МИНИСТЕРСТВО НА ОБРАЗОВАНИЕТО И НАУКАТА

УНИВЕРСИТЕТ „ПРОФ. Д-Р АСЕН ЗЛАТАРОВ“ - БУРГАС

Борис Иванов Бозвелиев

Обобщеномрежови модели на Data Mining техники, свързани с реални процеси

АВТОРЕФЕРАТ

На дисертационен труд за присъждане на образователна и научна степен „доктор” по докторска програма „Компютърни системи и технологии”, Област на висшето образование 5. Технически науки, Професионално направление 5.3. Комуникационна и компютърна техника

Научни ръководители

чл.-кор. проф. дмн дтн Красимир Т. Атанасов

проф. д-р инж. Станислав Денчев Симеонов

Бургас

2021

Представеният дисертационен труд беше обсъден на разширен катедрен съвет на катедра „Компютърни системи и технологии“, в Университет „Проф. д-р Асен Златаров“ - Бургас, на заседание, състояло се на 15.09.2021 г. и е насрочен за разкриване на процедура за защита пред научно жури със заповед УД-…../…….г. на Ректора на Университет „Проф. д-р Асен Златаров“ – Бургас.

Дисертационният труд съдържа 127 страници, от които 37 фигури и са използвани 166 литературни източника. Резултатите са публикувани в 5 статии.

Защитата на дисертационния труд ще се състои на от ……. часа в зала ….., Университет „Проф. д-р Асен Златаров“ – гр. Бургас.

Материалите по защитата са предоставени за заинтересованите в деловодството на Университет „Проф. д-р Асен Златаров“-Бургас.

Автор: Борис Иванов Бозвелиев
Заглавие: Обобщеномрежови модели на
Data Mining-техники, свързани с реални процеси

Изказвам искрената си благодарност на моите научни ръководители – чл.-кор. проф. дмн дтн Красимир Атанасов и проф. д-р инж. Станислав Денчев Симеонов *за споделените знания и опит, ценните им съвети и препоръки по време на изготвянето на този дисертационен труд.*

Благодаря също на всички мои колеги от катедра „Компютърни системи и технологии“, както и на моето семейство за безусловната подкрепа.

Увод

През последното десетилетие делът на интернет потреблението нарасна драстично. Това се случва във връзка с икономическото състояние на световно ниво както и други допълнителни фактори. През световната интернет мрежа преминава почти всичко, телефонни, видео разговори, др. онлайн приложения, социални мрежи, намиране на информация за стоки и услуги, изпращане и получаване на имейли и много други. Много важен аспект от всичко това са онлайн разплащанията и по точно специализираните портали "Payment Gateways", които са отговорни за цялостните транзакции от началната заявка на онлайн покупка на потребителя до финализирането на разплащането. И точно тук в тази област възникват доста неизвестни, бъгове и др. които имат нужда от специално изследване и усъвършенстване.

Друг важен аспект в днешно време е реализацията на така наречените умни къщи или "Smart House", тяхното цялостно управление и възможности които носят те със себе си за потребителите. Тук изключително важен момент е тяхната защита от външна намеса.

И не на последно място в последните няколко години все повече взеха да навлизат така наречените безпилотни летателни апарати или дронове "UAV" както също ги наричат. Те се използват в много сфери: военни за мисии, за заснемане на снимкови и видео материали, за спасителни мисии и др.. Така че в огромна степен тези устройства могат да бъдат както много полезни, също така могат да представляват и опасност за хората. Точно поради това, един много важен аспект от тяхното управление е защитата на комуникацията между управляващият и безпилотното летателно устройство. В този дисертационен труд ще използваме обобщеномрежови модели на Data Mining техники чрез които ще изследваме тези реални процеси които посочихме по горе.

Цел и задачи на дисертационния труд

Основната цел на настоящия дисертационен труд е да се изследват различни реални процеси чрез (Data Mining) техники и с помощта на обобщеномрежови модели. За да се постигне тази цел, са поставени следните задачи:

1. Разработване на обобщеномрежови модел на стандартен интернет портал за електронно разплащане с помощта на интуционистки размити оценки.
2. Програмна симулация на реалните процеси на стандартен интернет портал за електронно разплащане чрез софтуер GN IDE с помощта на интуционистки размити оценки.
3. Разработване на обобщеномрежови модел на протичането на реалният разплащателен процес.
4. Намиране на алтернативен метод за оценка на риска от кибер-атаки върху управлението на "Smart House" с помощта на интуционистки размити оценки.
5. Реализиране на нов подход за оценка на риска от кибер-вмешателство върху дронове чрез използването на интуционистки размити оценки.
6. Разработка на обобщено мрежови модел на възможно кибер-посегателство върху управлението на комуникацията на дрон чрез използването на интуционистки размити оценки.

В текста с [n*] са означени статиите на автора, включени в дисертационния труд.

1. Въведение в обобщените мрежи и Data Mining-техники свързани с реални процеси.

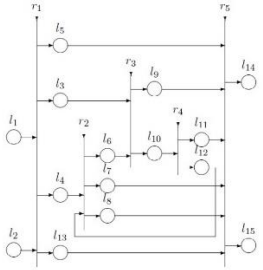
В тази глава са дадени основни дефиниции, които са необходими за изложението по-нататък, свързани с теорията на обобщените мрежи и на Data Mining-техники свързани с реални процеси.

1.1. Въведение в теорията на обобщените мрежи

Обобщените мрежи представляват значително разширение и обобщение на понятието мрежи на Петри, както и на други разширения и модификации на мрежи на Петри.

Обобщената мрежа е изградена от преходи (transitions). Преходът в контекста на обобщените мрежи е обект от статичната структура на мрежата, който съдържа условията за преминаването на ядра (token) от входните в изходните му позиции (places), след като преходът се е активирал. От позиция или в позиция на прехода може да излиза или съответно да влиза не повече от една дъга. Позиция, от която излиза дъга се нарича входна за прехода, а позиция, в която влиза дъга се нарича изходна за прехода. Всеки преход в ОМ има поне една входна и поне една изходна позиция. Входна позиция, в която не влиза дъга се нарича вход на мрежата, а изходна позиция, от която не излиза дъга – изход на мрежата. В позициите може да има ядра. Те се преместват от входните към съответните изходни позиции на преходите. Когато настъпи определения за прехода момент от време, и във входните позиции има достатъчен брой ядра, то ядрата от входните позиции придобиват възможност да се придвижат до изходните позиции. Този процес се нарича активиране на прехода. В началото ядрата, които постъпват в мрежата през входните й позиции имат т.нар. начални характеристики. При всяко преминаване през преход в мрежата те получават нови характеристики и така всяко ядро в мрежата е уникално и има своя история. Всяка позиция има свой капацитет.

Пример за ОМ е Фиг. 1.1.1, позиции l_1, l_2 са входни, а позиции l_{14} и l_{15} – изходни. Обикновено, входните позиции стоят вляво от прехода, а изходните – вдясно.



Фиг. 1.1.1 Обобщена мрежа с преход

1.1.2 Видове обобщени мрежи

Чрез отстраняване или добавяне на различни компоненти в описанието на обобщената мрежа се получават модификации на обобщената мрежа**.**

- *Редуцирани обобщени мрежи*, например ето как изглежда такава мрежа:

$$E' = <A', K, X, \Phi>,$$

- *Интуиционистки размити ОМ от тип 1* – като условия на преходите могат да бъдат задавани стойности в множеството [0, 1] със степен на вярност $\mu(r_{i,j})$ и степен на невярност $\nu(r_{i,j})$, за които е в сила $\mu(r_{i,j}) + \nu(r_{i,j}) \leq 1$;
- *Интуиционистки размити ОМ от тип 2* – това са *Интуиционистки размити ОМ от тип 1*, но с тази разлика, че вместо ядра имат „течности", протичащи по дъгите на мрежата и събиращи се в позициите й;
- *Интуиционистки размити ОМ от тип 3* – като *Интуиционистки размити ОМ от тип 1*, но с допълнението, че функцията Φ дава на всяко ядро като текуща характеристика две стойности: първата съвпада с характеристиката на ядрото в смисъла на ОМ, а втората е наредена двойка от множеството [0, 1], която е равна на вярностната стойност на предиката, който е пропуснал ядрото в текущата позиция;
- *Интуиционистки ОМ от тип 4* – това са *Интуиционистки размити ОМ от тип 3*, но с тази разлика, че вместо ядра имат „течности", протичащи по дъгите на мрежата и събиращи се в позициите й;
- Съществуват и други видове ОМ като: *ОМ с*

оптимизационни компоненти, ОМ със сложен тип на преходите, ОМ с условия за спиране, ОМ с ядра, които могат да приемат променливи за характеристики, Обратни ОМ, ОМ с ядра с време на живот, ОМ с множество дъги, ОМ с ядра с обеми, ОМ с характеристики на позициите.

