УДК 004.42 DOI: 10.31673/2786-8362.2023.010505

Семенов О.В., аспірант, **Сєрих С.О.**, к.т.н.,
Василенко В.В., к.т.н., **Гніденко М.П.,** к.т.н.

МОДИФІКАЦІЯ МОДЕЛІ РЕПУТАЦІЇ ТА ДОВІРИ В ЗАДАЧАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ GRID-СИСТЕМ ДЛЯ СТІЙКОСТІ ДО ЗАГРОЗИ «ЗЛОВМИСНІ ГРУПИ ХОСТІВ»

Semenov O.V., Sierykh S.A., Vasylenko V.V., Hnidenko M.P. Modification of the reputation and trust model in the tasks of information security of grid systems for resistance to the threat of "malicious host groups"

In Grid-systems, the key idea is the joint use of resources, therefore there is a need for mutual trust between users and resource providers. In small grid systems, all participants are in a relationship of complete trust. For example, in the Ukrainian Academic Grid segment, all participants belong to the National Academy of Sciences of Ukraine, and on this basis there is complete trust. But in larger Grid-systems, participants may often not be directly connected to each other, and there is a risk that one of the participants will turn out to be unscrupulous and malicious. Trust mechanisms are designed to reduce these risks. The main purpose of security mechanisms is to provide protection against malicious users and groups of persons. Traditional security methods usually protect resources from malicious influences by restricting access to authorized users. However, in most cases there is a need to protect the system and its components from those who provide resources and services within heterogeneous computing systems. Thus, there are a large number of problems in the field of security that cannot be solved within the framework of traditional approaches. Information providers can, for example, commit fraud by providing false and unreliable information, and traditional security mechanisms are unable to protect against this type of threat. On the other hand, systems of reputation and trust can provide protection against these risks. The distinction between these two approaches to information security was first described by Rasmussen and Jansson (1996), who used the term hard security to refer to traditional mechanisms such as authentication and access control, and the term soft security to refer to what they called public control mechanisms. in general, exemplified by reputation and trust systems.

Keywords: reputation and trust models, Grid-systems, the threat of "malicious host groups"

Семенов О.В., Сєрих С.О., Василенко В.В., Гніденко М.П. Модифікація моделі репутації та довіри в задачах інформаційної безпеки grid-систем для стійкості до загрози «зловмисні групи хостів»

З розвитком електронної комерції в Інтернет довірі стали приділяти підвищену увагу. Клієнти повинні довіряти продавцю, оскільки передають йому особисті дані, а продавець повинен довіряти клієнтові для того, щоб надавати йому свої послуги. В Grid-системах ключовою ідеєю є спільне використання ресурсів, тому виникає необхідність у взаємній довірі користувачів і постачальників ресурсів. В Grid-системах невеликого розміру всі учасники знаходяться у відношенні повної довіри. Наприклад, в Українському Академічному Grid-сегменті всі учасники належать до НАН України, і на цій підставі виникає повна довіра. Але в більш масштабних Grid-системах учасники найчастіше можуть бути безпосередньо не пов'язані один з одним, і існує ризик того, що хто-то з учасників виявиться недобросовісним і зловмисним. Зменшити ці ризики і покликані механізми довіри.

Ключові слова: моделі репутації та довіри, Grid-системи, загроза «зловмисні групи хостів»

Вступ

Головною метою механізмів безпеки є надання захисту від зловмисних користувачів та груп осіб. Традиційні методи безпеки зазвичай захищають ресурси від шкідливих впливів за допомогою обмеження доступу авторизованих користувачів. Проте, в більшості випадків існує необхідність захищати систему та її компоненти від тих, хто надає ресурси та послуги всередині гетерогенних обчислювальних систем. Таким чином, виникає велика кількість задач у сфері безпеки, які не вирішується в рамках традиційних підходів. Постачальники інформації можуть, наприклад, шахраювати шляхом надання неправдивої та недостовірної інформації, а традиційні механізми безпеки не в змозі захистити від такого типу загроз. З іншого боку, системи репутації та довіри, можуть забезпечити захист від цих ризиків. Різниця між цими двома підходами захисту інформації була вперше описана Расмуссеном та Янссоном (1996),

які застосовували термін жорстка безпека для таких традиційних механізмів, як автентифікація та управління доступом, і термін м'яка безпека – для позначення того, що вони називали механізмами громадського контролю в цілому, прикладом яких слугують системи репутації та довіри.

