. *SOFSEM 2006. Theory and Practice of Computer Science. Prague : Institute of Computer Science AS CR, 2006 - (Wiedermann, J.; Tel, G.; Pokorný, J.; Bieliková, M.; Štuller, J.)*, pages 166–173, 2006.

[40] R. Špánek and M. Tůma. Secure grid-based computing with social-network based trust management in the semantic web. *Neural Network World, International Journal on Neural and Mass-Parallel Computing and Information Systems*, 16(6):475–488, December 2006.

[41] R. Špánek. Security, privacy and trust in (semantic)web. *Inteligentní modely, algoritmy, metody a nástroje pro vytváření sémantického webu. Praha : Ústav informatiky AV ČR,(Štuller, J.; Linková, Z.)*, pages 114–122, 2006.

[42] R. Špánek. Security model based on virtual organizations for distributed environments. *Doktorandský den '06. Praha : Ústav informatiky AV ČR & MATFYZPRESS- (Hakl, F.)*, pages 164–171, 2006.

[43] R. Špánek and M. Tůma. Secure grid-based computing with social-network based trust management in the (semantic) web. *MoMM2006 & iiWAS2006, Frontiers in Mobile and Web Computing. Wien : Österreichische Computer Gesselschaft - (Barolli, L.; Abderazek, B.; Grill, T.; Nguyen, T.; Tjondronegoro, D.),Yogyakarta*, pages 663–667, 2006.

[44] R. Špánek and M. Tůma. Sdílení dat v prostředí s nehomogenními skupinami uživatelů. *Information Technologies - Applications and Theory. Košice : Prírodovedecká fakulta, Univerzita P. J. Šafárika, (Vojtáš, P.)*, pages 145–149, 2006.

[45] R. Špánek. Maintaining trust in large scale environments. *Doktorandské dny '07. Praha : Ústav informatiky AV ČR, v. v. i. & MATFYZPRESS,(Hakl, F.)*, pages 94–102, 2007.

[46] Martin Řimnáč, R. Špánek, and Zdeňka Linková. Sémantický web: vize globálního úložiště dat? *DATAKON 2007. Brno : Masaryk University, (Popelínský, L.; Výborný, O.)*, pages 176–186, 2007.

[47] Martin Řimnáč, R. Špánek, and Zdeňka Linková. Semantic web: Vision of distributed and trusted data environment? *ICDIM 2007, Lyon: INSA, 2007 - (Youakim Badr, Richard Chbeir, Pit Pichappan)*, pages 627–634, 2007.

[48] R. Špánek. Reputation system for large scale environment. *ICDIM 2007, Lyon: INSA, 2007 - (Youakim Badr, Richard Chbeir, Pit Pichappan)*, pages 627–634, 2007.

[49] R. Špánek and P. Kovář and P. Pirkl. The BlueGame Project: Ad-hoc Multilayer Mobile Game with Social Dimension. *CONEXT 2007, New York: Columbia University, 2007*

[50] R. Špánek, Martin Řimnáč, Zdeňka Linková. On Creating a Trusted and Distributed Data Source Environment. *SOFSEM 2008, Slovak Republic, Nový Smokovec, 2008.*

Annotation

Self-organizing and Self-monitoring Security Model for Dynamic Distributed Environments

Roman Špánek

The thesis deals with security hazards in distributed environments where traditional centralized approaches are only of limited serviceability. One of the very successful model for treating security and access management in distributed systems are so called reputation systems. The main goal of the reputation systems is to provide entities in the environment with mechanisms for inferring and building trust consequently used for access control. If the trust between two entities is high enough, transactions are likely to be allowed.

The thesis proposes a new security model with trust management system for dynamic and distributed environments with huge number of entities. In dynamic systems new entities or relationships are likely to emerge or existing entities or relationships may often disappear. Such dynamics pose severe problems for traditional reputation systems. Therefore our approach differs from the traditional ones in the way adopted for establishment and management of trust between entities – in our point of view trust is not assigned to particular relationships but the trust is common for a group of entities. In this way, our proposal significantly enhances ability to infer trust between entities with no previous personal experiences with each other.

As our proposal generalized understanding of trust, it uses an original hypergraph model for representation of entities. The security model proposed in the thesis contains algorithms for transformation of a general input graph structure into hypergraph model, an algorithm treating dynamics of the distributed environment and a security subsystem.

Our experimental implementation SecGrid is built on the proposed algorithms and it was used for experimental verification of the security models. The experiments investigate the ability of the transformation algorithms, the dynamic part of our proposal together and the security subsystem. Experiments showed that our model overcame the traditional graph model in many ways especially in dynamic environments with huge amount of entities.

Key Words: trust management systems, security, trust, distributed systems

Název:	Samostatně pracující bezpečnostní model pro dynamická distribuovaná prostředí
Autor:	Ing. Roman Špánek
Rozsah:	43 stran, 25 obrázků, 1 tabulka