1.1.3. Интуиционистки размити ОМ

Интуиционистки размити ОМ от първи тип

Очевидно, всяка РОМ 1 е и ИРОМ1. Всяка ИРОМ1 има вида

$E = \langle\langle A, \pi_A, \pi_L, c, f, \theta_1, \theta_2\rangle, \langle K, \pi_K, \theta_K\rangle, \langle T, t^0, t^*\rangle, \langle X, \Phi, b\rangle\rangle$,

където елементите на множеството A (преходите на ИРОМ1) имат същия вид, както и преходите на ОМ. Всички други компоненти в двете мрежи съвпадат с изключение на функции f и Ф. Сега функция Ф съпоставя на всяко ядро двойка характеристики - характеристиката, която би получило ядрото в стандартната ОМ, и наредената двойка реални числа от интервал [0, 1], които съответстват на степените на вярност и на невярност на предиката, съответстващ на позицията, в която е било ядрото преди прехода и на позицията, в която то е влязло и където получава характеристиката. Следователно, функция f за предикат r_i, има стойност:

$$f(r_{i,j}) = \langle \mu(r_{i,j}), \nu(r_{i,j})\rangle,$$

където $\mu(r_{i,j})$ и $\nu(r_{i,j})$ са посочените по-горе две стойности за предиката и

$$(r_{i,j}) + (r_{i,j}) \leq 1.$$

В стандартната ОМ, ядро от входна позиция преминава към изходна позиция на прехода само когато предикатът съответстващ на двете позиции има вярностна стойност “истина”.

1.2. Извличане на данни (Data Mining)

1.2.1 Въведение в Data Mining

Представлява процес на откриване на смислени корелации, зависимости, повтарящи се образци (на английски: patterns), тенденции и аномалии в големи масиви от данни, съхранявани в складове чрез използване на техники и алгоритми от областта на машинното обучение, разпознаването на образи, статистиката, невронните мрежи и визуализацията на данни.

Data mining представлява процес на анализ на съхраняваните

бази данни в посока на извличане нова полезна информация чрез разкриване на дълбоките и скрити взаимоотношения между на пръв поглед неизвестни и несвързани една с друга величини. Важна негова особеност е че той осигурява възможност за обработка на многомерни масиви и извличане на многомерни зависимости като същевременно автоматично разкрива изключителните ситуации – данни и случаи не включващи се в общите закономерности.

Нуждата в развитието на съвременните технологии от такава преработка на данните може да се обобщи в следното:

Неограниченият обем на данните.

Необходимост от конкретни и разбираеми резултати.

Инструменти за обработка на данните предоставящи възможност за лесно използване.

Голямата разнообразие и разнородност на данните (количествени, качествени и текстови).

В този труд ние ще използваме, една от техниките за изследванията и приложенията в областта на извличането на данни (DM), а по точно едно разширение на размитите множества и логика, наречено интуиционистки размито множество (Intuitionistic Fuzzy Set, IFS) и интуиционистки размита логика (IFL).

Основните стандартни техники които се използват за извличане на знания от данни са следните: *Дърво на решенията, Асоциативни правила, Невронни мрежи, Генетични алгоритми, Клъстерен анализ по „метода на най-близкия съсед“ , Размита логика (fuzzy logic).*

1.2.2. Интуиционистки размита логика като инструмент за оценка на процесите за извличане на данни

Кратки бележки за ***интуиционистко размито съждително смятане.***

На всяко твърдение (в класическия смисъл, виж например [M] можем да съпоставим вярностната му стойност: „истина“ – обозначена с 1 или „лъжа“ – с 0

Както посочихме по-горе, в случая на размита логика тази стойност на истинност на практика е рационално число в интервала [0, 1] и тя се нарича “степен на вярност” на конкретното съждение. В случая на интуиционистки размита логика се добавя една допълнителна стойност “степен на невярност” която също е в интервала [0,1]. Така тези две реални числа, $\mu(p)$ и $\nu(p)$, съпоставени на съждението p удовлетворяват следното ограничение:

$$\mu(p) + \nu(p) \leq 1.$$

Нека оценката на всяко съждение се задава чрез функцията за оценка V, дефинирана върху набор от съждения S, т.е.:

$$V(p) = \langle \mu(p), \nu(p) \rangle$$

Следователно функцията $V: S \rightarrow [0,1] \times [0,1]$ задава едновременно степените на истинност и на неистинност за всяко съждение от S.

Ако T е логическа истина, то

$$V(T) = \langle 0,1 \rangle,$$

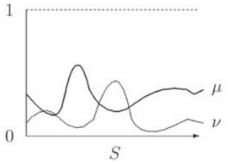
а ако е логическата лъжа F, то:

$$V(F) = \langle 0,1 \rangle.$$

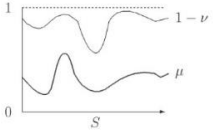
Интуиционистки размитите обекти (множества, съждения, предикати и други) имат няколко геометрични интерпретации

вж. Фиг. 1.2.2 и 1.2.4. Първата от тях има аналог за случая на размити обекти, докато втората е специфична само за интуиционистката размитост. Фиг. 1.2.1 е доста неинформативна и затова тя е била модифицирана до Фиг. 1.2.2

Първа геометрична интерпретация на интуиционистично размито множество.



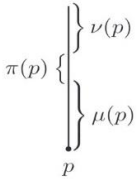
Фиг. 1.2.1.



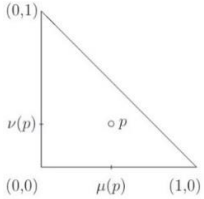
Фиг. 1.2.2.

Първа геометрична интерпретация на интуиционистки размито множество (модифицирана форма).

При модифицираната форма на първата геометрична интерпретация всеки интуиционистки размит обект има вида от Фиг. 1.2.3.



Фиг. 1.2.3.



Фиг. 1.2.4.

Първа геометрична интерпретация на елемент от интуиционистки размито множество.

Втората геометрична интерпретация използва единичен равнобедрен правоъгълен триъгълник (вж. Фиг. 1.2.4), който има аналитичен вид и се нарича интуиционистки размит интерпретационен триъгълник.

$$\{\langle x,y\rangle \mid x,y \in [0,1] \ \& \ x+y \leq 1\}$$

Втора геометрична интерпретация на интуиционистки размито множество.

Когато вярностните стойности $V(p)$ и $V(q)$ на съжденията p и q са известни, оценъчната функция V може да бъде разширена също и за операции "*&*" и "V" чрез различни (към момента – три) дефиниции.

$$V(p\&_1 q) = \langle \min(\mu(p), (\mu(q)), \max(\nu(p),\nu(q))\rangle,$$
$$V(pV_1 q) = \langle \max(\mu(p), (\mu(q)), \min(\nu(p),\nu(q))\rangle;$$
$$V(p\&_2 q) = \langle \mu(p).(\mu(q), \nu(p)+\nu(q)- \nu(p). \nu(q)\rangle,$$
$$V(pV_2 q) = \langle \mu(p)+(\mu(q)- \mu(p).(\mu(q), \nu(p). \nu(q)\rangle;$$
$$V(p\&_3 q) = \langle \min(1, \mu(p) +\mu(p)), \max(0, \nu(p)+ \nu(p)-1)\rangle,$$
$$V(p\&_3 q) = \langle \max 0, \mu(p) +\mu(p)-1), \min(1, \nu(p)+ \nu(p)-1))\rangle.$$

Навсякъде по долу ние ще приемем че за двете променливи p и q ще са в сила равенствата:

$$V(p)= \langle a, b\rangle,$$
$$V(q)= \langle c, d\rangle,$$

където a, b, c, d, a+b, c+d $\in$ [0,1]).

1.3. Извод

В Глава първа от дисертационния труд е направен кратък обзор на някои резултати от областта на обобщените мрежи и интуиционистки размитите множества и логики. Разгледани са някои от видовете обобщени мрежи. Обърнато е и внимание на интуиционистки размити ОМ, техните видове и типове.

Направено е въведение в Data Mining, като е разгледан какво представлява самият процес. В последната част на първа глава са разгледани интуиционистки размити множества, които са част от разширенията на размитите множества.

В следващите две глави на дисертационния труд са представени нови модели които представят различни реални процеси чрез Data Mining-техники с помощта на обобщеномрежови модели, които илюстрират взаимовръзката между теорията на обобщените мрежи и процесите на извличане на знания от данни чрез интуиционистки

размити оценки.

2. Изследване на обобщеномрежови модели на реални процеси на Payment Gateway чрез интуционистки размити оценки на Data Mining-техники.

2.1 ОМ на стандартен интернет портал за електронно разплащане с помощта на интуционистки размити оценки

Представените тук резултати са публикувани в [1*].

2.1.1. Представяне на модела стандартен интернет портал за електронно разплащане(PGW)

С този модел ще разгледаме обобщеномрежови модел на стандартен портал за електронно разплащане (Payment gateway), тъй като съществуват най различни такива разплащателни системи, ще използваме стандартен и ще покажем всички паралелни процеси които протичат в една такава система.