Модель репутації заснована на функції корисності, яка визначає рівень задоволеності користувача наданим сервісом. Для визначення функції корисності вводиться допоміжна функція узгоджена між користувачем ВО і постачальником ресурсів, яка показує заздалегідь обумовлений якість послуг (The service level agreement (SLA)) [16].

$$SLA\colon \cup_i\ u_i \times \cup_k r_k \times \cup_m VO_m \to R$$

Значення SLA показує, яка якість послуг очікує отримати користувач [16]. Метрики якість послуг (QoS), які можуть бути використані для визначення рівня задоволеності описані в [17, 18]. У деяких статтях також описуються механізми обчислення та управління якістю послуг QoS [19].

Подія - це:

$$Event = \cup_i\ u_i \times \cup_k r_k \times \cup_m VO_m \times \{QoS\ Name\} \times R$$

де T представляє часовий інтервал. Отже, подія характеризується

$$\{t, u, r, vo\_id, Qos, v\}$$

де t показує час, QoS показує бажаний рівень якості обслуговування, а v реальне значення QoS певне системою моніторингу в Grid після взаємодії користувача і ресурсу.

$$Trace = \cup_p Event_p = \cup_p \{t, u, r, vo\_id, QoS, v\}_p \quad (1)$$

Перед визначенням репутації і функції корисності вашій увазі пропонується три функції: перша буде характеризувати можливість змови користувача і ресурсу з метою уникнення шахрайства, друга буде враховувати час, коли була оцінена корисність, і третя буде надавати різні значення в залежності від типу сервісу, що надається. Ці функції забезпечують розширення для репутації функції корисності спочатку представленої в [16].

Функція z(t, t_c) буде показувати які попередні записи про взаємодію користувачів з ресурсами потрібно взяти до уваги для оцінки репутації конкретного ресурсу. Де t це час, а t_c -параметр. У найпростішому випадку z(t, tc) може бути ступінчастою функцією:

$$z(t, t_c) = \{1, t \geq t_c\ 0, t < t_c$$

Функція s (r) буде забезпечувати різні значення для різних типів сервісів, які надає ресурс r (функція вказує на категорію сервісу). Тепер можна визначити функцію корисності (згідно [11, 12, 13, 14, 15]).

$$utility\colon Event \to R \quad (2)$$

$utility\colon \{t, u, r, vo\_id, Qos, v\} = \{s(r), if\ v \geq SLA(u, r, vo\_id)\ \frac{v}{SLA(u,r,vo\_id)} s(r), if v <$ $SLA(u, r, vo\_id)$ Варто відзначити набір слідів (1), які використовуються для оцінки репутації ресурсу r у віртуальній організації з ідентифікатором vo_id до поточного часу t з:

$$Trace\ |_{(vo\_id,r,t)=\{t',u',r',vo'_{id},QoS',v'\}\ \epsilon\ Trace}\colon r = r', vo\_id = vo\_id', t' \leq t$$

Репутація – це математичне сподівання функції корисності utility (2) (в термінах теорії ймовірностей)

$$rep(vo\_id, r, t) = E\left[utility\left(O_{(vo_{id},r,t)}\right)\right] = \int \quad utility\left(O_{(vo\_id,r,t)}\right) P_{utility}\left(O_{(vo_{id},r,t)}\right) dO_{(vo_{id},r,t)}$$

Для того щоб розрізняти значення функції корисності за часом буде використовуватися:

$$z(t, t_c)\ =\ 1$$

Для апроксимації очікування можна використовувати вибіркове середнє [18]:

$$rep(vo\_id, r, t) = \frac{1}{|O_{(vo_{id},r,t)}|} \sum_{x \in O_{(vo\_id,r,t)}} \quad x$$

Репутація організації в віртуальної організації - це агрегація репутації всіх ресурсів, які вона надає для використання у віртуальній організації.

$$rep(vo\_id,t)=\frac{1}{|f_{vo_{id}}{}^{-1}(o\_id)|}\sum_{r\in f_{vo_{id}}{}^{-1}(o\_id)} r$$

Репутація ресурсу в усіх ВО можна обчислити таким чином [19]

$$rep(r,t)=\frac{1}{|VO|_r|}\sum_{vo\_id\in VO|_r} rep(vo_{id},r,t) \quad (3)$$

Із опису моделі [16] зрозуміло, що вона не є стійкою до загрози «Групи шкідливих хостів». Тому постає задача модифікувати модель таким чином, щоб вона стала стійкою до даної загрози

Опис загрози «зловмисні групи хостів». Найчастіше шкідливі користувачі надають погане обслуговування у % тих випадків, коли вони є провайдерами послуг. Небезпечні особи утворюють колективи за допомогою надання максимальної довіри іншим зловмисним учасникам мережі (Рис.1).

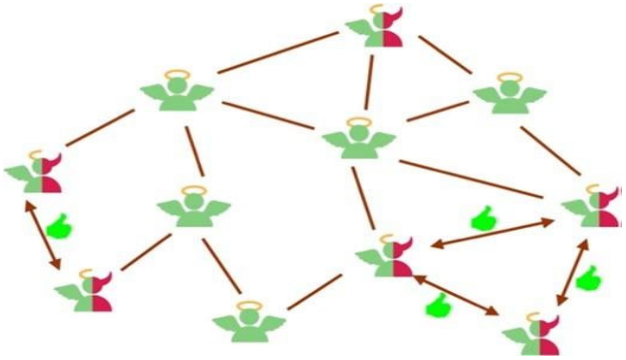

Рис. 1. Групи зловмисних хостів із маскуванням

Це, у багатьох випадках, загроза, від якої не вдається захиститися легко, оскільки її стійкість багато в чому залежить від поведінки шкідливих учасників. Тобто, вона не буде схожою на поведінку з коливаннями (з повністю доброзичливої для якогось певного періоду часу вона змінюється на повністю шахрайську для наступний періоду), також, наприклад, на поведінку збільшення і зменшення, або навіть на випадкову модель поведінки.

Крім того, така мінлива поведінка навіть не розглядається як загроза і не карається, а система безпеки намагається налагодити довіру та репутацію до цього користувача.

Аналіз останніх досліджень і публікацій.

На сьогоднішній день вже існує безліч концепцій довіри і їх реалізацій [1, 2, 3, 4, 5, 6]. В роботі [7] показано, що довіра - це високоефективна технологія, і її впровадження дозволить убезпечити електронні транзакції. При цьому довіру описується як важливий і складний предмет, пов'язаний з чесністю, правдивістю і надійністю довіреної особи або сервісу. Однак єдиної формулювання поняття довіри так і не досягнуто [8]. Наведемо основні два визначення довіри.

Коли ми говоримо, що довіряємо кому-то чи що хто-то заслуговує довіри, то ми неявно маємо на увазі, що ймовірність виконання дії, що буде корисною або як мінімум не завдасть шкоди нам, є достатньо високою, щоб вступити з ним у певні відносини [9].

В роботі [10] довіра визначається як межа, до якого одна сторона хоче покладатися в певній ситуації на когось або щось з відчуття відносної безпеки, навіть якщо можливі негативні наслідки.

Існуючі публікації лише поверхнево торкаються до загрози «зловмисні групи хостів» та не пропонують способів набуття стійкості до даної загрози.

Мета статті.