ОМ моделът на стандартен разплащателен портал съдържа следните преходи: За този модел ще разгледаме само преходи Z_1 и Z_6

$$A = \{Z_1, Z_2, Z_3, Z_4, Z_5, Z_6\},$$

където преходите описват следните процеси:

Z_1 = „Първоначална оторизация";

Z_2 = „Избор на стоки/услуги";

Z_3 = „Обработка на плащанията";

Z_4 = „Удържане на средства";

Z_5 = „Доставка на стоки и потвърждение на услуги".

Z_6 = „Оценка на възможни проблемни пакети с информация в системата".

$$Z_1 = \langle \{L_1, L_2, L_3, L_{11}\}\ \{L_6, L_3, L_2, L_4, L_5\}, R_1, \vee (L_1, L_2, L_3, L_{11}) \rangle$$

където

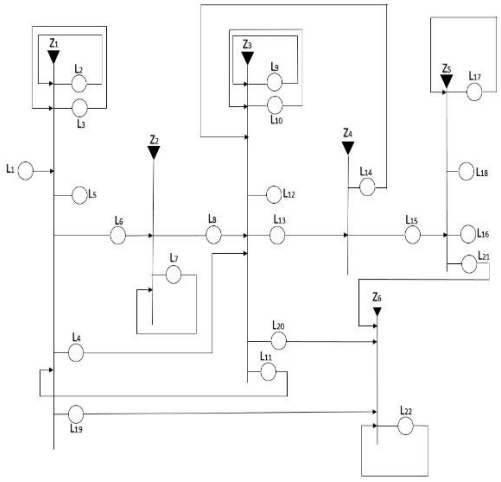
$R_1 =$

	L_2	L_3	L_4	L_5	L_6	L_{19}
L_1	*true*	*false*	*true*	*false*	*false*	*false*
L_2	*true*	$W_{2,3}$	*false*	$W_{2,5}$	$W_{2,6}$	$W_{2,19}$,
L_3	*false*	*true*	*false*	$W_{3,5}$	$W_{3,6}$	$W_{3,19}$
L_{11}	*false*	*false*	$W_{11,4}$	*false*	*false*	*false*

където:

$W_{2,3}$ = „Наличен е клиентски акаунт";

$W_{2,5} = \neg W_{2,3}$;
$W_{2,6} =$ „Позициите L_2, L_3, L_4 не могат за завършват“;
$W_{3,5} =$ „Възникнал е проблем с дебитна/кредитна карта”;
$W_{3,6} = W_{2,6}$;
$W_{11,4} =$ „Потвърден акаунт на търговеца“.
$W_{2,19} =$ „Неуспешна оторизация на кредитна карта“.
$W_{3,19} =$ „Неуспешна оторизация на потребителски акаунт“.
Ядрото което постъпва в позиция L_2 получава характеристика “База данни кредитни карти”.
Ядрото което постъпва в позиция L_3 получава характеристика “База данни потребителски акаунти”.
Ядрото което постъпва в позиция L_4 получава характеристика “База данни търговски акаунти ”.
Ядрото което постъпва в позиция L_5 получава характеристика “Грешка/изход”.



Фиг. 3.1.1 Стандартен интернет портал за електронно разплащане(PGW)

Направо показваме преход Z_6 всички останали преходи могат да се проследят в ОМ.

$Z_6 = \langle \{ L_{19}, L_{20,} L_{21}\, L_{22} \}\ \{L_{22}\}, R_6, \vee (L_{19}, L_{20,} L_{21}\, L_{22}) \rangle$

където

$$R_6 = \begin{array}{c|c} & L_{22} \\ \hline L_{19} & true \\ L_{20} & true \\ L_{21} & true \\ L_{22} & true \end{array},$$

където:

Ядрото което постъпва L_{19} получава характеристика

"Възможна неуспешна оторизация, оценка неизвестна ".

Ядрото което постъпва L_{20} получава характеристика

"Възможно неуспешно плащане оценка неизвестна ".

Ядрото което постъпва L_{21} получава характеристика

"Възможна неуспешна доставка оценка неизвестна".

Ядрото което постъпва L_{22} получава характеристика

"оценки $<\mu_k, \nu_k>$ ".

Първоначално, когато не е получена информация от позиции L_{19}, L_{20}, L_{21} L_{22}, всички оценки приемат първоначални стойности от $<0,0>$.

а когато $k \geq 0$, текущата $(k+1)-ва$ оценка е изчислена на базата на предишните оценки според рекурсивната формула:

$$<\mu_{k+1}, \nu_{k+1}> = \frac{\mu_k k + \mu}{k+1}, \frac{\nu_k k + \nu}{k+1},$$

Когато $k \geq 0$, Текущата $(k+1)$-ва е пресметната на база на предходните оценки според рекурсивната формула:

където $<\mu_k, \nu_k>$ е предишната оценка а $<\mu, \nu>$ е последната оценка .

2.2. Симулация на реалните процеси, статуси - протичащи в стандартен интернет портал за електронно разплащане чрез програмната среда GN IDE.

Извършена е симулация, чрез програмната среда GN IDE с цел демонстриране на реалната работа на един такъв модел с всички възможни грешки както и IFS оценките които се извършват в IFE алгоритъмът в позиция L_{22}.

GN IDE (Generalized Nets Integrated Development Environment)

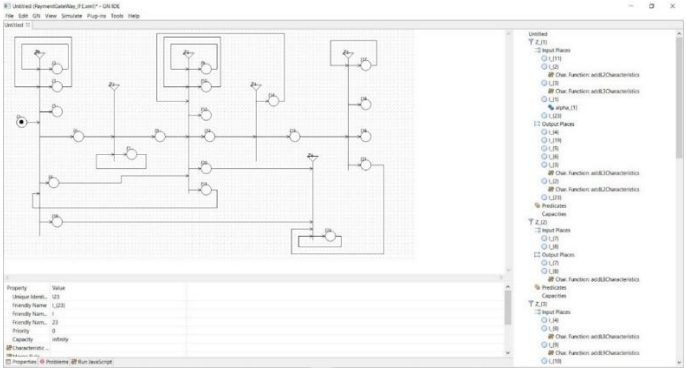
GN IDE е разработена на езика Java, и може да бъде стартирана на всяка платформа с инсталирана “Java Runtime Environment (JRE)”.

GN IDE позволява: визуализиране на ОМ модели, описни във файлове с XML базиран формат (GN XML, XGN); интерактивна симулация на тези модели и експортирането им до TeX формат.

На Фиг. 1 е посочена първа стъпка от процеса където L_1 постъпва в преход Z_1 следват няколко итерации на Z_1 на ядрата L_2, L_3 и L_4. Като при всяка девета итерация стартира нова симулация.

В програмният код правилата описани за симулацията на преходът Z_1 както следва за всяко позиция L_2, L_3 и L_4 е зададено да има 80% шанс за успех т.е. процеса да бъде успешен и различните проверки които протичат, също да бъдат успешни.

Зададени са още 15% неуспешни опити който завършват с изход на позиция L_5 и 5% шанс да има така неидентифицирана грешка която автоматично се изпраща от изход L_{19} и от там ядрото постъпва в позиция L_{22} където се намира нашият IFE алгоритъм, там се изпращат неидентифицирани грешки и системата прави интуционистки размити оценки на база събралата се там информации от ядрата които подават въпросната информация.



Фиг. 1 Итерация 1

Във Фиг. 1 е показан началният екран на симулацията. Итерация 1 показва L_1 в начална позиция преди да постъпи в преход Z_1. По-долу в Фиг. 2 се вижда активирането на прехода Z_1 и ядрото което постъпва в позиция L_2, за да бъде извършена първоначална проверка.

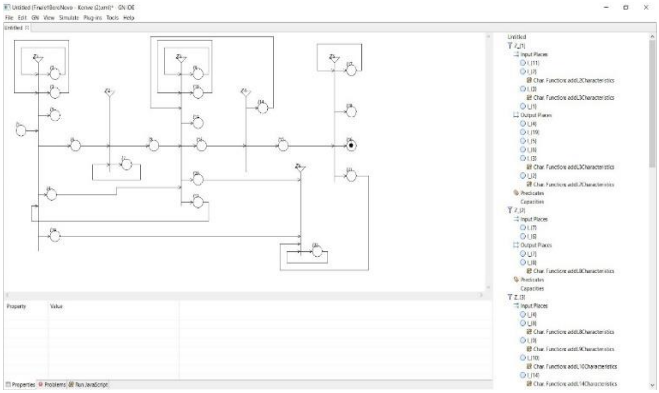
По този начин е направена програмната симулация като ние тук ще пропуснем всичките итерации а ще покажем само

първата и последната.

В Фиг.13 се вижда снимка на последната итерация.