Мета даної статті полягає в модифікації моделі репутації та довіри для забезпечення стійкості до загрози "зловмисні групи хостів". Пропонується внести зміни в функцію

корисності для врахування штрафу для хостів з певної групи, які надавали послуги поганої якості, але отримували від інших членів групи високі оцінки, щоб бути обраними провайдерами послуги іншими хостами. Основна ціль включає формальний опис модифікованої функції корисності та функції штрафу, а також перевірку модифікації за допомогою спеціально написаної програми, що імітує її використання системою моніторингу для різних ситуацій. Вони включають перевірку на хибнопозитивний результат, ситуацію, коли присутня конкретна зловмисна група хостів, а також ситуацію, коли існує певна кількість учасників, що за зовнішніми ознаками задовольняє шаблон групи зловмисних хостів і може бути віднесена системою моніторингу до такої групи.

Результати даного дослідження мають потенційне використання в реальних сценаріях обчислень у системах Grid, де питання безпеки та довіри відіграють ключову роль.

1. Пропозиції щодо модифікації моделі для набуття стійкості до загрози «зловмисні групи хостів»

Із формального опису моделі зрозуміло, що вона не є стійкою до загрози «Групи шкідливих хостів». Для надбання стійкості модифікуємо функцію корисності *utility*.

Нехай підмножина множина $VO_G \subseteq VO_m$ - множина шкідливих хостів/віртаульних організацій, елементи якої завжди надають обслуговування низької якості, якщо вони є постачальниками послуг. Зловмисні хости/віртуальні оргаізації утворюють небезпечні колективи шляхом надання максимальної довіри іншим шкідливим особам цієї ж мережі і не користуються послугами інших хостів взагалі, тобто оцінюють тільки учасників своєї групи.

Введемо функцію, що буде використовуватися для отримання усіх оцінок, що були надані хосту/віртуальній організації

$$M: VO \to M_v$$
$$VO \in VO_m$$

M_v - множина оцінок послуг наданих віртаульною організацією.

Введемо функцію M^o, що дозволить отримати оцінки послуг, які були надані данною віртуальною організацією іншим:

$$M^o: \overrightarrow{VO, VO_2} \to M_v^o$$
$$VO_2 \in VO_m$$

Де VO_2 - організація, якій була надана оцінка, M_v^o - множина оцінок наданих організацією VO організації VO_2.

Введемо функцію $EM(VO)$, що є множиною усіх віртуальних організацій, яким була надана оцінка віртуальною організацією VO.

$$EM(VO) = \{y \mid M^o(VO, y) \neq \emptyset\}$$

Таким чином, щоб з'ясувати, чи належить дана віртуальна організація до шкідливою групи достатньо дізнатися:

1) Які оцінки отримувала вона за свої послуги
2) Які оцінки надавала іншим віртуальним оранізаціям за отримані послуги.

Нагадаємо, що шаблон, по якому можна викрити групу шкідливих організацій наступний: члени групи надають неякісні послуги(а отже і отримують низькі оцінки), а також завжди надають одне одному високі оцінки для того, щоб вони могли бути обраними в якості провайдера послуг іншими учасниками.

На рис. 2 червоні елементи – члени зловмисної групи, що надають одне одному хорошу оцінку(g), зелені елементи – решта учасників, що надають зловмисним елементам негативну оцінку(b).

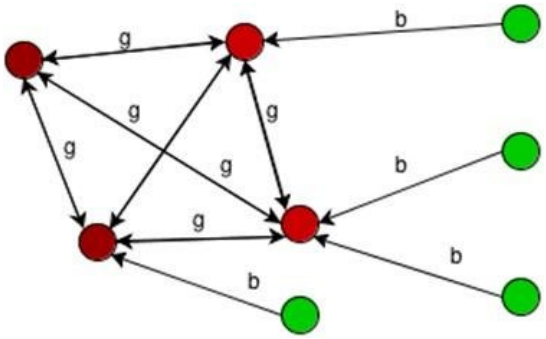

Рис. 2. Шкідлива група віртуальних організацій

Для того, щоб система моніторингу (СМ) змогла визначити з якою ймовірністю дана віртуальна організація належить до шкідливої групи, СМ повинна знайти усі оцінки отримані данною ВО та оцінки, які надавала ця ВО іншим та оцінки, що були отримані цими ВО від третіх учасників.

Нехай треба визначити, чи належить дана віртуальна організація *v* до шкідливої групи хостів.

$M(v) = \{m_1, m_2, \dots m_n\}$ – оцінки, що були надані ВО *v*

$$AM_v = \frac{\sum_{x \in M_v} x}{|M_v|}$$

AM_v – середня оцінка, що надана учаснику *v*

$$AM_v^o = \frac{\sum_{x \in M_v^o} x}{|M_v^o|}$$

AM_v^o – середня оцінка, що надана учасником *v* іншим

Таким чином, якщо $AM_v > AM_v^o$, тобто ця ситуація підпадає під шаблон шкідливих групп, ми маємо перевірити, чи можна нарахувати штраф.

Нехай $EM(v) = \{v_1, v_2, \dots v_n\} = Y^v$ – учасники, яким була надана оцінка від ВО *v*

$\forall y \in Y^v$:

$M(y) = R_y$ - множина оцінок, що надані *y* іншими учасниками

$M^o(v, y) = R_{v,y}$ - множина оцінок, що надавала *v y*

$$AR_y = \frac{\sum_{x \in R_y} x}{|R_y|}$$

AR_y - середня оцінка y від інших учасників

$$AR_{v,y} = \frac{\sum_{x \in R_{v,y}} x}{|R_{v,y}|}$$

$AR_{v,y}$ - середня оцінка y іншим учасникам

Визначимо функцію вибору штрафу:

$$ps(AR_y, AR_{v,y}) = \{0, \text{якщо } AR_{v,y} - AR_y \le 0\ AR_{v,y} - AR_y \text{ інакше}$$

Таким чином, якщо оцінка що була надана іншим елементам – нижча, ніж та, яку отримав учасник *y* від інших, то штраф рівний нулю, адже цей випадок не підпадає під шаблон шкідливих групп.

Сам штраф обчислюється наступним чином:

$$penalty(v) = \frac{\sum_{y \in Y^v} ps(AR_y, AR_{v,y})}{|Y^v|} \quad (4)$$

Модифікована функція корисності (2) матиме вигляд:

$$utility: \{t, u, r, vo\_id, Qos, v\} = \{s(r), if\ v \ge SLA(u, r, vo\_id)\ \frac{v}{SLA(u, r, vo\_id)} s(r)\ -\ penalty(vo_{id}),$$
$$if v < SLA(u, r, vo\_id)$$

2. Перевірка модифікації та функції штрафу

Для перевірки правильності функції штрафу (4) була написана программа, що імітує її використання системою моніторингу для декількох різних ситуацій.

Перша ситуація – існує конкретна шкідлива группа, постала задача перевірити, які штрафи отримає кожен учасник.

Вхідні дані:

Таблиця 1 – Вхідні параметри задачі

Параметр	*Значення*
Кількість учасників в системі	4
Сформована шкідлива группа	*Так*
Кількість учасників шкідливої групи	3
Початкові значення для:	
AM_v	v1: 0.2, v2: 0.12, v3: 0.3, v4: 0.8
AM_v^o	v1: 0.85, v2: 0.9, v3: 0.7, v4: 0.7

Так як для перших трьох учасників $AM^o_v > AM_v$, то вони входять до зловмисної групи.