След това ядрото постъпва в позиция L_{16} където е изхода за успешното завършване на процеса.

За този преход в програмният код е указано. От ядро с позиция L_{15} към L_{17}, следва L_{18} което представлява изход с възможност от 15 % шанс за грешка. За успешният изход на симулацията е зададено ядро с позиция L_{16} да има 80% шанс за успеваемост да завърши процесът. И съответно за позиция L_{21} е указано 5% шанс да изпраща грешките от тип неизвестен да отиват в позиция L_{22} където се правят IFE оценки.

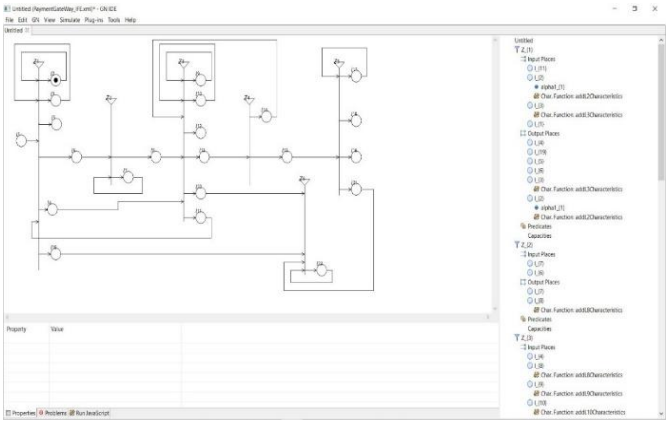


Фиг. 13 Итерация 13

2.2.1. Примери за различни сценарии при които се получават грешки от известен тип чрез симулацията на ОМ.

Тъй като симулацията на ОМ чрез “GN“ програмната среда трябва да бъде пускана N на брой пъти за да се генерират различни резултати по-долу ще посочим няколко примера за различни сценарии, генерирани от програмната симулация.

По принцип възможните сценарии са N на брой но по-долу чрез снимки от самата симулация, ще се опитаме да покажем възможни грешки от известен тип които се генерирани чрез N на брой итерации.

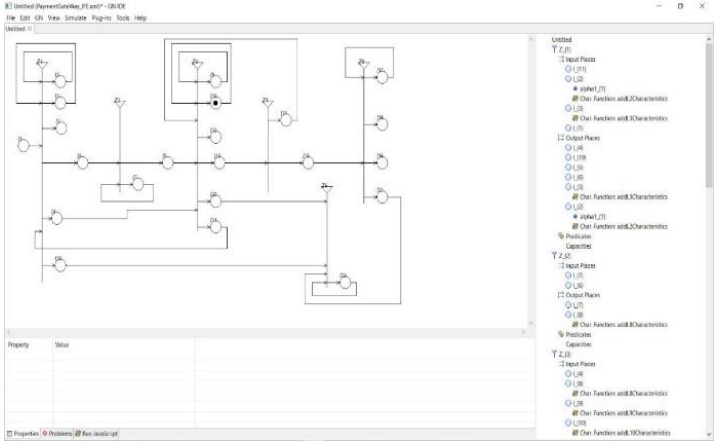


Фиг. 14 Снимка от итерация на GN IDE

Във Фиг. 14 се наблюдава преход Z_1 и ядро L_2 което се е активирало с характеристика “База данни за кредитни карти“

Тук се извършва проверка при което в една от следващите фигури 15 по-долу се е получила грешка от известен тип “Грешка с кредитна карта“ и ядрото постъпва в позиция L_5 с характеристика “Изход“.

По същия начин като по-горе, ще пропуснем всичките итерации, и ще покажем само първата и една от последните.



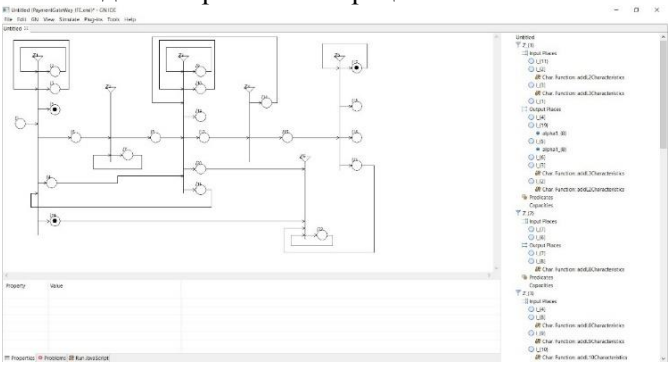
Фиг. 18 Снимка от итерация на GN IDE

Във Фиг. 18 се наблюдава преход Z_5 и ядро L_{17} което се е активирано с характеристика “Потвърждаване на

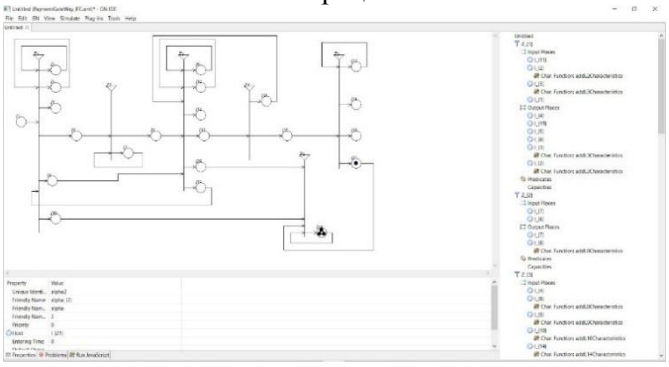
доставката“ тук се извършва проверка при което в следващата Фиг. 18 по-долу се е получила грешка от известен тип “Невъзможно потвърждаване на доставката“ и ядрото постъпва в позиция L_{18} с характеристика “Изход“ Грешката е показана чрез Фиг. 19.

2.2.2. Примери за изпращането на грешки от неизвестен тип към IFE алгоритъмът за оценка.

В следващите снимки ще видим как към ядра с позиции (L_{19}, L_{20} и L_{21}) постъпват грешки от неизвестен тип и как те се изпращат към IFE алгоритъмът за оценка в позиция L_{22}. И тук както по-горе ще покажем снимка само на началната Фиг.12 и една от крайните итерации.



Фиг. 12 Снимка от итерация на GN IDE



Фиг. 14 Снимка от итерация на GN IDE

Фиг.14 е една от последните итерации. В посочените фигури, Фиг.12 и Фиг.14 се виждат грешките от неизвестен

тип които минават през посочените позиции(L_{19}, L_{20} и L_{21}) а в L_{22} можем да видим натрупаните грешки и съответно IFE алгоритъмът който ще направи нужните IFE оценки.

2.2.3. Програмен код с коментари към него, описващ функциите и предикатите на стимулационният модел чрез програмната среда "GN IDE".

В следващите редове е в дисертацията е показан кода "Java Script" чрез които е нужно да се опишат процесите в програмната среда "GN IDE", предикатите, приоритетите като и ядрата и тяхната последователна а работата в самият процес.

Правилата и условията в този код важат само и единствено за ОМ модел на "Стандартен интернет портал за електронно разплащане "описан в втора глава в предходните точки 2.1., 2.1.1. и 2.1.2..

По самият код на различни редове са добавени описателни коментари поясняващи, какво точно прави кода на определените места, тези коментари са поместени в /*започват и свършват с */.

Кода може да се види в дисертационният труд точка 2.2.3 страница 52-61.

2.3. ОМ модел на протичането на състоянията на реалният разплащателен процес.

Представените тук резултати са публикувани в [2*].

2.3.1 Представяне на ОМ модел на реален разплащателен процес в Payment Gateway.

В този обобщеномрежови модел ще разгледаме Фиг. 4.1.1., различните състояния протичащи в самият процес на електронното разплащане.

Тук само са описани част от преходите и предикатите към тях $Z_{1,1}$ и Z_5 всичко останало може да се види в ОМ Фиг. 4.1.1..