Граф взаємодій:

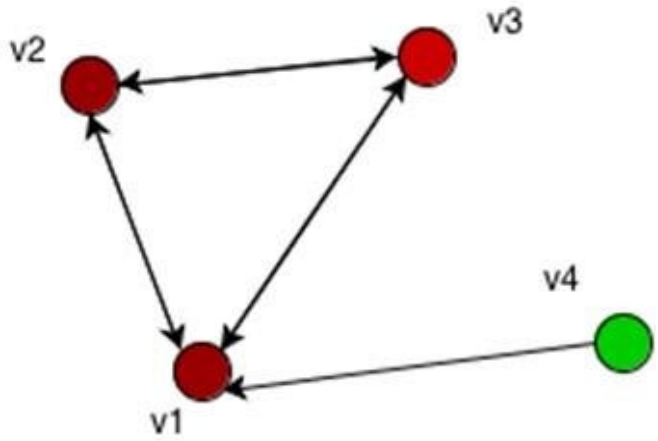

Рис. 3. Шкідлива група

Напрям стрілки означає «надавала оцінку». Учасник від якого виходить стрілка надає оцінку тому учаснику, на кого стрілка вказує.

Вихідні данні:

Таблиця 2 – Вхідні параметри задачі

Ім'я учасника	*Значення штрафу*
v1	0.59
v2	0.524
v3	0.715
v4	0

Функція штрафу визначила корректні значення штрафу для перших трьох учасників, що згідно із вхідними данними належали до зловмисної групи. Учасник із ім'ям v4 не отримав штрафу, що також э корректним результатом, адже вын не входить до зловмисної групи.

Друга ситуація – шкідливої група відсутня, постала задача перевірити функцію штрафу на хибнопозитивний результат.

Вхідні дані:

Таблиця 3 – Вхідні параметри задачі

Параметр	*Значення*
Кількість учасників в системі	4
Сформована шкідлива группа	*Ні*
Кількість учасників шкідливої групи	3
Початкові значення для:	
AM_v	v1: 0.9, v2: 0.12, v3: 0.6, v4: 0.7
AM_v^o	v1: 0.85, v2: 0.9, v3: 0.65, v4: 0.7

Граф взаємодій:

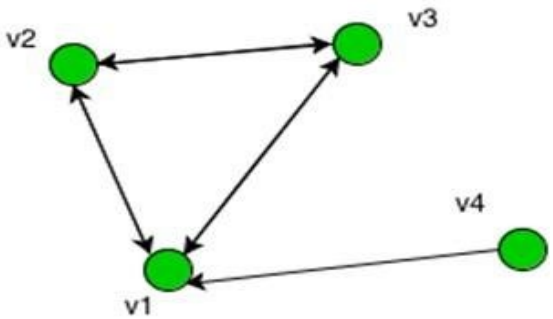

Рис. 4. Шкідлива група відсутня

Вихідні данні:

Таблиця 4 – Вхідні параметри задачі

Ім'я учасника	*Значення штрафу*
v1	0
v2	0
v3	0
v4	0

Функція штрафу коректно визначила значення штрафу для усіх учасників, адже жоден із них не є членом шкідливої групи.

Третя ситуація – існує певна кількість учасників, що за зовнішніми ознаками задовольняє шаблон групи зловмисних хостів і може бути віднесена системою моніторингу до такої групи.

Вхідні дані:

Таблиця 5 – Вхідні параметри задачі

Параметр	*Значення*
Кількість учасників в системі	4
Сформована шкідлива група	*Ні*
Кількість учасників шкідливої групи	3
Початкові значення для:	
AM_v	v1: 0.2, v2: 0.15, v3: 0.3, v4: 0.8
AM_v^o	v1: 0.85, v2: 0.9, v3: 0.7, v4: 0.7
Оцінка, що надалі надається кожним учасником:	0.5
Оцінка, що надалі надається кожному учасником:	0.55

Граф взаємодій:

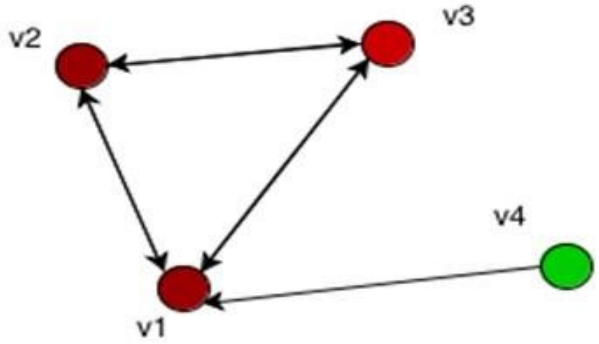

Рис. 5. Учасники v1, v2 та v3 можуть бути членами шкідливої групи

Функція штрафу надала правильні значення першим трьом учасникам, адже вони підозрілі на шкідливе угруповання. Нехай, кожен із цих трьох учасників надаватиме гарний сервіс і отримуватиме добрі оцінки надалі. Тоді, значення функції штрафу має залежати від подальших оцінок, які будуть отримані цими учасниками та надані їми. У випадку, якщо надалі учасники не демонстрували поведінку, що притаманна шкідливій групі вузлів, штраф, що має бути наданим їм має зменшуватися, аж поки не стане рівним нулеві.

Симуляція із використанням програми дала наступні результати:

Таблиця 6 – Вхідні параметри задачі

Ім'я учасника	*Значення штрафу*
Ітерація №1	
v1	0.575
v2	0.524
v3	0.7
v4	0
Ітерація №2	
v1	0.262
v2	0.2375
v3	0.3249
v4	0
Ітерація №3	
v1	0.158
v2	0.141
v3	0.199
v4	0
Ітерація №4	
v1	0.106
v2	0.093
v3	0.137
v4	0
Ітерація №5	
v1	0.0749
v2	0.065
v3	0.09
v4	0
Ітерація №6	
v1	0.054

Ім'я учасника	*Значення штрафу*
v2	0.045
v3	0.074
v4	0
Ітерація №7	
v1	0.039
v2	0.032
v3	0.052
v4	0
Ітерація №8	
v1	0.028
v2	0.021
v3	0.043
v4	0
Ітерація №9	
v1	0.019
v2	0.013
v3	0.033
v4	0
Ітерація №10	
v1	0.015
v2	0.010
v3	0
v4	0
Ітерація №11	
v1	0.011
v2	0.068
v3	0
v4	0
Ітерація №12	
v1	0.008
v2	0.004
v3	0
v4	0
Ітерація №13	
v1	0.005
v2	0.001
v3	0
v4	0
Ітерація №14	
v1	0.003
Ім'я учасника	*Значення штрафу*
v2	0
v3	0
v4	0
Ітерація №15	
v1	0

v2	0
v3	0
v4	0

Як видно із таблиці, на п’ятнадцятому кроці функція штрафу надала усім учасникам значення 0, що були підозрілі на шкідливу групу, але надалі поводили себе таким чином, не підпадали під шаблон шкідливої групи.

Функція штрафу надала коректні значення протягом усіх ітерацій, адже на кожній значення штрафу зменшувалось.

Висновки

Була розроблена модифікація моделі репутації на основі функції корисності, що стійка до загрози «Групи шкідливих учасників». Дано формальний опис модифікації моделі. Практична цінність полягає у отриманні модифікованої моделі що може бути використана як у Grid-системах так і будь-яких інших гетерогенних обчислювальних системах.

Список використаної літератури:

1. Foster I., Kesselman C., Tuecke S. The Anatomy of the Grid: Enabling Scalable Virtual Organizations // International Journal of Supercomputing Applications, 15(3), 2001. – p. 200-222

2. Castelfranchi C., Falcone R., Sadighi B., Tain Y.-H. Guest Editorial. Applied Artificial Intelligence, 14(9), 2000, Taylor & Frances,.

3. Waidner M.. Ercim News, Special Theme: Information Security. No 49, 2002.

4. Nixon P., Terzis S. First International Conference on Trust Management // Lecture Notes in Computer Science, vol. 2692, Springer, 2003.