Обобщеномрежови модел на електронно разплащане (Фиг. 4.1.1.). Той съдържа множеството от преходи:

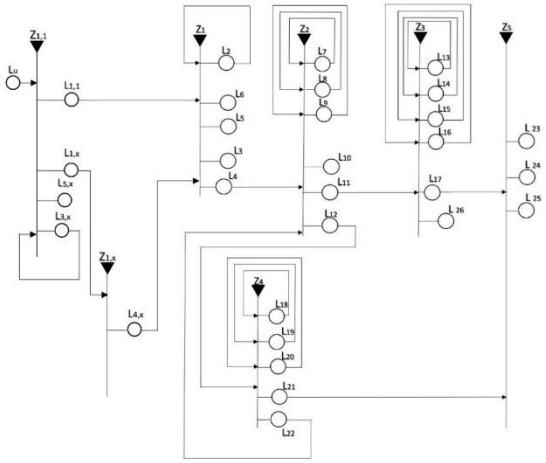
$A = \{ Z_{1,1}, Z_{1,x}, Z_1, Z_2, Z_3, Z_4, Z_5\}$,

Където преходите описват следните процеси:

$Z_{1,1}$ = „Първоначална валидация банка 1”
$Z_{1,x}$ = „Първоначална валидация на банка ‘X”
Z_1 = „Положителен паричен баланс ”
Z_2 = „Избор на метод за “разплащане”
Z_3 = „Ръчно разплащане /администратор/”
Z_4 = „Портал за автоматично разплащане”
Z_5 = „Потвърждение за завършена “транзакция”
Преходите на ОМ имат следния вид:
$Z_{1,1} = \langle L_u, L_{3,x}\}\{L_{1,1}, L_{1,x}, L_{3,x}, L_{5,x}\}, R_{1,1}, \vee(L_u, L_{3,x})\rangle$
където

$$R_{1,1}=\begin{array}{c|cccc} & L_{1,1} & L_{1,x} & L_{3,x} & L_{5,x} \\ \hline L_u & false & false & true & false \\ L_{3,x} & W_{3,x,1,1} & W_{3,x,1,x} & true & W_{3,x,5,x} \end{array},$$

където:
$W_{3,x,1,1}$ = „Първоначалната проверка на идентификационните данни на първата банка е успешна“ ;
$W_{3,x,1,x}$ = „Първоначалната проверка на идентификационните данни на банка “X” е успешна “ ;
$W_{3,x,1,5}$ = „Първоначалната проверка на идентификационните данни на банките е успешна “ ;



Фиг. 4.1.1. ОМ модел на реален разплащателен процес в PGW

$$Z_5 = \langle\{ L_{17}, L_{21}\} \{L_{23}, L_{24}, L_{25}\}, R_5, \vee (L_{17}, L_{21}) \rangle$$

където

$$R_5 = \begin{array}{c|ccc} & L_{23} & L_{24} & L_{25} \\ \hline L_{17} & W_{17,23} & W_{17,24} & W_{17,25} \\ L_{21} & W_{21,23} & W_{21,24} & W_{21,25} \end{array},$$

където:
$W_{17,23}$ = „ Успешно завършила транзакция “;
$W_{17,24}$ = „ Транзакцията е завършила, но с грешки“;
$W_{17,25}$ = „Транзакцията е завършила с 0 изтеглени “;
$W_{21,23}$=„ $W_{17,23}$ “;
$W_{21,24}$=„ $W_{17,24}$ “;
$W_{21,25}$=„ $W_{17,25}$ “;

2.4. Извод

Във втора глава на настоящият труд са разгледани 2 модела, портал за електронно разплащане както и реалните процеси които се случват по време на електронните разплащания. Първият модел “Обобщеномрежови модел на стандартен интернет портал за електронно разплащане“ разглежда паралелните процеси в един такъв портал, как протичат онлайн транзакциите, как протича тяхното одобрение и т.н.

Това е и първата спирка, където отива транзакцията, когато клиент изпрати поръчка онлайн. Моделът е представен с обобщена мрежа и показва потоците от транзакции през платежния портал и както и различни проверки и одобрения и възможни откази. Така че този ОМ модел ни помага да погледнем по-надълбоко в портала и да коригираме възможни проблеми, да симулираме други или просто да го използваме за оптимизация на поведението на платежният портал.

Следва програмна симулация на реалните процеси, статусите – протичащи в стандартният интернет портал за електронно разплащане чрез софтуер GN IDE.

Чрез помощта на този софтуер ние показваме симулация на ОМ модел и показваме реалните стъпки на всички ядра, тяхното преминаване през преходите, техните характеристики и предикати, които се случват по време на паралелният процес в самата система.

Следващият представен модел е продължение на предходния модел и разглежда, реален разплащателен процес в разплащателният портал и по-точно как се променят статусите и флаговете по време на самият процес.

Повечето такива модели са свързани с интелигентни системи като невронни мрежи, генетични и други алгоритми. ОМ моделът ще ни помогне лесно и ясно да разберем статусите които се променят в реалният процес на тази система и етапите на неговото функциониране като по този начин ще ни помогне да анализираме, отстраняваме и решаваме по-добре всички предстоящи въпроси, проблеми и задачи.

В следващата глава ще разгледаме 3 различни модела на теми които са много актуални в днешно време, а именно темата за интелигентни къщи (Smart House) както и управлението на дронове (UAV). Там са засегнати възможните рискове от кибер-атаки върху управлението на дронове както и на "Smart House", направени са оценки на риска от кибер-атаки засегнати са и проблемите на сигурността и защитата на комуникациите и управлението.

3. Изследване на обобщеномрежови модели на реални процеси на Smart House и UAVs. чрез интуционистки размити оценки на Data Mining техники.

3.1. ОМ модел за оценка на риска от кибер-атака върху управлението на Smart House.

Представените тук резултати са публикувани в [3*].

3.1.1. Представяне на ОМ модел за оценка на риска от кибер-атака върху управлението на Smart House.

В настоящото изследване е разгледана обобщена мрежа, модел на Smart House се управлява дистанцирано на базата на различни идентификации, канали и автоматизирани вътрешни и външни системи, както и чрез приложения, базирани в облачна платформа. Разглеждаме и възможностите за проникване на недоброжелатели в системата с цел поемане на контрола над Smart House и съответни злонамерени действия в него. Тук ще включим и няколко типа оценки посредством IFE. Системата на Smart House, която разглеждаме е реализирана чрез модули за управление от разстояние посредством телефон, таблет, лаптоп, PC и други устройства чрез облачна платформа. Крайните апликации се свързват с облачната платформа, верифицират се и подават заявките на системите ѝ. По същият начин се свързват и автоматизираните комуникационни канали. От своя страна облачната структура

комуникира с контролера на Smart House и чрез него управлява устройствата и системите, контролирани от него. Възможностите за проникване в системата са чрез крайните апликации, облачната структура, през контролера на Smart House и посредством каналите за комуникация между облачната структура и Smart House, както и между облачната структура и крайните устройства.

3.1.2. ОМ модел на един алтернативен метод за оценка на риска от кибер-атака при управлението на интелигентна къща с интуиционистки размити оценки.

По-долу са показани детайлно само преходи Z_1 и Z_6, като и описание на предикатите към тези преходи. Всичко останало може да се проследи от ОМ Фиг. 5.1.1.

Тук ще използваме IFS за да оценим възможното проникване в комуникацията. Оценките се представят чрез наредени двойки $\langle \mu, \nu \rangle$ от реални числа от множеството [0, 1], където:

$$\mu = \frac{S_1}{S}$$

където:

S - Всички опити за верификация.

S1 - Успешни опити за верификация когато ядрото влезе в позиция L_3, L_4, L_5, L_6, L_7, L_8, L_{11}, L_{12}, L_{15}.

$$\nu = \frac{S_2}{S}$$

където:

S2 – Неуспешни умишлени опити за проникване.

$$\pi = \frac{S_3}{S}$$

където:

S3 - Неуспешни неумишлени опити за верификация, като започнати и недовършени поради различни причини, както и при прекъсване на интернет връзката.

Тук ще разгледаме още четири варианта за оценка на възможностите за проникване в системите и каналите за

комуникация на Smart House.

Силно оптимистична формула:

$$\langle \mu_1, \nu_1 \rangle + \langle \mu_2, \nu_2 \rangle + ... + \langle \mu_n, \nu_n \rangle = \sum_{i=1}^{n} \langle \mu_i, \nu_i \rangle = \langle 1 - \prod_{i=1}^{n} (1 - \mu_i), \prod_{i=1}^{n} \nu_i \rangle$$

Оптимистична формула:

$$\max(\langle \mu_{1,} \nu_1 \rangle, \ldots, \langle \mu_{n,} \nu_n \rangle) = \langle \max(\mu_1, \ldots, \mu_n), \min(\nu_1, \ldots, \nu_k) \rangle;$$

Песимистична формула:

$$\min(\langle \mu_{1,} \nu_1 \rangle, \ldots, \langle \mu_{n,} \nu_n \rangle) = \langle \min(\mu_1, \ldots, \mu_n), \max(\nu_1, \ldots, \nu_k) \rangle;$$

Силно песимистична формула:

$$\langle \mu_1, \nu_1 \rangle . \langle \mu_2, \nu_2 \rangle ..... \langle \mu_n, \nu_n \rangle = \prod_{i=1}^{n} \langle \mu_i, \nu_i \rangle = \langle \prod_{i=1}^{n} \mu_i, 1 - \prod_{i=1}^{n} (1 - \nu_i) \rangle$$

ОМ – модел

Системите на “Smart House” улесняват потребителите..