5. Jensen C.D., Poslad S., Dimitrakos T. Second International Conference on Trust Management // Lecture Notes in Computer Science, vol. 2995, Springer,

6. Hermann P., Issarny V., Shue S. Third International Conference on Trust Management // Lecture Notes in Computer Science, vol. 3477, Springer, 2005..

7. Grandison T., Sloman M. A Survey of Trust in Internet Applications // IEEE Communications Survey and Tutorials, 3, 2000.

8. McKnight D.H., Chervany N.L. The Meaning of Trust // Technical Report MISRC Working Paper Series 96-04, University of Minnesota. Management Information Systems Research Center, 1996.

9. Gambetta D. Can We Trust Trust? In D. Gambetta (editor). Trust: Making and Breaking Cooperative Relations. Department of Sociology, Univ. of Oxford, 1988.

10. Josang A., Ismail R., Boyd C. A Survey of Trust and Reputation Systems for Online Service Provision // Decision Support Systems, 43(2), 2007. – p. 618-644,.

11. Rasmusson L., Janssen S. Simulated Social Control for Secure Internet Commerce // In C. Meadows. Proceedings of the 1996 New Security ParadigmsWorkshop. ACM.

12. CoreGrid. D.ia.03 survey material on trust and security. Technical Report D.IA.03, Core Grid, October 2005. http://www.coregrid.net/mambo/images/stories /IntegrationActivities/TrustandSecurity/d.ia.03.pdf

13. Abdul-Rahman A., Hailes S. Supporting trust in virtual communities // In HICSS ’00: Proceedings of the 33rd Hawaii International Conference on System Sciences-Volume 6, page 6007, Washington, DC, USA, 2000. IEEE Computer Society.

14. Kerschbaum F., et al. A trust-based reputation service for virtual organization formation. In Proceedings of the 4th International Conference on Trust Management, vol. 3986 of Lecture Notes in Computer Science, pp. 193–205. Springer, 2006.

15. Luke T.W.T., Jennings N.R., Rogers, Luck M. A Hierarchical Bayesian Trust Model based on Reputation and Group Behaviour // 6th European Workshop on Multi-Agent Systems, 18th-19th December, 2008, Bath, UK.

16. Arenas A.E., Aziz B., Silaghi G.C. Reputation Management in Grid-Based Virtual Organisations // Proc. International Conference on Security and Cryptography (SECRYPT 2008), Porto, Portugal, 26-29 Jul 2008, INSTICC.

17. Menasce D.A., Casalicchio E. Quality of service aspects and metrics in Grid computing // In: Proc. 2004 Computer Measurement Group Conference, Las Vegas, USA, 2004.

18. Hong-Linh T., Samborski R., Fahringer T. Towards a Framework for Monitoring and Analyzing QoS Metrics of Grid Services // In: Proc. Second IEEE Int Conf on e-Science and Grid Computing (e-Science'06), 2006.

19. Al-Ali R., von Laszewski G., Amin K., Hategan M., Rana O., Walker D., Zaluzec N. QoS Support for High-Performance Scientific Grid Applications // In: Proc. IEEE International Symposium on Cluster Computing and the Grid 2004. (CCGrid 2004). – p. 134–143.

Автори статті

Семенов Олександр – апірант , Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

Сєрих Сергій – кандидат технічних наук, доцент, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

Василенко Володимир – кандидат технічних наук, доцент, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

Гніденко Микола – кандидат технічних наук, доцент, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

Authors of the article

Semenov Oleksandr – postgraduate, State University of Information and Communication Technologies, Kyiv, Ukraine.

Sierykh Sergiy – Candidate of Science (technic), Associate Professor, State University of Information and Communication Technologies, Kyiv, Ukraine.

Vasylenko Volodymyr - Candidate of Science (technic), associate professor**,** State University of Information and Communication Technologies, Kyiv, Ukraine.

Hnidenko Mykola - Candidate of science (technic), associate professor, State University of Information and Communication Technologies, Kyiv, Ukraine.