Първоначално следните ядра постъпват в ОМ на управлението на Smart

GN моделът на Smart House система Фиг. 5.1.1. е представен чрез множеството от преходи:

$$A = \{Z1, Z2, Z3, Z4, Z5, Z6\},$$

където преходите описват следният процес:

- Z_1 = „ Действия на нарушителя”;
- Z_2 = „ Управление на облачната платформа “;
- Z_3 = „ Действия на потребителите “;
- Z_4 = „ Управление на системата “;
- Z_5 = „IFE Оценка“;
- Z_6 = „ Управление на протоколите “;

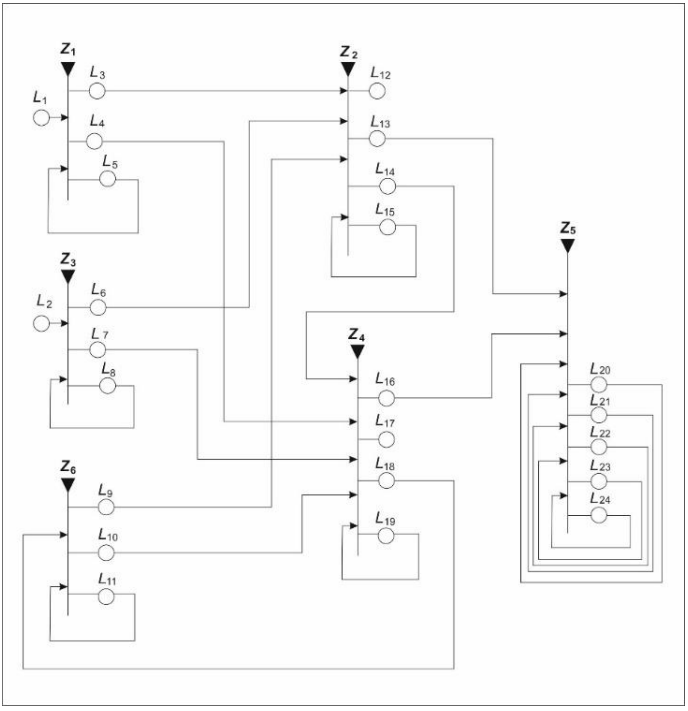
ОМ модел на Smart House система [4, 82, 88, 91, 104, 148, 158, 165].

$$Z_1 = <\{ L_1, L_5\}, \{ L_3, L_4, L_5 \}, R_1, \wedge (L_1, L_5) >,$$

където:

$W_{5,3}$ = “Нарушителят прави успешен пробив на проверката на облачната платформа”;
$W_{5,4}$ = “Нарушителят прави успешен пробив на проверката на системата за управление”;

$$Z_6 = \langle \{ L_{11}, L_{18} \}, \{ L_9, L_{10}, L_{11} \}, R_6, \vee (L_{11}, L_{18}) \rangle$$



Фиг. 5.1.1. ОМ модел на интелигентна къща за оценка на риска от кибер-атака

където

$$R_6 = \begin{array}{c|ccc} & L_9 & L_{10} & L_{11} \\ \hline L_{11} & W_{11,9} & W_{11,10} & False \\ L_{18} & False & False & True \end{array}$$

където:
$W_{11,9}$ = “Проверката е успешна”.
$W_{11,10}$ = “Проверката е неуспешна”.

Оптимистична формула:

$$\max(\langle \mu_{1,} \nu_{1} \rangle, \ldots, \langle \mu_{n,} \nu_{n} \rangle) = \langle \max(\mu_{1}, \ldots, \mu_{n}), \min(\nu_{1}, \ldots, \nu_{k}) \rangle;$$

Песимистична формула:

$$\min(\langle \mu_{1,} \nu_{1} \rangle, \ldots, \langle \mu_{n,} \nu_{n} \rangle) = \langle \min(\mu_{1}, \ldots, \mu_{n}), \max(\nu_{1}, \ldots, \nu_{k}) \rangle;$$

3.2. ОМ модел за оценка на риска от кибер-вмешателство върху дронове чрез използването на интуиционистки размити оценки.

Представените тук резултати са публикувани в [4*].

3.2.1. Представяне на теорията за модела, комуникацията и управлението на Дрон.

По-долу са показани детайлно само преходи Z_1 и Z_8, като и описание на предикатите към тези преходи. Всичко останало може да се проследи от ОМ Фиг. 6.1.1..

В текущото изследване разглеждаме модел на ОМ възможността за кибер-посегателство комуникацията на управлението на UAV. За да можем да управляваме UAV, имаме нужда от оборудване радиопредавател (Tx) и радиоприемник (Rx).

С този модел ние ще симулираме нарушител, който вероятно ще сканира комуникацията от 2,4 GHz и ще се опита да вземе контрол над някой от комуникационните канали и/или протоколи. ОМ система ще събира информация от всички входни и изходни ядра и ще я изпрати до БД с интуиционистки размит алгоритъм които ще трябва прецени дали върху контролът за комуникация е установено вмешателство от нарушител.

Възможната комуникационна намеса може да произтича от смущения в комуникацията между RX контролерът и TX приемникът.

В горния контекст ще направим оценка на възможностите за комуникационно вмешателство в комуникационната система на безпилотният хеликоптер. За целта ще използваме размити множества (IFS).

Нуждаем се от (IFS), за да преценим възможното вмешателство

в комуникацията.

Оценките са представени чрез подредени двойки $< \mu, \nu >$ от реални числа от множеството $[0,\ 1]$, където:

$$\mu = \frac{S_1 + S_2}{S},$$

където:

S - Всички възможни опити за ТХ-комуникация.

S_1 - Всички ядра от $\{L_3, L_6, L_9\}$ които постъпват в позиция L_{15}.

S_2 – Броят от неуспешни опити когато ядрото в позиция L_{12} влиза в позиция L_{16}.

$$\nu = \frac{S_3 + S_4}{S},$$

където:

S_3 - Всички ядра от позиции $\{L_3, L_6, L_9\}$ които постъпват в позиция L_{16}.

S_4 - Броят от неуспешни опити когато ядрото в позиция L_{12} влиза в позиция L_{15}

S_5 - Броят опити на нарушителят за вмешателство върху комуникацията.

S_6 - Всички успешни опити за превземане на комуникацията.

S_7 - Всички грешки.

$$\pi = \frac{S_5 - S_6 - S_7}{S},$$

където:

Степента на несигурност $\pi = 1 - \mu - \nu$ представлява, всички пакети от информация в комуникацията, които отиват до местоназначението си, и всички възможни манипулирани пакети от външен източник.

UAV ОМ модел на стандартен комуникационен процес между радиопредавател Тх и Rx радиоприемник (Фиг. 6.1.1.) е представено чрез множеството от преходи:

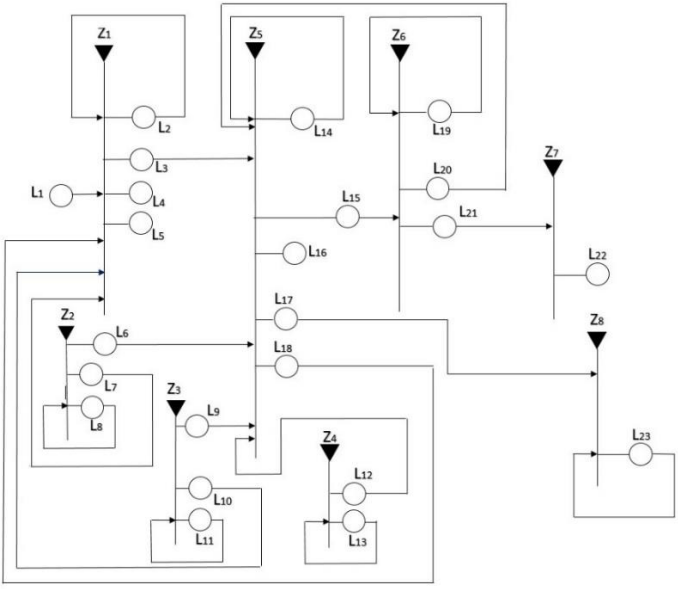
$$A = \{Z_1, Z_2, Z_3, Z_4, Z_5, Z_6, Z_7, Z_8\},$$

където преходите описват следните процеси

Z_1 = „Обработка на командите от предавателят”;

Z_2 = „Обработка на комуникационни протоколи ”;

Z_3 = „Обработка на избора на канали”;
Z_4 = „ Външна намеса в комуникацията между предавателят и приемникът“.
Z_5 = „Обработка на командите на приемникът“;
Z_6 = „Команди за обработка от контролерът на дрона“;
Z_7 = „Летящ дрон“;
Z_8 = „Оценка на възможният изход от външната намеса върху комуникацията с дрона“.



Фиг. 6.1.1. ОМ модел за оценка на риска от кибер-вмешателство върху дронове

$Z_1 = \langle \{L_1, L_2, L_7, L_{10}, L_{18}\} \{ L_2, L_3, L_4, L_5 \}, R_1, \vee (L_1, L_2, L_7, L_{10,} L_{18}) \rangle$

където

$$R_1 = \begin{array}{c|cccc} & L_2 & L_3 & L_4 & L_5 \\ \hline L_1 & true & false & false & false \\ L_2 & true & true & W_{2,4} & false \\ L_7 & true & false & false & false \\ L_{10} & true & false & false & false \\ L_{18} & false & false & W_{18,4} & true \end{array},$$

където:
$W_{2,4}$ = „Има грешка в комуникационните команди “;
$W_{18,4}$ = „Има телеметрична Rx грешка в сигнала“;
Ядрото което постъпва в позиция L_2 получава характеристика
“БД команди предавател“ ;

$$Z_8 = \langle \{L_{17}, L_{23}\}\ \{L_{23}\}, R_8, \vee (L_{17}, L_{23}) \rangle$$

$$R_5 = \begin{array}{c|c} & L_{23} \\ \hline L_{17} & true \\ L_{23} & true \end{array},$$

Ядрото което постъпва в позиция L_{17} получава характеристика “Натрупана информация от ядра L_{15}, L_{16} - оценка неизвестна”.

Ядрото което постъпва в позиция L_{23} получава характеристика
“IFE оценки $< \mu_k, \nu_k >$”.

Първоначално, когато не е получена информация от ядра в позиции L_4, L_{13}, L_{16} L_{17}, всички оценки взимат начални стойности от $< 0, 0 >$

Когато k ≥ *0*, текущата $(k+1)-ва$ оценка е изчислена на базата на предишните оценки според рекурсивната формула:

$$< \mu_{k+1}, \nu_{k+1} > = \frac{\mu_k k + \mu}{k+1}, \frac{\nu_k k + \nu}{k+1},$$

където $< \mu_k, \nu_k >$ е предишната оценка, и $< \mu, \nu >$ е последната оценка на възможната външна намеса в комуникацията, за $\mu, \nu \in [0,1]$ и $\mu + \nu \le 1$. По този начин ядрото в позиция L_{21} формира окончателната оценка от натрупаната информация от всички входни и изходни ядра въз основа на предишни и най-нови събития.

3.3. ОМ модел на възможно кибер-намеса върху управлението на комуникацията на дрон, чрез използването на

интуционистки размити оценки.
Представените тук резултати са публикувани в [5*].

3.3.1. Представяне на ОМ модел на възможността на кибер-намеса върху управлението на комуникацията с дрон.

В това изследване, с помощта на ОМ модели, ще използваме нов различен начин за оценка на риска от кибер-атака върху комуникационния контрол на безпилотен хеликоптер.

Това изследване е предшествано от предходното, тук са направени оценки на възможността за кибер-вмешателство над безпилотен хеликоптер [5*].

Нашият ОМ модел ще натрупа информация от всички входни и изходни ядра и ще я изпрати до интуиционисткият размит алгоритъм за оценка, който ще оцени риска от кибер-вмешателство, и ще направи оценка дали комуникационният контрол може да бъде превзет от кибер-намесата.

Възможна кибер-намеса може да дойде от смущения в радиокомуникацията между контролера и приемника на безпилотното летателно устройство.

В това изследване както и в предходните, ще използваме размити оценки (IFS).

3.3.2. ОМ модел на възможно кибер-посегателство върху управлението на комуникацията на дрон чрез използването на интуционистки размити оценки.

И тук както и по-горе са показани детайлно само преходи Z_1 и Z_8, като и описание на предикатите към тези преходи. Всичко останало може да се проследи от ОМ Фиг. 7.1.1..

За можем да оценим възможната външна намеса в комуникацията ще използваме(IFS). Оценките се представят чрез подредени двойки реални числа от множеството [0,1], където:

$$S = S_1 + ... + S_7$$

$$\mu = \frac{S_1 + S_2}{S},$$

където:
S - Всички възможни опити за ТХ-комуникация.

S_1 - Всичките ядра от $\{L_3, L_6, L_9\}$ които постъпват в позиция L_{15}.
S_2 – Броят на неуспешни опити когато ядрото в позиция L_{12} постъпи в позиция L_{16}.

$$\nu = \frac{S_3 + S_4}{S},$$

където:
S_3 - Всичките ядра от позиция $\{L_3, L_6, L_9\}$ които постъпват в позиция L_{16}.
S_4 - Броят на неуспешни опити когато ядрото е в позиция L_{12} постъпва в позиция L_{15}.
S_5 - Броят от опити на нарушителят да поеме върху комуникацията.
S_6 - Всички направени успешни опити да бъде превзета комуникацията.
S_7 - Всички грешки.

$$\pi = \frac{S_5 + S_6 + S_7}{S},$$

Степента на несигурност $\pi = 1 - \mu - \nu$ това са всички пакети с информация в комуникацията, които отиват до тяхната дестинация, както и всички възможни манипулирани команди от външен източник.

В допълнение към предходните изследвания [3*,4*]. тук са използвани четири допълнителни прийома за оценка на риска от атака с кибер-проникване върху комуникационните протоколи върху безпилотно летателно устройство те са:

Силно оптимистична формула:

$$\langle \mu_1, \nu_1 \rangle + \langle \mu_2, \nu_2 \rangle + ... + \langle \mu_n, \nu_n \rangle = \sum_{i=1}^{n} \langle \mu_i, \nu_i \rangle = \langle 1 - \prod_{i=1}^{n} (1 - \mu_i), \prod_{i=1}^{n} \nu_i \rangle$$

Оптимистична формула:

$$\max(\langle \mu_{1,} \nu_1 \rangle, \ldots, \langle \mu_{n,} \nu_n \rangle) = \langle \max(\mu_1, \ldots, \mu_n), \min(\nu_1, \ldots, \nu_k) \rangle;$$

Песимистична формула:

$\min(\langle \mu_{1,} \nu_1 \rangle, \ldots, \langle \mu_{n,} \nu_n \rangle) = \langle \min(\mu_1, \ldots, \mu_n), \max(\nu_1, \ldots, \nu_k) \rangle$;

Силно песимистична формула:

$$\langle \mu_1, \nu_1 \rangle . \langle \mu_2, \nu_2 \rangle ..... \langle \mu_n, \nu_n \rangle = \prod_{i=1}^{n} \langle \mu_i, \nu_i \rangle = \langle \prod_{i=1}^{n} \mu_i, 1 - \prod_{i=1}^{n} (1 - \nu_i) \rangle$$

ОМ модел на стандартен комуникационен процес между радиопредавател Tx на безпилотно летателно устройство и Rx радиоприемник (Фиг. 7.1.1.) е представен чрез множеството от преходи:

$$A = \{Z_1, Z_2, Z_3, Z_4, Z_5, Z_6, Z_7, Z_8\},$$

където преходите описват следните процеси:

Z_1 = „Обработка предавателният сигнал.";

Z_2 = „Обработка на комуникационните протоколи";

Z_3 = „Обработка на избора на канали";

Z_4 = „ Кибер-вмешателство върху радио комуникацията".

Z_5 = „ Обработка на команди от приемникът. ";

Z_6 = „Обработка на командите от процесорът на безпилотното устройство ";

Z_7 = „Летящ дрон";

Z_8 = „Интуиционистки размит алгоритъм за оценка, оценяващ риска от кибер-вмешателство".

ОМ модел на радиокомуникационно управление между приемник и предавател както и обратната комуникация с приемника, показващ възможна кибер-атака върху безпилотното летателно устройство.

$Z_1 = \langle \{L_1, L_2, L_7, L_{10}, L_{18}\} \{ L_2, L_3, L_4, L_5 \}, R_1, \vee (L_1, L_2, L_7, L_{10,} L_{18}) \rangle$,

където

$R_1 =$

	L_2	L_3	L_4	L_5
L_1	*true*	*false*	*false*	*false*
L_2	*true*	*true*	$W_{2,4}$	*false*
L_7	*true*	*false*	*false*	*false*
L_{10}	*true*	*false*	*false*	*false*
L_{18}	*false*	*false*	$W_{18,4}$	*true*

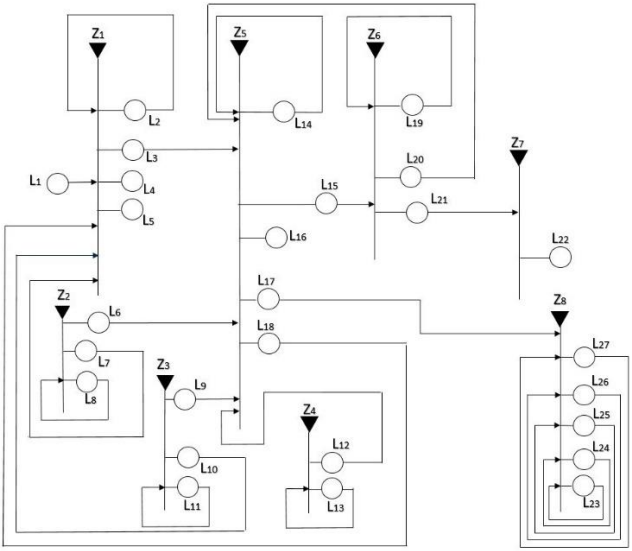
където:

$W_{2,4}$ = „ Има грешка в комуникационните команди “;

$W_{18,4}$ = „Има грешка в телеметричният Rx сигнал“;

Първоначално когато няма получена информация от ядрата L_4, L_{13}, L_{16} L_{17}, всички оценки приемат първоначална стойност от $\langle 0,0 \rangle$. Когато k ≥ *0*, текущата $(k+1)-ва$ оценката се изчислява въз основа на предишните оценки съгласно рекурсивната формула (както по-горе):

$$\langle \mu_{k+1}, \nu_{k+1} \rangle = \langle \frac{\mu_k k+\mu}{k+1}, \frac{\nu_k k+\nu}{k+1} \rangle,$$



Фиг. 7.1.1. ОМ модел на възможно кибер-посегателство върху управлението на комуникацията на дрон

$Z_8 = \langle \{L_{17}, L_{23}, L_{24}, L_{25}, L_{26}, L_{27}\}\ \{L_{23}, L_{24}, L_{25}, L_{26}, L_{27}\}, R_8,$

$$\vee (L_{17}, L_{23}, L_{24}, L_{25}, L_{26}, L_{27})\rangle,$$

където

$R_8 =$

	L_{23}	L_{24}	L_{25}	L_{26}	L_{27}
L_{17}	*True*	*True*	*True*	*True*	*True*
L_{23}	*True*	*False*	*False*	*False*	*False*
L_{24}	*False*	*True*	*False*	*False*	*False*
L_{25}	*False*	*False*	*True*	*False*	*False*
L_{26}	*False*	*False*	*False*	*True*	*False*
L_{27}	*False*	*False*	*False*	*False*	*True*

където $\langle \mu_k, \nu_k \rangle$ е предишната оценка, и $\langle \mu, \nu \rangle$ последната оценка от възможните комуникационни вмешателства , за $\mu, \nu \in [0,1]$ и $\mu + \nu \leq 1$. По този начин ядрото в позиция L_{21} формира окончателната оценка от натрупаната информация от всички входни и изходни ядра въз основа на предишни и най-нови събития.

3.4. Извод

В глава трета от дисертационния труд са разработени и представени няколко обобщеномрежови модела, при всички тези модели са използвани интуционистки размити оценки. Първият модел е посветен на намиране на алтернативен метод за оценка на риска от кибер-атаки върху управлението на "Smart House". Чрез този модел е показана алтернатива за показване на паралелната работа в една такава система като и нейният анализ и контрол. Изграденият обобщеномрежови модел може да способства за постигането на по-нататъшни подобрения на реалният процес.

Системата „Smart House“ се използва за улесняване на потребителите. Моделът е представен с ОМ и показва процесите, които протичат в системата, както и възможните грешки, които могат да възникнат.

Разгледана е и възможността за проникване в системата от външни лица с лоши намерения, като са използвани интуиционистки размити оценки.

Следващият модел е продължение на предходният проблем с тази разлика че тук се разглежда подход за оценка на риска от кибер-вмешателство върху дронове чрез използването на интуционистки размити оценки.

Този ОМ модел ни помага да анализираме риска от пробив в системата.

Моделът е представен с ОМ и показва потока от управляващи команди в тази система на безжична комуникация както и възможните нежелани смущения/намеси в управлението на безпилотния апарат.

Третият последен модел разгледан в тази глава е също така продължение на предходният модел тук също се разглежда обобщеномрежови модел на възможно кибер-посегателство върху управлението на комуникацията на (UAV)дрон.

Тук също се използва (IFE), като са добавени и някой допълнителни оценки като: Силно оптимистична оценка, оптимистична оценка, песимистична оценка и силно песимистична оценка.

Изградените обобщеномрежови модели може да се използват както за анализ и наблюдение на реалните процеси в тези системи, така и за оценка на риска от кибер-вмешателтва.

А сигурността е един изключително важен фактор за безпроблемна работа на различни системи във всички нива в човешкият живот.

Приноси към дисертационния труд

Основните приноси в дисертацията са с научен, научно-приложен и приложен характер и се свеждат до създаването на обобщеномрежови модели.

Приносите с ***научен*** характер могат да се формулират като:

Намиране на алтернативен метод за оценка на риска от кибер-атаки върху управлението на "Smart House" с помощта на интуционистки размити оценки.

Реализиране на нов подход за оценка на риска от кибер-вмешателство върху дронове чрез използването на интуционистки размити оценки.

Приносите с ***научен-приложен*** характер могат да се формулират като:

Разработване на обобщеномрежови модел на стандартен интернет портал за електронно разплащане с помощта на интуционистки размити оценки.

Разработване на обобщеномрежови модел на протичането на реалният разплащателен процес в PGW.

Разработка на обобщеномрежови модел на възможно кибер-посегателство върху управлението на комуникацията на дрон чрез

използването на интуционистки размити оценки.

Приносите с ***приложен*** характер могат да се формулират като:

Чрез софтуерният инструмент за симулация на модели разработени с обобщени мрежи "GN IDE" е направена пълна програмна симулация на реалните процеси на стандартен интернет портал за електронно разплащане, като тук са взети данни от ОМ модел в раздел 2.2.1 на Глава 2, и е направена успешна симулация на всички стъпки и преходи през които постъпват и преминават ядрата до края един на пълен успешен цикъл на реалният процес в обобщеномрежови модел. Посочени са и примери за грешки от неидентифициран тип които системата изпраща към IFE алгоритъм за оценка. Приложен и програмният код чрез който е направено описването на предикати, приоритети, характеристики и движенията на ядрата нужни за реализацията на симулацията в GN IDE.

Насоки за бъдещи изследвания

При изготвянето на дисертационния труд възникнаха следните идеи за бъдещи изследвания:

Нуждата от създаването на ОМ за оценка на риска от кибер-вмешателство в електронни портали за интернет разплащания.

Използване на IFE оценки както и ОМ модели на системата за верификация на банкови карти за бъдещо и евентуално предотвратяване на банкови измами.

По отношение на "Smart House" изграждане ОМ на "Smart" автономно захранване и използването на IFE оценки за приоритетно използване на захранваща мощност, на различните уреди в една такава система при прекъсване на основното захранване, за да е възможен оптимален разход на този ресурс.

Разработване на ОМ оценка на основните фактори при безпилотните летателни устройства UAV(Дронове), които засягат живота на батерията и по този начин да се оптимизира, полета на устройството и да се предотвратят евентуални произшествия.

ОМ модел и оценка на възможните нередности и грешки при управлението на дрон с оглед оценка на възможните грешки и проблеми, които могат да бъдат избегнати при управлението му.

Публикации по дисертационния труд

Bozveliev, Boris & Sotirov, Sotir & Simeonov, Stanislav & Videv, Tihomir. (2020). Generalized Net Model of Common Internet Payment Gateway with Intuitionistic Fuzzy Estimations. Intuitionistic and Type-2 Fuzzy Logic Enhancements in Neural and Optimization Algorithms: Theory and Applications (Oscar Castillo, Patricia Melin, Janusz Kacprzyk, Eds.), ISSN 1860-949X, Springer, Cham, 2020, 91-98. 10.1007/978-3-030-35445-9_8.

B. Bozveliev and T. Videv, Generalized NetET Modelling of the Payment Process Workflow. Proceedings of 10th IEEE International Conference "Intelligent Systems" Varna, Bulgaria, 2020, 529-532, ISSN: 1541-1672, doi: 10.1109/IS48319.2020.9200188.

Videv, Tihomir & **Bozveliev, Boris** & Sotirov, Sotir. (2021). An Alternative Method for Evaluating the Risk of Cyberattack Over the Management of a Smart House with Intuitionistic Fuzzy Estimation. Digital Transformation, Cyber Security and Resilience of Modern Societies (T. Tagarev, K. Atanassov, et al., Eds.), Springer, Cham, ISSN 2197-6503, Vol. 84. 2021 333-342 10.1007/978-3-030-65722-2_20.

Bozveliev, Boris & Sotirov, Sotir & Videv, Tihomir & Simeonov, Stanislav. (2021). A New Approach to Assess the Risk of Cyber Intrusion Attacks Over Drones Using Intuitionistic Fuzzy Estimations. Digital Transformation, Cyber Security and Resilience of Modern Societies (T. Tagarev, K. Atanassov, et al., Eds.), Springer, Cham, ISSN 2197-6503, Vol. 84 325-331 10.1007/978-3-030-65722-2_21.

Bozveliev, Boris & Sotirov, Sotir & Videv, Tihomir. (2019). Generalized Net Model of Possible Drone's Communication Control Cyber Theft with Intuitionistic Fuzzy Estimations. Information & Security: International Journal Information and Security. ISSN 0861-5160, Vol.43 35-44. 10.11610/isij.4303.